ASTES

Advances in Science, Technology & Engineering Systems Journal

VOLUME 8-ISSUE 6|NOV-DEC 2023

www.astesj.com
ISSN: 2415-6698

Editorial

In the ever-evolving landscape of science and technology, this issue brings together a collection of 14 accepted research papers that delve into diverse domains, ranging from robotics and healthcare to machine learning, cloud computing, neuroscience, cybersecurity, and control systems. Each paper represents a significant contribution to its respective field, offering novel methodologies, insights, and solutions to address contemporary challenges. The papers span a spectrum of cutting-edge topics, showcasing the breadth and depth of research endeavours undertaken by scholars and practitioners globally. As we navigate the intricate tapestry of technological advancements, these papers serve as beacons illuminating the path forward, each shedding light on unique aspects and applications within their domains. This compilation not only reflects the current state of research in these fields but also underscores the collaborative efforts of researchers pushing the boundaries of knowledge. In this editorial, we provide a glimpse into the key findings and contributions of each paper, highlighting the valuable insights they bring to their respective disciplines. Through this collection, we aim to foster a deeper understanding of the intricate intersections between technology and human progress, acknowledging the relentless pursuit of innovation that defines the essence of scientific inquiry.

In the realm of robotics, the paper on "Control Program Generator for Vehicle Robot using Grammatical Evolution" presents an innovative approach to designing control programs for autonomous mobile robots. Leveraging Grammatical Evolution (GE), the paper demonstrates the automatic generation of effective control programs for a LEGO MINDSTORMS EV3 robot. The integration with PyBullet for simulation ensures the reproducibility of the robot's trajectory, with calibrated parameters to bridge the gap between simulation and the real environment [1].

Moving into the healthcare domain, the "IoT System and Deep Learning Model to Predict Cardiovascular Disease Based on ECG Signal" paper addresses the critical issue of cardiovascular disease prediction. By combining Internet of Things (IoT) technology and deep learning models, the paper proposes an advanced system that analyzes Electrocardiogram (ECG) signals for accurate disease prediction, showcasing the potential for improving healthcare outcomes through technological interventions [2].

Shifting focus to machine learning, the paper on "Tree-Based Ensemble Models, Algorithms and Performance Measures for Classification" delves into the world of ensemble methods. Focusing on Tree-Based Ensemble Models with Decision Trees as base models, the paper introduces a Projective Decision Tree and explores algorithms for predictive performance. The study demonstrates promising results on datasets such as sonar and Breast Cancer Wisconsin, highlighting the potential of the proposed models in classification tasks [3].

In the era of information overload, the "Social Media Text Summarization: A Survey Towards a Transformer-based System Design" paper undertakes the challenge of summarizing text from social media. Recognizing the need for efficient summarization techniques, the paper reviews existing approaches and introduces a Transformer-based system design. This work opens avenues for leveraging advanced neural network models to distill valuable information from the vast sea of social media content [4].

Transitioning to cloud computing, the paper on "Infrastructure-as-a-Service Ontology for Consumer-Centric Assessment" contributes to informed decision-making in the adoption of cloud Infrastructure-as-a-Service (IaaS). By introducing an ontology tailored for consumers, the paper not only aids in decision-making but also enhances the competitiveness of IaaS providers. The

study exemplifies ontological engineering principles, ensuring a standardized representation for comprehensive consumer-centric assessments [5].

Addressing mental health concerns, the paper on "EEG Feature Extraction based on Fast Fourier Transform and Wavelet Analysis for Classification of Mental Stress Levels using Machine Learning" explores objective methods for assessing mental stress levels. By extracting features from EEG data using Fast Fourier Transform and wavelet analysis, the paper employs machine learning classifiers to achieve promising results. The proposed method holds potential for Computer-Aided Diagnosis (CAD) systems in mental stress assessment [6].

In the realm of medical diagnostics, the paper on "Comparative Study of J48 Decision Tree and CART Algorithm for Liver Cancer Symptom Analysis Using Data from Carnegie Mellon University" focuses on the correlation between hepatitis and liver disease symptoms. Employing J48 and CART decision tree algorithms, the study analyzes patient data to predict liver disease outcomes. The research underscores the potential of machine learning in medical prognosis and decision-making [7].

Turning to robotics, the paper on the "Design of Bio-Inspired Robot Hand Using Multiple Types of Actuators" presents a novel approach to prosthetic hand design. Emphasizing not only appearance and grip strength but also gestures, the paper introduces a bio-inspired robot hand with multiple types of actuators. This design allows for 10 hand gestures, resembling common emoji hand gestures, showcasing the potential for improved human-robot interaction [8].

In the realm of underwater rescue operations, the paper on "Implementation of a GAS Injection Type Prefabricated Lifting Device for Underwater Rescue Based on Location Tracking" addresses the need for efficient lifting systems in underwater accidents. The paper introduces a gas injection-type prefabricated lifting device with location tracking, ensuring fast and effective underwater rescue operations. The proposed device combines communication technology and efficient design for enhanced safety and efficiency [9].

The integration of technology in medical training takes centre stage in the paper on "Towards Real-Time Multi-Class Object Detection and Tracking for the FLS Pattern Cutting Task." Using YOLOv7 object detection neural networks, the paper aims to automate tool motion analysis during laparoscopic surgery training. The research underscores the potential of real-time object detection in enhancing surgical training and evaluation [10].

Ensuring secure and accessible healthcare information is the focus of the paper on "A Secure Medical History Card Powered by Blockchain Technology." Addressing data security concerns, the paper proposes a blockchain-powered medical history card, providing a secure and comprehensive repository of patient information. The research emphasizes the transformative impact of blockchain technology in fortifying healthcare systems [11].

Cybersecurity in cloud computing takes precedence in the paper on "Enhancing Cloud Security: A Comprehensive Framework for Real-Time Detection, Analysis and Cyber Threat Intelligence Sharing." The paper introduces a Hypervisor-based Virtual Machine Introspection (HVMI) framework for real-time detection and analysis of cyberattacks on cloud platforms. The proposed framework exemplifies a comprehensive approach to cloud security, integrating advanced technology with continuous refinement to navigate the evolving cybersecurity threat landscape effectively [12].

The realm of control systems and robotics is explored in the paper on "Dual Mode Control of an Inverted Pendulum: Design, Analysis and Experimental Evaluation." The paper presents a comprehensive analysis of an inverted pendulum system, featuring two distinct control modes for velocity and position. The research delves into the dynamics and control mechanisms, providing insights into optimizing the performance of such systems [13].

The closing paper on "Optimizing the Performance of Network Anomaly Detection Using Bidirectional Long Short-Term Memory (Bi-LSTM) and Over-sampling for Imbalance Network Traffic Data" addresses the critical issue of network security. Employing Bidirectional Long Short-Term Memory (Bi-LSTM) models, the paper optimizes the performance of network anomaly detection. The research underscores the significance of artificial intelligence in identifying and mitigating cybersecurity threats in network traffic data [14].

In conclusion, this compilation of papers represents a diverse array of cutting-edge research spanning robotics, healthcare, machine learning, cloud computing, neuroscience, cybersecurity, and control systems. Each paper contributes valuable insights, methodologies, and solutions to address contemporary challenges and advance their respective fields. The collective efforts showcased in these papers demonstrate the continuous pursuit of innovation and knowledge dissemination in the ever-evolving landscape of science and technology.

References:

[1] F. Sukarman, R. Sato, E. Kita, “Control Program Generator for Vehicle Robot using Grammatical Evolution,” Advances in Science, Technology and Engineering Systems Journal, **8**(6), 1–8, 2023, doi:10.25046/aj080601.

[2] N. Sakli, C. Baccouch, H. Bellali, A. Zouinkhi, M. Najjari, “IoT System and Deep Learning Model to Predict Cardiovascular Disease Based on ECG Signal,” Advances in Science, Technology and Engineering Systems Journal, **8**(6), 8–18, 2023, doi:10.25046/aj080602.

[3] J. Tsiligaridis, “Tree-Based Ensemble Models, Algorithms and Performance Measures for Classification,” Advances in Science, Technology and Engineering Systems Journal, **8**(6), 19–25, 2023, doi:10.25046/aj080603.

[4] A. Papagiannopoulou, C. Angeli, “Social Media Text Summarization: A Survey Towards a Transformer-based System Design,” Advances in Science, Technology and Engineering Systems Journal, **8**(6), 26–36, 2023, doi:10.25046/aj080604.

[5] T. Banditwattanawong, M. Masdisornchote, “Infrastructure-as-a-Service Ontology for Consumer-Centric Assessment,” Advances in Science, Technology and Engineering Systems Journal, **8**(6), 37–45, 2023, doi:10.25046/aj080605.

[6] N.K. Kit, H.U. Amin, K.H. Ng, J. Price, A.R. Subhani, “EEG Feature Extraction based on Fast Fourier Transform and Wavelet Analysis for Classification of Mental Stress Levels using Machine Learning,” Advances in Science, Technology and Engineering Systems Journal, **8**(6), 46–56, 2023, doi:10.25046/aj080606.

[7] R. Chi, “Comparative Study of J48 Decision Tree and CART Algorithm for Liver Cancer Symptom Analysis Using Data from Carnegie Mellon University,” Advances in Science, Technology and Engineering Systems Journal, **8**(6), 57–64, 2023, doi:10.25046/aj080607.

[8] T. Wimonrut, J. Trichada, N. Tirasuntarakul, E. Pengwang, “Design of Bio-Inspired Robot Hand Using Multiple Types of Actuators,” Advances in Science, Technology and Engineering Systems Journal, **8**(6), 65–77, 2023, doi:10.25046/aj080608.

[9] J.-H. Yoon, D.-H. Yoon, “Implementation of a GAS Injection Type Prefabricated Lifting Device for Underwater Rescue Based on Location Tracking,” Advances in Science, Technology and Engineering Systems Journal, **8**(6), 78–86, 2023, doi:10.25046/aj080609.

[10] K.N. Alkhamaiseh, J.L. Grantner, S. Shebrain, I. Abdel-Qader, “Towards Real-Time Multi-Class Object Detection and Tracking for the FLS Pattern Cutting Task,” Advances in Science, Technology and Engineering Systems Journal, **8**(6), 87–95, 2023, doi:10.25046/aj080610.

[11] S. Fairooz, S.Y. Miti, Z. Islam, M.T. Zaman, “A Secure Medical History Card Powered by Blockchain Technology,” Advances in Science, Technology and Engineering Systems Journal, **8**(6), 96–106, 2023, doi:10.25046/aj080611.

[12] F. Rehman, S. Hashmi, “Enhancing Cloud Security: A Comprehensive Framework for Real-Time Detection, Analysis and Cyber Threat Intelligence Sharing,” Advances in Science, Technology and Engineering Systems Journal, **8**(6), 107–119, 2023, doi:10.25046/aj080612.

[13] L. Álvarez-Hidalgo, I.S. Howard, “Dual Mode Control of an Inverted Pendulum: Design, Analysis and Experimental Evaluation,” Advances in Science, Technology and Engineering Systems Journal, **8**(6), 120–143, 2023, doi:10.25046/aj080613.

[14] T. Acharya, A. Annamalai, M.F. Chouikha, “Optimizing the Performance of Network Anomaly Detection Using Bidirectional Long Short-Term Memory (Bi-LSTM) and Over-sampling for Imbalance Network Traffic Data,” Advances in Science, Technology and Engineering Systems Journal, **8**(6), 144–154, 2023, doi:10.25046/aj080614.

Editor-in-chief

Prof. Passerini Kazmersk

ADVANCES IN SCIENCE, TECHNOLOGY AND ENGINEERING SYSTEMS JOURNAL

Volume 8 Issue 6 November-December 2023

CONTENTS

ASTES

Advances in Science, Technology and Engineering Systems Journal
Vol. 8, No. 6, 01-07 (2023)
www.astesj.com
Special Issue on Innovation in Computing, Engineering Science & Technology

ASTES Journal
ISSN: 2415-6698

Control Program Generator for Vehicle Robot using Grammatical Evolution

Firdaus Sukarman[1,3], Ryoma Sato[2], Eisuke Kita[*,1]

[1]*Graduate School of Informatics, Nagoya University, Nagoya, 464-8601, Japan*

[2]*Graduate School of Information Science, Nagoya University, Nagoya, 464-8601, Japan*

[3]*Faculty of Mechanical Engineering, Universiti Technologi MARA Selangor, 40450 Shah Alam, Malaysia*

ARTICLE INFO

Article history:
Received: 16 May, 2023
Accepted: 10 September, 2023
Online: 30 November, 2023

Keywords:
Evolutionary Computation
Robot Control
Grammatical Evolution
Vehicle Robot
Program Generation

ABSTRACT

A robot development has spread widely for various purposes. It is difficult to create a control program for an autonomous mobile robot manually. Therefore, an automatic design of the control program for an autonomous mobile robot is proposed in this research. The autonomous mobile robot is created with LEGO MINDSTORMS EV3, and the control program for the autonomous mobile robot is designed using Grammatical Evolution (GE). Grammatical Evolution (GE), which is one of the evolutionary computations, is designed to generate a program or a program fragment satisfying the design objective. PyBullet is used with GE to simulate the behavior of the robot. A robot traveling along a trajectory was considered as an example. GE can generate the control program of the robot behavior of a robot vehicle traveling along a trajectory. The computer simulation reveals the robot can travel along a designated line. Since there is a reality gap between the simulator and the real environment, the parameters of the vehicle robot such as produced power and sensor sensitivity are calibrated to reduce the gap. Comparison of the computer simulation and the experimental result shows that the reproducibility of the vehicle trajectory in the real environment is high.

1 Introduction

Evolutionary algorithm (EA), which is one of the heuristic search methods, is widely applied for complex and continuous optimization problems [1]. Specially, it is very effective for solving problem with too many design variables. Evolutionary Computation includes Genetic Algorithm (GA) [2, 3], Genetic Programming(GP) [4, 5], Evolutionary Strategy (ES), Evolutionary Programming (EP) and so on.

Genetic Algorithm is widely applied for the complex optimization problem. Candidate solutions of the problem are defined as the individuals [2, 3]. Each individual has the chromosome which defines binary design variables. Population is constructed by the group of the individuals. By applying the genetic operators such as selection, crossover and mutation, individuals evolve into new individuals so that the objective function is minimized. Genetic Programming(GP) is also well-known evolutionary algorithm [4, 5]. Genetic Algorithm aims at finding the solutions of functions, whereas Genetic Programming aims at designing functions and programs [6, 7]. Individuals are defined in a binary tree structure, which is very different from them in Genetic Algorithm. Since the individuals are defined in a binary tree structure, genetic operators for GP are very different from them for GA.

Grammatical Evolution (GE), which was presented in 1998 by O'Neill and C. Ryan, is the evolutionary algorithm for determining the function or program which satisfies the design objective [8]–[10]. The aim of GE is the same as GP. Its algorithm, however, is slightly different. Individuals of GE are defined in the binary or string, like GA. The translation from the binary or integer numbers to function or program is performed according to Backus-Naur form (BNF), which is defined by a user in advance. Authors' colleagues applied Grammatical Evolution to symbolic regression problem, stock price prediction problem and generation of control program of artificial ant in computer simulation [11]–[14]. In this study, Grammatical Evolution is applied for generating the control program of a real vehicle robot. A vehicle robot is made of LEGO MINDSORM EV3 [15, 16].

PyBullet is utilized for simulation of the actual robot motions [17, 18] . This environment is widely utilized as a robot learning environment for manipulation due to its portability and light weight

[*]Corresponding Author: Eisuke Kita, Email: kita@i.nagoya-u.ac.jp

for variety of machine learning tasks [19]. After the program is created in the simulation environment, it is applied to control the actual robot. Since there are differences in sensor sensitivity and motor output between the actual robot and the robot in the simulation environment, the program is modified to compensate for the differences. The results of the robots in the actual and the simulation environments are compared for discussing the validity of the generated program.

The remaining part of this paper is organized as follows. The evolutionary computations are introduced in Section 2. In Section 3, experiments and discussion of control program design using GE are performed. In Section 4, the designed control program is applied to the actual vehicle robot. The conclusion and future issues are summarized in Section 5.

2 Grammatical Evolution

2.1 Outline

Grammatical Evolution is designed to find a function or a program satisfying the design objective. GE composes the initial population by the individuals with randomly generated bit-strings or the sequence of integer numbers [20]. The translation from the integer-string to the program is performed according to the translation rules of Backus-Naur Form (BNF) grammar [21]. After the integer-string of each individual is translated into a function or a program, its fitness is evaluated. The individuals are updated by using genetic operators such as selection, crossover, and mutation with the individual fitness. These process are repeated till the design objective is satisfied. The process is summarized as follows.

1. Define translation rules based on targeted task, which translates integer string to a function or a program.
2. Generate individuals from integer string randomly to define an initial population.
3. Translate the integer-string of each individual into a program.
4. Select parent individuals from population according to fitness.
5. Apply genetic operators such as selection, crossover, and mutation to parent individuals to generate offspring individuals.
6. Update population.
7. If the individual satisfying the design objective can be found, the results are output. If not so, go back to Step 3.

2.2 Translation from Integer String to Program

The translation rules are defined with the set of non-terminal symbols N , the set of terminal symbols T , and the start symbol S. Non-terminal symbols are replaced with the other non-terminal or terminal symbols according to the translation rules. Terminal symbols, on the other hand, is no longer replaced. The sets of the symbols are summarize as follows.

N = { <code>,<op>,<var> }
T = { +,-<*,/,X }
S = { <code> }

The translation rule is shown in Table 1. The symbol "|" means "or". The symbol <code> (A) is replaced with one of three candidates; <code><code> (A0), <op> (A1), and <var> (A2). The symbol <op> and <var> have four candidates and one candidate, respectively.

Table 1: Example of Simple Translation Rules

(A)	<code>	::=	<code><code>	(A0)
		|	<op>	(A1)
		|	<var>	(A2)
(B)	<op>	::=	+	(B0)
		|	-	(B1)
		|	*	(B2)
		|	/	(B3)
(C)	<var>	::=	x	(C0)

Table 2: Evolution of Symbols

S_n	r_A	m	A	Selected symbols	Replaced symbol
			<code>		
3	3	0	<code>	<code><code>	<code><code>
0	3	0	<code>	<code><code>	<code><code><code>
2	3	2	<code>	<var>	<var><code><code>
			<var>	x	x<code><code>
1	3	1	<code>	<op>	x<op><code>
2	4	2	<op>	*	x*<code>
2	3	2	<code>	<var>	x*<var>
			<var>	x	x*x

The translation process is summarized as follows. For example, assuming that the individual is defined as "302122", the translation of "302122" according to Table 1 is shown in Table 2. The start symbol is α = <code>. The leftmost not-used gene is n_0 = 3. The symbol α = <code> has three potential symbols, $n_0 = 3$. Since the remainder of $n_0 = 3$ divided by $n_\alpha = 3$ is $n_r = 0$, the symbol α = <code> is replaced with 0-th symbol of the candidates <code><code>.

Next, the leftmost symbol α = <code> of the symbols <code><code> is replaced as follows. The second leftmost not used number of the individual is $n_0 = 0$. The symbol α = <code> has three candidates and thus, $n_0 = 3$. Since the remainder of $n_0 = 0$ divided by $n_\alpha = 3$ is $n_r = 0$, the symbol α = <code> is replaced with the symbol <code><code> and then, the symbols <code><code> becomes the symbols <code><code><code>.

Next, the leftmost symbol α = <code> of the symbols <code><code><code> is replaced as follows. The third leftmost not-used number of the individual is $n_0 = 2$. The symbol α = <code> has three candidates and thus, $n_\alpha = 3$. Since the remainder of $n_0 = 2$ divided by $n_\alpha = 3$ is $n_r = 2$, the symbol α = <code> is replaced with the symbol <var> and then, the symbols <code><code><code> becomes the symbols <var><code><code>. According to the similar process, the individual "302122" results in $x * x$. The whole process is shown in Table 2.

3 Design of Control Program

3.1 Robot Vehicle

The robot vehicle is created by LEGO MINDSTORMS EV3 (Fig.1). LEGO MINDSTORMS is an educational robot kit jointly developed by LEGO and Massachusetts Institute of Technology. LEGO MINDSTORMS EV3, which was released in 2013, contains an intelligent block with a 32bit ARM9 microprocessor which allows the robot to operate autonomously by downloading and executing

the program. Several sensor such as an ultrasonic sensor, a color sensor, a gyro sensor, and a touch sensor can be attached to the input port and then, the values of each sensor can be used to control the servo motor connected to the output port.

For rapid software development, the robot is loaded with MicroPython firmware for complete integration with a Python-based simulation environment. For uploading and debugging programs on robots, a standard IDE such as Visual Studio Code is utilized. Actual course used in this experiment is shown in Fig.2.

Figure 1: Lego Mindstorms EV3

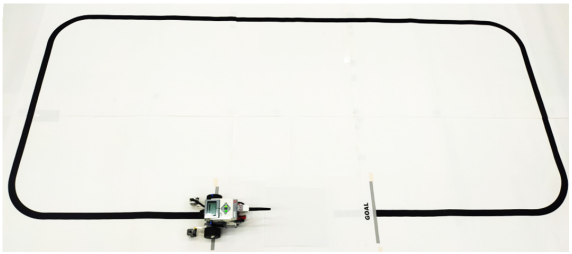


Figure 2: Actual Course

robot, which determines where and in what direction to place the robot first. The GOAL tile is the end of the robot motion. When the center of the robot's axle enters the GOAL tile, the simulation is terminated. The CHECKPOINT tile is functioned as Checkpoint for the robot motion. In Fig. 4, the tiles numbered with $i = 1, \cdots, 18$ denote the CHECKPOINT tiles. A robot has to pass all CHECKPOINT tiles when a robot moves along a line.

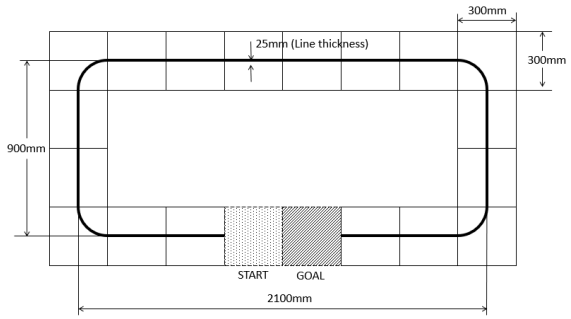


Figure 3: Dimension of Course

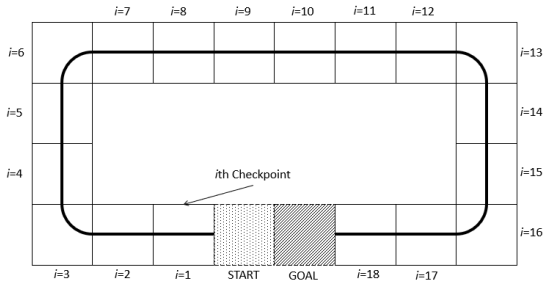


Figure 4: Course Checkpoint

3.2 Simulation Environment

PyBullet is utilized for simulation due to its capability to replicate actual robot motions using Bullet Physics Engine and stability in repetitive machine learning calculations [17] . This environment is widely utilized as a robot learning environment for manipulation due to its portability and light weight for variety of machine learning tasks.

Robot and track model is generated using standard Unified Robot Description Format (URDF) used in Robotics Operating System (ROS) [22]. Object physic characteristics can be defined deliberately in the XML-styled format thus comparatively fasten simulation environment with accurate parameters. Center of axle is configured as measurement point for positional analysis.

Detailed dimensions of the course is shown in Figure 3. The course design is performed by placing 30cm x 30cm tiles on a 240cm x 120cm field. Lines center is located at the center of the tiles with thickness 25mm to match attachment height of the reflection sensor. This setup will enable the reflection sensor to completely sense whether the surface reflect light or not. Tiles with various shapes are prepared, and it is possible to design a course according to the purpose. START, GOAL, and CHECKPOINT can be set for tiles as their specifications. The START tile is the starting position of the

3.2.1 Control Program Translation rules

Grammatical Evolution can generate the best control program from the randomly defined candidate programs according to translation rules known as Backus-Naur Form (BNF) Grammar.

Table 3 shows the translation rule defined for this experiment. In defining the translation rule, the control statements of LEGO MINDSTORMS EV3 are introduced. This statements consists control statement used in PyBullet and LEGO MINDSTORM EV3, and can be controlled with identical control statement both in simulator and real machine.

The translation rules are defined with the set of non-terminal symbols N, the set of terminal symbols T, and the start symbol S. The sets of the symbols are summarize as follows.

N = { <code>,<op>,<num> }
T = { if(SensorValue > (100+)/2): else:,
motor(, ,),-100,-90,-80,-70,-60,
-70,-60,-50,-40,-30,-20,-10,0,10,20,
30,40,50,60,70,80,90,100 }
S = { <code> }

The symbol <code> (A) can be replaced with one of three candidates; <code><code> (A0), <op> (A1) and if(SensorValue > (100+<num>)/2): <op> else:

<op>(A2). The symbol <op> and <num> have one candidate and 21 candidates, respectively.

Table 3: Translation rules

(A)	<code>::=	<code><code>	(A0)
	|	<op>	(A1)
	|	if SensorValue>(100+<num>)/2{<op>} else{<op>}	(A2)
(B)	<op>::=	motor(<num>,<num>,100+<num>)	(B0)
(C)	<num>::=	-100	(C0)
	|	-90	(C1)
	|	-80	(C2)
	|	-70	(C3)
	|	-60	(C4)
	|	-50	(C5)
	|	-40	(C6)
	|	-30	(C7)
	|	-20	(C8)
	|	-10	(C9)
	|	0	(C10)
	|	10	(C11)
	|	20	(C12)
	|	30	(C13)
	|	40	(C14)
	|	50	(C15)
	|	60	(C16)
	|	70	(C17)
	|	80	(C18)
	|	90	(C19)
	|	100	(C20)

At translation rule (A), the statement <code><code> in Rule (A0) adds the evolvable mechanism. Direct selection of motor control is added using the statement <op> in Rule (A1) that enable the selection of motor movement directly. For sensor input, if SensorValue>(100+<num>)/2{<op>}else{<op>} is used as *if*-statement to control the motor movements upon receiving the sensor value. The statement SensorValue get the output from color sensor which is integer between 0 to 100 and the conditional value (100+<num>)/2 is used to match the color sensor input in increments of 5. This conditional statement produces two executable statements <op>, first statement is executed when the sensor value is larger than selected value, otherwise the second statement is executed. This allows the color output of the sensor change the pattern of the motor input.

At translation rules in (B), the statement motor(<num>,<num>, 100+<num>) is the control statement for the motors, where the arguments are for left motor, right motor and waiting time for the movement to complete. The statement <num> for first and second argument is used to select the speed input range from -100 to 100 in 10 increments. Negative value means the motor will run backwards with percentage ratio. The statement 100+<num> is a control argument that sets the execution time (ms) of motor power input. Since the argument started with value of 100, only positive value will be produced from 0 to 200 in increments of 10.

At translation rule C, a common usable parameter with a value between -100 and 100 is set so that it can be used for sensor and motor input conditional values.

3.2.2 *Fitness Function and Parameters*

Each generated program is evaluated using a fitness function capable of achieving the goal by passing all checkpoints in less than 60 seconds. The fitness function is defined such that lower values indicate a better solution, so that the control program generation problem is appointed as a minimization problem. The objective function is defined as below.

$$\min f(x) = \begin{cases} T_{Goal} & (if N_{checkpoints} = 18, T_{Goal} \leq 60) \\ 10^4 & (otherwise) \end{cases} \quad (1)$$

where $N_{checkpoints}$ and T_{Goal} represent number of checkpoints tiles,*i*-th and total time taken,T (s) to reach the GOAL tile, respectively. Only individuals that pass through within all 18 checkpoints are evaluated and beyond that the fitness is penalized with very large number(10^4). Large number is used as fitness scaling to control diversity to prevent the populations converge to early toward a single optimal solution[3]. Solutions fitness that go beyond the tiles will also be deducted until the trajectories of robot follow the line and finally reach the determined target. Parameters used is shown in Table 4

Table 4: GE Parameters

Population size	200
Maximum generation	50
Gene length	1000
Number of elites	1
Selection	Tournament
Tournament size	5
Crossover type	One-point crossover
Crossover rate	0.4, 0.5, 0.7
Mutation rate	0.03, 0.05, 0.07

3.3 *Simulation Results*

In Figure 5 , we perform five simulations with different initial values and show the average value. This attempts to remove the influence of how the initial values were selected. The horizontal and the vertical axes represent the number of generations and the arrival time to the GOAL tile, respectively. The result of the crossover rate 0.5 and the mutation rate 0.05 demonstrates the quickest convergence during the initial generation. Table 5 shows the average fitness of the best individual in the final generation for different crossover rates and mutation rates. When the crossover rate is 0.4, the simulation did not converge for mutation rate 0.03 and 0.05, but shows lowest rate of convergence when mutaton rate is 0.07. The best fitness is obtained when the crossover rate is 0.5 and the mutation rate is 0.05.

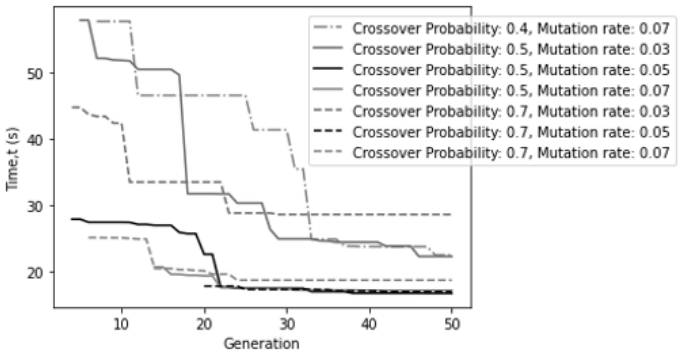


Figure 5: Convergence history travel time over generation

Table 5: Effect of Crossover and Mutation rate

Crossover rate \ Mutation rate	0.03	0.05	0.07
0.4	-	-	22.51
0.5	22.32	16.74	17.20
0.7	28.64	16.98	18.74

```
if(SensorValue > 80):
    motor(80,80,50)
else:
    motor(80,0,160)
```

Figure 6: Generated program

Fig.6 shows the program generated based on the best individual of the final generation. It is notice that the best generated program is a simple line tracing program. When the color sensor of a robot vehicle notices white on the course, the vehicle moves forward with the maximum motor output. When the color sensor notices black, the vehicle rotates to the right on the spot. At the start, the vehicle moves forward because the color sensor is positioned on the white field. When the color sensor enters the black line, the vehicle rotates to the right. After completing the rotation, the vehicle moves forward because the color sensor is positioned on the white field. After repeating forward and right turns alternately four times in this way, a robot vehicle goes straight and reach the GOAL tile.

4 Experiment

4.1 Performance Estimation of Robot Vehicle

LEGO MINDSTORMS EV3 robot can be controlled using motor power input (Duty Cycle) in percentage and speed input. When the motor is assigned with increments of speed in 2s interval time, rotational speed increases and reached the limit of 800degree/s as shown in the Fig. 7 which is equivalent to the maximum of 80% of the power input. Motor power input is capped to 80% and the limitations are also applied to the simulation.

Motor power input is a simple method to control the movement of the robot by supplying current to the motor in ratio. The estimation of motor speed require actual power input when the robot is under actual load when moving around the track with surface friction. Fig.8 shows the relation between power and rotational speed of motor in degree/s.

4.2 Kinematics of Robot

Grammatical Evolution program uses speed input to vary the velocities of the two wheels, thus determine the trajectories of the robot. Actual robot used in this experiment utilize Differential-drive Robot concept where two independent motor with wheel radius,r rotate about the same axis and low-friction caster wheel is used to keep the robot horizontal.

For left and right motor linear velocity, v_l and v_r, where R is distance from center of curvature to the center of the axle and l is effective distance between wheel (axle), kinematics equation based on Instantaneous center of curvature concept for the system is shown below;

$$v_l = \omega(R + l/2)$$
$$v_r = \omega(R + l/2)$$
$$\omega = \frac{v_l + v_r}{2} \quad (2)$$

By varying the motor speed for left and right, trajectories of the robot can be determined based on the turning rate, ω.

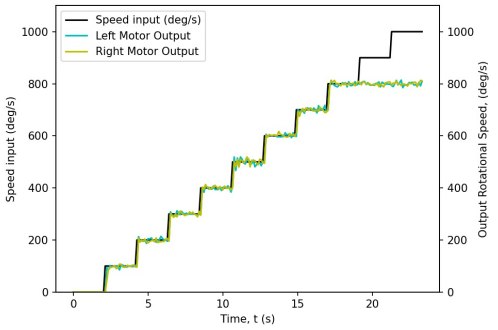


Figure 7: Relation between Speed input and Rotation Speed (degree/s)

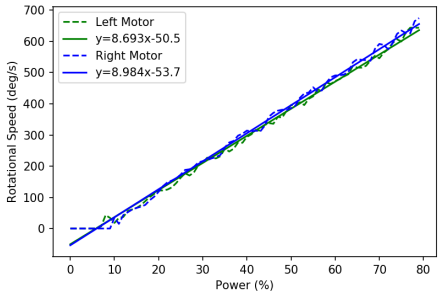


Figure 8: Relation between Power and Rotation Speed (degree/s)

4.3 Actual Robot Experiments

Evaluation of the simulation is done by using the actual robot with identical dimensions to prove the effectiveness of the program generated. Program generated from GE is executed to check the effectiveness.

Figure 9 shows the trajectory of the vehicle. A robot vehicle starts from the position of X=0 and Y=0 and then, makes one lap around the course clockwise. A solid line shows the computer simulation result and broken lines denote actual experiment results of five trials of vehicle robot, respectively. Table 6 shows the arrival time for 5 trials performed. Maximum, minimum, and mean arrival times are 18.71 (s), 19.92 (s) and 19.30 (s), respectively. Since the arrival time of the simulation is 16.74 (s), the errors of maximum, minimum, and mean arrival times are 11.8 (%), 19.0 (%) and 15.4 (%), respectively. In experiments using actual robots, it is expected that the arrival time becomes longer than that in simulations due to factors such as robot acceleration and control delay time.

This difference in time elapsed is caused by the actual robot movement take a longer path to make turn for each line corner. Longer sensor responses and efficiency of the motor are two main reasons which create a tiny small lag for the robot to make turns. Even there is a small time difference, the robot control program able to accomplish the main objective which is following the line. In addition, Figure 10 shows the difference between the vehicle position in the simulator and in the real environment at each time step (0.01s). The error fluctuates up and down with time, but basically increases with time.

The correlation coefficient between the vehicle coordinates in the simulator and the experiment is evaluated for the trajectory of the vehicle, and the result is show in Table 7. A high correlation is shown in both the x-coordinates and y-coordinates. It can be seen that the correlation coefficient for the y-coordinate is lower than that for the x-coordinate. From Fig. 9, it is expected that the deviation of the y-coordinate between the simulation and the experiment is relatively large.

Table 6: Running Time

Experiment	Arrival time (s)	Error (%)
Trial 1	18.98	13.4
Trial 2	19.51	16.5
Trial 3	18.71	11.8
Trial 4	19.92	19.0
Trial 5	19.47	16.3
Average	19.32	15.4

Arrival time at simulation : 16.74 (s)

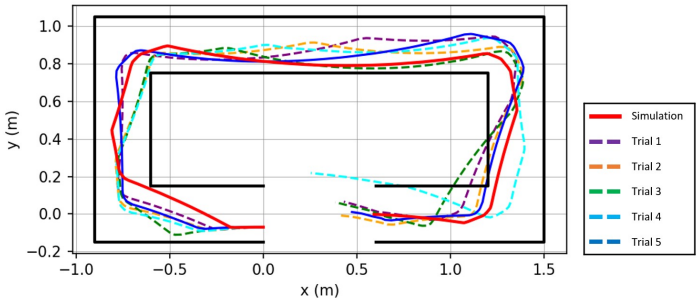


Figure 9: Robot path comparison between simulation and actual

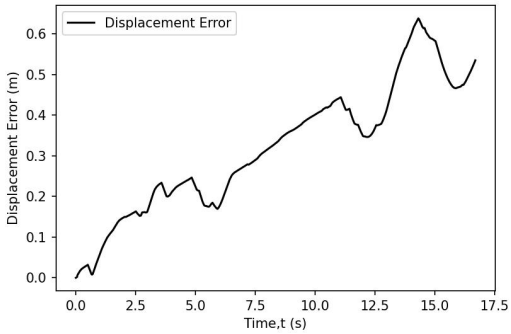


Figure 10: Displacement between vehicle position in simulator and real world

Table 7: Correlation coefficient between vehicle coordinates in simulation and experiment

x-coordinate	0.9553
y-coordinate	0.7743

5 Conclusion

A method of designing a control program for an autonomous mobile robot using Grammatical Evolution (GE) was proposed in this research. The autonomous mobile robot was created with LEGO MINDSTORMS EV3, and the control program for the autonomous mobile robot was designed using Grammatical Evolution (GE). Robot Virtual Worlds was used to simulate the behavior of the robot. A robot traveling along a trajectory was considered as an example. As a result, the fitness converged toward the optimal solution, and the running trajectory of the robot according to the designed control program was appropriate. A real machine experiment was performed by applying the control parameters that adjust the gap between the simulator and the real environment. Comparing the computer simulations and experimental results shows that the target achievement time in the running experiment was equivalent to that of the simulator. In addition, it was shown that the reproducibility of the vehicle trajectory in the real environment was high.
Finally, future issues is summarized as follows. First, to reduce the computational time, an algorithm should be revised to improve the convergence performance. Secondly, the experiments with complicated courses and conditions should be performed to verify the effectiveness of the proposed method for many problems.

References

[1] H.-P. P. Schwefel, Evolution and Optimum Seeking: The Sixth Generation, John Wiley & Sons, Inc., USA, 1993.

[2] J. H. Holland, “Adaptation in natural and artificial systems,” University of Michigan press, Ann Arbor, MI, **1**, 1975.

[3] D. E. Goldberg, “Genetic Algorithms in Search, Optimization, and Machine Learning,” NN Schraudolph and J., **1**, 1989.

[4] J. R. Koza, Genetic Programming II: Automatic Discovery of Reusable Programs, volume 1, MIT Press, 1994.

[5] J. R. Koza, Genetic Programming lll: Darwinian Invention and Problem Solving, Morgan Kaufmann, 1999.

[6] V. de Carvalho Santos, C. F. M. Toledo, F. S. Osorio, “An exploratory path planning method based on genetic algorithm for autonomous mobile robots,” 62–69, IEEE, 2015, doi:10.1109/CEC.2015.7256875.

[7] R. Kala, “Multi-robot path planning using co-evolutionary genetic programming,” Expert Systems with Applications, **39**, 3817–3831, 2012, doi:10.1016/j.eswa.2011.09.090.

[8] C. Ryan, J. Collins, M. O. Neill, Grammatical evolution: Evolving programs for an arbitrary language, volume 1391, 83–96, 1998, doi:10.1007/BFb0055930.

[9] M. ONeil, C. Ryan, “Grammatical evolution: Evolutionary automatic programming in an arbitrary language,” Norwell, MA, **10**, 1–978, 2003.

[10] C. Ryan, M. ONeill, J. J. Collins, Introduction to 20 years of grammatical evolution, 2018, doi:10.1007/978-3-319-78717-6_1.

[11] T. Kuroda, H. Iwasawa, E. Kita, "Application of advanced Grammatical Evolution to function prediction problem," Advances in Engineering Software, **41**, 1287–1294, 2010, doi:10.1016/j.advengsoft.2010.09.005.

[12] E. Kita, Y. Zuo, H. Sugiura, T. Mizuno, "Acceleration of Grammatical Evolution with Multiple Chromosome by Using Stochastic Schemata Exploiter," Proceedings - 2017 4th International Conference on Mathematics and Computers in Sciences and in Industry, MCSI 2017, **2018-Jan**, 190–195, 2018, doi:10.1109/MCSI.2017.40.

[13] H. Sugiura, M. Nagao, Y. Zuo, E. Kita, "Grammatical evolution using two-dimensional gene for symbolic regression: An advanced improvement with conditional statement grammar," International Journal of Critical Infrastructures, **13**, 2017, doi:10.1504/IJCIS.2017.083634.

[14] E. Kita, H. Sugiura, Y. Zuo, T. Mizuno, "Application of grammatical evolution to stock price prediction," Computer Assisted Methods in Engineering and Science, **24**, 2017.

[15] L. Group, "LEGO MINDSTORMS EV3," 2023.

[16] L. G. 2019-2020, "LEGO MINDSTORMS Education EV3 MicroPython," 2020.

[17] E. Coumans, Y. Bai, "PyBullet, a Python module for physics simulation for games, robotics and machine learning," 2017.

[18] F. Sukarman, E. Kita, "Auto-generated Control Program in Mobile Robot using Grammatical Evolution," 1–5, Association for Computing Machinery, 2022, doi:10.1145/3573910.3573921.

[19] X. Yang, Z. Ji, J. Wu, Y.-K. Lai, "An Open-Source Multi-goal Reinforcement Learning Environment for Robotic Manipulation with Pybullet," Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), **13054 LNAI**, 14–24, 2021, doi:10.1007/978-3-030-89177-0_2.

[20] M. Fenton, J. McDermott, D. Fagan, S. Forstenlechner, E. Hemberg, M. O'Neill, "PonyGE2: Grammatical evolution in python," GECCO 2017 - Proceedings of the Genetic and Evolutionary Computation Conference Companion, 1194–1201, 2017, doi:10.1145/3067695.3082469.

[21] G. Dick, P. A. Whigham, "Initialisation and grammar design in grammar-guided evolutionary computation," 534–537, ACM, 2022, doi:10.1145/3520304.3529051.

[22] O. R. 2021, "ROS - Robot Operating System," 2021.

Advances in Science, Technology and Engineering Systems Journal Vol. 8, No. 6, 08-18 (2023)

www.astesj.com

ASTESJ

ISSN: 2415-6698

IoT System and Deep Learning Model to Predict Cardiovascular Disease Based on ECG Signal

Nizar Sakli[1,2], Chokri Baccouch[3,4,*], Hedia Bellali[5], Ahmed Zouinkhi[1], Mustapha Najjari[6]

[1]*MACS Research Laboratory RL16ES22, National Engineering School of Gabes, Gabes University, Gabes, 6029, Tunisia.*

[2]*EITA Consulting, 5 Rue du Chant des Oiseaux, 78360 Montesson, France.*

[3]*SYS'COM Laboratory LR99ES21, National Engineering School of Tunis, Tunis El Manar University, Tunis, 1002, Tunisia.*

[4]*CHArt Laboratory (Human and Artificial Cognitions), University of Paris 8, Paris, France.*

[5]*Department of Epidemiology and Statistics, Abderrahmen Mami Hospital, Ariana, Tunisia, Section of Preventive Medicine and Public Health, Medical Faculty of Tunis, Tunis El Manar University, Tunisia.*

[6]*LR18ES34 PEESE, National Engineering School of Gabes, Gabes University, Gabes, 6029, Tunisia.*

ARTICLE INFO

Article history:
Received:28 August, 2023
Accepted:29 October, 2023
Online: 30 November, 2023

Keywords:
Telemedicine
Healthcare
ECG monitoring system
Motion Noises
Cardiovascular Diseases
Heart Diseases
IoT
Artificial Intelligence
Deep Learning

ABSTRACT

In this work, our contribution will intervene to reduce the impact of noises on the ECG signals. Various ECG denoising approaches were tested to see how efficient they were in removing dominant noises that add to pure ECG signals. Due to different causes such as interference, muscular noise, body movement related to breathing, and so on, the original signal acquired by the electrodes produces noises. In this article, the electrode signals are monitored using an Internet of Things system that combines an Arduino board and an AD8232 module to generate a one-dimensional signal. These ECG signals are displayed on a computer using the Matlab interface. Following that, an efficient deep learning model was developed to facilitate cardiologists in their diagnosis of ECG signals. These experimental results obtained demonstrate the effectiveness of our proposed model compared to other existing methods in the literature. Finally, the filtered and classified ECG signals are given to the doctor for correct treatment of the patient's condition.

1. Introduction

An ECG is a signal that shows how the heart's electrical system is working. The relaxation (repolarization) and contraction (depolarization) of the heart's ventricular and atrial muscles produce an ECG signal [1]. A P wave (due to atrial depolarization), a QRS complex wave (due to atrial repolarization and ventricular depolarization), and a T wave (due to ventricular depolarization) make up the ECG signal. Transducers (electrodes) are placed in certain locations on the human body to mark the ECG signal. Noises (artifacts) are undesired signals that mix with the ECG signal and may prevent doctors from making a correct diagnosis. As a result, proper signal processing procedures must be used to eliminate them from ECG signals [2]. Powerline interference, baseline wander, EMG noise, and electrode motion artifacts are the four main forms of artifacts seen in ECG signals. They are discussed briefly below.

The electrical activity of the heart is represented by an electrocardiogram signal. ECG is an essential component for monitoring cardiovascular disease patients [1]. The theoretical and practical bases for recording cardiac electrical activity were laid out by Einthoven in 1901 and, although the postulates proposed are highly debatable, are still used in electrocardiography [2]. In the following paragraphs, we briefly describe the inactivity of the heart, the modes of recording this electrical activity, and the main frequency characteristics presented by the ECG.

The electrocardiogram (ECG) facilitates the diagnosis of many heart (or extra cardiac) diseases in association with clinical, laboratory or echocardiographic data. The analysis of an ECG must be methodical and rigorous. The criteria for a normal ECG

*Corresponding Author: Chokri Baccouch, chokri.baccouch13@gmail.com

https://dx.doi.org/10.25046/aj080602

and the variants of normal should be well known. Abnormalities in rhythm, conduction, chronic or acute pathologies that can also be detected [3].

You must first inquire about the clinical situation / symptoms motivating the performance of the ECG, age, sex and sometimes ethnicity, examination conditions (half-seated, lying down, etc.), the morphology of the rib cage, pathologies or taking medication(s) with possible repercussions on the heart and the existence of a pacemaker. All of this information is useful but can sometimes bias the interpretation (" expectation bias").

One of the main steps in the data acquisition operation is filtering. The latter is a relative operation, that is to say to apply it, we must determine what is filtered (determine useful signals and parasitic or disturbing signals). For example, if our system is radar tracking an airplane, the useful signal will be the position of this airplane and any other signal will be considered as an interruption; in our case, the useful signal is the electrocardiogram signal, and the parasitic signals will be all other signals circulating in the human body (EMG, EEG, and others.). Therefore, we can say that the main function of a filter is to minimize the effect of disturbances and provide a smoother useful signal.

Demand for accurate and portable ECG monitoring has increased. Only a few hospitals in semi-developed countries own instruments that measure electrocardiographic (ECG) or cardiovascular activity. Despite the compact size of these portable devices, precision filtering, high-performance processing power, and integrated high-resolution graphics control distinct from the main microcontroller core are still required [4]. The necessity for physical capacity has become important as medical observation of patients becomes more remote. The Microchip Connected Body and Body ECG Demonstration Board may be used to create advanced fitness monitoring devices, as well as remote patient monitoring and diagnostic systems.

The essential goal of this article is to collect or get data on the electrical activity of the patient's heart and, following a well-studied optimal filtering, to use telecommunication equipment to send this ECG signal to the doctor. We are talking about an act of telemedicine called tele-surveillance or remote monitoring. In the first section of this work, we describe a generality on ECG signals as well as the difficulties of monitoring these signals. The second section of this work focuses on our contribution to monitoring ECG signals via IoT system as well as the interpretation of real measurement results performed on three patients. In the last section of the work, we describe the different types of noises that can generate ECG signals as well as the different digital techniques to remove them before sending them to the doctor for good medical treatment.

The rest of this paper is organized as follows: related works are investigated in section 2. Material and methods are presented in detail in section 3. In Section 4, we described implementation and testbed, followed by the experimental results in sections 5. Finally, the paper concludes.

2. Related Work

The value chain research and analysis of the ECG monitoring system helps to understand the useful contribution of each operation in the device, the best practices that each process can adopt, and the overall purpose of the system to assure improved disease diagnosis. The information collection, feature extraction, pretreatment, analysis, processing, and visualization operations are all part of the ECG surveillance importance chain. The majority of published studies support the above-mentioned primary ECG monitoring approach. Some studies have defined additional different or overlapping methods such as information cleansing, encryption, and compression, depending on the type of control application, however they may be included as part of the approach.

Various signal treatment approaches for removing artifacts from ECG data are presented in this section. The classification of ECG signal denoising techniques in the literature is shown in Figure 1. This part also includes the results of the methodologies discussed.

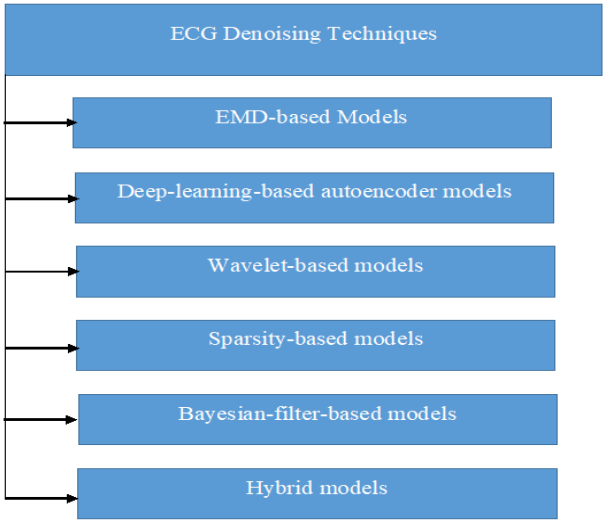


Figure 1: Techniques of ECG signal denoising techniques.

In [5], an adaptive iterative algorithm that breaks the signal down into a series of oscillation segments, called an Intrinsic Mode Function (IMF) was studied. This is an EMD (Empirical Mode Decomposition). With this iterative decomposition of the signal, EMD will be able to divide the whole signal into ordered elements whose frequency varies from the highest to the lowest of each IMF level.

In [6], the authors claim that the local time characteristics of the signal are the bases for the decomposition of the EMD process, so it is suitable for nonlinear and nonstationary processes.

In [7], an EMD based on a completely information-driven instrument was developed, which does not require an outset known basis and differs from data analysis techniques such as the Fourier transform.

In [8], the author discuss denoising methods based on auto-encoders. This type of ECG denoising, the deep learning-based model, is built on the basis of the function of the denoising auto-encoder (DAE). This is the first step in unsupervised learning, mapping the input to the intermediate representation. To regenerate an input signal as accurately as possible, the automatic learning model that can be used is that of the auto-encoder. It is a combination between two non-linear sub-parts, namely the encoder and the decoder.

In [9], a novel set of approaches for removing noise from ECG signals is discussed. The signal is extended as a function of frequency and time using the wavelet transforms (WT). WT can provide good temporal and frequency resolution in HF and LF, respectively. As a result, using WT to analyze ECG data is quite effective. The signal can be decom-posed into a collection of fundamental functions using this method, including ctraction, translation of the mother function x (mother wavelet), and expansion. The usage of Dyadic WT (DWT) for evaluating ECG data is particularly favorable due to its calculation speed and multi-resolution properties [10].

A sparse decomposition was used in [11] to reduce noise in the ECG signal. The signal is divided down into components, with each component being separated into scattered residues and parts. As a result, these empty regions are employed to estimate proper signals because they hold the useful information in the signals. The shares are deconstructed using a nonlinear optimization approach to find the sparsest illustration.

The authors of [12] describe a more advanced version of the standard Kalman (KF) filter. To decouple ECG signals, many model-based approaches have been developed. Model-based techniques are founded on the idea of estimating an essential model's hid-den states. The latter is noticed using a series of measurements, one of which is the Kal-man filter (KF). Although this simple filter uses a linear model of system dynamics and surveillance equations, most systems are not linear. EKF, EKS (Extended Kalman Smoother), and UKF are three different editions of the original KF (Unscented Kalman Filter).

The researchers combined several denoising techniques to diagnose ECG signals in order to improve the performance of essential dancing procedures, i.e. they attempted to combine procedures from various fields to denoise the ECG signals in order to achieve top results in the standard. We will explore successful hybrid ways to denoising the ECG signal in this section of the study.

The authors of [13] attempted to combine the EMD process with the concept of an adaptive transition thought filter (ASMF). In the same method, the advantages of both strategies are combined to reduce ECG signal noise. Classical EMD rejects attempts to re-duce HF sounds using a window-based approach or initial IMFs, but for HF noise reduction, an ASMF operation is used to track a wavelet-based soft thresholding strategy.

In [14] authors proposes and investigates a new ECG denoising approach based on a combination of vibrational mode decomposition (VMD), NLM (Non-local Means) assessment, and discrete WT filtering method (DWT).

FFT was used in combination with an adaptive R peak identification method to de-noise and detect ECG signals in [15].

In [16], the EMD algorithm was combined with Savitzky–Golay (SG) filtering and Riegmann-Liouvelle (RL) fractional integral filtering to create a novel ECG denoising approaches.

ECG denoising was done with a wavelet neural network in [17], which approximated the signal with the maximum precision achievable. The backpropagation neural network was created with two hidden layers and ten neurons using conjugate gradient optimization. Parent wavelets from libraries such as Daubachies, Symlet, and others are used as hidden layer triggering functions for ECG signal estimation. An investigation of DWT-NN for denoising ECG data was provided in [18]. The authors of this research present a technique with high efficiency for real-time hardware and the best accuracy (96%) for ECG denoising only.

The authors of [19] propose a hybrid technique in which EMD enhanced output is delivered to a DWT-based denoiser in addition to EMD enhanced output. The most recent versions combine an adaptive flexible threshold with a generic threshold that is changed based on signal strength.

For noise suppression, the NLM and EMD models are mixed in [20]. A four-step technique has been presented, including landmark detection (R peak detection), differential standard deviation computation, NLM framework, and EMD framework. Table 1 summarizes the many works provided.

Table 1: Comparative analysis with main recent research studies.

Ref	ECG Dataset	Efficiency for Real-Time Hardware	Performance
[5]	MIT-BIH Arrhythmia Database	Medium	93%-96% Sensitivity and Positive Predictivity
[6]	MIT-BIH Arrhythmia Database	High	94.1% Accuracy
[7]	MIT-BIH Arrhythmia Database	High	94.7% Accuracy
[8]	MIT-BIH Arrhythmia Database	High	N/A Time complexity most efficiency
[9]	MIT-BIH Arrhythmia Database	High	96.1% Accuracy
[10]	MIT-BIH Arrhythmia Database	High	92%-94% Sensitivity and Positive Predictivity
[11]	MIT-BIH Normal Sinus Rhythm Database	High	94%-96% Sensitivity and Positive Predictivity
[12]	MIT-BIH Normal Sinus Rhythm Database	High	95.3% Accuracy
[13]	MIT-BIH Normal Sinus Rhythm Database	Medium	N/A Time complexity most efficiency
[14]	MIT-BIH Normal Sinus Rhythm Database	Medium	N/A Time complexity most efficiency
[15]	MIT-BIH Normal Sinus Rhythm Database	Medium	94.3% Accuracy
[16]	MIT-BIH Noise Stress Test Database	High	96.8% Accuracy for ECG Denoising only
[17]	MIT-BIH Noise Stress Test Database	High	95.6% Accuracy for ECG Denoising only
[18]	MIT-BIH Noise Stress Test Database	High	96% Accuracy for ECG Denoising only
[19]	MIT-BIH Noise Stress Test Database	High	N/A Time complexity most efficiency
[20]	MIT-BIH Noise Stress Test Database	Medium	97.9% Accuracy for ECG Denoising only

Generation and monitoring of ECG signals will be studied in sections III and IV respectively.

3. ECG Signal Generation

The ECG can be analyzed by examining the waveform component. These global components indicate the body of the active electrical board. The first rising line of the ECG path is the P wave. It shows atrial contraction. The activation wave allows the repolarization and depolarization of cardiac cells which can be received by electrodes located in certain places [21]. These methods result in the global waveform called normal ECG, as shown in figure 2.

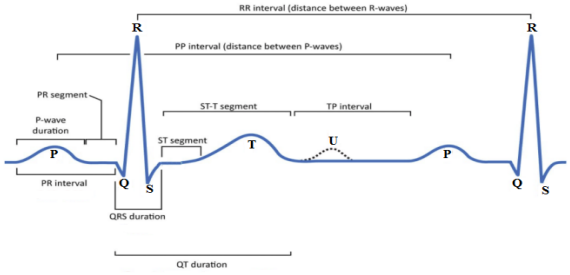


Figure 2: ECG Signal.

You must read the entire ECG trace like a book, from top to bottom then from left to start with the frontal leads then the precordial leads and end right, that is to say with the long trace of one or more leads (generally 10 seconds provided at the bottom of the page by the manufacturers). Each deflection described by Einthoven must be analyzed.

The following are the waveforms that make up the ECG: a P wave is a deviation response to the depolarization of the right and left atria, whereas a T wave, which is usually less ascending, represents the QRS complex, which starts with Q and ventricular repolarization, small downward deviation, and then more upward deviation, a peak(R), and then a falling S wave. This QRS complex show off ventricular and depolarization contraction. The QRS complex is the same to a series of decreases because of the depolarization of the ventricles. Normal values for declination times are Q-wave ≤ 0, 04 s, P-wave ≤ 0, 11 s, QRS complex at 0,1 s, usually 0. 06 and 0, 08 s and the length of the QT wave varies depending on the heart rate. It gets longer as the rate decreases and down as it increases.

4. ECG Signal Monitoring

Over the past few decades, heart disease has become a big problem as many people die from health problems. Thus, heart disease cannot be relieved. By initially diagnosing or monitoring an ECG, this disease can be prevented. In this study, we are interested in a complete system for monitoring patients at home in real time. We'll need a sensor to create this system, which will be affixed to the patient's body. This sensor is part of a WSN network that can be found in a hospital or a house. All patient information is recorded and transmitted to the hospital via a WSN network. To take all necessary corrective measures in an emergency, the hospital transmits the data to the doctor. In the event of a sudden, unassisted relapse with patients, a WSN email address was used to determine the patient's whereabouts. The Wireless Sensor Network (WSN) is used to monitor the environment or physical phenomena, such as noise, pressure, motion, or temperature, and to transmit data to the destination.

Nowadays, with the explosive growth of IoT technology, more and more practical applications can be found in many fields, including security, smart metering, agriculture, smart cities, and more home intelligence. There are other applications, in particular military, home automation, industrial, sanitary, and above all medical and sanitary. This article proposes and explores home health care [22]. The Arduino can be used to perform a portable ECG with the heart condition reading function. The main component of this system is the AD8232 sensor which can read the heart rate and process the voltage of the electrodes connected to the body. By combining the Arduino and HC 05 FC-114 microprocessor like Bluetooth or Wifi, ZigBee, GSM / GPRS and even XBee, the ECG screen is displayed in real time on a smartphone. We used an ECG simulator as an artificial corrective agent which is used as a tool to justify the performance of a portable ECG based on the results obtained from the test. The EGC can be sent via the simulator to the smartphone or to the Matlab interface via a wireless communication module (ZigBee, Bluetooth, Wifi, GSM / GPRS or XBee) [23]. The precise result depicts the patient's current state in real time. The ECG results are presented in this paper using the Matlab interface [24].

Currently, with the development of electronic media, especially with the appearance of the Arduino module and thanks to the advantages it presents, the realization of any project has become an easy task (figure 3). In this work, we will use the Arduino module, XBee module and other ways to monitor an ECG signal and its remote emission [25].

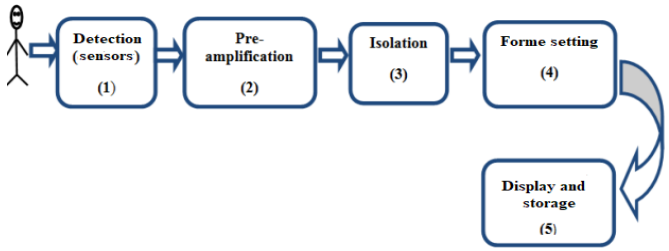


Figure 3: Block diagram of an ECG.

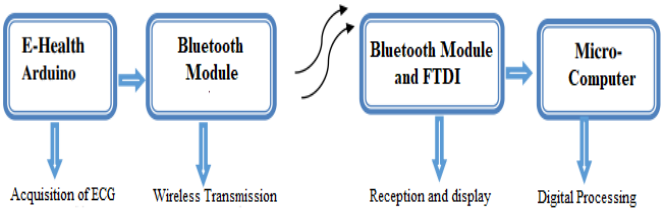


Figure 4: Block diagram of our Remote ECG signal monitoring application.

The first step of our project is to acquire the ECG signal. The electrodes implanted on the patient's body to explore and transfer the signal to an E-Health 2.0 acquisition card ensure this procedure (figure 4). The latter guarantees the format and processing of the electrode signal. The e-Health acquisition board is then attached to an Arduino board, which converts the ECG signal to analog-to-digital (ADC) format [26]. As a result, using an Xbee transmission module, the resulting digital signal can be sent remotely to another station [27]. At the reception point, another XBee reception

module on an FTDI card will allow reception of the transmitted signal [28]. This XBee reception module is connected to a microcomputer to view and process the received signal.

An ECG is a paper or digital recording of the heart's electrical signals. It is used to determine heart rate and other information about heart disease, such as heart attacks, pacemaker function, and heart failure. The synthesis (or conclusion) is intended to answer the question posed by the clinical situation. For example, we can conclude that:

- Normal or variant ECG: atrial repolarization, early repolarization, wandering pacemaker, etc.
- Nonspecific QRS or repolarization abnormality): microvoltage, intraventricular block, fragmented QRS complexes, ST depression, Chatterjee effect, secondary repolarization disorder ...
- Specific anomaly: sinus dysfunction, sinus bradycardia, sinus tachycardia, atrial fibrillation . . .; atrial or ventricular hypertrophy, preexcitation, sequelae of necrosis, amyloidosis. . .; bundle branch block, bifascicular block, AV block. . .; Brugada repolarization, long QT interval ...
- ECG in favor of an acute pathology: infarction, coronary ischemia, acute pericarditis, pericardial effusion, pulmonary embolism, hyperkalaemia, hypothermia, intoxication.

In the first phase of this work, we performed a generation of ECG signals with their spectral concentration in MATLAB. A study of ECG signals is performed for three patients whose characteristics are listed in Table 2.

Table 2: Patient Diagnosis.

Patient	Patient1	Patient2	Patient3
Sex	Female	Male	Male
Age	35	48	81
Diabetic	No	No	Yes
Smoking	No	No	No

Figure 5 shows a complete portable ECG on the patient's body during a monitoring test as well as data collection and transfer via a Bluetooth module.

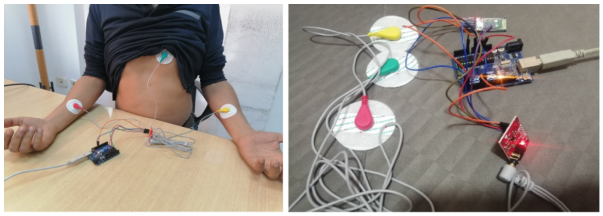


Figure 5: ECG monitoring test and data collection with Bluetooth module.

4.1. Test for acquiring data

The Bluetooth-enabled wearable ECG was then tested on a real human body with heart problems. The results are provided, followed by an explanation based on medical logic and a conclusion. These signals have a 10 second period and a 1000 Hz sample frequency. Each patient conducted 15 tests, each of which is an ECG signal, with the results shown in the figures below. The results of a healthy heart are explained by Figure 6. The two key values obtained from the data were the form of the PQRST wave and the heart's BPM. An ECG wave was recorded and visualized using a Matlab interface in this example. The P wave, the QRS complex, and the T wave are all clearly split into three components in this ECG wave. A P-type wave is caused by the register of the SA node, which was a heart stimulating node. The QRS complex is formed when the ventricular muscle relaxes and contracts at the same time. A recording is made as the ventricular muscles repolarize to prepare for the next heartbeat; this is the T wave.

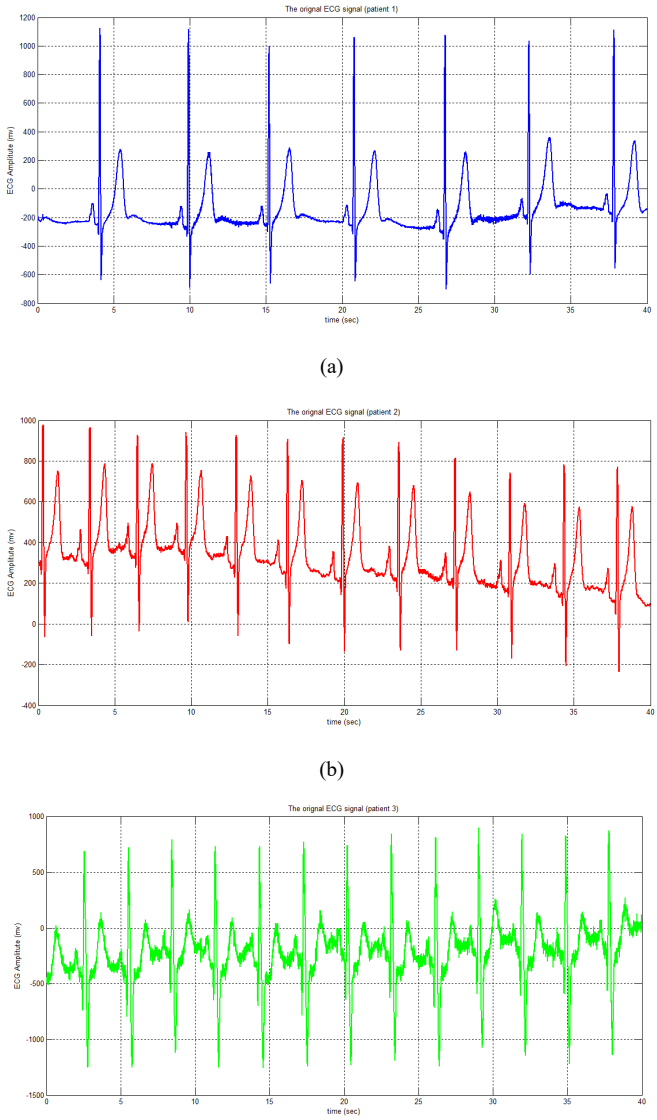
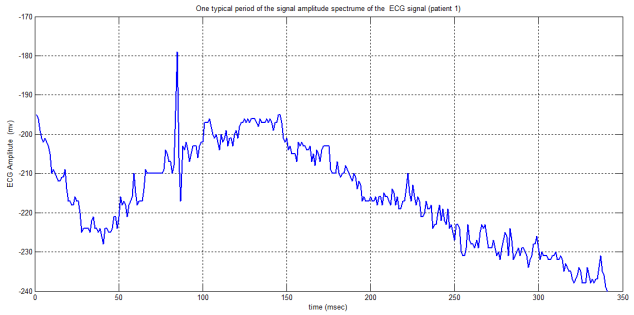


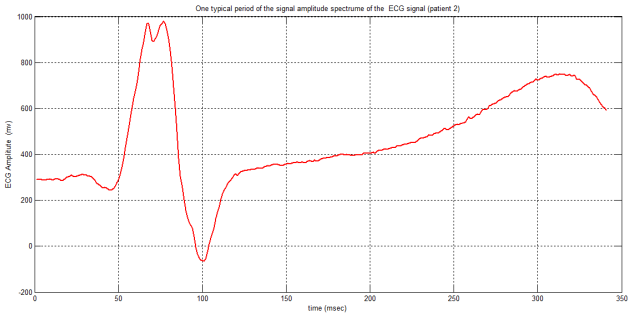
Figure 6: ECG signals for three patients

4.2. Detection of the number of beats

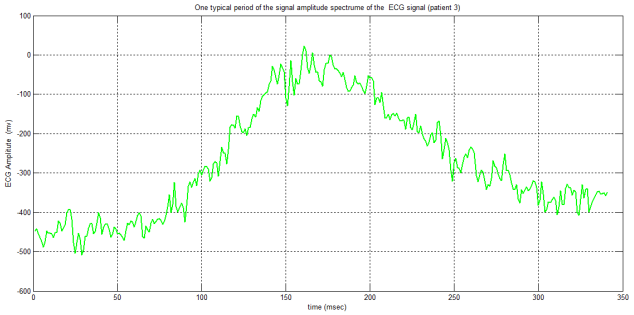
In an ECG signal, the R-wave represents the patient's heart-beat [29]. We determine the main "R" peaks for each patient's ECG signal, as well as the typical period of the signal amplitude (figure 7).



(a)



(b)



(c)

Figure 7: Typical Period Variation of ECG Signal Amplitude for Three Patients

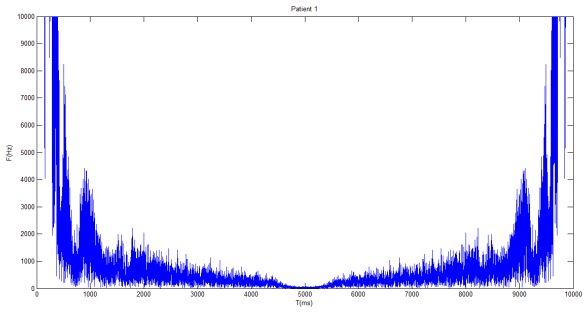
The heart rate is measured in beats per minute (BPM) over a 60-second period. A healthy heart rate is 60-100 beats per minute at rest, but it increases to around 110-150 beats per minute during exercise and 40-60 beats per minute during sleep [30]. When collecting data about a patient's heart, it's best to put them to sleep. The patient is affected by bradycardia if the heart rate is below 60 BPM or tachycardia if the rate is beyond 100 BPM for a heart rate externally ranging between 60 to 100 BPM (Table 3).

Table 3: Number of dominant peaks" R".

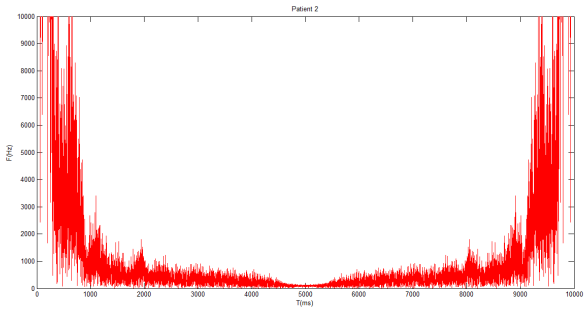
Patient	Patient1	Patient2	Patient3
Number of dominant peaks" R"	8	33	13
Number of beats (BPM)	12	49	20

4.3. ECG Signal Spectral Analysis

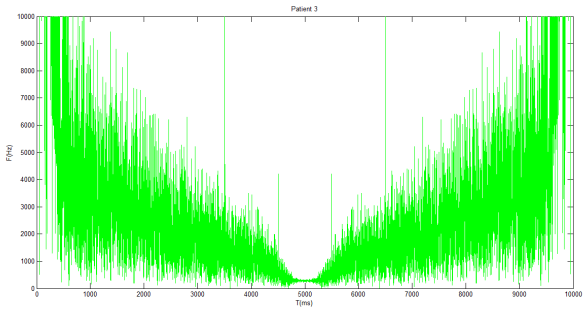
For each patient, we determined the spectrum of the ECG signal (figure 8), Nyquist frequency (Table 4), and figure 9 depicts the PQRST cycle of three patients' ECG signals.



(a)



(b)

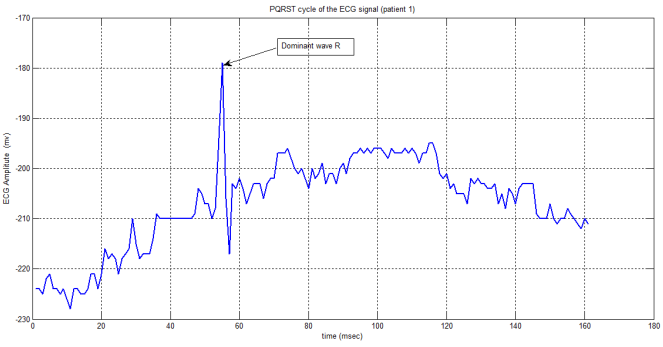


(c)

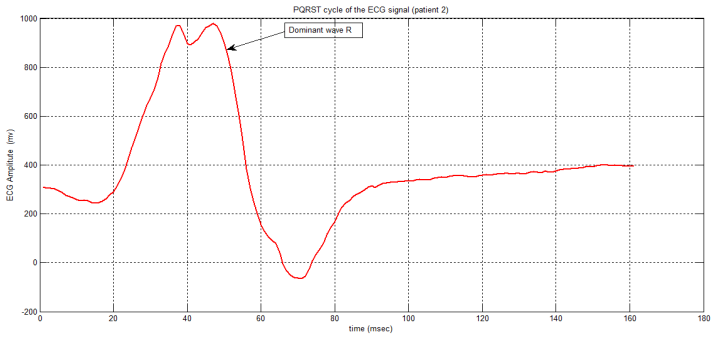
Figure 8: ECG signal spectral of patients

Table 4: Patient Diagnosis.

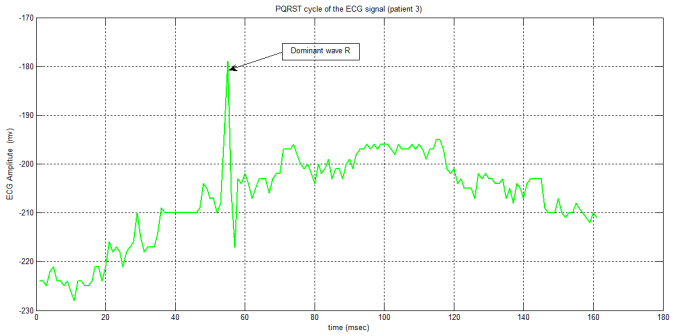
Patient	Patient 1	Patient 2	Patient 3
Nyquist frequency (Hz)	2.9511	6.5968	4.2440



(a)



(b)



(c)

Figure 9: PQRST cycle of the ECG signal

5. ECG Noises

The ECG program contains a variety of noises. Baseline wander, power-line interference, and muscular artefacts are the most common. Body movement, breathing, poor electrode contact, and skin electrode impedance promote baseline wander [31]. The consequences of distortion of the ST segment and LF components of the ECG signal are dependent on electrode and electrolyte characteristics, skin impedance, and body movement, and range between 0.05 and 1Hz. Power-line interference [32], caused by capacitive and inductive couplings of ubiquitous power lines in the ECG signal acquisition circuit, with an amplitude and peak duration of 50% of the ECG signal amplitude, a spectrum with narrowband noise centered at 50/60 Hz with a bandwidth of 1 Hz, and the effect of produced is a distortion of the local low amplitude waveform of the ECG signal, amplitude, and duration. Muscle artefacts [33] are caused by electrical activity in muscles during contractions or when the body moves suddenly, with 10% of the ECG signal amplitude and spectrum at 20-1000 Hz. It has the effect of changing the local waveforms of the ECG signal [34].

5.1. Baseline Wander

The equipotential line of the heart is called the baseline; if the heart has no electrical activity, this is the trace that can be seen on the electrocardiogram [35]. During an ECG examination in the office or during a night Holter recording, this line is generally horizontal because the patient does not move, and the signal is little disturbed by outside noise. On the other hand, during the day, the movement of the patient will modify the relative position of the electrodes, so that this line appears wavy.

5.2. Power line Interference

It is activated at the same time by two myocardial regions which are flowing at the same time. This results, for example, in fusion complexes, aberrations or pseudo-blocks. This phenomenon also explains the aspects of QRS during atrial fibrillation caused by accessory bundles (see Atrial fibrillation / flutter and accessory bundles) [36].

5.3. Muscle artefacts

Motion noises are similar to the characteristics of the baseline drift signal, but because their spectral content significantly overlaps the spectral content of the PQRST complex, it is more difficult to resolve. Stretching of the skin, which affects the impedance of the skin around the electrode, is the most common cause of electrode movement abnormalities. They mostly appear in the 1 to 10 Hz range, and on ECGs, these aberrations appear as greater amplitude waveforms that can be mistaken for QRS complexes. Electrode motion artifacts are a key source of a misperceived heartbeat in Holter surveillance [37].

6. Remove noises from our ECG signals

Filtering the ECG signal is a technique for removing noise around the signal generated by the ECG machine. High frequency noise is caused by extracardiac muscle activity and interference from electronic equipment. Low frequency noise is caused by body movements associated with breathing, physical and chemical changes caused by electrodes placed on the skin, and small changes in blood flow. To reduce these noises (see parasites), the patient should breathe calmly and avoid moving or touching metal. Before placing the electrodes, the skin must be perfectly prepared (shaving, simple washing and rubbing to improve the capillary flow of the peripheral electrodes, do not use alcohol). It is also important to avoid overlapping recording threads (loops). Several types of filters can be used in the event of interference:

- To remove interference from electric current (removal of 50 or 60 Hz depending on the country).
- To remove very low frequency noise, we use a classic high-pass filter which removes in real mode noises below the threshold of 0.05 Hz. A 0.5 Hz, real time high pass filter records / generates ST segment distortions. This threshold can simulate an anteroseptal ST + infarction or a Brugada ECG.

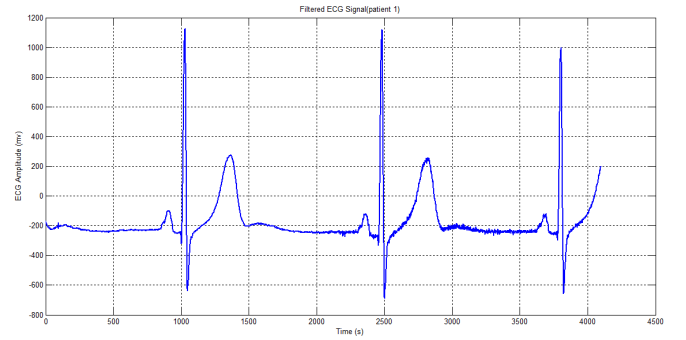
On the other hand, in automatic mode (analog recording then digital signal processing, usual mode of modern ECGs) a digital linear filter is acceptable up to the threshold of 0.67 Hz, because it eliminates the deviations from the baseline).

A conventional low pass filter is used to eliminate high frequency noise, which removes noise over 150 Hz in real mode. A low pass filter calibrated to 75 Hz or less will slightly reduce the amplitude of QRS and the ability to detect small deviations (Q microwave, QRS fragment complex wave, J wave, wave). It further smooths the path and removes many fast artifacts. A low pass filter calibrated to 35 Hz or even 20 Hz can significantly reduce the amplitude of the QRS and reduce the signs of ventricular hypertrophy.

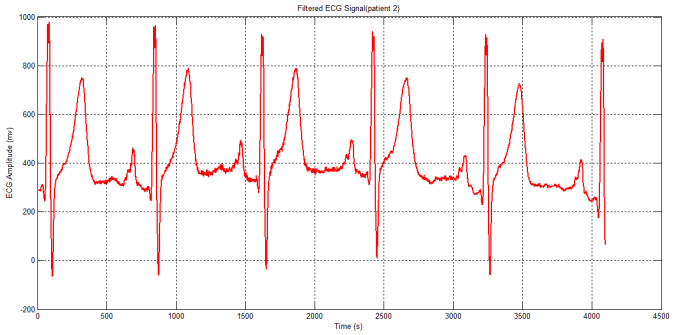
The general recommended bandwidth for adults is between 0.05 Hz and 150 Hz (250 Hz for children). But most devices on the market offer preset filters between 0.5 and 40-50 Hz, because the design is more stable and the noise is less, which makes basic users more satisfied. This is a compromise generally adopted by users

who are new to the more refined ECG ... and accept the risk of false positives / negatives, although rare this can be caused by improper filters. It is best to decide whether to enable low pass and / or high pass filters before printing depending on the quality of the drawing.

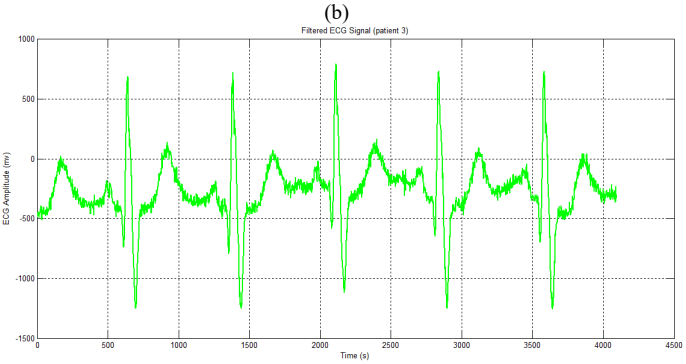
After applying filtering steps to each patient's ECG signals, we transfer those signals to the right doctors and physicians to make the right decisions about the patient's health (figure 10 and figure 11).



(a)

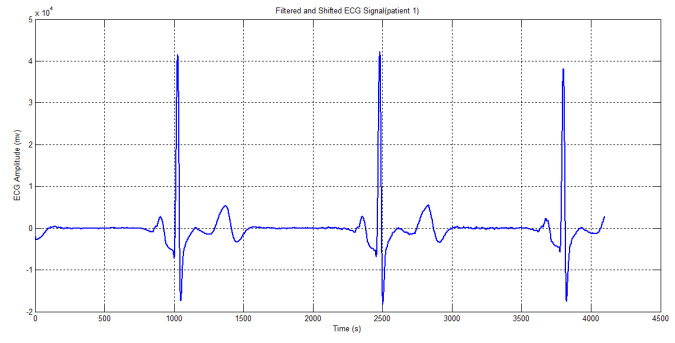


(b)

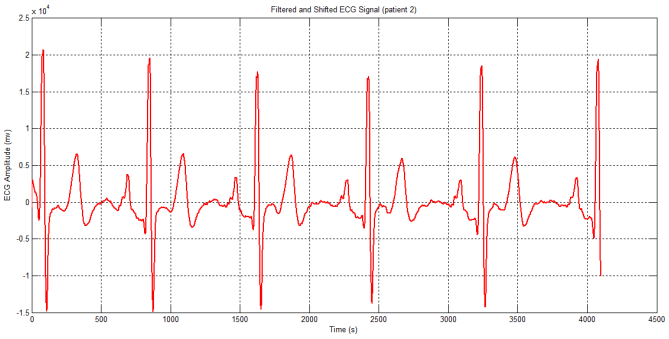


(c)

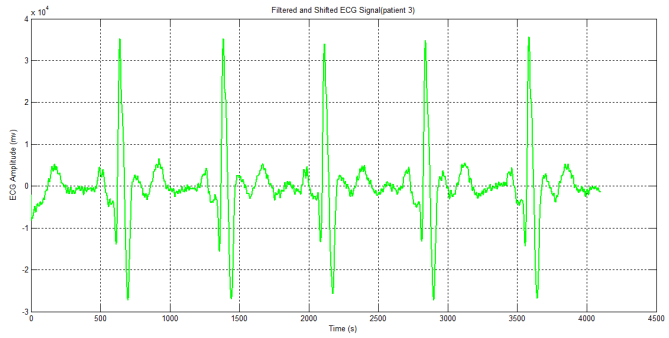
Figure 10: Filtered ECG Signal



(a)



(b)



(c)

Figure 11: Filtered and Shifted ECG Signal

To develop our IoT system for monitoring ECG signals, we have opted to use artificial intelligence, so we will offer an application of IoT and embedded AI for detection, monitoring of ECGs and learning for the detection of noises which generate these signals.

7. The effect of filtering on ECG data classification for cardiovascular disease using a deep learning model

Deep Learning-based classification methods for detecting cardiovascular disease ECG features are gradually gaining attention. In this section, we will discuss the importance of ECG signal filtering in detecting cardiovascular disease. The main contribution of this comparison is to highlight the importance of signal filtering in improving cardiovascular disease.

Deep learning requires a large database to effectively train the model; thus, we decide to train our model with the PTB-XL database [38], which comprises 21 837 recordings. PTB XL is a dataset containing 23 classes; the ratio of each database is presented in Figure 12.

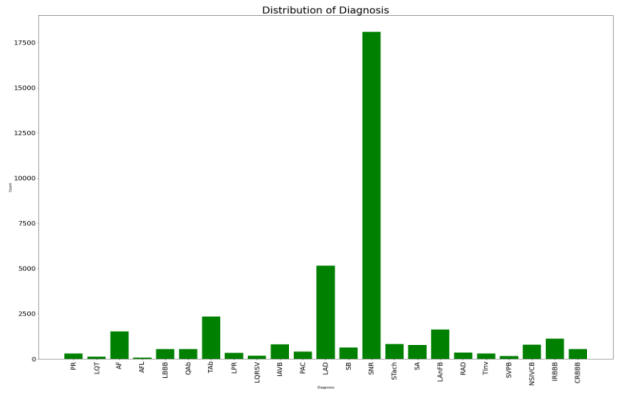


Figure 12: Data Distribution.

7.1. Data preprocessing

Classification researchers usually passed preprocessing of the data and feature extraction of the signal to train and evaluate the model correctly [39]. Data preprocessing is the process of preparing data for training by removing noise and filtering signals. Many researchers employed different noise removal approaches, such as wavelet transform-based algorithms [40] and adaptive digital filters [41].

In this paper, we propose to compare two methods one that does not filter ECG data and method 2, which is based on filtering, wavelet transform method was used to enhance the ECG signal. The wavelet transform technique decomposes nonstationary data into scale signals with various frequency bands [42].

This study has selected 23 ECG recordings for classification with length varies from signal to other, since the deep learning model requires a normalized dataset, in our study, the signal length has been segmented to 5000 samples (10 seconds).

The use of embedded AI can be very useful for detecting ECG signals. For this, it is possible to design a learning model based on a convolutional neural network (CNN) for the detection of ECG signals. This model is trained on an image database, which is then processed and tested to improve detection performance. Experiment results reveal that our model outperforms other common object classifiers. The major improvements enable the model to work effectively in real ECG applications. In the second step, we applied this learning model on a database of ECG signals, these real signals were measured and monitored by our IoT monitoring system proposed and studied in the first section of this work.

7.2. Model training

For the training step, the two methods have been trained using Inception model figure 13, which is a variant of CNN, to classify 23 cardiovascular diseases. To extract the deep features, five Inception blocks, concatenated with max polling (MaxPool), are used, each block contains six convolutional layers (Conv1d), five batch normalization layers (BatchNorm1d), six rectified linear unit (ReLU) activation layers, and max polling (MaxPool). Figure 13 illustrates an overview of the model architecture.

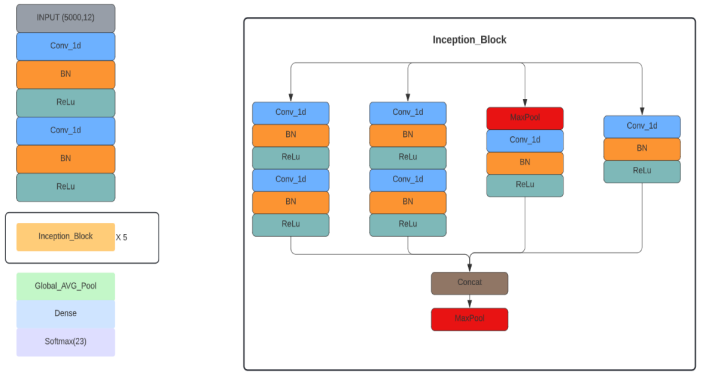


Figure 13: Model architecture.

The dataset used was split into two sets: training & validation set contains recordings and test set contains 19653 & 2184 recordings respectively, using cross-validation the dataset was randomly divided into 10 folds. In each round 9 out of 10 folders have been utilized for training, while one folder is used for validation, 5 epochs are created per each training fold, in total 50 epochs.

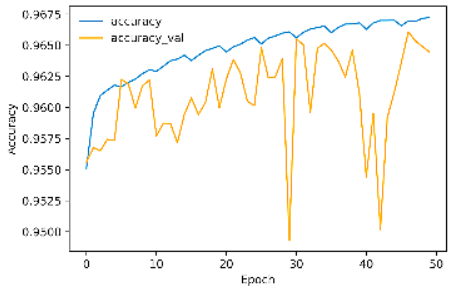
To train the model, the Adam optimizer has been used as the optimization method and binary cross-entropy as the loss function.

7.3. Results and discussion

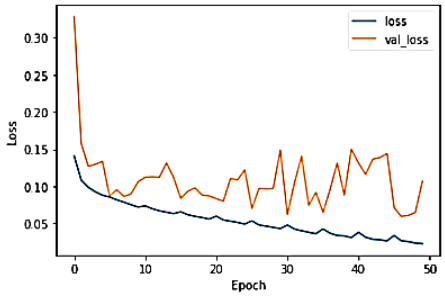
This paper presented a model based on convolutional neural networks, optimized to limit the complexity of ECG detection and classification of cardiovascular diseases. Our proposed technique was implemented in Python 3.7 utilizing the Keras framework with a Tensorflow backend.

The accuracy acquired throughout the training and validation phases is 96.72% and 96.45%, respectively in filtering method and 96,23% and 96,20% for no filtering method. For loss, each phase reached 0.0227 and 0.1070 for no filtering and 0.0849 and 0.0866 for filtering method. The data split is the usage of ten stratified folds that leads the model grow disorderly from the fold to fold until it stabilizes in the final fold. We can note that there is a disorder in value from one epoch to another caused by the usage of ten stratified folds, since each fold contains 5 epochs the disorder is clear after every 5 epochs. The results are relatively close in both methods accuracy of 96,72 % and loss of 0.0227 without filtering, 96,23 % in term of accuracy and loss of 0.0849 with filtering. The relevance of filtering is that the model's results with filtering are more stable than without filtering.

The Metrics results of model proposed in each method are illustrated in Figures 14 and 15.

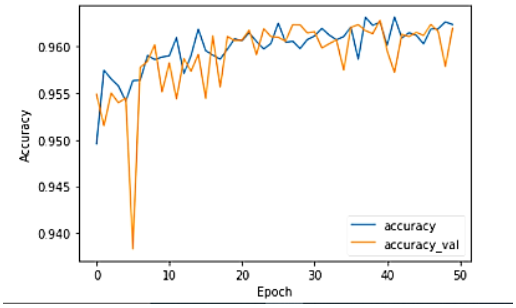


(a) Accuracy : Validation phase: 96.20% ; Training phase: 96.23%

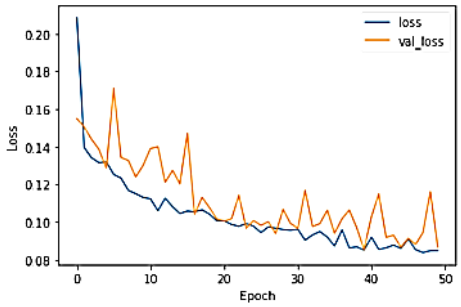


(b) Loss : Validation phase : 0.1070 ; Training phase : 0.0227

Figure 14: Method 1: without filtring.



(a) Accuracy : Validation phase: 96.45% ; Training phase: 96.72%



(b) Loss : Training phase : 0.0845; Validation phase :0.0866

Figure 15: Method 2: with filtring.

A deep convolution neural network (DCNN) to classify 5 types of ECG, and their approach achieves an accuracy of 93.19%. In [43] authors proposed an 11 layers CNN to detect 2 types of heartbeats, they achieve an accuracy of 95.22 %, meanwhile in [44] authors succeed to achieve 97.2% in term of accuracy to detect five cardiovascular diseases using a CNN network. Comparing to resultants achieved in the literature, our results for classifying 23 cardiovascular diseases are significant and acceptable.

Table 5 compares the accuracy and loss of our research to the literature studies.

Table 5. Comparison of different literature studies.

Author, year	Preprocssing	ECG classes	Classifier used	Results
Atal et al, 2020	Gabor filter and wavelet transform	5 classes	DCNN	Acc: 93.19%
Acharaya et al, 20	Denoising	2 classes	CNN	Acc: 95.22%
Wu et al, 2021	wavelet transform method	1 classe	CNN	Acc: 97.2%
Proposed approach, 2022	wavelet transform method	23 classes	Inception	Acc: 96.72%

The disorder in second method, after filtering the signals, is more stable than in the first method. As a result, we may conclude that filtering is critical for model stability, even if the gap between the validation and training phases is tiny enough to ensure that our model learns effectively.

It is more crucial to raise the metrics of the classification model for disease diagnosis because the correct detection of a cardiovascular disease is more significant than a misdiagnosis our future work will be based on model improvements to obtain important results.

8. Conclusions

The use of ECG monitoring equipment has been extensively studied in the literature. We have provided an in-depth overview of the literature related to ECG monitoring systems in this article, focusing on a variety of factors such as application, technologies used, architecture, life cycle, categorization, and defiance. The Internet of Things (IoT) delivers remote, infinite connection and services that harness data and enable fast, relevant and vital lifestyle decisions. We proposed a new compact IoT system for remotely monitoring ECG signals in patients. The data are shown via the Matlab interface after converting the data gathered by the electrodes and the AD8232 sensor built into the Arduino board into a "csv" or ".m" extension file. Following that, we used various digital filtering methods to remove any noise that could have caused these ECG readings. To that purpose, we support this work, as well as a detailed assessment of other related research projects that provide a comprehensive overview of the state of the art in ECG monitoring systems. It can serve as a resource for various researchers and field participants to compare, assess, and evaluate the functionality of ECG monitoring systems. It also highlights the main defiance that occurs with these systems. We also developed a deep learning model based on a convolution neural network to evaluate the results of metrics (accuracy and loss) with and without filtering, and we were able to attain an important and acceptable accuracy when compared to results achieved in the literature. We attain an accuracy of 96.23% with filtering and 96.72% without, they are relatively close but filtering with wavelet transform makes our model more stable. Finally, it discusses how next-generation ECG monitoring devices for healthcare will be perceived in the future.

Conflict of Interest

The authors declare no conflict of interest.

Acknowledgment

This research was funded by the Deanship of Scientific Research at EITA Consulting, Montesson, France.

References

[1] E. Balestrieri, L. De Vito, F. Picariello, I. Tudosa, "A novel method for compressed sensing-based sampling of ECG signals in medical-IoT era," Proc. of the IEEE Int. Symp. on Medical Meas. and Applications (MeMeA), Istanbul, Turkey, 1-6, 2019, DOI:10.1109/MeMeA.2019.8802184.

[2] P. Kamble, A. Birajdar, "IoT based portable ECG monitoring device for smart healthcare," Proc. of the 5th International Conference on Science Technology Engineering and Mathematics (ICONSTEM), Chennai, India, 471-474, 2019, **DOI:** 10.1109/ICONSTEM.2019.8918776.

[3] Gupta, A.K., Chakraborty, C., Gupta, B, "Monitoring of epileptical patients using cloud-enabled health-IoT system," Traitement du Signal, **36**(5), 425-431, 2019, **DOI:** https://doi.org/10.18280/ts.360507.

[4] E. Span, S. Di Pascoli and G. Iannaccone, "Low-Power Wearable ECG Monitoring System for Multiple- Patient Remote Monitoring," in IEEE Sensors Journal, July 1, 2016, DOI:10.1109/JSEN.2016.2564995.

[5] Chang, K.M., "Arrhythmia ECG noise reduction by ensemble empirical mode decomposition," Sensors, **10**(6), 6063–6080, 2010, doi: 10.3390/s100606063.

[6] Munirathinam, R., Ponnan, S., Chakraborty, C, "Improved performance on seizure detection in an automated electroencephalogram signal under evolution by extracting entropy feature," Multimed Tools Appl, 2021, https://doi.org/10.1007/s11042-021-11069-7.

[7] Blanco-Velasco, M., Weng, B., Barner, K.E., "ECG signal denoising and baseline wander correction based on the empirical mode decomposition," Comput. Biol. Med., **38**(1), 1–13, 2008, DOI: 10.1016/j.compbiomed.2007.06.003.

[8] Ehnesh, M., Abatis, P. &Schlindwein, F.S, "A portable electrocardiogram for real-time monitoring of cardiac signals," SN Appl. Sci, **2**(8), 1419,2020, DOI:10.1007/s42452-020-3065-9

[9] Akansu, A.N., Haddad, P.A., Haddad, R.A., et al., "Multiresolution signal decomposition: transforms, subbands, and wavelets," Academic Press, USA, 2001.

[10] Chen, B., Li, Y., Zeng, N., "Centralized wavelet multiresolution for exact translation invariant processing of ECG signals," IEEE Access, **7**, 42322–42330, 2019, **DOI:** 10.1109/ACCESS.2019.2907249.

[11] Zhu, J., Li, X., "Electrocardiograph signal denoising based on sparse decomposition," Healthc. Technol. Lett, **4** (4), 134–137, 2017, doi: 10.1049/htl.2016.0097.

[12] Sameni, R., Shamsollahi, M.B., Jutten, C., "A nonlinear Bayesian filtering framework for ECG denoising," IEEE Trans. Biomed. Eng, **54** (12), 2172–2185, 2007, **DOI:** 10.1109/TBME.2007.897817.

[13] Rakshit, M., Das, S, "An efficient ECG denoising methodology using empirical mode decomposition and adaptive switching mean filter," Biomed. Signal Process. Control, 40,140–148, 2018, DOI:10.1016/j.bspc.2017.09.020.

[14] Singh, P., Pradhan, G., "Variational mode decomposition-based ECG denoising using non-local means and wavelet domain filtering," Australas. Phys. Eng. Sci. Med, **41**(4), 891–904, 2018, DOI: 10.1007/s13246-018-0685-0

[15] Kumar, A., Ranganatham, R., Komaragiri, R., "Efficient QRS complex detection algorithm based on fast Fourier transform," Biomed. Eng. Lett, 9(1), 145–151. 2019, doi: 10.1007/s13534-018-0087-y.

[16] Jain, S., Bajaj, V., Kumar, A, "Riemann liouvelle fractional integral based empirical mode decomposition for ECG denoising," IEEE J. Biomed. Health Inf, **22**(4), 1133–1139, 2018, DOI:10.1109/JBHI.2017.2753321.

[17] Rajankar, S.O., Talbar, S.N, "An optimum ECG denoising with wavelet neural network," Int. Conf. on Pervasive Computing (ICPC), Pune, 1–4, 2015, DOI:10.1109/PERVASIVE.2015.7087204.

[18] Kaergaard, K., Jensen, S.H., Puthusserypady, S, "A comprehensive performance analysis of EEMD-BLMS and DWT-NN hybrid algorithms for ECG denoising," Biomed. Signal Process. Control, **25**,178–187, 2016, DOI: 10.1016/j.bspc.2015.11.012.

[19] Kabir, M.A., Shahnaz, C, "Denoising of ECG signals based on noise reduction algorithms in EMD and wavelet domains," Biomed. Signal Process. Control, 7 (5), 481–489, 2012, doi: 10.1016/j.bspc.2011.11.003.

[20] Kumar, S., Panigrahy, D., Sahu, P.K, "Denoising of electrocardiogram (ECG) signal by using empirical mode decomposition (EMD) with non-local mean (NLM) technique," Biocybern. Biomed. Eng, **38**(2), 297–312, 2018.

[21] Wang Y et al, "Design and evaluation of a novel wireless reconstructed 3-lead ECG monitoring system," In: Proc. IEEE 2013 Biomedical Circuits and Systems Conference (BioCAS), Rotterdam, Oct, 362-365, 2013, DOI:10.1109/BioCAS.2013.6679714.

[22] P. Singh and A. Jasuja, "IoT based low-cost distant patient ECG monitoring system," International Conference on Computing, Communication and Automation, Greater Noida, 1330-1334, 2017, DOI:10.1109/CCAA.2017.8230003.

[23] M. Neyja, S. Mumtaz, K.M.S. Huq, S.A. Busari, J. Rodriguez and Z. Zhou, "AnIoT-Based E-Health Monitoring System Using ECG Signal," IEEE Global Communications Conference, Singapore, 1-6, 2017, DOI: 10.1109/GLOCOM.2017.8255023.

[24] L. Yang, K. Yu, S. X. Yang, C. Chakraborty, Y. Lu and T. Guo, "An Intelligent Trust Cloud Management Method for Secure Clustering in 5G enabled Internet of Medical Things," in IEEE Transactions on Industrial Informatics, doi: 10.1109/TII.2021.3128954.

[25] Gandhi, P., Khan, M. Z., Sharma, R. K., Alhazmi, O. H., Bhatia, S. et al. "Software Reliability Assessment Using Hybrid Neuro-Fuzzy Model," Computer Systems Science and Engineering, **41**(3), 891–902, 2022, DOI:10.32604/csse.2022.019943.

[26] Z. Yang, Q. Zhou, L. Lei, and K. Zheng, "An IoT-cloud Based Wearable ECG Monitoring System for Smart Healthcare," J. Med. Syst., **40**(12),286, 2016, DOI: 10.1007/s10916-016-0644-9.

[27] S. Pal, "ECG monitoring: present status and future trend," in: Reference Module in Biomedical Sciences Encyclopedia of Biomedical Engineering, Roger Narayan, Elsevier, ISBN 9780128051443, 363-379, 2017, DOI:10.1016/B978-0-12-801238-3.10892-X.

[28] Leo Louis, "Working Principle of Arduino and Using it as a Tool for Study and Research," International Journal of Control, Automation, Communication and Systems (IJCACS), July 2018, DOI:10.5121/ijcacs.2016.1203.

[29] Miguel Bravo-Zanoguera, Daniel Cuevas Gonzalez, Juan Pablo Garc´ıa-Vazquez, Roberto Lopez Avitia, Portable ECG System Design using the AD8232 Microchip and Open-source Platform, 6th International Electronic Conference on Sensors and Applications, **42**(1), 2019, DOI:10.3390/ecsa-6-06584.

[30] Ayaskanta Mishra, Biswarup Chakraborty, Debajyoti Das, Priyankar Bose, "AD8232 based Smart Healthcare System using Internet of Things (IoT)," International Journal of Engineering Research, April 2018, DOI: 10.17577/IJERTV7IS040040.

[31] Bernard Abi-Saleh, Bassam Omar, "Einthoven's Triangle Transparency: A Practical Method to Explain Limb Lead Configuration Following Single Lead Misplacements," Reviews in Cardiovascular Medicine **11**(1):33-8, 2010, DOI:10.3909/ricm0506.

[32] Freeman T. Bennett, MD, Kenneth R. Bennett, MD, Angel K. Markov, "MD, Einthoven's Triangle: Lead Errors and an Algorithm for Solution," The American Journal of the Medical Sciences, **329** (2), 71-77, 2005, https://doi.org/10.1097/00000441-200502000-00004

[33] Clifford, G.D, "ECG statistics, noise, artifacts, and missing data," Adv. Meth. Tools ECG Anal, 6, 55–99, 2006.

[34] Friesen, G.M., Jannett, T.C., Jadallah, M.A., et al, "A comparison of the noise sensitivity of nine QRS detection algorithms," IEEE Trans. Biomed. Eng, **37**(1), 85–98, 1990, DOI: 10.1109/10.43620

[35] Van Alsté, J., Schilder, T, "Removal of base-line wander and power-line interference from the ECG by an efficient FIR filter with a reduced number of taps," IEEE Trans. Biomed. Eng, **32**(12), 1052–1060,1985, DOI: 10.1109/TBME.1985.325514

[36] Rana A, Chakraborty C, Sharma S, Dhawan S, Pani SK, Ashraf I, "Internet of medical things-based secure and energy-efficient framework for health care," Big Data 3:X, 1–16, 2021, DOI: 10.1089/big.2021.0202

[37] Frølich, L., Dowding, I., "Removal of muscular artifacts in EEG signals: a comparison of linear decomposition methods," Brain. Inform, **5**(1),13–22, 2018, doi: 10.1007/s40708-017-0074-6

[38] P. Wagner et al., "PTB-XL, a large publicly available electrocardiography dataset," Sci. Data, 7(1), 154, 2020, doi: 10.1038/s41597-020-0495-6.

[39] M. R. Fikri, I. Soesanti, and H. A. Nugroho, "ECG Signal Classification Review," IJITEE Int. J. Inf. Technol. Electr. Eng., **5**(1), 15, 2021, doi: 10.22146/ijitee.60295.

[40] Yadav, S. K., Sinha, R., and Bora, P. K, "Electrocardiogram signal denoising using non-local wavelet transform domain filtering," IET Signal Proc. 9, 88–96, 2015, doi: 10.1049/iet-spr.2014.0005.

[41] M. Wu, Y. Lu, W. Yang, et S. Y. Wong, "A Study on Arrhythmia via ECG Signal Classification Using the Convolutional Neural Network", Front. Comput. Neurosci., **14**, 2021, DOI: 10.3389/fncom.2020.564015

[42] Awal, M. A., Mostafa, S. S., "Ahmad, M., and Rashid, M. A, "An adaptive level dependent wavelet thresholding for ECG denoising," Biocyber. Biomed. Engin. 34, 238–249, 2014, doi: 10.1016/j.bbe.2014.03.002

[43] Atal, D. K., and Singh, M, "Arrhythmia classification with ECG signals based on the optimization-enabled deep convolutional neural network", Comp. Methods Prog. Biomed. 196:105607, 2020, doi: 10.1016/j.cmpb.2020. 105607

[44] Acharya, U. R., Fujita, H., Oh, S. L., Hagiwara, Y., Tan, J. H., and Adam, M. "Application of deep convolutional neural network for automated detection of myocardial infarction using ECG signals", Inform. Sci. **415**, 190–198, 2017, doi: 10.1016/j.ins.2017.06.027.

ASTES Advances in Science, Technology and Engineering Systems Journal Vol. 8, No. 6, 19-25 (2023)

www.astesj.com

Special Issue on Innovation in Computing, Engineering Science & Technology

ASTESJ
ISSN: 2415-6698

Tree-Based Ensemble Models, Algorithms and Performance Measures for Classification

John Tsiligaridis*

Heritage University, Mathematics & Computer Science Department, Toppenish, WA, 98948 USA

ARTICLE INFO

History:
Received:15 July, 2023
Accepted:29 October, 2023
Online: 30 November, 2023

Keywords:
Decision Trees
Ensemble Models
Bagging

ABSTRACT

An ensemble method is a Machine Learning (ML) algorithm that aggregates the predictions of multiple estimators or models. The purpose of an ensemble module is to provide better predictive performance than any single contributing model. This can be achieved by producing a predictive model with reduced variance using bagging, and bias using boosting.

The Tree-Based Ensemble Models with Decision Tree (DT) as base model is the most frequently used. On the other hand, there are some individual Machine Learning algorithms that can provide more competitive predictive power to the ensemble models. It is a problem, and this issue is addressed here. This work has two parts. The first one presents a Projective Decision Tree (PA) based on purity measure. Next node criterion (CNN) is also used for node decision making. In the second part, two sets of algorithms for predictive performance are presented. The Tree-Based Ensemble model includes bagging and boosting for homogeneous learners and a set of known individual algorithms. Comparison of two sets is performed for accuracy. Furthermore, the changes of bagging and boosting ensemble performance under various hyperparameters are also investigated. The datasets used are the sonar and the Breast Cancer Wisconsin (BCWD) from UCI site. Promising results of the proposed models are accomplished.

1. Introduction

Decision Trees (DTs) are an important type of algorithm for predictive modeling machine learning. It's often used to plan and plot business and operational decisions as a visual flowchart. The approach sees a branching of decisions which end at outcomes, resulting in a tree-like structure. This paper is work extended of an original one that appeared at the ICAIIC 2023 [1].

Decision tree induction is the method of learning the decision trees from the training set. The training set consists of attributes and class labels.[2]-[4]. Ensemble method is an algorithm that aims to improve the predictive performance on a task by aggregating the predictions of multiple estimators or models. The goal of the ensemble methods is to combine the predictions of several base estimators to produce improved results. Use of an ensemble model and optimization with parameter tuning can provide higher accuracy.

An easy way to combine the predictions is the majority voting where for each base estimator is assigned an equal weight. If we have m base estimators each base estimator has weight of 1/m. The weighted predictions of the individual base estimators are combined, and the most voted class is predicted. This way the classifier with the higher accuracy is selected. The ensemble models have more abilities to generalize compared to the single DT's predictions since it provides comparable bias and smaller variance. The Tree-Based Ensemble models belong to homogenous ensemble ones and use the same base learning algorithm; the DT classifier which is sensitive to small data variations. Random Forest (RF), an ensemble of randomized DTs, is used to further promote ensemble diversity. It predicts using the majority vote of all DTs [2]-[4].

One of the DTs problems is the creation of over-complex trees with replication and repetition of subtrees that do not generalize the data well. The Projective Decision Tree Algorithm (PA) can avoid this disadvantage by selecting the partition that maximizes the purity of the split with the use of CNN. The ensemble methods [5] produce an optimal predictive model with the combination of several base models. For the creation of the ensemble models the PA is used as base model. For creating and testing the prediction, two bagging methods are generated from PA, Random Forest (PARF) and the Extra Tree (PAET) along with two boosting methods; AdaBoost (AB) and Gradient Boosting (GB). A set of

*Corresponding Author: John Tsiligaridis, Heritage University,3240 Fort Rd,Toppenish,WA98948 ,USA, tsiligaridis_j@heritage.edu

https://dx.doi.org/10.25046/aj080603

individual algorithms; the PA, the k Nearest Neighbor (kNN), and the Support Vector Machine (SVM) are included in the examination of the performance improvement with tuning methods.

SVM models are also used in medical informatics to classify persons with or without diseases and especially for diabetes categories (undiagnosed diabetes, or no diabetes) [6]. In [7] SVM is a strong tool that has been used for cancer genomic classification or subtyping. Logistic regression (LR) estimates the probability of event occurrence given a dataset of independent variables [3].

A set of tree-based ensemble models comprise Random Forest (RF) [8] and the Extra Tree (ET) [9]. Both are based on PA. Since ET trees work randomly, they are faster than RF that looks for optimal split at each node. To decrease bias, ET uses original training samples instead of bootstrap replicas. Recent applications include land cover classification using Extremely Randomized Trees [10]. Tree-Based Ensemble model is used for investment in the stock market facilitating financial decision making. The purpose of the model is to minimize the prediction error and reduce the investment risk [11]. In [12], Tree-based machine learning models predict microbial fecal contamination in beach water for public health awareness. Ensemble methods, RFs and ETsare used for sensitivity analysis of environmental models [13].

The set of individual algorithms consists of PA, the Logistic Regression (LR) [14], the k Nearest Neighbor (kNN) [15], and the Support Virtual Machine (SVM) [16]. In [17] an Ensemble Model with Random Forest (RF), AdaBoost (AB) and XGBoost is used for weather forecasting. The ensemble learning model outperforms the simple Decision Tree (DT) in either calm or stormy environment. An AdaBoost ensemble method with reduced entropy for Breast Cancer prediction is developed in [18]. For this purpose, the target column is created from weighted entropy. In [19] a new ensemble Machine Learning method based on AdaBoost is developed for placement data classification analysis. It increases performance in terms of time complexity and accuracy for the student dataset.

Tuning parameter methods are applied before proceeding with the ensemble models. The comparison of the two sets' components shows individual algorithms could have better performance than the ensemble models after parameter tuning.

The paper's organization is as follows. In section 2, performance evaluation and process description are included. Section 3 deals with the Algorithms (DT, PA, kNN and SVM). Section 4 covers the Ensemble models, PARF, PAET, AB and GB. Section 5 contains the Ensemble Performance Issues. Bagging Hyperparameters, Boosting Hyperparameter and Control Overfitting are included in Section 6,7,8 respectively. Simulation results are provided in Section 9.

2. Performance Evaluation and Process Description

To evaluate learning models' performance the cross-validation technique is used. Cross-validation provides a more robust estimate of the model's performance on unseen data, and it prevents overfitting. The data are randomly divided into k folds almost of the same size. The k-1 folds are used for training while the one-fold is selected for validation. It is a method that generally results in a less biased estimate of the model compared to the simple train/test split. The out of sample testing refers to cross-validation where the model is built on a subsection of data and then tested on data that were not used to build it. The out of sample provides us with the information on how well the model predicts results for the "unseen" data (validation set). For each individual algorithm, the hyperparameters are tuned using the grid search method. The process of this work has two phases as below:

- Preparation phase:

  Prepare: PA (purity measure with the CNN criterion), the algorithms (LR, kNN, SVM), parameters tuning (kNN, SVM), PARF, and PAET.

- Execution phase:

  Accuracy: for algorithms, and ensemble models.

The model process is led by PA (base model) which provides the DTs for RF (PARF) and for ET (PAET). The implementation starts with the PA and then follows the PARF and PAET. Details of the used algorithms are presented in the next section.

3. Algorithms

3.1. Decision Tree (DT)

Inductive inference uses specific examples to make a general conclusion. It is a widely used method for DTs learning and produces a target function with discrete output values (i.e., binary). DTs tend to overfit the training data, in case of very deep or complex tree, mainly due to replication problems. In that case, two or more copies of the same subtree can be created. These DTs fail to generalize since they provide poor performance on new, unseen data [3]. Instability can be created to the structure of the DT due to the sensitivity of the training set when a small change of data (i.e., irrelevant attribute) or noise appears [3].

3.2. Projection Algorithm (PA)

The Projection algorithm (PA) a top-down DT inducer, can create a new model by learning the relationships between the descriptive features and a target feature. In PA, the next splitting node is decided by the CNN criterion based on purity using conditional probabilities. In the splitting process the data partition is achieved so that the highest purity attribute in the new nodes is selected. The dataset splitting process continues with the creation of new subset until pure sets are acquired. CNN uses conditional probability values to define the new internal node.

There are two PA phases. The primary one is to discover the root node that has the feature with the lowest impurity.For each feature (d) the number of instances with feature value t, with target feature value k is given by :

$a_{d,t,k} = |\text{features}_d = t| \text{ U } |\text{target} = k|, \;\; b_{d,t} = \text{purity}(a_{d,t,k})$.

The $a_{d,t,k}$ stands for projection of feature d, with value t over the target feature value =k

The feature with the maximum value of purity can be found as

$c = \max_d \sum_{t=1}^{n} b_{d,t}$ where n= the number of feature values.

The second phase is for branch selection. The next node for all feature values is created by the previous node. The new node is determined by the maximum value of conditional probabilities as follows.

$$p' = p(f1_{d1} = t, f2_{d2} = t, f3_{d3} = t / f_n = s)$$

$$= p(f1_{d1} = t, f2_{d2} = t, f3_{d3} = t) / p(f_n = s)$$

$f1_{d1} = t$ means the value of feature $f1$ is t, and $f2_{d2} = t$ means the value of feature $f2$ is t.

CNN determines the next internal node according to the following p' values.

if $p' \neq 1$, next internal node is created (purity ≠1). CNN is valid.
if p'=1 terminal node is created (purity=1). CNN is not valid.
if p'=0 no internal or terminal node created

A simple version of Zoo Animal Classification is used as the dataset containing animals' properties as features, and their species as target feature.

Example 1: (Phase 1: root discovery)

The s1= {toothed (True, False), breathes (True, False), legs (True, False) and the target feature (Mammal, Reptile).

From the dataset counting the total number of instances for feature values and target feature values is as follows.

For toothed: True + mammal: 6 false + mammal: 1 true +reptile: 2 false + reptile: 2 purity (true) = 5/7, purity(false) = 2/3 tot_purity = 1.3802

For breathes: True + mammal: 6 false + mammal: 1 true +reptile: 2 false + reptile: 1 purity (true) = 6/8, purity(false) = 1/2 tot_purity = 1.25

For legs: True + mammal: 6 false + mammal: 0 true +reptile: 1 false + reptile: 3 purity (true) = 6/7, purity(false) = 3/3=1 tot_purity = 1.857.

Root will be the legs feature due to the maximum value of tot_ purity.

Example 2:

The next step after the discovery of the root node from phase 1, the conditional probabilities are estimated from the two feature values of the previous node. Assume that "toothed" will be the next node and the branch is: "legs=true".

For the branch: "legs=true".

The process computes the conditional probability for all the feature values of the branch "legs=true" having any target feature value: Mammal, Reptile.

$$p'(1) = p(f1_{d1} = t, f2_{d2} = t, f3_{d3} = t)/p(f_n = s)$$
$$= p(\text{toothed} = \text{true}, \text{breathes} = \text{true}, \text{species} = \text{mammal})/p(\text{length} = \text{true})$$
$$= (5/10) / (7/10) = 5/7$$

$p'(2) = p$ (toothed = true, breathes = false, species = mammal/ legs = true) = 0.

$p'(3) = p$ (toothed = false, breathes = true, species = mammal/ legs = true) = 1/7.

$p'(4) = p$ (toothed = false, breathes = false, species = mammal/ legs = true) = 0.

$p'(5) = p$ (toothed = false, breathes = false, species = reptile/ legs = true) = 1/7.

The sum of probability values of "legs=true" branch equals 1, with 6 mammal and 1 reptile instances. This is an intermediate node with 7 instances. The PA's counting process examines the number of instances arising with the feature values' projection over a target feature value. The database split is accomplished by each feature's values providing a new subset for the next split. This process continues to attain pure sets.

3.3. kNN

kNN is a distance-based non-parametric algorithm. It classifies objects based on their proximate neighbors' classes. The k value (hyperparameter) selected specifies the examples' number closest to the query. The tuning parameter k considers 7 neighbors from all odd values (1 to 21). The 10-fold cross validation performs evaluation of each k value on the training dataset.

3.4. SVM

In SVM, a data item is represented by a point of n-dimensional space. These points become inputs and outputs of the hyperplane. Each feature value has a certain coordinate. The hyperplane tries to ensure that the margin between the closest points of different classes should be as maximum as possible. The classification is performed discovering the hyperplane that differentiates classes. SVM's effectiveness is apparent in high dimensional cases. For the decision functions different kernel functions can be specified. The C tuning parameter has value 1 (0,…,2.0) with Radial Base Function (RBF) kernel . A grid search is used for 10-fold cross validation as with kNN.

3.5. LR

LR is often used for probability estimation of an instance to belong to a certain class. It is a linear algorithm, and it is used for binary classification, computing the cost function for each instance. This convex function is used with Gradient Descent for global minimum discovery .

4. Ensemble Models

4.1. Ensemble Methods, Bagging

Ensemble models use a combination of multiple other models for prediction that are considered as base estimators. They do better in terms of technical challenges instead of building a single estimator. Ensemble methods use a variety of aggregation techniques depending on the task, including majority vote, model averaging, weighted mean, etc.

Bagging is the most basic homogenous parallel ensemble method we can construct. As an example, for a bagging ensemble with 500 Decision Trees, each of depth 12 and trained on bootstrap samples of 300 size has accuracy of 89,9% compared to a single tree with accuracy of 83,8%.

Bagging has a smoothing behavior due to the model aggregation. In the case of many nonlinear classifiers, where each trained on a slightly different replicate of training data, and then each one might create an overfit, but the difference is that do not all overfit the same way. Hence, the aggregation leads to

smoothing which finally reduces the effect of overfitting. In this way the bagging with aggregation smooths out the errors and improves the ensemble performance.

4.2. PARF

RF, after the creation of multiple DTs, combines them to reach a single accurate and stable result. It provides a higher level of accuracy in predicting outcomes over the DTs and reduces the overfitting of datasets. The DTs created with Bagging can have a lot of structural similarities and finally high correlation in their predictions. On the contrary, the RF changes this procedure. Because of that, the sub-trees from a random sample are learned and, in this way the resulting predictions from all the subtrees have less correlation. For the RF, the bagging ensemble is used. Bagging chooses random sample with replacement from the entire training dataset. PA is applied to each dataset. DTs are created to fit each training set.

PARF is based on PA. Attributes are discovered randomly by bagging from the training set which PA uses to create DTs. To this end, PA works iteratively with the different random subsets. CNN criterion performs splitting operation to produce internal nodes repeatedly up to pure leaves. In this way, for each randomly selected feature, CNN discovers the most appropriate cut-point.

Generalization should be more successful by using ensemble's predictions instead of single PA's predictions. With the training of all the predictors the ensemble model will be able to predict a new instance with better accuracy using aggregation. According to the majority vote, the final choice will be the outcome of the most DTs.

4.3. PAET

The ET is similar to RF because of a random attribute selection but ET uses the whole dataset. For node splitting, the cut-points are randomly selected with the use of random thresholds for each feature. In the RFs, it is time consuming to grow a tree due to the fact that the best possible threshold needs to be found for each feature and for every node. On the contrary, the ETs are considerably faster for a training dataset because the splitting is selected randomly for each feature. In some cases, the obtained PAET results are better than the RFs' ones. The DTs are generated using PA with random splitting. The CNN criterion for purity is applied. ET reduces bias because the sampling refers to the entire dataset and the various data subsets might cause varying bias. Also, it reduces the variance resulted by the random node splitting in DT.

4.4. AB

AB is a boosting technique that aims at combining multiple weak classifiers to build a strong one. Weak learners in AB, named decision stumps, are DTs with a single split. AB puts more weight on hard to classify instances and less weight on the ones operating well. The stumps are produced for every feature iteratively and are stored in a list until a lower error is received. Weight assignment to each training example determines its significance in the training dataset. Weight update with a formula, at each iteration provides the stumps' performance. The AB trains predictors sequentially as happens in most boosting methods, where each predictor tries to correct its predecessor [15]. A major plus for both AB and boosting is that they seem to be very robust against overfitting. AB can be combined with other learning algorithms for performance improvement.

4.5. GB

Another boosting method is GB. This is an alternative to weights on training examples to convey the misclassification using the loss function based on residual (or negative loss gradients). It uses the residual errors to measure the amount of misclassification and define which training examples should be tested in the next iteration. Training examples correctly classified will have small gradients. GB consists of an additive model, a loss function and a weak learner.

5. Ensemble Performance Issues

An ensemble is a ML model that incorporates multiple model predictions. Ensemble learning methods are not always the most appropriate techniques to use or the best methods to use.

The bias and the variance of a model's performance are connected. We have a trade-off of bias and variance, and it is not hard to get a method with extremely low bias rather than high variance or vice versa. The use of hyperparameters can change the high bias or high variance [15] for some models and provide regularization (regularization by hyperparameters). In most cases, ensemble models provide a method to decrease the prediction variance. This reduction of variance provides improved predictive performance [16]. Since bagging tends to reduce variance, it provides an approach to regularization (regularization via bagging). This happens because although each learned classifier from $f_1, f_2, ..., f_m$ is overfit on its own, may also be overfit to other various things. By voting, it can largely avoid overfitting. Bagging reduces variance and minimizes overfitting.

Bagging does not always offer an improvement. In models with low variances that perform well, the bagging can result in degrading the performance. The bagged decision trees are effective since each of them can fit on a different training dataset, which in turn allows to have less differences and, in this way, they make slightly different useful predictions. Bagging with DTs is effective because the trees have low correlation between predictions which means low prediction errors. The randomness used in the model construction can provide a slightly different model by running the same data. Working with bagging using randomness (stochastic learning algorithms) one technique is to evaluate them by averaging their performance with multiple runs or repeat cross-validation method. The latter technique is preferred in our experiments.

6. Bagging Hyperparameters

Bagging and random forest belong to homogenous parallel ensemble methods because they use the learning algorithm on the same dataset. Adaboost and GBoost, LightGBM, XGBoost belong to sequential ensemble learning algorithms.

The main difference between parallel and sequential ensembles is that the base estimators in parallel ensembles can be usually trained independently while for the sequential ensembles, the base estimator in the current iteration depends on the base estimator of the previous one. There are important points related

to the ensemble performance. The ensemble size, the base learner complexity and the learning rate are the most critical.

a. The ensemble size can be measured by the number of estimators. Three algorithms are used: the bagging with decision trees based on PA(PABAG), the PARF and PAET. The test errors can inform how well they do with the future data which is the generalization.

b. The base learner complexity is considered for the base decision trees, and it can be controlled by the maximum number of leaf nodes. The same three algorithms as previously are used as well.

7. Boosting Hyperparameter

The learning rate is another hyperparameter that is used to control the rate of the model learning to avoid overfitting. It shows how fast the model learns. It is time consuming, but it can control how quickly the complexity of the ensemble grows. Apart from avoiding overfitting it also offers generalization after training. The lower the learning rate the slower the model learns which means that the model becomes more robust and generalized.

However, it is possible for the weak learners to increase the tree depth in a sequential ensembles' methods, as boosting, to have a stronger classifier and the improvement of the performance. But to have an arbitrarily increment is not possible because there is the overfit during the training which in turn decreases the performance. A control mechanism is needed to prevent that.

8. Control Overfitting

Generally, increasing the complexity of the base learners it will make more difficult to reduce the variability of the ensemble. The complexity of the ensemble is increasing with the number of the base estimators which basically leads to overfitting. To avoid this bad situation, it is possible to stop the training process before it reaches the limit of ensemble size. This can be applied to the gradient boosted decision trees. The XGBoost is used to provide an efficient implementation of the gradient boosting algorithm. The early stopping decreases the training time, and this can be achieved by using fewer base estimators.

9. Simulation

The experiments are as follows.

9.1. Experiments

For the first 3 tests, various experiments with sonar dataset [20] are used with PA, PARF, PAET, and GB for classification. Through discretization continuous attributes are transformed to categorical ones by first providing the number of categories and then mapping their values to them. This facilitates split points creation for PA. Depiction with box plot diagrams is a streamlined way of summarizing the distribution of groups of data.

- In Figure 1 boosting with AB and default configuration shows higher accuracy compared to PARF, PAET, and GB ensemble methods.
- In Figure 2 kNN with low variance surpasses PA, SVM, and LR individual algorithms.
- In Figure 3 SVM using polynomial kernel offers slightly higher accuracy than ensemble method.

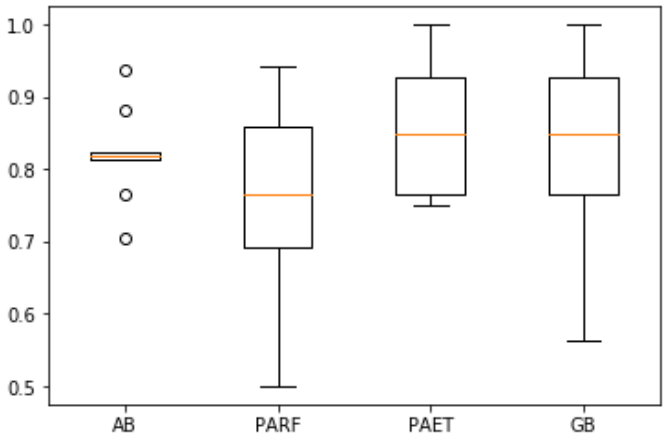


Figure 1: Ensemble algorithms' performance

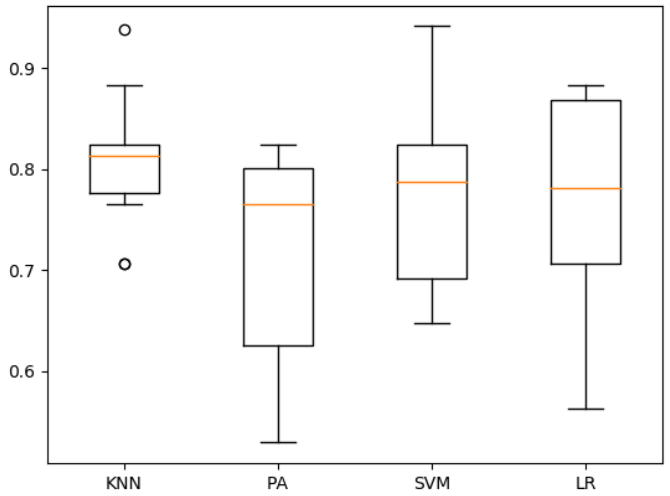


Figure 2: Algorithms performance

- In Figure 4 the size of estimators is examined for the ensemble performance (Figure 4). Three models are used in the experiment: PABAG, PARF, PAET. The Breast Cancer Wisconsin dataset (BCWD) from UCI site is used. The accuracy of each method over various numbers of estimators using a 10-fold cross validation is examined. All methods tend to perform similarly and yield high accuracies for over 10 estimators.
- In Figure 5 for the base estimator (decision tree), which is common for the three models, the tree depth is the most important measure of complexity since deeper trees are more complex. In Figure 5 the complexity of the models against the performance using the depth of the base decision trees is examined. Again here, a 10-fold cross validation shows average performance values in all tested methods over various maximum depths. All three methods tend to yield high accuracy values over all chosen depths but all of them obtain their best accuracies at a depth equal to 8. In general, we see that PABAG tends to yield larger accuracies over all other methods for various depths.
- In Figure 6 learning rate using XGBoost (boosting algorithm) for defining the appropriate rate for the performance. Cross Validation is used to set the learning rate. The XGBoost degrades the performance as the boosting process exhibits the

overfitting behavior. From Figure 6 the value of 1.2 or any value between 1.0 and 1.5 could be appropriate.

- In figure 7 control technique to stop the training with XGBoost. The accuracy is improving while the XGBoost continues training. When there is not any improvement of accuracy XGBoost terminates the training. In this way, the process terminates in a round which will be less than the predefined number of iterations. The training stops when the accuracy has better value after the next five rounds, From Figure 7 it is the 32 rounds when the training stops since the next five values are less than the one of 32 round (0.993449).

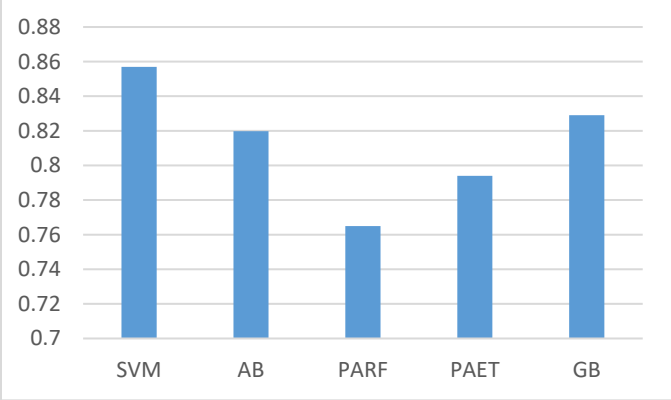


Figure 3: Accuracy with SVM and ensemble models

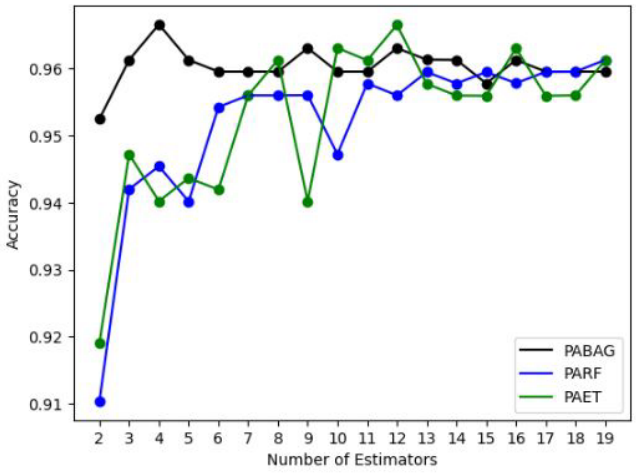


Figure 4: Performance vs Size of Estimators

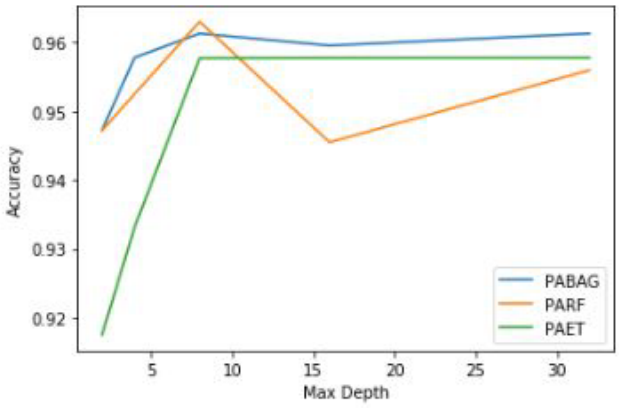


Figure 5: Accuracy vs Depth of trees in Ensemble

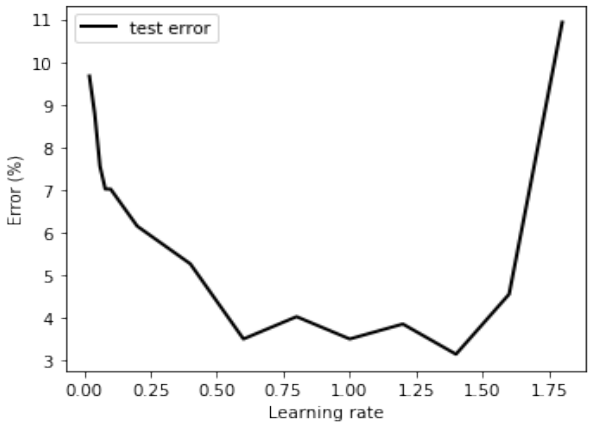


Figure 6: Learning rate discovery

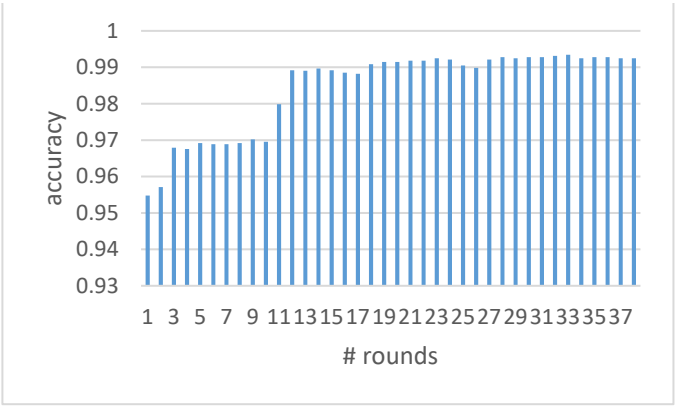


Figure 7: Accuracy vs # of rounds

10. Conclusion

Tree-based ensembles are considered state-of-the-art. The augmentation of the prediction power using individual algorithms or tree-ensemble models and their internal composition is an open issue. For this purpose, PA has been developed as the base model for the proposed ensemble since it avoids the replication problem of DTs by using the CNN criterion.

Ensemble learning helps improve overall accuracy by combining the results from several models. These models are known as weak learners trained to solve the same problem while their combination leads to more accurate and robust models. The kNN surpasses PA, SVM and LR. AB outperforms PARF, PAET, and GB. The SVM with the polynomial kernel exceeds even the ensemble models. Higher accuracy is achieved by an appropriate algorithm rather than ensemble models.

From the comparison of the two sets of algorithms the selection of models with their hyperparameters for creating an ensemble model could be an issue if other algorithms with their tuning parameters can provide good performance. The ensemble size and the depth of the trees affect the performance of the model. For boosting ensemble, the best learning rate with the use of XGBoost allows a good training strategy for the creation of the appropriate model. A reactive approach for terminating the training time by enforcing early stopping is also achieved.

Future work could be based on the stacking of heterogenous ensemble models.

References

[1] J. Tsiligaridis, "Tree-Based Ensemble Models and Algorithms for Classification", in 2023 International Conference on Artificial Intelligence in Information and Communication (ICAIC 2023), 103-106, 2023, doi: 10.1109/ICAIIC57133.2023.10067006

[2] J. Han, M. Kamber, J. Pei, "Data Mining Concepts and Techniques",Morgan Kaufman, 2012

[3] M.Karntardzic,"Data Mining: Concepts, Models, Methods, and Algorithms", IEEE Press, 2003.

[4] L. Rokach, O. Maimon, "Data Mining with Decision Trees". World Scientific , 2008

[5] I. Nti, A. Adekoya, B. Weyon, "A comprehensive evaluation of ensemble learning for stock-market prediction" , Journal of Big Data , **7**(1), 1-40, 2020, doi: 10.1186/s40537-020-00299-5

[6] W. Yu, T. Liu, R. Valdez, M. Gwinn, M. Khoury, " Application of support vector machine modeling for predictiion of common diseases: the case of diabetes and pre-diabetes", BMC Medical Informatics and Decision Making, 10(1): 16, 2010, doi: 10.1186/1472-6947-10-16

[7] S. Huang, N. Cai, P. Pacheco, S. Narandes, Y. Wang, W. Xu, "Applications of Support Vector Machines (SVM) Learning in Cancer Genomics", Cancer Genomics&Proteomics,Journal, **15**(1), 41-51, 2018, doi: 10.21873/cgp.20063

[8] R. Couronne, P. Probst, A. Boulesteix, "Random Forest versus Logistic Regression: a large-scale benchmark experiment", BMC Bioinformatics, **19**, 270, 2018, doi: 10.1186/s12859-018-2264-5

[9] E.K. Ampomah, Z. Qin, G. Nyame, "Evaluation of tree-based Ensemble Machine Learning Models in predicting Stock Price Direction of Movement", Information Journal, MDPI, **11**(6), 332, 2020, doi:10.3390/info11060332

[10] A. Zafari, R. Zurita-Milla, E. Izquierdo-Verdiguier, "Land Cover Classification Using Extremely Randomized Trees: A Kernel Perpective" IEEE Geoscience and Remote Sensing Letters, **17**(10),1702-1706, 2020, doi: 10.1109/LGRS.2019.2953778.

[11] L. Li, J. Qiao, G. Yu, L. Wang, H. Li, C. Liao, Z. Zhu, "Interpretable tree-based ensemble model for predicting beach water qaulity", Water Research, 211, 118078, 2022, doi:10.1016/j.watres.2022.118078

[12] M. Jaxa-Rozen, J. Kwakkel, "Tree-based ensemble methods for sensitivity analysis of environmental models: A performanced comparison with Sobol and Morris technique", Science Direct, **107**, 245-266, 2018 doi:10.1016/j.envsoft.2018.06.011

[13] P.Han, M.Steinbach, A. Karpatne, V. Kumar, "Introduction to data Mining",Pearson, 2019

[14] A. Geron, "Hands On Machine Learning with Scikit-Learn & Tensorflow",O'REILLY,2017

[15] J.Gareth, D. Witten, T. Hastie, R. Tibshirani, ".An Introduction to Statistical Learning with Applications in R", Springer, 2017

[16] L.Rokach,"Ensemble Learning: "Patern Classification Using Ensemble Methods", World Scientific, 2009

[17] R. Natras, B.Soja, M. Schmidt, " Ensemble Machine Learning of Random Forest, AdaBoost, and XGBost for Vertical Total Electron Content Forecasting ", Remote Sensing, MDPI, **14**(15), 3547, 2022 doi:10.3390/rs14153547

[18] M.Ramakrisna,V.Venkatesan,I Izonin, M.Havryliuk, C.Bhat, "Homogenous Adaboost Endemble Machine Learning Algorithms with Reduced Entropy on Balanced Data", Entropy, MDPI, 25, 245,2023, doi:10.3390/e25020245

[19] B. Kalaiselvi, S. Geetha, "Ensemble Machine Learning AdaBoost with NBtree for Placement Data Analysis", in 2nd International Conference on Intelligent Technology (CONIT) , 1-4 , 2022, doi: 10.1109/CONIT55038.2022.9847993

[20] Sonar dataset: http://archive.ics.uci.edu/ml/datasets/connectionist+bench+(sonar,+mines+vs.+rocks)

Advances in Science, Technology and Engineering Systems Journal Vol. 8, No. 6, 26-36 (2023)

www.astesj.com

Special Issue on Innovation in Computing, Engineering Science & Technology

ASTESJ

ISSN: 2415-6698

Social Media Text Summarization: A Survey Towards a Transformer-based System Design

Afrodite Papagiannopoulou*, Chrissanthi Angeli

School of Engineering, University of West Attica, Athens, 122 43, Greece

ARTICLE INFO

Article history:
Received:19 September, 2023
Accepted:13 November, 2023
Online: 30 November, 2023

Keywords:
Social Media Summarization
Natural Language Generation
Neural Networks
Transformers

ABSTRACT

Daily life is characterized by a great explosion of abundance of information available on the internet and social media. Smart technology has radically changed our lives, giving a leading role to social media for communication, advertising, information and exchange of opinions. Managing this huge amount of data by humans is an almost impossible task. Adequacy of summarizing texts is therefore urgently needed, in order to offer people knowledge and information avoiding time-consuming procedures. Various text summarization techniques are already widely used. Artificial intelligence techniques for automated text summarization are a major undertaking. Due to the recent development of neural networks and deep learning models like Transformers, we can create more efficient summaries. This paper reviews text summarisation approaches on social media and introduces our approach towards a summarization system using transformers.

1. Introduction

Today's abundance of information on the Internet and social media makes it imperative to create summaries to keep readers informed in an accurate and timely manner. Social media posts are based on events. When an event breaks out, a huge amount of posts flood social media platforms. These posts can be documents, articles, discussions and conversations on different topics and events, that are time-consuming to read. Therefore, text summarization is essential for retrieving useful knowledge in a reasonable amount of time.

We can proceed summarization in two ways: a) writing a summary manually, which is time-consuming, b) writing algorithms and performing artificial intelligence techniques, which requires much less time. This method is called Automatic Summarization, whose aim is to create a shorter text of the original document, without losing its meaning intact [1,2]

Many algorithms have been applied to generate text summaries. We can consider two main classes of algorithms: Pre-neural, that do not make use neural networks and b) Deep Learning or Machine Learning techniques that make use of neural networks. The later have been successfully applied to various NLP tasks, yielded excellent results, and have been extensively used in recent years [3]. Various deep learning models have been used, mainly based on both recurrent neural networks (RNN) and convolutional neural networks (CNN). These models have proven highly satisfactory in predicting complex relationships that simple structured or semantic approaches cannot do alone [4]. In recent years, the use of Transfer leaning and Transformer models has gained popularity mainly in the field of Natural Language Understanding, Processing and Generation [5].

1.1 Text Summarization Methods

The aim of text summarization is to convert a large text document into a shorter one by preserving the critical information and ensuring the meaning of the text. Due to large amounts of data available on social media, it is almost impossible for anyone to read all the comments generated by the users under a post. It is therefore necessary to properly code and program machines so that they can create coherent summaries just like humans. The process of text summarization done by machines or artificial intelligence programs is known as "Automatic Text Summarization". Automatic text summarization is the process of generating a text summary which, using artificial intelligence techniques and deep learning algorithms, is based on the original text while preserving the information content and overall meaning [1, 6]. Automatic text summarization presents some challenges: First, appropriate information must be selected from the original document so that the summary preserves the meaning of the document. Second, the output text must be fluid and coherent and also expressed in a way that is direct and understandable to the

*Corresponding Author: Afrodite Papagiannopoulou, apapagiannop@uniwa.gr

reader [2]. We recognize two main categories of text summarization:

- *Extractive summarization* extracts important words and phrases from the original text, uses them as they are and, gathering them together, with a slight rearrangement, generates the summary. [1].
- *Abstractive summarization* abstracts the meaning of the original text and, using paraphrasing, creates a new shorter text which looks completely different but essentially has the same meaning as the original text [1].

1.2 Importance of Social Media Summarization.

The role of social media is becoming increasingly important, especially in public life, as posts and comments made by users are important in shaping public opinion on various issues. These topics refer to economics, politics, entertainment, education, psychology and society. Social media data excels at extracting sentiment and patterns of social behaviour that can be used for social research, economic and political decision-making. So creating summaries seems vital. There is a lot of information flooding the internet and most of it is redundant or repetitive resulting in confusion for readers. For this reason, a mechanism is needed to select the necessary information to provide correct, fast and accurate information.

Recent years have shown that abstractive summarization has achieved great results in the field of document summarization by producing more human-like summaries. Unlike formal documents, online conversations and web communication present three great challenges: 1) tend to be informal, consisting of slang expressions and special characters, 2) show deviations from the original theme and dependencies on previous opinions and, 3) since they are short, they lack lexical richness.

It is important to emphasize that, in the field of social media summarization, few research works [7, 8, 9] have demonstrated transformer-based social media abstractive text summarization systems. Our system aims to optimize the results achieved so far in two main points. First, we focus on creating coherent and meaningful summaries of user comments since they present greater specificity, in terms of: a) the nature of the language, b) their conceptual grouping and c) their dynamic upgrading. Second, unlike other research works that consider only two social media platforms, Reddit and Twitter, our goal is to explore how different data sets and training models can be applied to more social media platforms.

This paper is a survey of social media summarization techniques and approaches as well as a presentation of our work toward a system that generates summaries of user comments on social media posts using transformers. The rest of the paper is organized as follows: Section 2 is a literature review of the research that has been carried out so far in the field of text summarization. Section 3 illustrates the importance of transformers against previous deep learning methods and gives a basic description of transformer model architecture. Section 4 depicts the motivation and design of our system and compares 3 pre-trained transformer models based on a selected dataset. Section 5 shows the results of the comparison between 3 pre-trained model pipelines and Section 6 contains concluding remarks and our future work.

2. Literature review

In the field of Automated Text Summarization on Social Media, several attempts have been made by researchers as seen in Table 1. APPENDIX I. We have grouped them in two main categories: 1) Pre-neural approaches that do not use neural networks and 2) Deep learning approaches that use neural networks. A further division of deep learning approaches has been done, based on transformer architecture, into the following three categories:1) *Social media summarization systems that do not use Transformer architecture,* 2) *Transformer-based Social media summaries* and 3) *Transformer-based projects that do not generate social media summaries.* Finally, recent trends on large language models (LLMs) lead us to prompt engineering that give a new perspective to the fields of text generation and summarization. A more detailed presentation follows:

2.1 Pre-neural approaches

In the early stages of natural language research, summarizing web posts, microblogs, and social networks researchers used probabilistic and optimization methods to generate a summary from different types of data such as text, videos, images, hashtags and so on. In some cases the summary is not only text but a multimedia representation.

A typical example of multimedia representation is the model proposed by [10] & [11]. This model takes as input real-time user interaction in the social media stream and provides a multimedia representation as output. The summarization process takes minimal linguistic information into account. The output is a multimedia representation combining photos, video and some text. The algorithm uses an optimization process under a score-based input to find the topic of greatest importance. Specifically, for each Multimedia Social Network (MuSN), they use graph-based modeling and influence analysis methodologies to identify the most important media objects related to one or more topics of interest. Then a media summary is extracted from a list of candidate objects. This is achieved with the help of heuristic models based on the following properties: Priority, Continuity, Variety and Non-Repeatability. This project does not follow one of the text summary models, either extractive or abstract, because it does not create a text summary.

A second example of multimedia summarization is the model proposed by [12] which is a framework for generating a visualized summary from microblogs with multiple media types. The main goal of this work is to separate the different parts of an event published on social media by creating sub-events. Then for each secondary event it creates a clear and precise summary. Thus a fragmentary summary is produced. Each microblog is taken as a separate information mining unit, so a microblog digest is considered a multi-document digest (MDS). MDS faces two challenges: 1) Word limit and 2) Unstructured social media content. The proposed framework consists of 3 stages: 1) Noise removal in which the authors apply a filtering model to clean data that calculates the probability that the data is irrelevant. 2) Sub-event extraction where the authors propose a multi-media probabilistic model, called Cross-Media-LDA (CMLDA), which explores the associations between the different media types of the published event or separates the sub-events. 3) Creation summary. An algorithm is implemented to identify representative microblog texts considering three criteria: vagueness, importance and

diversity. Based on these criteria, the summarizing ability is also measured. The important point of this work is that the knowledge acquired in the previous stages is used, thereby reinforcing each other for the proper functioning of both the textual and visual summarizing mechanisms.

Another research work that considers each post as a separate text is the work of [13] & [14]. This model generates a summary using Twitter posts by performing a search on the Twitter API based on trending topics. It automatically generates an abstract based on multiple papers published on the same topic by applying a Phrase Reinforcement (PR) algorithm by adding the TF-IDF technique to it. The algorithm performs the following steps: 1) finds a specific phrase of each document that matches the topic. This is done on the one hand because users often use the same word or phrase to describe an event that usually matches the title of the event and on the other hand because very often the most relevant post is "retweeted". 2) Based on this phrase it starts asking Twitter.com to retrieve related posts, 3) filters posts based on related content. The longest sentence from each post is isolated. The collected sentences become the input to the PR algorithm, 4) creates a graph with a common root node representing the topic sentence. Next to the root node there are other nodes, the word nodes and the word count nodes that show how many times the word appears in the sentence, 5) the PR algorithm searches for the path with the highest word frequency (count) starting from the root node to the final. Following this path the words are combined and an initial summary is produced. The algorithm iterates using the partial summary each time as the root node and reconstructs the graph, arriving at the final summary.

In the work [15] the authors create a model that aims to summarize tweets that have sports as their topic. The key point in their research is finding real-time events, which is of particular importance in repetitive and real-time events such as sports. The design of the model includes two stages: 1) Application of the modified Hidden Markov Model according to which the timeline of events is segmented, based on the tweet-stream and the distribution of the words used in the tweets. Each part is a separate "sub-event" of different importance. 2) Selection of tweets that can provide information about the section that was considered most important.

A framework that searches for categories of topics on Twitter and then generates summaries of tweets corresponding to that topic is presented in [16]. To determine the topic categories to use in summarization, the time sequence of the tweet event is taken into account. An important factor is the detection of tweets written at the same time for an underlying event to extract important data. To this end they apply two topic models: the Decomposition Topic Model (DTM) and the Gaussian Topic Model (GDTM) that exploit the temporal correlation between tweets under predicted conditions to produce a concise and information-rich summary of events.

2.2 Deep Learning Models

Since deep learning algorithms require a ton of data to learn from, this increase in data generation is one reason deep learning capabilities have grown in recent years. Additionally, deep learning algorithms benefit from the most powerful computing power available today, as well as the proliferation of Artificial Intelligence (AI) as a Service. Deep Learning has achieved significant success in various fields, such as computer vision and natural language processing. In the following paragraphs we present models that make use of neural networks to generate summaries. Various deep learning models have been employed, including Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs) and RNNs with Long-Short Term Memory (LSTM). In addition, recent years have seen the emergence of new techniques in abstractive summarization, such as those based on transformers. The specificity of these techniques lies in the use of an attention mechanism and not a recurrent or convolutional neural network.

The idea of transformers was first introduced in the paper "Attention is All You Need" [5] where transformers achieved state-of-the-art results for translation tasks over previous NLP models. The idea has been extended to all NLP tasks and many researchers have adopted transformer models to build their own applications. The social media summarization field is in the early stages of research. Referring to the literature we distinguish, so far, the following aspects:

- *Social media summarization systems that do not use Transformer architecture*.

The authors of the paper [17] introduce a project which summarizes social media posts by incorporating user comments in order to capture the reader focus. They use a model named reader-aware summary generator (RASG). Their model is based on a sequence to sequence framework rather than transformer architecture to generate abstractive summaries. It consists of 4 main parts: 1) Sequence-to-sequence summary generator, 2) an attention module which captures the reader's focus, 3) a supervisor module that matches the semantic gap between the generated summary and the reader's focus and 4) a goal tracker that defines the goal of each generation step. Specifically, the seq2seq architecture with an attention mechanism is used to generate summaries. First, words from user comments are correlated with those in the document. This correlation is then calculated because it is considered an important indicator of the "reader-centered aspect". At the decoding layer, attention weights are defined as the "decoder focused aspect" of the produced summary. Finally, a supervisor calculates the deviation of the "reader-centered view" and "decoder-centered view" with the goal of reducing the deviation.

Another attempt of text summarization that is related to social media posts and customer reviews is presented in [18]. The main idea is the use of a Sequence-To-Sequence Model with Attention approach to produce abstractive text summarization with no use of transformers. It is based on bidirectional RNN with attention layer on input data. The model uses also LSTM as encoder and decoder to build summaries. LSTM encoders partly extract a fixed length of sequence of the input and LSTM decoder generates a translation of this sequence. With the attention layer in this architecture the decoder is allowed to have more direct access to the input sequence.

The authors of [19] proposed a summary-aware attention model that aims to generate abstractive text summarization in social media. This mechanism helps the decoder to make the right decision. The authors have based this novel proposal on two important limitations that have been faced on previous models: 1)

the original text is not structured, like social network texts, making the decoder's task difficult, and 2) the calculation of attention weight does not take into account the summary information created in previous layers, which negatively affects the consistency of the summary. To overcome the above limitations, a new model of attention computation is proposed, called "summary-aware attention" mechanism for abstractive summary generation. According to this, attention is calculated at each level, taking into account the data of the previous level.

The work of [20] generates an abstractive text summary on social media, in Turkish. The data is collected and the Word2Vec model is used to preserve the meaning of the text, which is a very important factor for generating summaries. The GRU (Gated Recurrent Unit) neural network is then applied to divide user posts into positive and negative. Finally, using the Latent Semantic Analysis (LSA) method, a summary text in Turkish is generated from user comments on Twitter. The LSA algorithm accepts as input the content of a text and reveals the hidden semantic relationship between terms and sentences of that text.

The model of [21] produces an abstract digest of social media text based on Attentional Encoder-Decoder recurrent neural networks. The model is based on the encoder-decoder architecture by enhancing it with an additional hidden layer before the encoder unit. In this layer it is decided which information is useful and which should be removed. In this way, invalid information is better filtered in the encoder unit and through the reinforcement learning policy, better results are achieved. More specifically, this work meets the following three main contributions: (i) They have applied to summarization, the attentional RNN encoder-decoder originally developed for machine translation, showing that it already outperforms technology systems in two different English corpora. (ii) Since the model that is already used for machine translation addresses specific problems when applied in summarization model, the authors propose new models and show how additional performance is improved. (iii) Finally, they introduce a new dataset for the multi-sentence abstract summation task and establish benchmarks. The authors also propose a variety of selective gating methods to better filter the information while preserving the meaning of the original text.

- *Transformer-based Social media summaries*.

An abstractive Event Summarization on Twitter [8] framework uses a pre-trained BERT-based model as an encoder and a not pre-trained transformer model as a decoder. An event topic prediction component helps the decoder to focus on more specific aspects of posts. The most liked comments are used to produce more coherent summaries. The framework consists of the following features: 1) a mechanism that selects the most important tweets to be used by the decoder that is implemented in the following steps: a) tweets are selected based on their timestamp in ascending order. b) After the initial selection, in order to determine their importance, each tweet will be compared to each of those already selected. Selection is based on how representative and informative a tweet is. This gives the summary precision and coherence. 2) a mechanism that predicts the thematic category of the event. Topic information is used by the decoder to generate different summary styles from different events, thereby focusing on very specific aspects of topics. 3) A BERT model as encoder, to better exploit the grammatical and semantic information of tokens pre-trained model and Transformer-based model as decoder. 4) two separate optimizers to smoothly integrate the pre-trained BERT model and the untrained transformer.

A new model is introduced in [22] which generates summaries of each text posted on a Chinese web platform. The model combines BERT, reinforcement learning and other technologies. Their work based on LCSTS, a dataset constructed from a Chinese social media platform named "Sina Weibo".

What is highlighted in [9] is the importance of summarizing user feedback. In their paper, they propose a multi-document text summarization scenario that includes meaningful comment detection, extending previous single-document approaches. They use BERT as the encoder and the transformer-based model as the decoder and produce an abstract summary of the embedded news discussions. This architecture is extended with an attention encoding level that is fed with user preferences. Attention encoding focuses on comments with the highest social impact. Consequently, the model summarizes the most relevant aspects of a discussion gathered from a news article. To encourage the model to pay attention to important comments, they introduce a data-driven strategy that focuses the model on those comments. The key element of this research is that to summarize the discussion there is the approach of many works by many authors. This has the consequence that users are considered co-authors of the original news story, to which they can add new information. Comments are rated as important based on user preferences.

A Transformer-based abstractive summarization is presented in [7] which creates summaries in three languages from posts and comment pools. The datasets are from Reddit and Twitter. The authors fine-tune T5 and LongFormer, test them against BART, and consecutively test them to pools of comments. In addition, they apply enlarged Transformer-based models on Twitter data in three languages (English, German, and French) to discover the performance of these models on data with non-English text. The main part of this work is the comparison of open source models for social media summarization. Three stages are applied: 1) Performance is optimized and one of three models is selected: LongFormer, Bart and T5. 2) The selected model is tested on pools of comments from Reddit and evaluated based on the similarity of posts and comment summaries. 3) The models are also applied to Twitter data in three languages (English, German and French). This study concludes that using transformer-based models, such as LongFormer and T5, give better results in generating summaries on social networks.

In [23] model for extractive summarization with transformers is introduced. This system summarizes a single web document by exploiting relevant information of social media to enhance the document summarization. The intuition behind this model is that they make use of relevant user posts and transformers to enrich the sentences of the output summary. They stack a Convolutional Neural Network (CNN) on the top of transformers (BERT) for classification.

- *Transformer-based projects that do not generate social media summaries.*

In [24] a two-stage transformer-based approach is proposed to generate abstractive summaries from articles in Chinese. The model produces fluent and variable length abstractive

summarization according to the user's demands. It consists of two modules: text segmentation module and two-stage transformer-based module. A pre-trained BERT model and a bidirectional LSTM are used first to divide the input text into segments. Subsequently the extractive based BERTSUM model is constructed in order to extract the most important information of the segments. Then, collaborative training is used to train the two-stage Transformer-based model. The training process begins with the document Transformer in the second stage. The input of the document Transformer is the outputs of the extractive model and the output of the document Transformer is the headline summary.

An abstractive summarization system of meeting conversations using transformers is presented in [25]. The system takes as input human dialogues and by applying the classic Transformer model summarizes the dialogues.

In their work [26] compare three pre-trained transformer-based models in an attempt to produce abstractive summarization of news articles on web. The pre-trained models used in this project are BART, PEGASUS and T5. When the transformer-based pre-trained language models are fine-tuned they give satisfactory results and fluent summaries. After evaluating each model with ROUGE the T5 model outperformed all other models.

Authors of [27] use dataset from Wikihow knowledge base and then deploy bidirectional encoder representations from transformers (BERT) and text-to-text transfer transformer (T5) models in order to produce abstractive summaries of the articles and then use the ROUGE scores to assess the performance of the two models and compare them.

2.3 Prompt Engineering

In the field of natural language processing (NLP), Prompt Engineering has emerged as one of the most innovative and powerful techniques for improving the performance and adaptability of language models. This recent technique has its roots in the development of LLMs whose history dates back to the 1950s, but until the introduction of BERT and GPT models in 2018, LLMs had the main role in NLP tasks. These models still use complex algorithms and massive amounts of training data to understand natural language. Their ability to learn patterns and structures in language has proven invaluable in various NLP tasks. However, due to the significant time and computational resources required to train these models, researchers have turned to prompt engineering. By designing and configuring the appropriate prompts, which can be shaped to improve behaviour and results of these models to achieve specific tasks. These tasks involve extracting information, summarizing text, answering questions, generating code, and classifying text. The detailed reference to this technique is beyond the purposes of this work, as in the current phase of our project we will use transformer models as presented in the following paragraphs.

3. Transformer models and methodology

3.1 Transformers and Model Explanation

Transformer models are a new development in machine learning and neural networks based on transfer learning. The Transformer model was first proposed in the paper "Attention Is All You Need." [5]. These models can handle the context of a text exceptionally well forming a state-of-the-art architecture in various NLP tasks such as translation, text generation, summarization, question-answering, classification and sentiment analysis. Transformer models are significant because:

- They have given exceptional results in many natural language tasks that use sequential data.
- Unlike recurrent neural networks (RNNs), they support parallelization and, they have replaced repetition with attention. Therefore calculations can be done simultaneously.
- Their architecture allows for the creation of better-quality models because they can handle better long distance dependencies. Based entirely on the attention mechanism, they solve the problem of Recurrent Neural Networks with Long-Short Term Memory (LSTM) and CNNs, which is mainly the inability to model larger sequences without data loss.

The architecture of the transformer model inspires from the attention mechanism used in the encoder-decoder architecture in RNNs to handle sequence-to-sequence (seq2seq) tasks. Unlike RNNs the transformer eliminates the factor of sequentiality meaning that, it does not process data in sequence which allows for more parallelization and reduces training time. The transformer works as encoder-decoder architecture because it is composed of two large building blocks: an encoder and a decoder. As we can see in (Figure1) the encoder is on the left and the decoder is on the right. Both encoder and decoder can consist of a stack of Nx identical layers (in original paper Nx = 6). Since the model does not contain any recurrence or convolution, it adds a positional encoding layer at the bottom of the encoder and decoder stacks to take advantage of the order of the sequence. Each layer mainly consists of Multi-Head Attention and feed forward layers. Inputs and outputs are first integrated in an n-dimensional space [5].

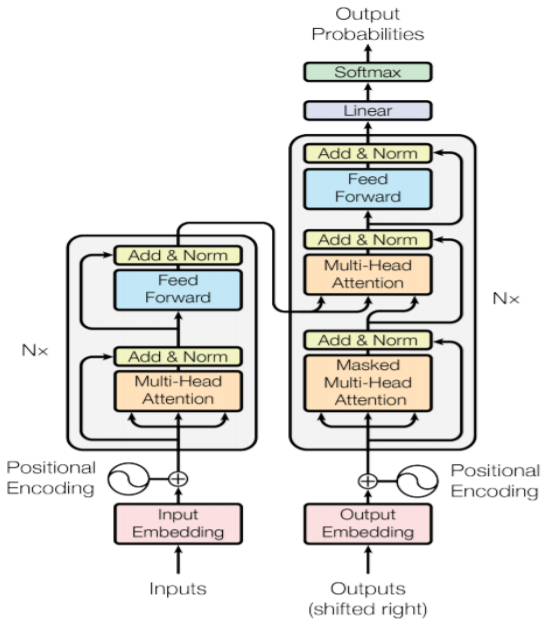


Figure. 1: Transformer Model Architecture

Encoder: The encoder is comprised of two major components: a multi-head attention (self-attention) mechanism which is followed by normalization and a feed-forward neural network.

- Inputs: Since transformers, as any other model, do not understand natural language, the input text is tokenized and processed to convert every word into a unique numeric id.
- Embedding layer: In the embedding layer the transformer uses learned embeddings to transform the input tokens into vectors of dimension d = 512.
- Positional encoding: A positional encoding is a fixed-size vector representation that provides the transformer model with information about where the words are in the input sequence, since there is no use of any recurrence or convolution.
- Multi-head Attention and Self-Attention: Self-attention is a mechanism that captures the contextual relationship between the words of a sentence. Based on a scale dot-product attention, it creates a vector of every input word. The main role of this vector is to understand how relevant every word in the input sentence is, with respect to other words in the sentence. Since self-attention is not only applied once, but also several times (in the original paper it is applied 8 times), is called multi-head attention. The objective is to generate several attention-based vectors for the same word. This helps the model to have different representations of the words' relations in a sentence. The different attention-based matrices generated by the multiple heads are summed and passed through a linear layer to reduce the size to a single matrix.

Decoder: The decoder side has a lot of shared components with the encoder side. The decoder takes in two inputs: (a) the output of the encoder and the output text shifted to the right. Then it applies multi-head attention twice with one of them being "masked". The final linear layer in the decoder has the same size of words as the target dictionary. Each unit will be assigned a score. The softmax function is applied to convert the scores into probabilities indicating the probability of each word to be present in the output.

4 Systems design

4.1 Motivation

Automatic Text Summarization in both formal documents (such as articles and books) and Social Media texts are grouped into two main categories: Extractive and Abstractive summarization. Initially, researchers focused on creating summaries using the extractive summarization method. According to this technique, the summarizer extracts important words or sentences from the original document. In order not to lose its meaning it uses statistical and linguistic methods. It then rearranges slightly these words and phrase, to produce the output summary. This technique, while simple to apply, does not produce satisfactory results, as the summary is not coherent and accurate. This effect is enhanced when the length of the sentence starts to grow.

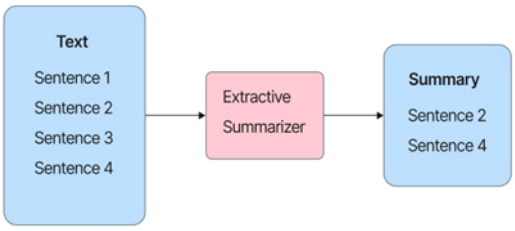


Figure 2: Extractive Text Summarization

In recent years, researchers have turned to the abstractive summarization technique. In this technique the summarizer extracts the meaning of the original document and the output document is produced without losing this meaning. This process adopts the way the human mind produces summaries and despite its complexity, it tends to give better results. All of the research papers that applied the Abstractive Summarization technique used deep neural network methods and attention mechanisms to train their models, adopting the way the human mind might be trained to summarize documents.

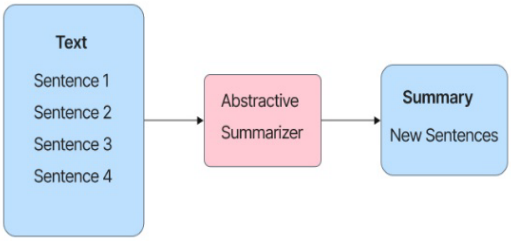


Figure 3: Abstractive Text Summarization

The area of social media summarization is in its early stages and remains challenging due to the particularity of social media content. As already mentioned in the literature review, various models, based either on pre-neural or deep learning techniques, have been proposed giving interesting results, but also facing several limitations. Transformer-based neural networks try to overcome these limitations giving state-of-the-art results. The perspective of our work concerns the following areas:

- Transformer-based models.
- Abstractive summarization techniques
- The discussions of users under the post

4.2 Methodology

As we have mentioned earlier Social Media posts and user comments provide great challenges on text summarization: 1) tend to be informal, consisting of slang expressions and special characters, 2) show deviations from the original theme and dependencies on previous opinions and, 3) since they are short, they lack lexical richness, 4) due to the massive amount of comments generated under each post, many of them are repetitive. It is therefore considered necessary to use data pre-processing techniques in order to improve the performance of the model. The original idea of our approach is to use the pre-trained transformer models. For a correct decision we fed with data 3 pre-trained pipelines of T5, BART and PEGASUS models comparing the generated summaries (Figure. 4). All three of the aforementioned pre-trained models generate abstract summaries and use the

encoder-decoder transformer architecture that performs best in text generation tasks. Our model uses a Facebook dataset of news posts and their corresponding comments and consists of the following steps:

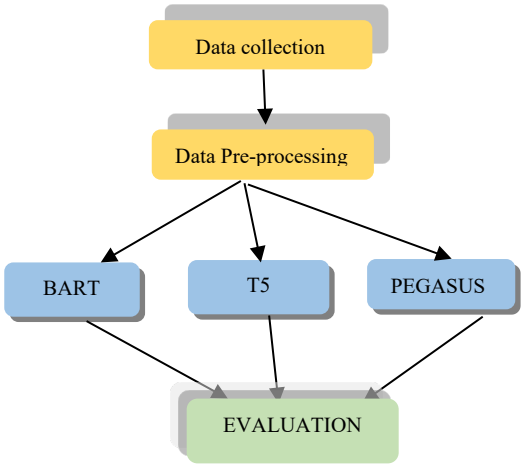


Figure. 4: Pre-trained model evaluation

- Data collection and pre-processing using Python libraries.
- Feed this text into the transformer-based encoder.
- Clustering and attention rendering based on the topics.
- Feed this encoding to the Transformer decoder and
- Produce the summary text

4.3 Data Collection and pre-processing

Finding the right datasets from social media is a really complex task. Especially for data that will be used for summary. Several social media platforms are limited in receiving data, and in those that are open, the data must be reformatted to meet the needs of the project. The dataset we are looking at for this project is Facebook news posts accompanied by user comments below each post. The raw data has 7 columns, namely 'created_time', 'from_id', 'from_name', 'message', 'post_name', 'post_title', 'post_num' and 1,781,576 rows. The dataframe consists of the 3 columns: 'message', 'post_title', 'post_num' where the 'post_title' as well as the 'post_num' identify a specific post while the 'message column represents the user comments under the post. We focused on creating summaries of user comments, as they are more discrete in terms of (a) the nature of the language and (b) their conceptual grouping. After downloading the dataset and reshaping it in a meaningful way for summary generation, the first step is to apply some basic pre-processing before building the model. Using impure and unclean data does not lead to issuing the desired results. Hence in this step, using python packages NLTK and regex, we have removed punctuation, special characters, emoji and link threads, as long as NULL values. The second step is to perform data clustering according to the topic of the discussion. Since we on the first stages of our ongoing research work we need to decide which of the pre-trained models can be better trained and fine-tuned based on our dataset. Therefore, the cleaned and classified data is first fed to the pre-trained-models and the results of the comparison are extracted.

4.4 Pre-trained Transformer models and pipelines

Today excellent results have been achieved in all tasks thanks to the wide variety of pre-trained transformer models available. Pre-trained language models have been trained on large-scale datasets and due to their capabilities and recourses can be reused even with small amount of datasets. PTLMs are differentiated based on their architectures and pre-training tasks. In order to make a correct choice of the appropriate model for a particular task on a particular dataset, knowledge of these details is crucial. For example, BERT is better suited for task understanding than task generation. Furthermore, another differentiation of pre-trained models is their architecture. There are many models whose architectural backbone is Transformers, but some of which pre-train only the encoder, such as BERT and UniLM, while others pre-train only the decoder, such as GPT. Therefore, PTLMs must be chosen wisely based on these details when adapting them to downstream tasks. Based on the above, in order to proceed with the correct model selection, we have set the following criteria:

- Both input and output of the system are text
- The output will be abstractive summary generation, which means that we chose the models that produce abstractive summaries and are based on the Encoder-Decoder architecture [28].
- All the pre-trained models can fine-tuned on our target task according to the limitations of our datasets.

The HuggingFace hub [29], acts as an open source library and provides a huge number of pre-trained models as well as datasets, on a wide range of different NLP tasks. These models can be used to predict a summary and then accurately fit any data set. Due to the large number of models available in Hugging Face, it is quite difficult to decide which one to use as the best one for our dataset in order to produce the desired results. Pipelines are a fast, easy and efficient way to use different pre-trained models and can be applied to many NLP tasks. The pipelines meeting the above criteria are BART, T5 and PEGASUS and are presented thoroughly below:

- BART – stands for Bidirectional and Auto-Regressive Transformers [30]. BART supports tasks involving Natural Language Creation, such as the summarizing task, which requires new text to be generated to summarize a large input text, unlike the traditional summarizing task that extracts some parts of the input text to make the summary. It combines the pre-training processes of BERT and GPT within the encoder-decoder architecture (Figure 5). Input sequences undergo one of many possible transformations,

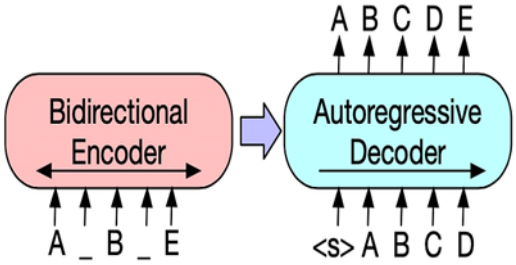


Figure 5: BART (source original paper)

from simple masking to model sentence permutation, token deletion, and document rotation. These modified inputs are passed through the encoder and the decoder must reconstruct the original texts. This makes the model more flexible, as it can be used for NLU as well as NLG tasks, and achieves top performance in both. BART pre-training involves 2 steps: a) the input text is free of unnecessary noise, which may change the length of the text. b) the seq2seq model learns to reconstruct the original text from the corrupted text. BART is known for its excellent performance in tasks that require complex language handling, such as text summarization and machine translation. BART's pre-training task encourages the model to learn representations that are robust to noise and variations in the input text. This makes BART suitable for tasks that require handling text that is noisy, ambiguous, or written in different languages. It has a more complex architecture, which makes it more suitable for tasks that require handling large sequences of text or that require text generation.

- T5 - stands for "Text-to-Text Transfer Transformer" [31]. The T5 model is a task-agnostic model meaning that unifies all NLU and NLG tasks by converting them into text-to-text tasks, such as Translation, Language Inference, Information extraction and Summarization. All tasks are framed as sequence-to-sequence tasks, where adopting encoder-decoder architecture is natural thus it's capable of

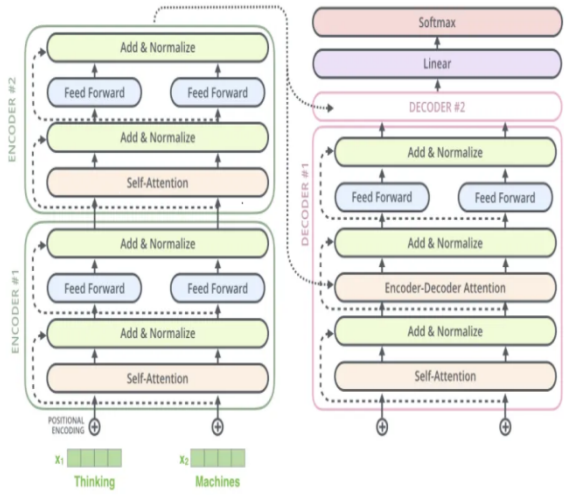


Figure 6: T5 model (source original paper)

handling architecture uses the original Transformer architecture different sequence lengths for input and output. The T5 using the large crawled C4 dataset, the model is pre-trained with masked language modelling as well as the SuperGLUE tasks by translating all of them to text-to-text tasks. The largest model with 11 billion parameters yielded state-of-the-art results on 17 of the 24 tasks tested. It achieved high scores on Corpus of Linguistic Acceptability (CoLA), Recognizing Textual Entailment (RTE) and Natural Language Inference on WNLI tasks. It also achieved very high performance on the SQuAD dataset but less satisfactorily on the CNN/Daily Mail abstractive summarization task. The pre-training process involves two types of training: supervised and self-supervised. During supervised training, downstream tasks from the GLUE and SuperGLUE benchmarks are used and tasks, as explained before. On the other hand, self-supervised training is done using corrupted tokens. This converted into text-to-text is achieved by randomly removing 15% of the tokens and replacing them with individual sentinel tokens.The encoder takes the corrupted sentence as input, while the decoder takes the original sentence as input. The target is then the dropped-out tokens, delimited by their sentinel tokens.

- *PEGASUS* – stands for Pre-training with Extracted Gap-sentences for Abstractive Summarization Sequence-to-sequence models [32]. It is also based on the Transformer architecture but with some modifications for abstractive text summarization. It is a task-specific architecture where every component in pre-training closely maps text summarization. PEGASUS uses a gap-sentence generation task, where whole encoder input sentences are replaced by a second mask token and fed to the decoder, but which has a causal mask to hide the future words like a regular auto-regressive transformer decoder. It is designed explicitly for abstractive text summarization, where it generates summaries that have the same meaning but different phrases from the source text. The model is pre-trained on CNN/DailyMail dataset, which consists of large volumes of articles. The pre-training objective, Gap Sentence Generation (GSG), is designed to have a well performance on text summarization and text generation tasks and is not used in other domains. It is adaptable and can be fine-tuned on limited data, achieving human performance.

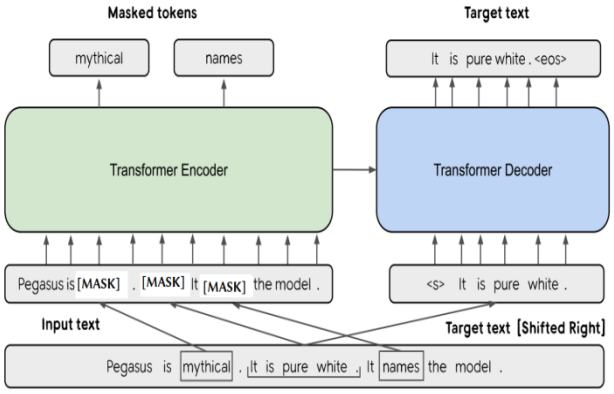


Figure 7: PEGASUS model (source original paper)

5 Results

Measuring performance in a text generation task is not as easy as in other domains such as sentiment analysis or named entity recognition. It is very important to use the appropriate evaluation metrics to illustrate the best performance of the models. To measure the performance of our own work we used one of the most well-known NLP job evaluation mechanisms, ROUGE. ROUGE stands for “Recall-Oriented Understudy for Gisting Evaluation” and evaluates the similarity between a candidate document and a collection of reference documents. The use of the

ROUGE score to evaluate the quality of document translation and summarization models [33]. There are variations of ROUGE metrics such as ROUGE-N, ROUGE-L and ROUGE-Lsum where the N in ROUGE-N stands for the numbers 1 and 2. More specifically, ROUGE-1 compares the monograms between the machine-generated summaries and the human reference digest, ROUGE-2 uses digrams instead of monograms, while ROUGE-L does not compare n-grams, instead treating each digest as a sequence of words and then searching for the greatest common subsequence (LCS). These measures, by comparing the ground truth and the generated text, automatically determine the quality of a generated summary. The number of overlapping n-grams, word sequences, and word pairs between the generated text and the ground truth are used for the metrics. In this work we use ROUGE-1, ROUGE-2, ROUGE-L and ROUGE-Lsum. In Table 2 we show the results of the comparison between 3 pre-trained model pipelines, T5, BART and PEGASUS, on asample text of Facebook news posts and comments. As we have already mentioned above, the use of these particular three models was made because all of them meet the following constraints: they based on Transformers with the Encoder-Decoder architecture and they produce abstractive summarization. T5 pipelines give better results than BART and PEGASUS. We are led to the conclusion that by applying this model to our own data we will produce more accurate summaries. Moreover, T5 is a modern model that has already been successfully used in summarization studies, but in the field of social media it is less explored. This is an initial estimate for our own model design, but by enriching our study with additional assumptions to optimize the results the pre-trained models will be re-evaluated for their performance.

Table 2: Evaluation and Comparison of ROUGE scores

Models	Evaluation Metrics			
	ROUGE-1	*ROUGE-2*	*ROUGE-L*	*ROUGE-Lsum*
T5	0.585034	0.524138	0.544218	0.585034
BART	0.529032	0.483660	0.516129	0.529032
PEGASUS	0.365079	0.306452	0.349206	0.349206

6 Conclusions and future work

The constant increase in the volume of information on social media makes the summarization of texts decisive and necessary to save users' time and resources. Social media is event based. When an event occurs, social networks are flooded with posts related to the event as well as user comments under each post. Since the volume of published data is growing dynamically, reading all these posts in a reasonable time is almost impossible for anyone. Summarizing your social media feed posts is important to keep your readers informed correctly, accurately and in a timely manner. On the other hand, another important issue is the summary of user comments and sub-comments under each post. As their number increases, reading them is a time-consuming and difficult process. User comments are important to read because they express the public's opinion on an important topic. For this reason creating a summary of the comments is of utmost importance. Social media is a challenging area because it offers different types of information, but also because online discussions and chat threads are not formal. They usually contain slang expressions, special symbols such as hashtags or emoticons. Generating summaries from user comments is a difficult task, since they confront language informality and lack lexical richness. Additionally, there is one main question: “How many and which comments will the summary model consider”. Comments are updated dynamically. Working with the most liked, is not an option, as it has been observed that comments readers pay attention to, are the initial comments on the list, finding it tedious to go even deeper. In this paper the overall literature of social media text summarization was reviewed. The result of this literature review shows that various technologies can be used to develop social media summarization models. However, each technology is implemented under different assumptions and constraints. Research around social media text summarization and, in particular, those involving abstractive summarization, are based mainly on Neural Network models. In light of these models, our approach focuses on developing an abstractive, Transformer-based summarization system. The field of text summarization in social media, especially with Transformer models, is still underexplored for both posts and user comments. We focused on creating summaries of user comments since they present greater specificity both in terms of the nature of the language and in terms of their conceptual grouping. In particular, we took user comments on facebook posts and after pre-processing we used them as input to pre-trained language models, based on transformer encoder-decoder architecture. We used ROUGE metrics to compare 3 different pre-trained models and we concluded that T5 gives the highest performance, leading us to the conclusion that T5 will be applied better to our dataset. We proceeded to cluster the data so that T5 can be fed and fine-tuned with the desired text to be summarized. Certainly this is an initial consideration in the design of our model. Through our research we learned about several state-of-the-art models that use a transformer architecture for text summarization. Despite adopting the transformer architecture, these models differ in pre-training strategies and results. Choosing the most appropriate model is necessary, considering the size and training data set of the model. For future work we consider optimizing the results and generating summaries by fine-tuning or prompt-tuning the models to achieve even better outputs. Collecting and classifying datasets from various social media platforms is a difficult task thus our intention is to check the performance of multiple datasets. Since this is an on-going research process we will be able to present more detailed results shortly.

Conflict of Interest

The authors declare no conflict of interest.

Acknowledgment

The publication fees were totally covered by ELKE at the University of West Attica.

References

[1] A. Nenkova, K. McKeown, “A survey of text summarization techniques”, Springer US: 43–76, 2012, doi:10.1007/978-1-4614-3223-4_3.

[2] V. Varma, L.J. Kurisinkel, P. Radhakrishnan, “Social Media Summarization”, In A practical Guide to Sentiment Analysis, Chapter 7, 135-153. 2017.

[3] D. Suleiman, A. Awajan, "Deep Learning Based Abstractive Text Summarization: Approaches, Datasets, Evaluation Measures, and Challenges," Mathematical Problems in Engineering, **2020**, 2020, doi:10.1155/2020/9365340.

[4] V. Gupta, G.S. Lehal, "A Survey of Text Summarization Extractive techniques," in Journal of Emerging Technologies in Web Intelligence, 258–268, 2010, doi:10.4304/jetwi.2.3.258-268.

[5] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A.N. Gomez, L. Kaiser, I. Polosukhin, "Attention Is All You Need,". In 31st Conference on Neural Information Processing Systems (NIPS 2017), Long Beach, CA, USA., June 2017.

[6] S. Haque, Z. Eberhart, A. Bansal, C. McMillan, "Semantic Similarity Metrics for Evaluating Source Code Summarization," in IEEE International Conference on Program Comprehension, IEEE Computer Society: 36–47, 2022.

[7] I.S. Blekanov, N. Tarasov, S.S. Bodrunova, "Transformer-Based Abstractive Summarization for Reddit and Twitter: Single Posts vs. Comment Pools in Three Languages," Future Internet, **14**(3), 2022, doi:10.3390/fi14030069.

[8] Q. Li, Q. Zhang, "Abstractive Event Summarization on Twitter," in The Web Conference 2020 - Companion of the World Wide Web Conference, WWW 2020, Association for Computing Machinery: 22–23, 2020, doi:10.1145/3366424.3382678.

[9] I.T. Palma, M. Mendoza, E. Milios, "Neural Abstractive Unsupervised Summarization of Online News Discussions". In: Arai, K. (eds) Intelligent Systems and Applications. IntelliSys 2021. Lecture Notes in Networks and Systems, vol 295. Springer, Cham 2021.

[10] F. Amato, F. Moscato, V. Moscato, A. Picariello, G. Sperli', "Summarizing social media content for multimedia stories creation". The 27th Italian Symposium on Advanced Database Systems (SEB 2019).

[11] F. Amato, A. Castiglione, F. Mercorio, M. Mezzanzanica, V. Moscato, A. Picariello, G. Sperlì, "Multimedia story creation on social networks," Future Generation Computer Systems, **86**, 412–420, 2018, doi:10.1016/j.future.2018.04.006.

[12] J. Bian, Y. Yang, H. Zhang, T.S. Chua, "Multimedia summarization for social events in microblog stream," IEEE Transactions on Multimedia, **17**(2), 216–228, 2015, doi:10.1109/TMM.2014.2384912.

[13] J. Kalita, B. Sharifi, M.-A. Hutton, "Summarizing Microblogs Automatically". Association for Computational Linguistics, Human Language Technologies: The 2010 Annual Conference of the North American Chapter of the ACL, pages 685-688, 2010.

[14] B. Sharifi, D. Inouye, J.K. Kalita, "Summarization of Twitter Microblogs". *The Computer Journal*, Volume 57, Issue 3, March 2014, Pages 378–402, https://doi.org/10.1093/comjnl/bxt109

[15] D. Chakrabarti, K. Punera, "Event Summarization Using Tweets". Proceedings of the International AAAI Conference on Web and Social Media, 5(1), 66-73. https://doi.org/10.1609/icwsm.v5i1.14138. 2011

[16] F. Chong, T. Chua, S. Asur, "Automatic Summarization of Events From Social Media". Proceedings of the International AAAI Conference on Web and Social Media, **7**(1), 81-90. https://doi.org/10.1609/icwsm.v7i1.14394, 2021.

[17] S. Gao, X. Chen, P. Li, Z. Ren, L. Bing, D. Zhao, R. Yan, "Abstractive Text Summarization by Incorporating Reader Comments". In The Thirty-Third AAAI Conference on Artificial Intelligence (AAAI-19), 2019.

[18] P. Bhandarkar, K.T. Thomas, "Text Summarization Using Combination of Sequence-To-Sequence Model with Attention Approach", Springer Science and Business Media Deutschland GmbH: 283–293, 2023, doi:10.1007/978-981-19-3035-5_22.

[19] Q. Wang, J. Ren, "Summary-aware attention for social media short text abstractive summarization," Neurocomputing, **425**, 290–299, 2021, doi:10.1016/j.neucom.2020.04.136.

[20] A. Varol, "Innovative Technologies for Digital Transformation". In the 1st International Informatics and Software Engineering Conference (IISEC-2019) proceedings book : 6-7 November 2019, Ankara/Turkey.

[21] Z. Liang, J. Du, C. Li, "Abstractive social media text summarization using selective reinforced Seq2Seq attention model," Neurocomputing, **410**, 432–440, 2020, doi:10.1016/j.neucom.2020.04.137.

[22] Z. Kerui, H. Haichao, L. Yuxia, "Automatic text summarization on social media," in ACM International Conference Proceeding Series, Association for Computing Machinery, 2020, doi:10.1145/3440084.3441182.

[23] M.T. Nguyen, V.C. Nguyen, H.T. Vu, V.H. Nguyen, "Transformer-based Summarization by Exploiting Social Information," in Proceedings - 2020 12th International Conference on Knowledge and Systems Engineering, KSE 2020, Institute of Electrical and Electronics Engineers Inc.: 25–30, 2020, doi:10.1109/KSE50997.2020.9287388.

[24] M.H. Su, C.H. Wu, H.T. Cheng, "A Two-Stage Transformer-Based Approach for Variable-Length Abstractive Summarization," IEEE/ACM Transactions on Audio Speech and Language Processing, **28**, 2061–2072, 2020, doi:10.1109/TASLP.2020.3006731.

[25] D. Singhal, K. Khatter, A. Tejaswini, R. Jayashree, "Abstractive Summarization of Meeting Conversations," in 2020 IEEE International Conference for Innovation in Technology, INOCON 2020, Institute of Electrical and Electronics Engineers Inc., 2020, doi:10.1109/INOCON50539.2020.9298305.

[26] A. Gupta, D. Chugh, R. Katarya, "Automated News Summarization Using Transformers.", In Sustainable Advanced Computing, 2022, Volume 840. ISBN : 978-981-16-9011-2, 2022

[27] A. Pal, L. Fan, V. Igodifo, Text Summarization using BERT and T5. https://anjali001.github.io/Project_Report.pdf

[28] K. Pipalia, R. Bhadja, M. Shukla, "Comparative analysis of different transformer based architectures used in sentiment analysis," in Proceedings of the 2020 9th International Conference on System Modeling and Advancement in Research Trends, SMART 2020, Institute of Electrical and Electronics Engineers Inc.: 411–415, 2020, doi:10.1109/SMART50582.2020.9337081.

[29] T. Wolf, L. Debut, V. Sanh, J. Chaumond, C. Delangue, A. Moi, P. Cistac, T. Rault, R. Louf, M. Funtowicz, J. Davison, S. Shleifer, P. von Platen, C. Ma, Y. Jernite, J. Plu, C. Xu, T. Le Scao, S. Gugger, M. Drame, Q. Lhoest, A.M. Rush, "HuggingFace's Transformers: State-of-the-art Natural Language Processing," 2019.

[30] M. Lewis, Y. Liu, N. Goyal, M. Ghazvininejad, A. Mohamed, O. Levy, V. Stoyanov, L. Zettlemoyer, "BART: Denoising Sequence-to-Sequence Pre-training for Natural Language Generation, Translation, and Comprehension," 2019.

[31] C. Raffel, N. Shazeer, A. Roberts, K. Lee, S. Narang, M. Matena, Y. Zhou, W. Li, P.J. Liu, "Exploring the Limits of Transfer Learning with a Unified Text-to-Text Transformer," 2019.

[32] J. Zhang, Y. Zhao, M. Saleh, P.J. Liu, "PEGASUS: Pre-training with Extracted Gap-sentences for Abstractive Summarization," 2019.

[33] C.-Y. Lin, "ROUGE: A Package for Automatic Evaluation of Summaries". In Text Summarization Branches Out, pages 74–81, Barcelona, Spain. Association for Computational Linguistics, 2004

APPENDIX I

Table 1: Methods and Summarization Techniques on Social Media

Author	Summarization Technique	Implementation Method	Pre-neural Approaches	Deep-Learning Approaches		
				RNN/CNN	Transformer-based	Social Media
[10]	Summarization Graph with multimedia output	Influence Maximization and ABC algorithms	V	X	X	V
[11]	Summarization Graph with multimedia output	Influence Maximization and ABC algorithms	V	X	X	V
[12]	Extractive Summarization	A cross-media probabilistic model, termed Cross-Media-LDA (CMLDA),	V	X	X	V
[13] & [14]	Extractive Summarization	Phrase Reinforcement Algorithm & TF-IDF algorithm	V	X	X	V
[15]	Extractive Summarization	A modified Hidden Markov Model	V	X	X	V
[16]	Extractive Summarization	Gaussian Decay Topic Model (GDTM)	V	X	X	V
[17]	Abstractive Summarization	Reader-aware model based on CNN and Bi-RNN with Seq2Seq **(No Transformer)**	X	V	X	V
[18]	Abstractive Summarization	Sequence-to-Sequence with Attention Approach **(No Transformer)**	X	V	X	V
[21]	Abstractive Summarization	Selective Reinforced Sequence-To-Sequence Attention Model **(No Transformer)**	X	V	X	V
[19]	Abstractive Summarization	Summary-aware attention neural model **(No Transformer)**	X	V	X	V
[20]	Abstractive Summarization	Word2Vec with Recurrent Neural Network model GRU **(No Transformer)**	X	V	X	V
[8]	Abstractive Summarization	NNs with BERT model as the encoder and Transformer architecture as the decoder	X	X	V	V
[22]	Extractive Summarization	BERT, reinforcement learning and other technologies	X	X	V	V
[9]	Abstractive Summarization	NNs with BERT model as the encoder and Transformer architecture as the decoder	X	X	V	V
[7]	Abstractive Summarization	Transformer-based NNS LongFormer Large and T5 Large	X	X	V	V
[23]	Extractive Summarization	BERT with use of CNN	X	X	V	V
[24]	Extractive Summarization	Pre-trained BERT, RNN/LSTM, BERTSUM	X	X	V	X
[25]	Abstractive Summarization	Classic Transformer Model	X	X	V	X
[26]	Abstractive Summarization	Pre-trained Transformer Models BART, PEGASUS, T5	X	X	V	X
[27]	Abstractive Summarization	BERT, T5	X	X	V	X

ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 8, No. 6, 37-45 (2023)

www.astesj.com

Special Issue on Innovation in Computing, Engineering Science & Technology

ASTESJ

ISSN: 2415-6698

Infrastructure-as-a-Service Ontology for Consumer-Centric Assessment

Thepparit Banditwattanawong[1], Masawee Masdisornchote[*,2]

[1]*Department of Computer Science, Kasetsart University, Krung Thep Maha Nakhon, 10900, Thailand*

[2]*School of Information Technology, Sripatum University, Krung Thep Maha Nakhon, 10900, Thailand*

ARTICLE INFO

Article history:
Received:07 September, 2023
Accepted:09 November, 2023
Online: 30 November, 2023

Keywords:
Cloud computing
Infrastructure-as-a-Service (IaaS)
Knowledge engineering
Ontology
Taxonomy

ABSTRACT

In the context of adopting cloud Infrastructure-as-a-Service (IaaS), prospective consumers need to consider a wide array of both business and technical factors associated with the service. The development of an intelligent tool to aid in the assessment of IaaS offerings is highly desirable. However, the creation of such a tool requires a robust foundation of domain knowledge. Thus, the focus of this paper is to introduce an ontology specifically designed to characterize IaaSs from the consumer's perspective, enabling informed decision-making. The ontology additionally serves two purposes of other relevant parties besides the consumers. Firstly, it empowers IaaS providers to better tailor their services to align with consumer expectations, thereby enhancing their competitiveness. Additionally, IaaS partners can play a pivotal role in supporting both consumers and providers by understanding the protocol outlined in the ontology that governs interactions between the two parties. By applying principles of ontological engineering, this study meticulously examined the various topics related to IaaS as delineated in existing cloud taxonomies. These topics were subsequently transformed into a standardized representation and seamlessly integrated through a binary integration approach. This process resulted in the creation of a comprehensive and cohesive ontology that maintains semantic consistency. Leveraging Protégé, this study successfully constructed the resultant ontology, comprising a total of 340 distinct classes. The study evaluated the syntactic, semantic, and practical aspects of the ontology against a worldwide prominent IaaS. The results showed that the proposed ontology was syntactically and semantically consistent. Furthermore, the ontology successfully enabled not only the assessment of a real leading IaaS but also queries to support automation tool development.

1. Introduction

In the process of cloud adoption, there are three parties involved [1]. First, cloud service customers need to assess potential services to determine the best fit for their business and technical requirements. Presently there are numerous Infrastructure as a Service (IaaS) options available across multiple providers. This makes it challenging for potential IaaS customers to assess the different options and make optimal decisions about cloud adoption and/or migration. Second, cloud service providers strive to deliver cloud services that fully satisfy customers' expectations. However, these expectations remain partially unknown due to the lack of comprehensive checklists. This hinders the readiness improvement of offered IaaSs. Finally, cloud service partners facilitate the activities of both customers and providers based on mutually agreed-upon protocols between both IaaS customers and providers. Unfortunately, such protocols are currently lacking.

One promising solution to address these problems is to enhance the comprehension of customers' concerns and service judgment criteria via the introduction of an IaaS knowledge base that is understandable by all parties. As such, the contributions of this paper are twofold.

- Firstly, this paper proposes a semantic model, an ontology, that facilitates the decision making of IaaS adoption. The ontology is constructed from a consumer perspective and potentially serves as a foundational knowledge base for the development of various IaaS assessment tools, such as score-based comparing systems, recommendation systems, and expert systems.

[*]Corresponding Author: Masawee Masdisornchote, masawee.ma@spu.ac.th

- Secondly, this paper demonstrates an innovative approach to constructing this ontology by leveraging existing IaaS taxonomies. This approach not only extends benefits to researchers but also to industry practitioners. For instance, it can serve as a launchpad for further research and development concerning Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS) ontologies, thus fostering advancement in the field as a whole.

The paper is organized as follows. Next section reviews related ontologies and their limitations in addressing our research problem. Section 3 describes the systematic formulation of a proposed ontology using the ontology engineering principle. Section 4 evaluates the practicality of the ontology with real-world IaaSs. The paper concludes in Section 5, summarizing our key findings.

2. Related Work

Aiming to facilitate cloud customers as our work, the author in [2] recently proposed a KPI-based framework for evaluating and ranking IaaSs, PaaSs, and SaaSs to help cloud users identify cloud services that best suit their needs. However, the framework consists of only 41 KPIs, lacking several practical details for effective decision making. The framework has not been evaluated using real cloud service data. In [3], the authors proposed a recommender system using quality of cloud services for selecting cloud services that satisfied end user requirements. However, the quality of service (QoS) attributes were rather limited: response time, availability, throughput, dependability, reliability, price, and reputation. The authors in [4] proposed a signature-based QoS performance discovery algorithm to select IaaS. The algorithm leveraged the combination of service trial experiences and IaaS signatures. Each signature represented a provider's long-term performance behavior for a service over a fixed period. Similarities between users' service trial experiences and IaaS signatures were measured to select proper IaaSs. Nevertheless, the algorithm merely focused on a performance aspect. In [5], the authors proposed an IaaS selection algorithm based on utility functions and deployment knowledge base, which stored application execution histories. Unfortunately, the authors provided no details about the knowledge base's abstraction structure to be evaluated for its IaaS aspect coverage.

Cloud computing ontologies that encompass IaaS concepts, which particularly represented decision-making factors in cloud service adoption, are limited as follows. As many clouds vendors and standards employed inconsistent terminology to define their services, a common ontology in [6] was proposed to provide an approach to discover and use services in cloud federations. The ontology enables applications to negotiate cloud services as requested by users. Although the ontology included IaaS related terms such as some resources and specific services, it fell short of encompassing the complete spectrum of IaaS-related aspects essential for a comprehensive customer-oriented IaaS ontology. An ontology in [7] was proposed to implement intelligent service discovery and management systems for searching and retrieving appropriate cloud services in an accurate and quick manner. The ontology consisted of cloud computing concepts in general including some IaaS related ones such as compute, network, and storage services. Nevertheless, it remained incomplete as an IaaS ontology in its entirety. The authors in [8] proposed an ontology to define functional and non-functional concepts, attributes and relations of infrastructure services and used it to implement a cloud recommendation system. The ontology was composed of detailed services, compute, network, and storage, totally 26 classes. So, the ontology left several additional IaaS facets unaddressed. Several years later, the authors in [9] improved the ontology in [8] by adding 11 classes of price and quality-of-service concepts. The ontology was evaluated by being deployed in the development of semantic data sets sourced from Azure and Google Cloud services.

In summary, the IaaS concepts in aforementioned ontologies are only parts of our proposed ontology, which is more comprehensive by incorporating numerous customer-perspective IaaS taxonomies. Our preliminary work [10] is significantly extended in this paper to incorporate more recent taxonomies as follows. The authors in [11] extended [8] to derive the taxonomy of interoperability in IaaS cloud. The taxonomy's main topics were access mechanism, virtual appliance, network, and service level agreement (SLA). In [12], the author proposed the taxonomy of IaaS services where its main topics were Hardware as a Service (HaaS), which provisions hardware resources, and Infrastructure Services as a Service (ISaaS), which provided a set of auxiliary services to enable successful HaaS provision. The authors in [13] proposed a cloud computing services taxonomy including main topics: main service category, license type, intended user group, payment system, formal agreement, security measures, and standardization efforts. In [14], the authors proposed the taxonomy of fundamental IaaS components consisting of main topics: support layer, management layer, security layer, and control layer. In [15], the authors proposed a comprehensive taxonomy of cloud pricing consisting of three pricing strategies (i.e., value-based pricing, market-based pricing, and cost-based pricing) and nine pricing categories (e.g., retail-based pricing and utility-based pricing). The authors in [16] proposed a SLA taxonomy for PaaS and SaaS besides IaaS.

Furthermore, this paper resolves all conflicts and redundancy among the taxonomies and merges them by using a binary approach, which is more natural but less automated than an identified tabular list previously introduced in [17]. In addition, this paper transforms the integrated taxonomies into a unified ontology in order to allow wider applicability.

3. Ontology Formulation

This section presents the formulation of our proposed ontology based on the principle of ontology engineering [18]. The formulation process entails four steps: taxonomy reuse, refinement, formalization, and evaluation.

3.1. Taxonomy Reuse

A taxonomy serves as a structured arrangement of pertinent topics and subtopics designed for classification purposes. This study conducted a thorough examination of existing IaaS-related taxonomies. The period from 2009 to 2011 marked a significant juncture for cloud computing when Gartner Inc. positioned it at the zenith of the emerging technology hype cycle, garnering worldwide attention. Consequently, our focus was directed exclusively towards taxonomies created after 2009, as they began to gain widespread conceptual clarity and recognition during this

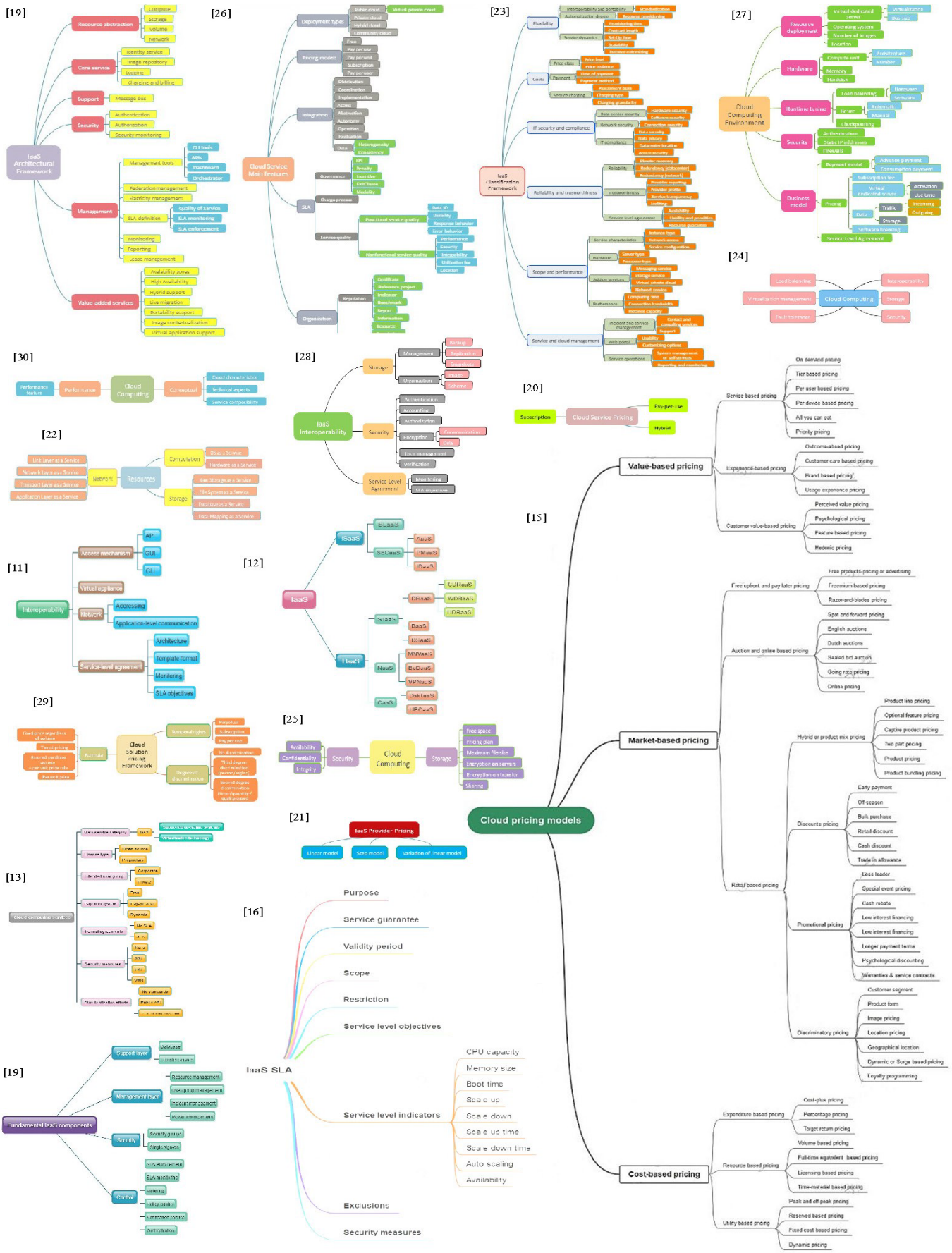


Figure 1: Tenant-centric IaaS excerpted and transformed taxonomies

period. While these taxonomies encompassed concepts found in all the ontologies examined in the preceding section, they were not primarily geared towards IaaS. Therefore, a careful analysis was required to identify IaaS-specific topics that are directly relevant to customers. Table 1 provides an overview of the taxonomies employed in this paper, along with the proportion of tenant-centric IaaS topics extracted from each taxonomy.

Table 1: Customer-centric topic excerption from IaaS taxonomies

Taxonomy	Excerption	Taxonomy	Excerption
[19]	100%	[24]	67%
[20]	100%	[25]	65%
[21]	100%	[26]	61%
[15]	100%	[27]	60%
[22]	98%	[11]	54%
[12]	96%	[28]	49%
[23]	95%	[29]	41%
[19]	75%	[16]	41%
[13]	73%	[30]	33%

Reusing these taxonomies in their original formats presents a challenge, given their diverse presentation styles, which encompass textual descriptions and various graphical models such as mind maps, feature models, decision trees, layered block diagrams, SBIFT models, and textual lists. To create a cohesive and consistent representation while eliminating conflicts and redundancies, this study chose to employ a standardized mind map approach. This allowed us to amalgamate all the extracted taxonomies into a unified model. Figure 1 visually depicts the consumer-centric IaaS excerpts that have been individually transformed into mind maps.

3.2. Refinement

This step analyzed semantic consistencies among the taxonomies from the previous step and subsequently merged them into a unified taxonomy by employing a binary integration approach. The algorithm of the binary integration is as follows.

- Step 1: A pair of taxonomies from Figure 1 that have some common topic(s) (which will be used as a merging point) is selected each time. For example, taxonomies in [20] and [26] have cloud service pricing and pricing models, respectively, as a common topic.
- Step 2: Any redundant and inconsistent topics between both taxonomies from step 1 were identified. For example, subscription in [20] is redundant with subscription in [26].
- Step 3: All redundant topics if there is any, except the one to be used as merging point(s), in both taxonomies are removed to retain the topic's uniqueness. For example, only subscription in [26] is removed.
- Step 4: Any synonymous topics are resolved by choosing the most appropriate topic and renamed the others to be the chosen one. For example, since cloud service pricing in [20] is synonymous with pricing models in [26], cloud service pricing in [20] is renamed to pricing models as that of [26].
- Step 5: Any homonymous topics are resolved by renaming each of them to a distinct term. For example, since availability in [25] and availability in [23] refer to the availability aspect of security and SLA, respectively, availability in [23] is renamed to availability aspect instead.
- Step 6: Merge both taxonomies into a single one by using the merging points. For example, taxonomy in [20] and taxonomy in [26] are merged by using the same topic pricing models.
- Step 7: Repeat step 1 to step 6 for the remaining pairs of taxonomies, including the merged one resulting from step 6, until a unified and consistent taxonomy is achieved.

As a result of refinement, the algorithm resolved 121 (sub)topics out of the total (sub)topics that were redundant and 67 inconsistent (sub)topics that held synonyms and homonyms to obtain a unified taxonomy at last.

3.3. Formalization

All of nonredundant topics and subtopics in the unified taxonomy were converted into classes and subclasses that were connected to other classes and subclasses based on semantic domains. The root class is denoted as "owl: Thing". Consequently, the proposed ontology is composed of 15 direct subclasses, as illustrated in Figure 2: Performance, Resource abstraction, Core service, Support, Costs, Security, Management, Value-added services, Resource deployment, Control, Standardization efforts, Flexibility, Deployment types, Integration, and Organization. The total number of subclasses is 340, such as Performance feature, Computing time, and Connection bandwidth, that are arranged hierarchically in a tree structure with a height of 7, as depicted in Figure 3.

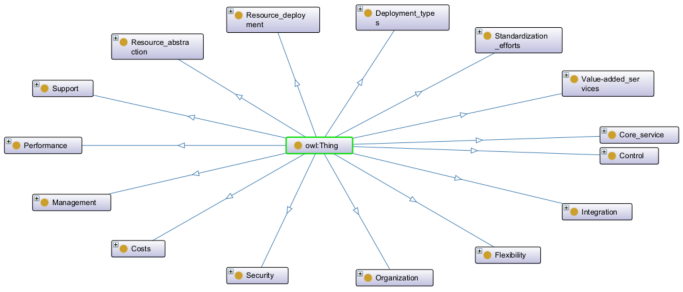


Figure 2: Proposed ontology and its direct subclasses

To provide a comprehensive understanding of the proposed ontology, each of direct subclasses is essentially described one by one, including its nested subclasses enclosed within curly brackets. Furthermore, supplementary explanations are provided within parentheses immediately following respective (sub)classes.

- Performance of IaaS has the following subclasses : Performance feature (identifying the atomic elements of cloud-service performance evaluation), Computing time, Connection bandwidth, Instance capacity, and Load balancing of Hardware or software type.
- Resource abstraction is various resources offered as services. Its subclass and nested subclasses are as follows. Compute = {OS as a Service = {Software licensing = {Open-source,Proprietary}}, Desktop as a Service (DskTaaS), High Performance Computing as a Service (HPCaaS)}, Storage = {Raw Storage as a Service (i.e., block level storage), File

System as a Service, Storage management = {Free space, Maximum file size, Encryption on servers, Encryption on transfer, Sharing, Backup, Replication, Snapshots}, Storage organization = {Image, Scheme (i.e., block, file, or object storage)}, Data Storage as a Service (DRaaS) = {Cold-site DRaaS (CDRaaS), Warm-site DRaaS (WDRaaS), Hot-site DRaaS (HDRaaS)}, Backup as a Service (BaaS) = { Data Storage as a Service (DSaaS)}}. Network = {Link Layer as a Service, Network Layer as a Service, Transport Layer as a Service, Application Layer as a Service, Traffic = {Incoming, Outgoing}, Addressing (providing accessibility to applications and underlying virtual machines once moved to new networks), Application-level communication (specifying API to be RESTful to decouple client from server components and advocate interoperable IaaSs via standard interfaces), Mobile Network Virtualization as a Service (MNVaaS), Bandwidth on Demand as a Service (BoDaaS), Virtual Private Network as a Service (VPNaaS)}, Infrastructure Services as a Service (ISaaS) (which provides a set of auxiliary services) = {Billing as a Service (BLaaS), Security as a Service (SECaaS) (encompassing Identity as a Service (IDaaS) for managing authentication and authorization), Auditing as a Service (AaaS) (for checking providers for standard compliance), Policy Management as a Service (PMaaS) (for handling all access policies across multiple providers)}}.

- Core service is fundamental to all other services. Its subclasses are {Image repository, Charging and billing, SECaaS = {Auditing as a Service (AaaS) (i.e., Logging), Policy Management as a Service (PMaaS), Identity as a Service (IDaaS)}}.
- Support is services used to operate some other services. It has three subclasses: Message bus (providing a means for passing messages between different cloud services), Database, and Transfer service (for other layers to communicate and interact).
- Costs = {Price class = {Price level (all factors affecting resulting cost directly), Price resilience (price options for flexibility purpose)}, Payment = {Time of payment, Payment method, Payment model = {Advance payment, Consumption payment}}, Service charging = {Assessment basis (how regular billing occurs such as hourly or monthly), Charging granularity}, Pricing models = {Value-based pricing (estimating customers' satisfaction) = {Service-based pricing (focusing on service content) = {On-demand pricing, Tier-based pricing, Per-user-based pricing, Per-device-based pricing, All-you-can eat (buffet pricing), Priority pricing}, Experience-based pricing (based on performance) = {Outcome-based pricing, Customer-care-based pricing, Brand-based pricing, Usage-experience pricing}, Customer-value-based pricing (a price from a subjective view of a customer) = {Perceived-value pricing, Psychological pricing, Feature-based pricing, Hedonic pricing}}, Market-based pricing (equilibrium of customers and providers) = {Free-upfront-and-pay-later pricing = {Free products-pricing-on-advertising, Freemium-based pricing, Razor-and-blades pricing (giving away nonconsumable element and charging consumable replacement element)}, Auction-and-online-based pricing = {Spot-and-forward pricing (i.e., current and future prices), English auctions (Open Ascending), Dutch auctions (Open Descending), Sealed-bid auction, Going-rate pricing, Online pricing}, Retail-based pricing (for small quantity purchase) = {Hybrid-or-product-mix pricing (combining different pricing models) = {Product-line pricing, Optional-feature pricing, Captive-product pricing (i.e., cheap core part with costly accessory), Two-part pricing, By-product pricing, Product-bundling pricing}, Discounts pricing = {Early payment, Off-season, Bulk purchase, Retail discount, Cash discount, Trade in allowance (discount in exchange of buyer's asset)}, Promotional pricing = {Loss leader (selling below market price), Special event pricing, Cash rebate, Low interest financing, Longer payment terms, Psychological discounting, Warranties & service contracts}, Discriminatory pricing (charging different prices to different customers) = {Customer segment, Product form (different prices for different versions of a product), Image pricing, Location pricing, Geographical location, Dynamic or surge-based pricing (based on current market demands), Loyalty programming (rewarding customers to continue buying from the brand}}}, Cost-based pricing (covering Capex and Opex) = {Expenditure-based pricing = {Cost-plus pricing (cost plus margin), Percentage pricing, Target-return pricing}, Resource-based pricing = {Volume-based pricing, FTE (full-time equivalent)-based pricing, Licensing-based pricing, Time-material-based pricin}, Utility-based pricing = {Peak-and-off-peak pricing, Reserved-based pricing (e.g., Subscription or no up-front, partial up-front, and all up-front), Fixed-cost-based pricing, Dynamic pricing}}}}, Formula = {Linear model, Step model, Variation of linear model}, Degree of discrimination (how a service is offered for different buyers for different prices) = {No discrimination, Second degree discrimination (when providers sell different units for different prices where customers must do self-selection to choose from the offers), Third degree discrimination (vendor identifies different customer groups based on their willingness-to-pay and can be personal (e.g., student discounts) or regional (e.g., different prices for developing countries))}}}.
- Security = {Availability = {Confidentiality, Integrity, Fault tolerance, Authentication, Authorization, Accounting, Security monitoring, Static IP address, Firewalls, Data center security = {Hardware security, Software security, Data center redundancy}, Network security = {Connection security, Network redundancy}, IT compliance = {Data security, Data privacy, Datacenter location, Access security, Disaster recovery}, User management, Verification, Security groups, Single sign-on, Security measures = {None, SSL, PKI, VPN}}.
- Management = {Management tools = {CLI tools, APIs, Dashboard, Orchestrator, Federation management, Elasticity management}, Formal agreement = {No SLA, SLA = {SLA objectives (defining quality-of-service measurement in SLAs), Scope, Quality of Service, Functional service quality = {Data IO, Usability, Response behavior, Error behavior}, Nonfunctional service quality = {Availability aspect, Performance aspect, Security aspect, Integrability, Utilization fee, Location}, SLA monitoring, SLA enforcement, Governance = {KPI, Penalty, Incentive, Exit clause, Modality}, Charge process, Liability and penalties, Validity period (of negotiated SLA), Resource guarantee, Architecture

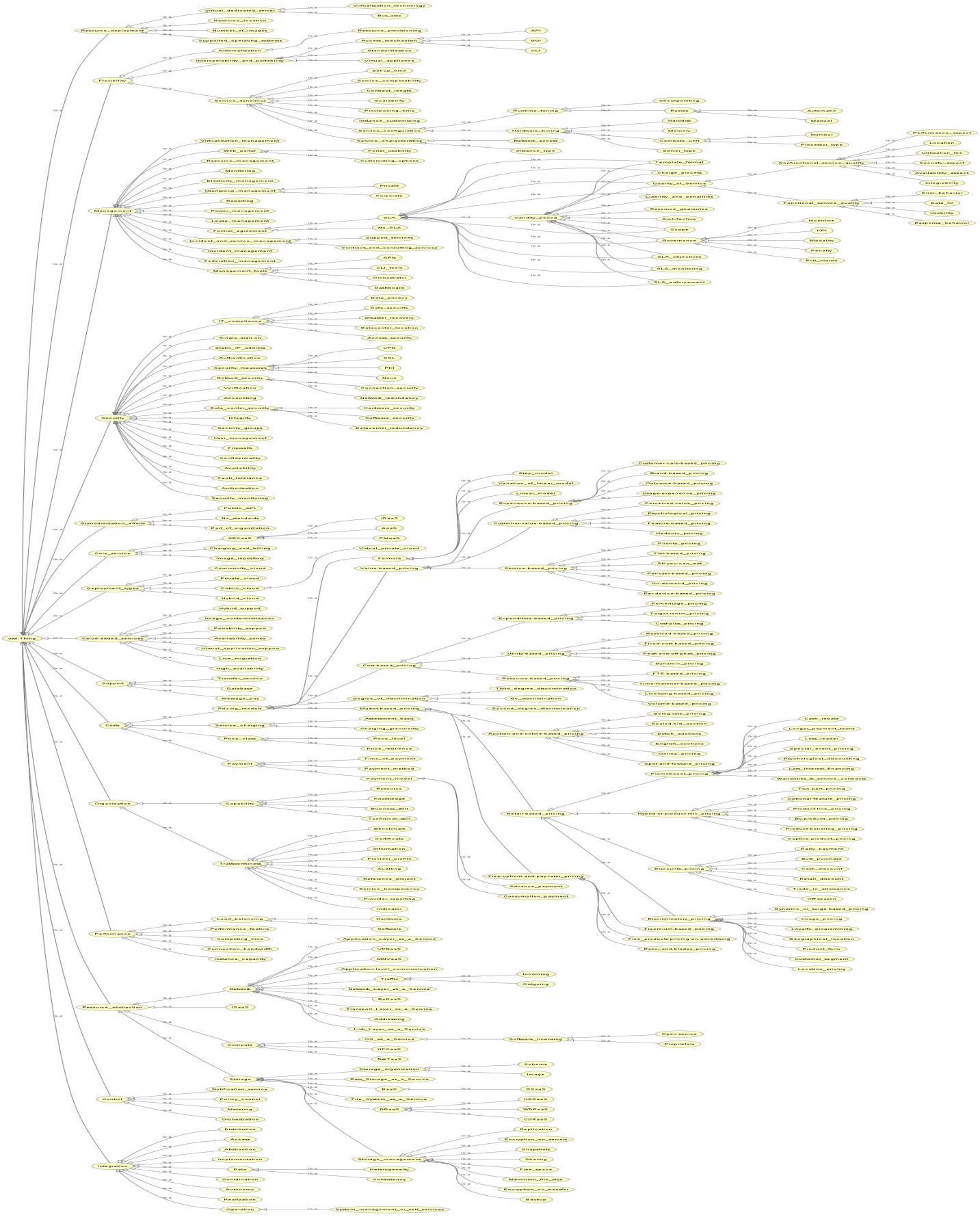


Figure 3: Proposed ontology's complete class hierarchy

(of SLA measures and SLA requirement management for different IaaSs; For example, Web Service Agreement Specification (WSA) is the standard for the SLA management architecture in Web service environments), Template format (used to electronically represent SLA for automated management)}, Monitoring, Reporting, Lease management, Incident and service management = {Contract and consulting services, Support services}, Web portal = {Portal_usability, Customizing options}, Virtualization management, Resource management, User/group management = {Corporate, Private}, Incident management, Power management}.

- Value-added services = {Availability zones, High availability, Hybrid support (facilitating the implementation of hybrid cloud by resource extension to external), Live migration, Portability support, Image contextualization (enabling virtual machine (VM) instance to be deployed in the form of a shared customized image for specific context such as VM with a turnkey database), Virtual application support (i.e., containers consisting of several VMs and allowing design and configuration of multi-tier applications)}.
- Resource deployment = {Virtual dedicated server = {Virtualization technology, Bus size (or processor register size e.g. 64 bits)}, Number of images, Resource location, Supported operating systems (OS supported by providers)}.
- Control provides cloud systems with basic control features. Its subclasses are Metering, Policy control, Notification service, and Orchestration.
- Standardization efforts = {No standards, Public API (i.e., common API enabling interoperability and customization), Part of organization (i.e. organization involves in public standardization)}.
- Flexibility = {Interoperability and portability = {Standardization, Access mechanism = {API, GUI, CLI}, Virtual appliance (delivering a service as a complete software stack installed on a VM)}, Automatization = {Resource provisioning}, Service dynamics = {Provisioning time, Contract length, Set-up time, Scalability, Instance customizing, Service composability, Service characteristics = {Instance type, Network access}, Service configuration = {Hardware tuning = {Compute unit = {Number, Processor type}, Server type, Memory, Harddisk}, Runtime tuning = {Resize = {Automatic, Manual}, Checkpointing}}.
- Deployment types = {Public cloud = {Virtual private cloud}, Private cloud, Hybrid cloud, Community cloud}.
- Integration = {Distribution, Coordination, Implementation, Access, Abstraction, Autonomy, Operation = {System management or self-services}, Realization, Data = {Heterogeneity, Consistency}}.
- Organization = {Trustworthiness = {Certificate, Reference project, Indicator, Benchmark, Provider reporting, Information, Provider profile, Service transparency, Auditing}, Capability = {Resource, Knowledge, Technical skill, Business skill}}.

The properties of the classes are hasDirectCost, hasMgmtAspect, hasSecurityAspect, and useTechnology as depicted in Figure 4.

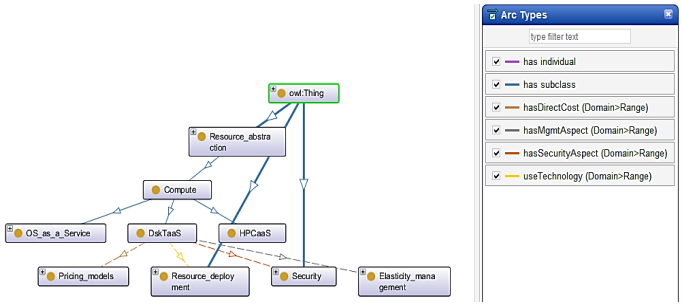


Figure 4: Ontology's class properties

4. Evaluation

The proposed ontology is evaluated into two crucial parts, a technology-focused evaluation and a user-focused evaluation, as follows.

For technology-focused evaluation, this paper employed a HermiT reasoner to rigorously determine whether the proposed ontology is syntactically and semantically consistent and identify subsumption relationships between classes. The result of this evaluation is an inferred ontology that is prominently displayed in yellow background in Figure 5 without any error (which will be indicated by red text if there is any).

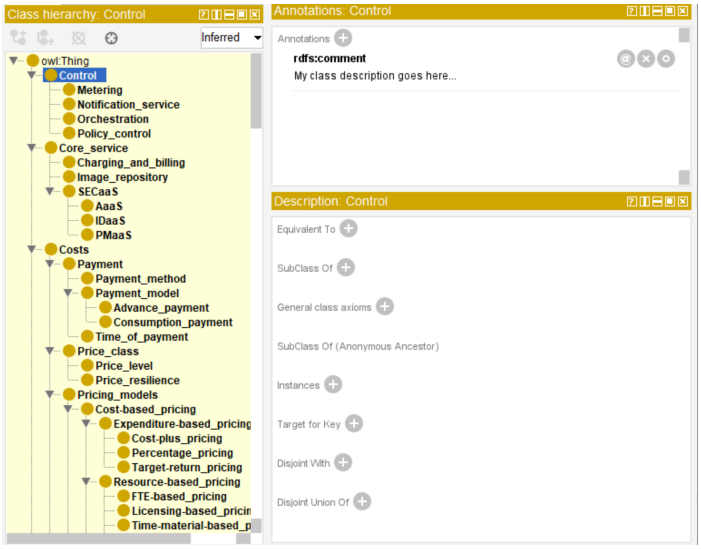


Figure 5: Inferred ontology by using HermiT

Complementing the technological assessment, the study conducted a comprehensive user-focused evaluation. This evaluation entailed applying our ontology to assess a worldwide recognized Infrastructure as a Service (IaaS) platform, namely, AWS EC2. To accomplish this, the study carefully generated ontology individuals by drawing from publicly available information pertaining to AWS EC2, as exemplified in Figure 6, where these individuals are denoted by prefix violet diamond symbols. All pieces of information regarding AWS EC2 offerings for consumers can be seamlessly mapped into the ontology's

existing classes (denoted by prefix orange oval symbols) to facilitate comprehensive IaaS selection.

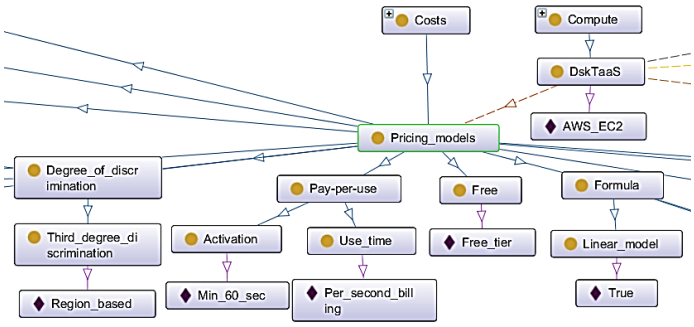


Figure 6: Ontology's instance portion for AWS EC2's offerings

Furthermore, in Figure 7, the study performs two distinct SPARQL queries against the ontology. The first query below

```
SELECT ?subject WHERE {
    ?subject rdf:type owl:Class.
}
```

aims to list all (sub)classes. Part of the resulting classes of the query are listed in the bottom pane in the figure. The second query below

```
SELECT ?subject WHERE {
    ?subject rdf:type owl:NamedIndividual.
}
```

identifies and enumerates individual instances as partially displayed in the resulting pane in the figure. The successful execution of both queries substantiates the potential for automating IaaS assessment processes using our ontology.

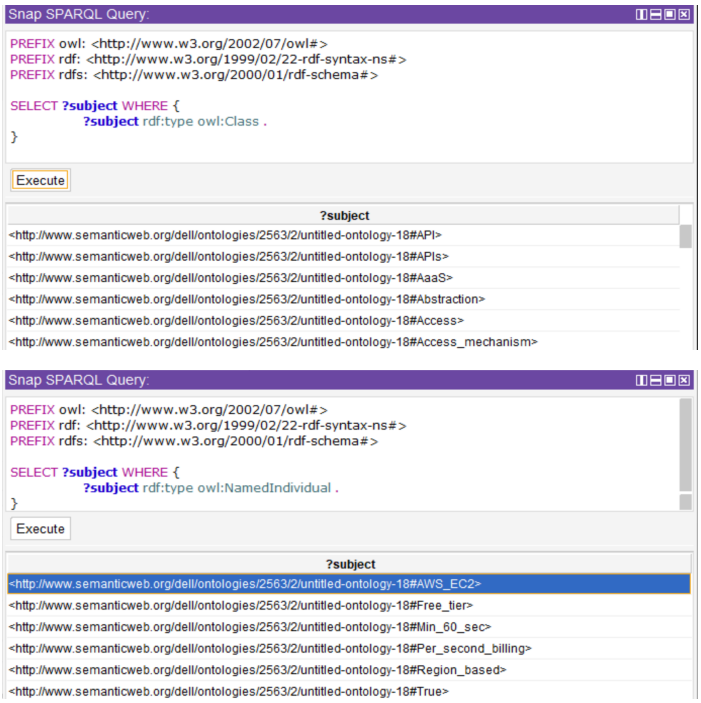


Figure 7: SPARQL queries for classes and individuals

5. Conclusion

This paper presents a novel customer-perspective IaaS ontology developed from various 18 IaaS taxonomies in present existence. This ontology stands out for its exceptional comprehensiveness, encompassing a total of 15 primary subclasses (e.g., performance, costs, and security) and 340 individual classes (e.g., instance capacity, availability, and price class). The evaluation shows that the proposed ontology is syntactically and semantically consistent. Furthermore, the ontology successfully enables not only the assessment of AWS EC2 IaaS but also SPARQL queries. This has affirmed that the ontology holds significant semantic value, offering utility not only to researchers but also to practitioners by leveraging it as a foundational component to develop a sophisticated assessment tools for facilitating effective IaaS adoption. The tool will be definitely helpful for IaaS customers, IaaS providers, and IaaS partners. The future work of this study is to develop an expert system in the form of SaaS to facilitate IaaS selection based on the proposed ontology.

Conflict of Interest

The authors declare no conflict of interest.

Acknowledgment

This research was financially supported by Department of Computer Science, Kasetsart University, Krung Thep Maha Nakhon, Thailand.

References

[1] ISO/IEC, ISO/IEC 17789: Information technology — Cloud computing — Reference Architecture, ISO/IEC, 2014.

[2] F. Nadeem, "Evaluating and Ranking Cloud IaaS, PaaS and SaaS Models Based on Functional and Non-Functional Key Performance Indicators," IEEE Access, **10**, 63245-63257, 2022, doi: 10.1109/ACCESS.2022.3182688.

[3] E. Al-Masri, L. Meng, "A Quality-Driven Recommender System for IaaS Cloud Services," in 2018 IEEE International Conference on Big Data (Big Data), 5288-5290, 2018, doi: 10.1109/BigData.2018.8622017.

[4] S. M. M. Fattah, A. Bouguettaya, S. Mistry, "Signature-based Selection of IaaS Cloud Services," in 2020 IEEE International Conference on Web Services (ICWS), 50-57, 2020, doi: 10.1109/ICWS49710.2020.00014.

[5] K. Kritikos, K. Magoutis, D. Plexousakis, "Towards Knowledge-Based Assisted IaaS Selection," in 2016 IEEE International Conference on Cloud Computing Technology and Science (CloudCom), 431-439, 2016, doi: 10.1109/CloudCom.2016.0073.

[6] F. Moscato, R. Aversa, B. Di Martino, T. -F. Fortiş, V. Munteanu, "An analysis of mOSAIC ontology for Cloud resources annotation," in 2011 Federated Conference on Computer Science and Information Systems (FedCSIS), 973-980, 2011.

[7] A. Abdullah, S.M. Shamsuddin, F.E. Eassa, Ontology-based Cloud Services Representation. Research Journal of Applied Sciences, Engineering and Technology. **8**(1), 83-94, 2014, doi:10.19026/rjaset.8.944.

[8] M. Zhang, R. Ranjan, A. Haller, D. Georgakopoulos, M. Menzel, S. Nepal, "An ontology-based system for Cloud infrastructure services' discovery," in 8th International Conference on Collaborative Computing: Networking, Applications and Worksharing (CollaborateCom), 524-530, 2012.

[9] Q. Zhang, A. Haller, Q. Wang, CoCoOn: Cloud Computing Ontology for IaaS Price and Performance Comparison. in International Semantic Web Conference. 325-341, 2019, doi.org/10.1007/978-3-030-30796-7_21.

[10] T. Banditwattanawong, "The survey of infrastructure-as-a-service taxonomies from consumer perspective," in the 10th International Conference on e-Business, 2015.

[11] Z. Zhang, C. Wu, D.W.L. Cheung, "A survey on cloud interoperability: taxonomies, standards, and practice," ACM SIGMETRICS Performance Evaluation Review, **40**(4), 13-22, 2013, doi.org/10.1145/2479942.2479945.

[12] M. Firdhous, "A Comprehensive Taxonomy for the Infrastructure as a Service in Cloud Computing," in 2014 Fourth International Conference on Advances in Computing and Communications, 2014, 158-161, doi: 10.1109/ICACC.2014.45.

[13] C.N. Höfer, G. Karagiannis, "Cloud computing services: taxonomy and comparison," Journal of Internet Services and Applications, **2**, 81-94, 2011, doi.org/10.1007/s13174-011-0027-x.

[14] R. Dukarić, J. Matjaz, "A Taxonomy and Survey of Infrastructure-as-a-Service Systems," Lecture Notes on Information Theory, **1**, 29-33, 2013, doi: 10.12720/lnit.1.1.29-33.

[15] C. Wu, R. Buyya, K. Ramamohanarao, "Cloud Pricing Models: Taxonomy, Survey, and Interdisciplinary Challenges," ACM Computing Survey, 52(6), 1-36, 2019, doi.org/10.1145/3342103.

[16] Shivani and A. Singh, "Taxonomy of SLA violation minimization techniques in cloud computing," in Second International Conference on Inventive Communication and Computational Technologies (ICICCT), 1845-1850, 2018, doi:10.1109/ICICCT.2018.8473230.

[17] T. Banditwattanawong, M. Masdisornchote, "Federated Taxonomies Toward Infrastructure-as-a-Service Evaluation," International Journal of Management and Applied Science, **2**(8), 33-38, 2016.

[18] S. Staab, R. Studer, Handbook on Ontologies (2nd. ed.). Springer Publishing Company, Inc., 2009.

[19] R. Dukaric, M.B. Juric, "Towards a unified taxonomy and architecture of cloud frameworks," Future Generation Computer System, **29**(5), 1196–1210, 2013, doi.org/10.1016/j.future.2012.09.006..

[20] S. Kansal, G. Singh, H. Kumar, S. Kaushal, "Pricing models in cloud computing," in International Conference on Information and Communication Technology for Competitive Strategies, 33:1–33:5, 2014, doi.org/10.1145/2677855.2677888.

[21] M.K.M. Murthy, H.A. Sanjay, J.P. Ashwini, "Pricing models and pricing schemes of iaas providers: A comparison study," in Proceedings of the International Conference on Advances in Computing, Communications and Informatics, 143–147, 2012, doi:10.1145/2345396.2345421.

[22] S. Kächele, C. Spann, F. J. Hauck, J. Domaschka, "Beyond IaaS and PaaS: An Extended Cloud Taxonomy for Computation, Storage and Networking," in IEEE/ACM 6th International Conference on Utility and Cloud Computing, 75-82, 2013, doi: 10.1109/UCC.2013.28.

[23] J. Repschlaeger, S. Wind, R. Zarnekow, K. Turowski, "A Reference Guide to Cloud Computing Dimensions: Infrastructure as a Service Classification Framework," in The 45th Hawaii International Conference on System Sciences, 2178-2188, 2012, doi: 10.1109/HICSS.2012.76.

[24] B.P. Rimal, E. Choi, I. Lumb, "A Taxonomy and Survey of Cloud Computing Systems," in The Fifth International Joint Conference on INC, IMS and IDC, 2009, 44-51, doi: 10.1109/NCM.2009.218.

[25] H. Kamal Idrissi, A. Kartit, M. El Marraki, "A taxonomy and survey of Cloud computing," in National Security Days (JNS3), 1-5, 2013, doi:10.1109/JNS3.2013.6595470.

[26] S. Gudenkauf, M. Josefiok, A. Göring, O. Norkus, "A Reference Architecture for Cloud Service Offers," in The 17th IEEE International Enterprise Distributed Object Computing Conference, 227-236, 2013, doi: 10.1109/EDOC.2013.33.

[27] R. Prodan, S. Ostermann, "A survey and taxonomy of infrastructure as a service and web hosting cloud providers," in The 10th IEEE/ACM International Conference on Grid Computing, 17-25, 2009, doi: 10.1109/GRID.2009.5353074.

[28] R. Teckelmann, C. Reich, A. Sulistio, "Mapping of Cloud Standards to the Taxonomy of Interoperability in IaaS," in IEEE Third International Conference on Cloud Computing Technology and Science, 522-526, 2011, doi:10.1109/CloudCom.2011.78.

[29] G. Laatikainen, A. Ojala, O. Mazhelis, "Cloud services pricing models," in Software Business. From Physical Products to Software Services and Solutions - 4th International Conference, 117–129, 2013, doi: 10.1007/978-3-642-39336-5_12.

[30] F. Polash, A. Abuhussein, S. Shiva, "A survey of cloud computing taxonomies: Rationale and overview," in The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014), 459-465, 2014, doi:10.1109/ICITST.2014.7038856.

ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 8, No. 6, 46-56 (2023)

www.astesj.com

Special Issue on Innovation in Computing, Engineering Science & Technology

ASTESJ

ISSN: 2415-6698

EEG Feature Extraction based on Fast Fourier Transform and Wavelet Analysis for Classification of Mental Stress Levels using Machine Learning

Ng Kah Kit[1,*], Hafeez Ullah Amin[1], Kher Hui Ng[1], Jessica Price[1], Ahmad Rauf Subhani[2]

[1]*School of Computer Science, University of Nottingham Malaysia, 43500 Semenyih, Selangor*

[2]*College of Electrical and Mechanical Engineering, National University of Science and Technology, Islamabad, Pakistan*

ARTICLE INFO

Article history:
Received:24 July, 2023
Accepted:05 November, 2023
Online: 30 November, 2023

Keywords:
Electroencephalography (EEG)
Feature Extraction
Mental Stress
Discrete Wavelet Transform
Fourier Transform
Machine Learning

ABSTRACT

Mental stress assessment remains riddled with biases caused by subjective reports and individual differences across societal backgrounds. To objectively determine the presence or absence of mental stress, there is a need to move away from the traditional subjective methods of self-report questionnaires and interviews. Previously, it has been evidence that EEG Oscillations can discriminate mental states, for instance, stressed and non-stressed. However, it is still not clear in which range of EEG oscillations the neural activities are associated with the mental states. This paper presents a wavelet-based EEG feature extraction method for the classification of mental stress using machine learning classifiers. An EEG dataset of 22 participants was used to test the performance of the proposed wavelet-based feature extraction method. The dataset includes both stress and control conditions, and the stress condition has multiple levels of stress, starting from low, mild, and high stress. The Daubechies mother wavelet of the fourth order was used to separate the EEG oscillations into 7 levels for the extraction of the absolute powers. Whereas Fast Fourier Transform were implemented to obtain the average power of the oscillations. The features were then used in support vector machine, decision tree, linear discriminant analysis and artificial neural network classifiers. A comparison between the classifiers using average power, absolute power, and a combination of both is provided. The EEG alpha, theta, and beta frequency bands showed promising results for the classification of mental stress vs. control conditions by achieving an average accuracy of 95% using the decision tree. The results of the proposed method suggest the potential use of wavelet analysis for mental stress detection despite FFT performing better. The proposed method has the potential to be used in Computer-Aided Diagnosis (CAD) systems for mental stress assessment in the future alongside the discovery of significant wave bands in relation to mental stress detection.

1. Introduction

The Latin verb ‘strictus’, which merely means to draw tight, is whence the word "stress" gets its original meaning. The term "stress" didn't have psychological connotations until the late 19th century, thanks to the groundbreaking work of Hans Selye, who is regarded as the father of stress study. Before then, stress was always thought of as the act of applying physical pressure or force to an object. However, we also experience internal emotional pressures and invisible forces, which has led to a biological investigation into the causes of stress. This was illustrated in the work of W.B. Cannon, who detailed how biological systems have developed an internal system to preserve homeostasis, a stable internal state. In order to test his views concerning acute stress responses as opposed to chronic stress, Hans Selye carried out experiments. He then came up with the phrase "stress responses," defining stress as pressures or mutual actions that occur across any part of the body, whether it be psychological or physical.

The broad term for stress can be further broken down into two categories: positive stress (Eustress) and negative stress (Distress). Eustress is perceived as a type of pressure that encourages a person to overcome obstacles by learning to see outside pressures as challenges rather than obstacles. On the other hand, distress results from a failure to use these needs as a motivator, which eventually stifles any advancement or success. Distress can also be divided

*Corresponding Author: Ng Kah Kit, kahkitng@gmail.com

into two categories: acute distress, which is short-term, and chronic distress, which is long-term. It should be highlighted that current definitions and understanding suggest that stress results in a physical reaction as a stressor rather than a physical reaction to perceived threats or challenges.

Both adults and children are afflicted by mental stress. Every human being suffers stress at some point in their lives, whether it is from work-related homework or just plain peer pressure from their employer. Short-term stress may be good for encouraging the improvement of work performed, while long-term stress can be destructive to one's physical and mental health [1]. If untreated or without an appropriate management strategy, it can seriously damage cognitive abilities and, as a result, the person's quality of life [2]. Studies have also revealed that prolonged work stress diminishes the grey matter volumes of the dorsolateral prefrontal cortex and the anterior cingulate cortex, which are accountable for memory, attention, and mood [3].

Despite advances in medicine, particularly in psychology, have made it possible for regular people to get the care or assistance they want. Patients only seek treatment when they can no longer tolerate to live in a situation of extended stress, therefore there is still much to learn and develop in this area. As a result, the general public continues to be untreated and lacks access to expert assistance to lessen future stress. Even worse, because conventional techniques for detecting mental stress primarily depend on self-report questionnaires and interviews, the results are still largely ambiguous. Therefore, subjective interpretations may be used to assess the degree to which a patient's stress level can be deemed harmful as well as whether or not the patient is experiencing stress. Therefore, the ability to anticipate a patient's likelihood of experiencing stress in the future or even just identify stress without consulting a medical practitioner may make it possible for patients to receive treatment and possibly even seek it out more voluntarily.

Many attempts have been made up to this point to use a machine learning technique to swiftly evaluate and forecast a patient's state of health. Results in certain instances point to machine learning's potential to diagnose conditions more accurately than qualified medical professionals. But in many of these instances, there are numerous flaws and biases, which contribute to the widespread belief that machine learning can supplement, if not completely replace, medical professionals [4]. Nevertheless, we think that machine learning applications in the healthcare industry will only grow. Medical practitioners should then use artificial intelligence and machine learning as a tool to give patients better and more advanced medical care.

By placing tiny electrodes on the scalp, an electroencephalogram (EEG) is a non-invasive, affordable, easily accessible, and painless test that looks for irregularities in brain waves. The potential difference between the cortical neuronal activity and the electrodes' detection of it is amplified and shown as a waveform. The cortical excitatory and inhibitory postsynaptic potential summations serve as the primary sources of electrographic activity [5]. Additionally, EEG scans reflect changes in brain activity almost instantaneously due to their high temporal resolution, while other scan types require several minutes following the occurrence of an event. Unfortunately, the limited spatial resolution of EEG makes it impossible to pinpoint the precise location of the cerebral waveforms. Furthermore, there will be significant contamination from other electrical noise as a result of the potential difference's amplification. Even though EEG signals are fascinating, they cannot be used by an interpreter to make future predictions. It's possible that any waveform anomalies that have happened before won't happen again.

Based on their frequency range, the waveforms found in an EEG can be grouped. The frequencies at which delta activity, theta activity, alpha activity, beta activity, and gamma activity occur are as follows in increasing order: delta activity occurs between 0.5 and 4 Hz, theta activity between 5 and 7 Hz, alpha activity between 8 and 13 Hz, beta activity between 14 and 30 Hz, and gamma activity between 30 and 80 Hz. Each of these waveforms, in turn, represents distinct brain states, including relaxation, sleep, anxiety, passive attention, and concentration [6]. EEG signal information is a well-known neuroimaging modality that records brain electrical activity for the diagnosis of various brain abnormalities, such as the identification of epileptic seizure activity, depression, stroke, and Alzheimer's disease [5]. Despite the vast amount of data that can be gleaned from an EEG reading, little research has been done on using it to identify mental stress. Furthermore, the research that has already been done does not consistently point to a general strategy for methodically combining machine learning with EEG for stress assessment [7]. This was demonstrated when various machine learning classifiers and feature extraction techniques were used in comparable circumstances.

Since it has been shown in numerous studies that the alpha, theta, and beta bands of an EEG reading correlate to cognitive workload processing and, in turn, mental stress, here we propose to extract information from these bands in order to classify mental stress [8,9]. Therefore, the purpose of this study is to propose a machine learning (ML) framework for the extraction of EEG features based on fast Fourier transform and wavelet transform for the classification of mental stress, including high- and low-level stress. EEG information from an earlier investigation [10] were decomposed with discrete wavelet transform and fast Fourier transform into different frequency bands, including alpha, theta, and beta, and computed EEG frequency bands power. Widely used ML classifiers, including Support Vector Machine (SVM), Linear Discriminant Analysis (LDA), Decision Trees (DT), and Artificial Neural Networks (ANN), were used to model the EEG dataset in order to illustrate the performance of the suggested ML framework. Next, the Fourier Transform method—a conventional transformation technique for determining power spectral density—is compared to the wavelet transform.

The remaining sections of the paper are organized as section II explains the dataset and feature extraction and classification methodology, section III reports the findings, followed by the discussion in section IV, and finally section V concludes the paper.

2. Literature Review

2.1. Stress Detection and Appraisal

It's interesting to note that stress is not a medical diagnosis or condition that calls for medical professionals to thoroughly and methodically evaluate their patients. In actuality, subjective questionnaires like the Perceived Stress Scale (PSS), which has 14 questions (later lowered to 10) that the patient must answer, are the closest measurements of stress that are utilized in a medical setting [11], Stress Response Inventory [11], Holmes and Rahe Stress Scale (Social Readjustment Rating Scale) [12], Depression Anxiety Stress Scale [13], The Hospital Anxiety and

Depression Scale [14], The State Trait Anxiety Inventory [15] and Life Events and Coping Inventory [16]. The PSS was created in 1983 and is still a widely used tool to help us comprehend how various circumstances impact our emotions and our perceived stress levels, which range from low to high. The current problem, however, is that despite all the subjective questionnaires currently in use, the only stress that patients perceive is the stress that they observe and rate for themselves without any concrete data to support the presence or absence of stress. Given that mental stress is the psychological and physiological condition that has afflicted humans for the longest duration, it is unexpected that there isn't a methodical way to conclusively determine whether stress is present.

Further, doctors and psychologists attempted to use physiological changes mentioned above for an objective measure such as increased heart rate through heart rate variability (HRV) [17]. HRV is where the amount of time between the heartbeats fluctuates slightly usually measured using an electrocardiogram (ECG) that detects the electrical activity of the heart using sensors attached to the skin of the chest. Galvanic Skin Responses (GSR) also known as electrodermal activity (EDA) measures the changes in sweat gland activity that are reflective of the intensity of our emotional state [18]. Moreover, research has tapped into the area of measuring stress through pupil dilation and blood pressure [19]. Consequently, salivary alpha-amylase and cortisol levels were used as a biomarker for stress indication due to their association with the activation of the sympathetic nervous system [20].

2.2. Electroencephalography

The use of electroencephalography (EEG) to measure stress has been the subject of recent research due to its relative affordability when compared to other methods that involve the collection of blood samples or the ingestion of radioactive chemicals, such as PET scans. But since this method is still relatively new, researchers have had differing degrees of success in identifying stress [5]. Many methods for using EEG signals to detect mental stress have been reported in the literature. These methods include using SVM, Multilayer Perceptron, and Convolutional Neural Networks in a virtual environment to detect mental stress [6]. The detection of stress is still very new and in its early stages, where researchers are still trying to determine electrical signals and patterns related to stress. One drawback of EEG is its limited spatial resolution, which makes it difficult to locate the precise region involved or responsible for stress because the electrical signals measured are only on the surface of the brain. Although there are studies that use direct experimentation and specific regions to identify stress using PET or MRI scans, these approaches are deemed impractical due to the high cost and limited accessibility of the necessary equipment. Furthermore, unlike the other resolution methods mentioned, using an EEG machine does not require extensive training.

2.3. Machine Learning Methods for Stress Detection

There has been much research that uses artificial intelligence for mental stress assessment through machine learning classifiers and algorithms. A machine learning classifier uses an independent set of information from a dataset known as features to predict the corresponding class it belongs to by having several parameters. Such features need to have unique characteristics that separate one class from another. Further, machine learning classifier will undergo either supervised or unsupervised training to predict the classes of new instances in an unseen testing dataset. Several machine learning techniques and algorithms often used in mental stress assessment are described below.

Machine learning classifiers like SVM, ANN and k-NN have shown immense potential in stress detection with each classifier achieving accuracies of more than 85% [6,21,22]. However, it seems that each classifier is feature specific when comparing each studies above. For example, SVM seems to favor frontal alpha asymmetry as a feature whereas convolutional neural network, a branch of ANN performed much better when simply considering all the brain waves. K-NN on the other hand used only a few selective electrodes and achieved accuracies of 94 and 93.7% [22]. Meanwhile, LDA relied on multiple bio-signals besides EEG such as electrocardiography (ECG), electromyography (EMG) and galvanic skin response (GSR) to perform well [23].

Further, given the complexities of the EEG signals alongside the variability in terms of the experimental conditions, a machine learning end-to-end approach may not be feasible. Among the many limitations of such an approach includes the huge amounts of data that is required to train the classifier alongside the difficulty to validate the output. Therefore, a traditional framework to train each classifier before forming an ensemble is required, especially in domain generalization, nullifying any opportunities to allow for an end-to-end deep learning model to be framed without considering the usual pre-processing and feature extraction process when training a classifier.

It is interesting to note that SVM tops the list of classifiers used when analyzing EEG for stress detection in several review papers [5,24–26]. In fact, SVM is used in almost all the experiments when the Montreal Imaging Stress Task is used as a stressor [24]. This may be because SVM has stronger discriminatory powers than LDA, and less overfitting issues compared to neural networks. However, the field of deep learning for signal processing has been growing lately, especially the usage of pretrained CNN models for robust BCI framework [27].

Recent studies performed also involved the use of SVM classifier alongside Naïve Bayes, and K-Nearest Neighbours (KNN) achieved accuracies of up to 99.98% [28] whereby the participants were induced with stress through the performance of the Stroop Colour Word Test (SCWT). In this study, four different bands were explored, namely the alpha, beta, theta, and delta band before concluding that alpha and beta bands showed a higher accuracy than the other two. Other studies involving the use of K-NN achieved maximum classification accuracy of 91.26% [29]. However, this may be caused by the low number of participants who participated in the study. Another paper involving the use of SVM and Naïve Bayes classifier successfully classified stress and

control subjects with up to 98.21% accuracies by focusing on all the power density of the frontal lobes [30]. While both achieved high accuracies in the experiment, it should be noted that these were conducted on subject-wise classification instead of a mixed classification such as control versus mental stress. When dealing with mixed classification, the accuracies dropped to around 80%, a problem that we are trying to address in our study.

2.4. EEG Wavebands

Alpha waves range from 8 to 12 Hz where it occurs in the occipital head area in the awake state. Regular meditation and relaxation have been shown to enhance alpha waves and the reason for why it is most recommended for lowering stress. Beta waves are most frequently observed around the frontal head zones and most closely associated with stress when there is an increased in beta waves. Delta waves are found in the frontocentral brain area, and these waves are associated with tiredness and early stages of sleep. Theta band is detected in anxiety activation and strongly observed in hypervigilance states such as meditation, prayer, and awareness. Finally, Gamma band is more related to ADHD and knowledge disabilities when there is an inadequate of the activity. Although the Gamma band has been associated with depression when there's inadequate gamma signals which in turn suggests a relation between mental stress and depression, it remains a relatively unexplored area. There have been multiple findings with regards to the relation of stress and the associated wavebands. Namely the alpha, theta, and beta waves [31,32]. Gamma and Delta bands has been omitted from our experimental design as it has been found that Gamma band is more closely associated to wakefulness than in relation to stress [33]. Whereas Delta band has always been associated with slow brain activity and its occurrence is most prominent during sleep. Nonetheless, some studies have suggested the delta-beta relationship with regards to anxiety [34], a trait that is closely related to mental stress.

3. Materials and Methodology

3.1. Dataset

Twenty-two healthy individuals (ages 19 to 25) without a history of illness or head trauma make up the EEG dataset. They don't take any kind of medication that could cause their heart rate to increase. Every participant participated in both the stress and control experimental sessions. They completed the Montreal Imaging Stress Task (MIST)-based Mental Arithmetic Task (MAT) [35] as it has shown the capability of producing stress-related responses involving the hypothalamic pituitary-adrenal (HPA) axis. Accordingly, eight distinct conditions—four stress levels and four control levels—were applied to each participant based on the task's level of difficulty. Only levels 1 and 4 of stress, along with the controls that go with them, were used in this experiment; level 1 is referred to as low stress, and level 4 as high stress. 128 channels are used to record the EEG data, with a 500 Hz sampling rate. In addition, the other channels are referenced to the 129th channel. Each subject has a total of two sets of 129 channels of EEG data—one for control and one for stress. Prior to being sent to the machine learning classifier for classification, the dataset is normalized. According to the experiment's original report [10], The EEG trials lasted 2200ms for high stress and control and 1100ms for low stress and control. Therefore, averaged EEG power rather than absolute power is used to compare stress vs. control trials. EEG data from two experimental conditions—low stress versus control condition and high stress versus control condition—were analyzed.

3.2. EEG Feature Extraction

EEG features are usually divided into three broad categories, the statistical time domain features, frequency domain features, and synchronicity domain features. Statistical time domain features are obtained directly from the raw EEG signals such as calculating the average amplitudes, standard deviation, and variance. Other time domain features frequently used are Hjorth parameters, entropies estimation and Higuchi's fractal dimension. It should be noted that the raw EEG signals are usually filtered for noise and artefact removal before obtaining any features for machine learning classification. Whereas frequency domain features are usually computed by first converting the raw EEG signals that are in the time domain to the frequency domain alone by applying Fourier transforms or a time-frequency domain via wavelet transforms. Common wavelet transforms usually use Daubechies set of wavelets in the fourth order. In frequency domain features, we can obtain the power spectral density, the distribution of power in its frequency components where power is defined as the amount of energy transferred per unit time, once the raw EEG has been converted. Moreover, absolute and relative powers are commonly used to check the rhythm of EEG signals.

Next, synchronicity domain features use an effective and functional measure of brain connectivity to examine significant coincidences that appear to have no apparent reason. The energy in each frequency is obtained by applying discrete wavelet transforms and Fourier transforms, which are then added to determine the absolute power or averaged to determine the power. With 129 channels and 22 participants from the experimental and control groups, the feature matrix for each EEG frequency band was 44x129x1, yielding a minimum of 5676 (22 x 2 x 129 x 1) features.

3.2.1 Wavelet Transforms

A collection of wave-like oscillations known as wavelets is produced by wavelet transforms, which break down EEG data. Wavelets are a class of functions with a variety of characteristics, including their ability to be stretched to capture high- or low-frequency data; a stretched wavelet will typically capture data at a lower frequency. Furthermore, the function's integral must have zero mean and finite energy, and its integral squared function must yield a finite number, for a function to be considered a wavelet function. This is how wavelet differs from Fourier analysis, which assumes an infinite integral squared of a sin wave. Subsequently, the wavelet's location can be adjusted to precisely pinpoint the oscillation point. The wavelet's location and "stretch-ness" can therefore be changed as we slide it across any given signal. By doing this, the signal input can be represented by the wavelet transforms in both the time and space domains.

Traditionally, the mathematical formula is represented in (1) using the first derivative of a Gaussian function. Increasing the value "a" will stretch the wavelet to capture low frequency information. In contrast, by lowering the value, the parameter "b"

establishes the wavelet's location; a left shift is necessary, and vice versa.

$$f(x) = -(x-b)e^{\frac{-(x-b)^2/(2a^2)}{\sqrt{2\pi}a^3}} \quad (1)$$

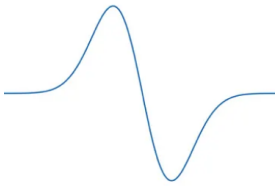


Figure 1: First Gaussian Derivative Function

Figure 2: Squishing (left) or Stretching (right) by decreasing or increasing the value of 'a'

Figure 3: Sliding the gaussian derivative left (left) or right (right) by decreasing or increasing the value of 'b'

Since a wavelet is made up of a chosen function, such as Gaussian, Harr, Daubechies, and so on, we have chosen to break down the EEG signal into sub-band frequencies using the Daubechies wavelet transform of fourth order (figure 4). This is mostly because, when compared to Haar, Morlet, and other wavelets, an EEG signal's Daubechies wavelet exhibits striking similarities to it. Moving on, we decompose the signal into 7 levels such that, in each level, half of the signal range is obtained, as shown in figure 1, where A1 to A7 is the approximate coefficient and D1 to D7 is the detailed coefficient. The sampling rate of the EEG data is set at 512 Hz.

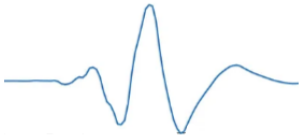


Figure 4:Daubechies Wavelet Function of the fourth order 'db4'

As a result, we can derive the EEG data's absolute power within its frequency range. To get the absolute power from all 129 channels, each of the estimated coefficients is squared before being added up. This gives us 129 channels in the alpha, beta, and theta bands, giving us three different sets of features.

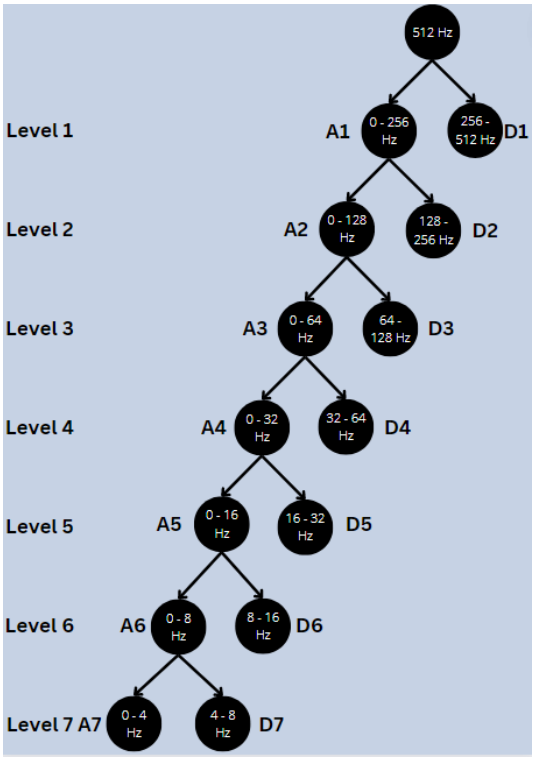


Figure 5: Wavelet Decomposition into 7 Levels

3.2.2 Fourier Transforms

Any given signal can be broken down using Fourier transforms by expanding a periodic function f(x) with an infinite sum of sines and cosines, which is a generalization of the complex Fourier series. It changes the time domain representation of the EEG data to the frequency domain. This is accomplished by using the formula in (2), where N is the number of time samples we have, n is the sample we are currently examining, x_n is the signal's amplitude at time n, k is the frequency, and X_k is the signal's amount of frequency k.

$$X_k = \sum_{n=0}^{N-1} x_n * e^{-i2\pi kn/N} \quad (2)$$

$$x_n = \frac{1}{N}\sum_{k=0}^{N-1} X_k * e^{-i2\pi kn/N} \quad (3)$$

We can determine the average power for each frequency band to be used as a feature by averaging the power obtained across the EEG dataset's sampling rate. Given that Fourier transforms data from the time domain to the frequency domain, it is limited in its applicability to time domain data. As a result, throughout the entire experimental process, we will be unable to determine when exactly the brain region responds to the stressful stimuli.

3.3. Machine Learning Classifiers

3.3.1 Support Vector Machines

A machine learning classifier called the Support Vector Machine (SVM) looks for a hyperplane in an N-dimensional space, where N is the number of features needed to clearly separate the data points. The SVM will identify the ideal hyperplane by maximizing the margins between two or more data points because there are numerous hyperplanes available to divide data points. In

order to construct the position and orientation of the hyperplane, data points that are closest to it are referred to as support vectors.

Since we are only classifying between stress and control classes, the kernel trick method suggested for non-linear dataset was not used. Consequently, MATLAB's default settings have our SVM's kernel function set to be linear, and its scale set to "automatic." The SVM's box constraint level is set to 1, and its multiclass method is configured as "One vs. One.".

3.3.2 Linear Discriminant Analysis

Linear Discriminant Analysis (LDA) is an extension of Fisher's linear discriminant, which looks for a linear feature set that clearly divides two or more classes. The multivariate Gaussian function to be used for prediction is subjected to a calculation of mean and variance when there are multiple feature variables. Plotting the data, however, is assumed by (LDA) to follow the Gaussian function in a bell-curve fashion. It also presumes that the variance around the mean of each feature variable is the same. As a result, the mean, value of each feature variable, x for each class, k, can be calculated by dividing the total number of instances by the sum of values, as shown in the following formula.:

$$\mu_k = \frac{1}{N_k * \sum x} \tag{4}$$

The variance is then calculated across each class, k as follows:

$$\sigma^2 = \frac{1}{(N-K) * \sum (x-\mu)^2} \tag{5}$$

Using the input feature x from equation (6), where pi_k is the prior probability and $f_k(x)$ is the density function, LDA will apply the Bayes Theorem to estimate the probability of the predicted output class. LDA will use Bayes Theorem to estimate the probability of the predicted output class using the input feature, x that has been given in (6) where is the prior probability and is the density function.

$$P(Y = k \mid X = x) = \frac{pi_k f_k(x)}{\sum_{l=1}^{K} pi_k f_k(x)} \tag{6}$$

The default implementation of LDA from MATLAB's classification learner app was used whereby the covariance structure is set as "full".

3.3.3 Decision Tree

A decision tree is conceptualized as a tree root with numerous branches that eventually grow into leaves at the tip. But decision trees are illustrated in reverse, with the root at the top. This means that after applying a starting condition and a given value, the tree may split into branches based on a splitting criterion, ultimately leading to a final output at the leaf. Decision tree splitting criteria are typically based on the ecological diversity index, which provides a quantitative representation of the various species or classes within a dataset.

The Simpson index, on which the Gini's diversity index is based, gauges the concentration levels when people are categorized into types such that the following probabilities apply when two people are randomly selected from the dataset to represent the same type:

$$\lambda = \sum_{i=1}^{R} p_i^2 \tag{7}$$

Where R is the total number of classes in the dataset. Gini's diversity index transforms equation (5) to capture the probability that the two individual data represent different types from the following equation:

$$1 - \lambda = 1 - \sum_{i=1}^{R} p_i^2 = 1 - \frac{1}{^2D} \tag{8}$$

MATLAB's preset for a fine tree to model our decision tree such that the maximum number of splits is set at 100 while the split criterion is based on Gini's diversity index.

3.3.4 Artificial Neural Network

Artificial neural networks (ANN) are based on the idea of biological neural networks of the brain. Just as a biological neural network consists of the firing of neurons interconnected with synapses, ANN would generally consist of a few layers with connected neurons to simulate the human brain. Mainly, the first layer is known as the input layer as it receives external data as an input. The following layer is the hidden layer that obtains the raw information from the input layer and processes it by applying weights to the inputs and subsequently directs them through an activation function as the output. Finally, the output from the hidden layer is passed to the final layer known as the output layer where the ultimate result such as classifying between stress and non-stress is determined. Most ANNs allow for weight adjustments of the hidden layers by computing the gradient of the loss function with respect to its individual weight. To simplify our experimental set up for neural network models, we decided to use narrow neural network as preset by MATLAB's built in function whereby there is only one fully connected layer with the first layer size of 10 and the activation function of ReLU.

3.4. Machine Learning Framework

We extract the absolute and average power features from the collected data using the Fourier and Daubechies wavelet transforms. Next, we'll feed it into the four machine learning classifiers (SVM, LDA, DT, and NN) that were previously mentioned. Next, the dataset is divided using the ten-fold cross-validation method, which divides the training data into ten distinct subsets, or folds, with 90% of the data in each fold being used for training and the remaining 10% for validation. To get the expected validation accuracy, this is done ten times over. Lastly, ten independent trials are used to train and validate each model to determine the average accuracy, which is displayed in the results section.

4. Experimental Setup, Results and Discussion

MATLAB R2022a was used to develop our machine learning classifiers through the help of the classification learner application using a Windows 10 Operating System running with 8GB RAM and 11th Generation Intel® Core @ 2.40GHz.

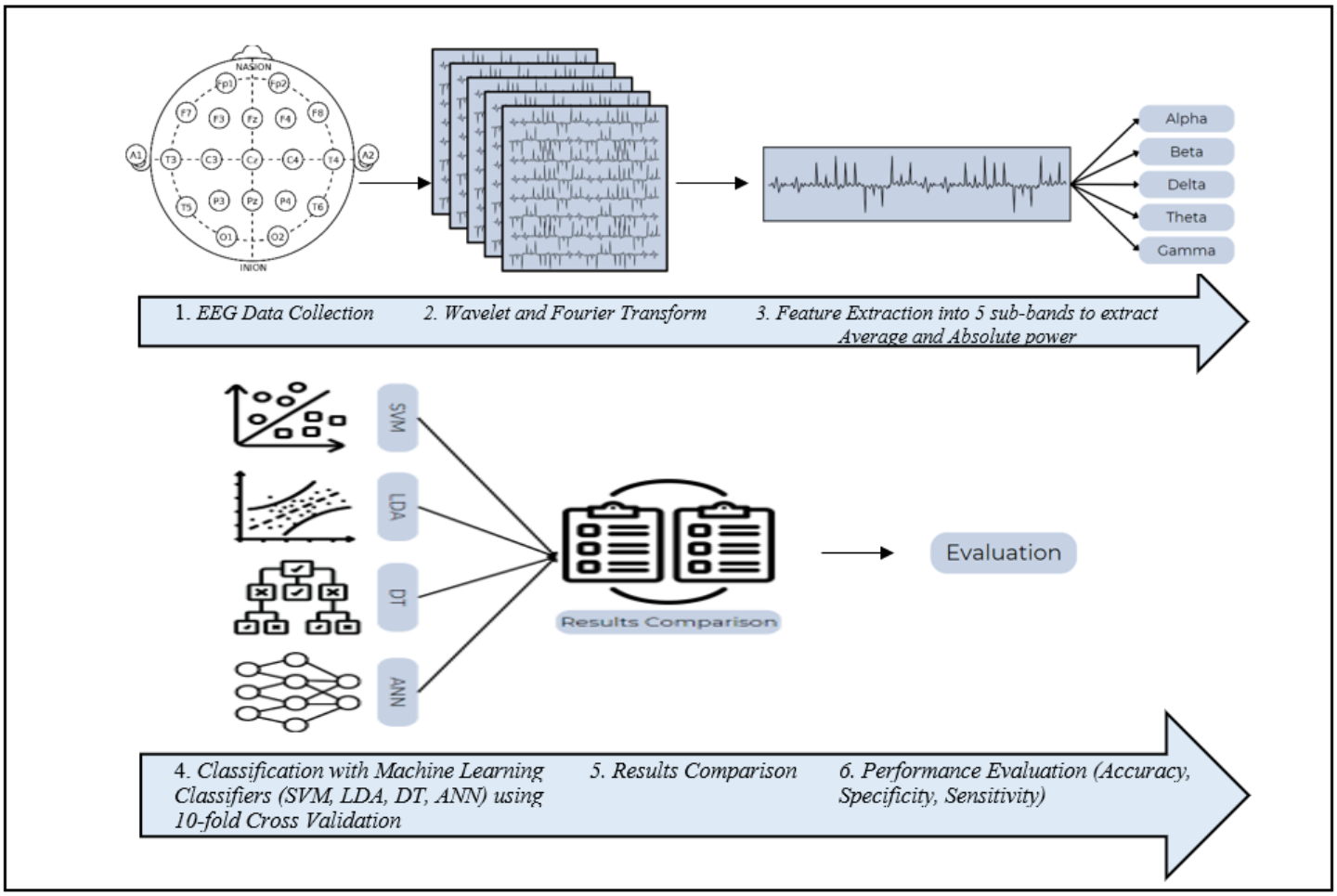


Figure 6: Proposed Machine Learning Framework

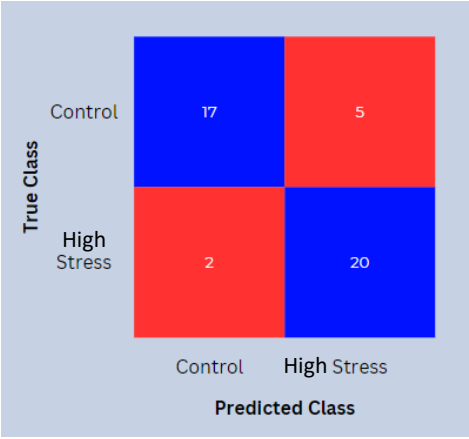


Figure 7 a: Sample of Confusion Matrix in Number of Participants

A fair assessment and evaluation are required to determine the usefulness and accuracy of the model. To validate the performance of the model, we have computed the accuracy, sensitivity and specificity of each model using the following equations in (5, 6, 7) based on the confusion matrix from figure 7. True Positive (TP) is used to denote correctly predicted cases while True Negative (TN) is used to denote correctly predicted non-cases. Likewise, False Positive (FP) and False Negative (FN) denotes incorrectly predicted cases and non-cases respectively. A sample of the confusion matrix is shown in figures 7a and 7b respectively where the control group is compared to stress such as low stress or high stress.

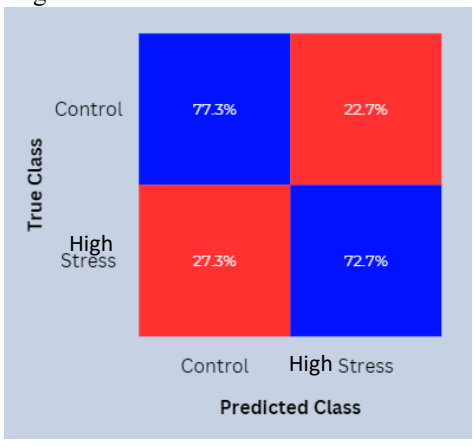


Figure 7 b: Sample of Confusion Matrix in Percentages

4.1. Accuracy

The accuracy of the classifier is denoted by the percentage of true positive (first quadrant) and true negative (fourth quadrant) over the total sum of true positive, true negative, false positive and false negative.

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (9)$$

4.2. Sensitivity

The sensitivity of a classifier is the percentage of correctly predicted cases (True Positives – first quadrant) over the sum of the true positives and false negatives (first and third quadrant).

$$Sensitivity = \frac{TP}{TP+FN} \quad (10)$$

4.3. Specificity

The specificity of a classifier is the percentage of correctly predicted non-cases (True Negatives – fourth quadrant) over the sum of the true negatives and false positives (fourth and second quadrant).

$$Specificity = \frac{TN}{TN+FP} \quad (11)$$

4.4. Standard Deviation

The standard deviation of each result mentioned is calculated based on formula (12) to indicate the average range of values obtained in 10 trials whereby a small standard deviation value tells us that the accuracy/sensitivity/specificity achieved does not deviate too far from the average value obtained. This is also an indication in our evaluation of whether the classifier performs in a stable manner instead of an erratic manner.

$$Standard\ Deviation = \sqrt{\frac{\sum(x_i-\mu)^2}{N}} \quad (12)$$

The rest of this section is arranged in the order of the type of machine learning classification used, followed by the experimental conditions of either control vs low stress or control vs high stress and a comparison between low stress vs high stress. Each table shows the result of the averaged validation accuracy, sensitivity, specificity, band spectrum and features used for each classification. Associated alongside is the standard deviation of the model after performing 10 trials. Finally, the best-performing features combination is bolded in each table. Given that absolute power was only used for comparison between stress and control of the same levels, it is not used in different levels as shown in control vs high stress and low stress vs high stress conditions.

Table 1: Support Vector Machine Classifier Results

Support Vector Machine Classification				
Control VS Low Stress				
Validation Accuracy (%)	***Sensitivity (%)***	***Specificity (%)***	***Band Spectrum***	***Features***
64.99±2.32	65.79±2.08	60.69±1.21	Alpha	Absolute Power
65.00±3.39	65.62±6.20	58.96±3.29	Theta	Absolute Power
67.05±3.26	72.38±10.42	63.45±5.12	Alpha, Theta	Absolute Power
65.92±3.53	72.79±6.40	63.39±3.16	Alpha, Theta, Beta	Absolute Power
Control VS High Stress				
82.03±1.24	92.69±2.28	75.13±1.97	Alpha	Average Power
86.83±2.64	**94.61±0.23**	**83.10±2.60**	**Theta**	**Average Power**
82.88±1.24	91.80±2.68	76.36±2.33	Beta	Average Power
84.10±2.69	94.07±0.16	77.54±1.55	Beta, Theta	Average Power
Low Stress VS High Stress				
59.09±3.52	39.11±6.49	79.10±2.20	Beta	Average Power
72.95±4.01	66.82±8.12	79.10±2.20	Alpha	Average Power
69.54±5.38	70.00±7.94	69.07±3.96	Theta	Average Power
73.64±3.81	**74.54±5.45**	**72.72±2.88**	**Beta, Theta**	**Average Power**

Table 2: Linear Discriminant Analysis Classifier Results

Linear Discriminant Analysis Classification				
Control VS Low Stress				
Validation Accuracy (%)	***Sensitivity (%)***	***Specificity (%)***	***Band Spectrum***	***Features***
71.15±2.88	71.84±4.18	67.39±3.54	Alpha	Absolute Power
51.14±7.47	59.02±5.15	56.14±3.83	Theta	Absolute Power
73.19±5.16	80.82±4.60	71.19±2.33	Alpha, Theta	Absolute Power
75.91±1.82	80.77±5.08	67.34±2.93	Alpha, Theta, Beta	Absolute Power
47.74±4.55	51.62±4.42	51.2±3.18	Alpha	Average Power
72.95±5.50	72.48±2.39	69.04±1.97	Theta	Average Power
64.60±3.50	61.82±2.48	62.88±4.00	Alpha, Theta, Beta	Average Power
85.01±2.74	**93.25**±3.26	**79.53**±3.66	**Alpha, Theta, Beta**	**Absolute Power, Average Power**
Control VS High Stress				
71.82±3.81	73.70±5.89	70.45±3.46	Alpha	Average Power
68.41±4.14	72.32±6.12	68.04±3.34	Theta	Average Power
78.17±3.08	82.19±1.61	70.04±2.97	Beta	Average Power

Linear Discriminant Analysis Classification				
Control VS Low Stress				
Validation Accuracy (%)	***Sensitivity (%)***	***Specificity (%)***	***Band Spectrum***	***Features***
82.53±3.22	**86.08±4.90**	**77.83±2.65**	**Beta, Theta**	**Average Power**
Low Stress VS High Stress				
81.14±4.70	**72.27±8.75**	**90.02±4.46**	**Beta**	**Average Power**
63.43±7.49	67.26±8.33	59.53±10.1	Alpha	Average Power
63.18±3.49	61.35±5.48	64.98±6.13	Theta	Average Power
79.54±3.21	75.01±5.83	84.10±2.30	Beta, Theta	Average Power

Table 3: Decision Tree Classifier Results

Decision Tree Classification				
Control VS Low Stress				
Validation Accuracy (%)	***Sensitivity (%)***	***Specificity (%)***	***Band Spectrum***	***Features***
51.82±4.52	48.09±4.34	47.21±5.87	Alpha	Absolute Power
52.73±7.31	52.48±4.29	53.08±5.27	Theta	Absolute Power
54.57±3.81	52.91±5.35	53.46±5.33	Alpha, Theta	Absolute Power
58.88±3.11	56.32±5.12	58.14±7.26	Alpha, Theta, Beta	Absolute Power
47.73±4.55	49.00±7.71	49.60±12.78	Alpha	Average Power
62.30±6.67	**63.32**±2.91	**59.38**±2.73	**Theta**	**Average Power**
61.83±5.35	51.23±5.59	50.61±4.27	Alpha, Theta, Beta	Average Power
59.78±3.37	54.48±7.17	54.31±6.75	Alpha, Theta, Beta	Absolute Power, Average Power
Control VS High Stress				
70.92±3.92	68.76±4.19	73.85±3.34	Alpha	Average Power
89.99±2.32	90.1±2.28	90.46±2.19	Theta	Average Power
92.95±3.13	94.81±6.61	93.28±3.07	Beta	Average Power
94.55±2.52	**95.64±6.39**	**92.14±3.70**	**Beta, Theta**	**Average Power**
Low Stress VS High Stress				
54.54±5.65	52.73±6.48	57.27±7.09	Beta	Average Power
67.98±2.37	**61.80±2.20**	**74.09±4.11**	**Alpha**	**Average Power**
61.57±8.53	67.72±10.24	55.44±13.3	Theta	Average Power
61.83±4.96	67.26±6.69	56.35±6.15	Beta, Theta	Average Power

Table 4: Artificial Neural Network Classifier Results

Artificial Neural Network Classification				
Control VS Low Stress				
Validation Accuracy (%)	***Sensitivity (%)***	***Specificity (%)***	***Band Spectrum***	***Features***
60.22±3.09	58.62±5.15	61.79±4.17	Alpha	Absolute Power
62.73±4.58	56.34±5.46	69.09±6.37	Theta	Absolute Power
71.37±3.55	65.45±5.07	77.27±5.38	Alpha, Theta	Absolute Power
70.69±5.60	67.27±6.03	74.10±6.75	Alpha, Theta, Beta	Absolute Power
42.73±2.66	41.82±6.98	43.65±5.44	Alpha	Average Power
68.65±3.91	68.18±7.04	69.09±5.69	Theta	Average Power
58.40±4.99	54.09±6.56	62.71±6.37	Alpha, Theta, Beta	Average Power
76.59±4.76	**79.99±9.59**	**73.18±5.17**	**Alpha, Theta, Beta**	**Absolute Power, Average Power**
Control VS High Stress				
74.32±2.29	75.69±2.07	72.99±4.45	Alpha	Average Power
81.35±2.46	84.56±3.64	78.18±4.46	Theta	Average Power
85.46±2.54	85.93±2.46	85.02±3.55	Beta	Average Power
86.83±1.34	**83.65±3.03**	**90.00±1.80**	**Beta, Theta**	**Average Power**
Low Stress VS High Stress				
64.38±1.43	63.63±4.54	65.13±3.52	Beta	Average Power
67.68±2.85	72.73±3.52	62.62±5.31	Alpha	Average Power
76.36±3.10	**76.81±5.95**	**75.92±2.01**	**Theta**	**Average Power**
73.64±2.58	71.91±7.16	76.37±2.61	Beta, Theta	Average Power

5. Discussion

The results show that we can effectively classify between low stress and control and high stress and control by using the average and absolute power in the alpha, theta, and beta bands. We expanded the experimental setup even further to compare high and low stress levels while utilizing an artificial neural network as a fourth classifier. Notably, as table I, II, III, and IV demonstrate, the absolute power feature by itself does not perform well across all classifiers. For the most part, however, average power works better as a feature than other combinations of features and bands; this is not the case for LDA, which needs a combination of features from the theta band's average power and the alpha and beta bands' absolute power in order to improve the classifier's performance.

According to a previous report, in the low stress condition, the average power obtained from the theta band using Fourier transforms analysis consistently performed better across all classifiers. This is in line with previous studies that propose using theta range oscillations as a tool to identify mental illnesses and markers of mental stress [31,36]. Furthermore, all three of the initial classifiers demonstrated a significant increase in classification accuracy between high stress and control, averaging

87% ((86.83 + 82.53 + 94.55)/3) for SVM, 82.53% for LDA, and 94.55% for DT. The accuracy falls between 50% and 75% when there is less stress and control. This is expected given the strong similarities between the low levels of stress and control in terms of brain region activation. Surprisingly, the LDA classifier outperforms the other classifiers in this condition, achieving an accuracy of 85% in the classification between low stress and control by aggregating the Alpha, Theta, and Beta bands in table II. In contrast, DT performs better than all other classifiers—including LDA—in the second condition of control vs. high stress. But LDA performs better than the other classifier once more when it comes to the final condition of low stress vs. high stress. Except in the second case, LDA outperforms the other classifier in general. However, because LDA has a simpler discriminatory power to classify between two classes linearly, it did not perform significantly worse than DT, staying above the 80% range.

Although it has been suggested that Alpha and Theta bands correlates to mental stress and cognitive workload [31,36], studies have suggest the capabilities of Beta waves associated to stress [37] as well. This explains the surprising effects of aggregating the average power from the beta band to the Theta band in the control VS high-stress condition as it has been shown that beta band is used as a dynamic marker for stress assessment [32,38]. Further, our results point to the fact that alpha band waves from average or absolute power features do not perform as well generally compared to beta and theta features. This is likely because alpha waves are often correlated to awake states where further and more distinctive pre-processing methods to further segment alpha wave bands is needed to use it as a feature for stress detection.

It is therefore very likely that future research will call for the reduction of such channels in order to prevent noisy data from being used as a feature by classifiers. Furthermore, we discovered that the validation accuracy for individual Alpha and Theta waves absolute power classification using SVM is 68% and 71% when utilizing only 13 channels, specifically those from the parietal, frontal, and temporal lobes. This yields an accuracy that is comparable to, and in the case of Alpha waves, better than, using 129 channels. We further hypothesize that, since a decision tree has low discriminatory power, reducing its features should be able to achieve higher accuracy because it won't overfit the classification model like other classifiers like SVM and LDA tend to do. Nevertheless, this will be examined in later research when examining the classification of stress and control using decision trees. Furthermore, since we only have 22 subjects in our dataset, our findings are not indicative of the whole population. Larger dataset samples will be needed for future research in order to properly extrapolate our findings to other populations.

Moving on, the results produced from the neural network classifier are comparatively well given that we only used the minimum settings provided by MATLAB's toolbox extension. To be able to perform with accuracies of 76% to 86% suggests that fine-tuning the hyperparameters of the neural network and the implementation of a search strategy will aid the improvement of the results. Moreover, genetic algorithm such as swarm optimization can be implemented in addition to usual search strategies such as was done in [39] to detect emotional stress.

Additionally, there are studies involving the use of alpha asymmetry and the frontal region of the brain to determine the presence of stress. These are then used in a neurofeedback system to train people how to better manage their stress [40]. The authors also suggested the potential use of gaming simulation to better alleviate stress among university students, providing a good platform for future works regarding this.

The overall sensitivities and specificities of the best performing models tend to classify the participants as stressed compared to control. Finally, our result is comparable to the original author's dataset and its classification with our proposed features and classifiers where linear regression and naïve bayes classifiers were used to obtain accuracies from 75% to 83% [10] whilst ours ranged from 68% to 83% with SVM, LDA, DT and ANN classifiers. One aspect to consider in our slightly underperforming accuracies could be caused by the lack of features used as the original author had use absolute powers, relative powers, coherence, amplitude asymmetry and phase lag. Furthermore, our study only used three sets of features, alpha, beta, and theta to achieve the reported accuracies. This contrasts with another study using four sets of features whereby the delta waveband is included to achieve 99.98% accuracy [28]. However, it should be emphasized that the accuracy reported in this study drops to around 80% when looking at mixed classification (between stress and control) as opposed to subject-wise classification, providing a useful platform for further studies. Our future work intends to focus on the usage of singular value decomposition (SVD) to obtain the features of all the channels with minimal loss of information and possibly the use of PCA-enabled classifiers for dimensionality reduction of features.

6. Conclusion

We have successfully shown the usefulness and effectiveness of classifying mental stress states from control conditions using alpha, theta, and beta waves with the LDA, SVM, DT and ANN classifiers of up to 95% accuracy. This is in line with existing work to suggest the usage of the potential application of discrete wavelet transform with Machine Learning classifiers for EEG extraction and classification of mental states efficiently. The proposed framework based on wavelet transform shows significant potential for mental stress assessment, which could be further improved for developing a Computer-Aided Diagnosis (CAD) technique for automatic mental assessment in the future.

Conflict of Interest

The authors declare no conflict of interest.

Acknowledgment

This research work was supported from the University of Nottingham, Malaysia. The authors, therefore, acknowledge that there is no potential conflict of interest in the experiment conducted.

References

[1] M. Esler, Mental stress and human cardiovascular disease, Neuroscience and Biobehavioral Reviews, **74**, 269–276, 2017, doi:10.1016/j.neubiorev.2016.10.011.

[2] M.F. Marin, C. Lord, J. Andrews, R.P. Juster, S. Sindi, G. Arsenault-Lapierre, A.J. Fiocco, S.J. Lupien, Chronic stress, cognitive functioning and mental health, Neurobiology of Learning and Memory, **96**(4), 583–595, 2011, doi:10.1016/j.nlm.2011.02.016.

[3] E. Blix, A. Perski, H. Berglund, I. Savic, "Long-Term Occupational Stress Is Associated with Regional Reductions in Brain Tissue Volumes," PLoS ONE, **8**(6), 2013, doi:10.1371/journal.pone.0064065.

[4] M. Nagendran, Y. Chen, C.A. Lovejoy, A.C. Gordon, M. Komorowski, H. Harvey, E.J. Topol, J.P.A. Ioannidis, G.S. Collins, M. Maruthappu, "Artificial intelligence versus clinicians: Systematic review of design, reporting standards, and claims of deep learning studies in medical imaging," The BMJ, **368**, 2020, doi:10.1136/bmj.m689.

[5] S. Gedam, S. Paul, A Review on Mental Stress Detection Using Wearable Sensors and Machine Learning Techniques, IEEE Access, **9**, 84045–84066, 2021, doi:10.1109/ACCESS.2021.3085502.

[6] D. Kamińska, K. Smółka, G. Zwoliński, "Detection of mental stress through EEG signal in virtual reality environment," Electronics (Switzerland), **10**(22), 2021, doi:10.3390/electronics10222840.

[7] V. Sulimova, D. Windridge, S. Bukhonov, V. Mottl, Quick breast cancer detection via classification of evoked EEG potentials in the mammologist's brain.

[8] H.U. Amin, W. Mumtaz, A.R. Subhani, M.N.M. Saad, A.S. Malik, "Classification of EEG signals based on pattern recognition approach," Frontiers in Computational Neuroscience, **11**, 2017, doi:10.3389/fncom.2017.00103.

[9] H.U. Amin, A.S. Malik, N. Badruddin, W.T. Chooi, "Brain behavior in learning and memory recall process: A high-resolution EEG analysis," in IFMBE Proceedings, Springer Verlag: 683–686, 2014, doi:10.1007/978-3-319-02913-9_174.

[10] A.R. Subhani, W. Mumtaz, M.N.B.M. Saad, N. Kamel, A.S. Malik, "Machine learning framework for the detection of mental stress at multiple levels," IEEE Access, **5**, 13545–13556, 2017, doi:10.1109/ACCESS.2017.2723622.

[11] S. Cohen, T. Kamarck, R. Mermelstein, A Global Measure of Perceived Stress, 1983.

[12] T.H. Holmes, R.H. Rahe$, THE SOCIAL READJUSTMENT RATING SCALE"?, Pergamon Press, 1967.

[13] S.H. Lovibond, P.F. Lovibond, "Manual for the Depression Anxiety Stress Scales," in Psychology Foundation, 1995.

[14] A.S. Zigmond, R.P. Snaith, "The Hospital Anxiety and Depression Scale," Acta Psychiatrica Scandinavica, **67**(6), 361–370, 1983, doi:10.1111/j.1600-0447.1983.tb09716.x.

[15] C. Spielberger, R. Gorsuch, R. Lushene, P.R. Vagg, G. Jacobs, Manual for the State-Trait Anxiety Inventory (Form Y1 – Y2), 1983.

[16] J.E. Dise-Lewis, The Life Events and Coping Inventory: An Assessment of Stress in Children, 1988.

[17] T. Pereira, P.R. Almeida, J.P.S. Cunha, A. Aguiar, "Heart rate variability metrics for fine-grained stress level assessment," Computer Methods and Programs in Biomedicine, **148**, 71–80, 2017, doi:10.1016/j.cmpb.2017.06.018.

[18] S. Betti, R.M. Lova, E. Rovini, G. Acerbi, L. Santarelli, M. Cabiati, S. Del Ry, F. Cavallo, "Evaluation of an integrated system of wearable physiological sensors for stress monitoring in working environments by using biological markers," in IEEE Transactions on Biomedical Engineering, IEEE Computer Society: 1748–1758, 2018, doi:10.1109/TBME.2017.2764507.

[19] A. Barreto, J. Zhai, M. Adjouadi, Non-intrusive Physiological Monitoring for Automated Stress Detection in Human-Computer Interaction, 2007.

[20] S. Cozma, L.C. Dima-Cozma, C.M. Ghiciuc, V. Pasquali, A. Saponaro, F.R. Patacchioli, "Salivary cortisol and α-amylase: Subclinical indicators of stress as cardiometabolic risk," Brazilian Journal of Medical and Biological Research, **50**(2), 2017, doi:10.1590/1414-431X20165577.

[21] S.M.U. Saeed, S.M. Anwar, H. Khalid, M. Majid, U. Bagci, "EEG based classification of long-term stress using psychological labeling," Sensors (Switzerland), **20**(7), 2020, doi:10.3390/s20071886.

[22] L.D. Sharma, R.K. Saraswat, R.K. Sunkaria, "Cognitive performance detection using entropy-based features and lead-specific approach," Signal, Image and Video Processing, **15**(8), 1821–1828, 2021, doi:10.1007/s11760-021-01927-0.

[23] J. Minguillon, E. Perez, M.A. Lopez-Gordo, F. Pelayo, M.J. Sanchez-Carrion, "Portable system for real-time detection of stress level," Sensors (Switzerland), **18**(8), 2018, doi:10.3390/s18082504.

[24] R. Katmah, F. Al-Shargie, U. Tariq, F. Babiloni, F. Al-Mughairbi, H. Al-Nashash, A review on mental stress assessment methods using eeg signals, Sensors, **21**(15), 2021, doi:10.3390/s21155043.

[25] S.S. Panicker, P. Gayathri, A survey of machine learning techniques in physiology based mental stress detection systems, Biocybernetics and Biomedical Engineering, **39**(2), 444–469, 2019, doi:10.1016/j.bbe.2019.01.004.

[26] S. Lotfan, S. Shahyad, R. Khosrowabadi, A. Mohammadi, B. Hatef, "Support vector machine classification of brain states exposed to social stress test using EEG-based brain network measures," Biocybernetics and Biomedical Engineering, **39**(1), 199–213, 2019, doi:10.1016/j.bbe.2018.10.008.

[27] M.T. Sadiq, M.Z. Aziz, A. Almogren, A. Yousaf, S. Siuly, A.U. Rehman, "Exploiting pretrained CNN models for the development of an EEG-based robust BCI framework," Computers in Biology and Medicine, **143**, 2022, doi:10.1016/j.compbiomed.2022.105242.

[28] Y. Badr, F. Al-Shargie, U. Tariq, F. Babiloni, F. Al Mughairbi, H. Al-Nashash, "Classification of Mental Stress using Dry EEG Electrodes and Machine Learning," in 2023 Advances in Science and Engineering Technology International Conferences, ASET 2023, Institute of Electrical and Electronics Engineers Inc., 2023, doi:10.1109/ASET56582.2023.10180884.

[29] M. Maruf Hossain Shuvo, T. Rahman, A. Kumer Ghosh, M. Mostafizur Rahman, Mental Stress Recognition using K-Nearest Neighbor (KNN) Classifier on EEG Signals, 2015.

[30] O. AlShorman, M. Masadeh, M.B. Bin Heyat, F. Akhtar, H. Almahasneh, G.M. Ashraf, A. Alexiou, "Frontal lobe real-time EEG analysis using machine learning techniques for mental stress detection," Journal of Integrative Neuroscience, **21**(1), 2022, doi:10.31083/j.jin2101020.

[31] S.A. Awang, P.M. Pandiyan, S. Yaacob, Y.M. Ali, F. Ramidi, F. Mat, "Spectral density analysis: theta wave as mental stress indicator," in Communications in Computer and Information Science, 103–112, 2011, doi:10.1007/978-3-642-27183-0_12.

[32] H.M. Díaz, F.M. Cid, J. Otárola, R. Rojas, O. Alarcón, L. Cañete, "EEG Beta band frequency domain evaluation for assessing stress and anxiety in resting, eyes closed, basal conditions," in Procedia Computer Science, Elsevier B.V.: 974–981, 2019, doi:10.1016/j.procs.2019.12.075.

[33] E.T. Attar, Review of electroencephalography signals approaches for mental stress assessment, Neurosciences, **27**(4), 209–215, 2022, doi:10.17712/nsj.2022.4.20220025.

[34] K.L. Poole, B. Anaya, K.E. Pérez-Edgar, "Behavioral inhibition and EEG delta-beta correlation in early childhood: Comparing a between-subjects and within-subjects approach," Biological Psychology, **149**, 2020, doi:10.1016/j.biopsycho.2019.107785.

[35] K. Dedovic, R. Renwick, N. Khalili Mahani, V. Engert, S.J. Lupien, J.C. Pruessner, K. Mahani, P. -Douglas, The Montreal Imaging Stress Task: using functional imaging to investigate the effects of perceiving and processing psychosocial stress in the human brain, 2005.

[36] T. Okonogi, T. Sasaki, "Theta-Range Oscillations in Stress-Induced Mental Disorders as an Oscillotherapeutic Target," Frontiers in Behavioral Neuroscience, **15**, 2021, doi:10.3389/fnbeh.2021.698753.

[37] Universiti Teknologi MARA. Faculty of Electrical Engineering, IEEE Control Systems Society. Chapter Malaysia, Institute of Electrical and Electronics Engineers, Proceedings : 2015 6th IEEE Control and System Graduate Research Colloquium (ICSGRC 2015) : 10 - 11 August 2015, Shah Alam, Malaysia : Faculty of Electrical Engineering, Universiti Teknologi MARA, Shah Alam, Malaysia.

[38] W. Junaidee bin Wan Hamat, H. Majdi bin Ishak, K. Hashikura, T. Suzuki, K. Yamada, Detection of Anxiety Expression From EEG Analysis Using Support Vector Machine.

[39] D. Shon, K. Im, J.H. Park, D.S. Lim, B. Jang, J.M. Kim, "Emotional stress state detection using genetic algorithm-based feature selection on EEG signals," International Journal of Environmental Research and Public Health, **15**(11), 2018, doi:10.3390/ijerph15112461.

[40] Y. Hafeez, S.S.A. Ali, R.A. Hasan, S.H. Adil, M. Moinuddin, M. Ebrahim, M.S.B. Yusoff, H. Amin, U. Al-Saggaf, "Development of Enhanced Stimulus Content to Improve the Treatment Efficacy of EEG-Based Frontal Alpha Asymmetry Neurofeedback for Stress Mitigation," IEEE Access, **9**, 130638–130648, 2021, doi:10.1109/ACCESS.2021.3114312.

ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 8, No. 6, 57-64 (2023)

www.astesj.com

Special Issue on Innovation in Computing, Engineering Science & Technology

ASTESJ

ISSN: 2415-6698

Comparative Study of J48 Decision Tree and CART Algorithm for Liver Cancer Symptom Analysis Using Data from Carnegie Mellon University

Renhe Chi*

Department of Management Information Systems, National Chengchi University, Taipei,116 Taiwan

ARTICLE INFO

Article history:
Received:22 August, 2023
Accepted:22 October, 2023
Online: 30 November, 2023

Keywords:
Liver Cancer
Machine learning
J48(Gain ratio)
CART

ABSTRACT

Liver cancer is a major contributor to cancer-related mortality both in the United States and worldwide. A range of liver diseases, such as chronic liver disease, liver cirrhosis, hepatitis, and liver cancer, play a role in this statistic. Hepatitis, in particular, is the main culprit behind liver cancer. As a consequence, it is decisive to investigate the correlation between hepatitis and symptoms using statistic inspection. In this study, we inspect 155 patient data possessed by CARNEGIE-MELLON UNIVERSITY in 1988 to prognosticate whether an individual died from liver disease using supervised machine learning models for category and connection rules based on 20 different symptom attributes. We compare J48 (Gain Ratio) and CART (Classification and Regression Tree), two decision tree classification algorithms elaborate from ID3 (Iterative Dichotomiser 3), with the Gini index in a Java environment. The data is preprocessed through normalization. Our study demonstrates that J48 outperforms CART, with an average accuracy rate of nearly 87% for the complete specimen, cross-validation, and 66% training data. However, CART has the supreme accurate rate in all samples, with an accuracy rate of 90.3232%. Furthermore, our research indicates that removing the conjunction attribute of the Apriori algorithm does not impact the results. This research showcases the potential for physician and researchers to apply brief machine learning device to attain accurate outcomes and develop treatments based on symptoms.

1. Introduction

This paper is an extension of work originally presented in 4th IEEE Eurasia Conference on Biomedical Engineering, Healthcare and Sustainability 2022 (IEEE ECBIOS 2022) under the name of "Comparison of Decision Tree J48 and CART in Liver Cancer Symptom with CARNEGIE MELLON UNIVERSITY Data" [1].

In the year 2020, liver cancer affected more than 900,000 individuals globally, leading to over 830,000 deaths. It ranks sixth among the top ten cancers worldwide and is the primary cancer in the United States [2]. Accordingly, it is crucial to conduct research on the expression of symptoms in adult liver cancer to facilitate clinical intervention. Previous research on symptoms for Liver Carcinoma and Cancer have provided valuable insights, with physical searches of article references yielding additional findings [3]. Logic-based approach such as supervised models, including linear regression, decision trees, association learning algorithms such as Random Forest and Generalized Boosting Machines, and Support Vector Machines (SVM), are commonly employed in this field. SVMs use a polynomial kernel function and a non-probabilistic approach [4]. Decision trees are an example of a prognostic model that maps entity attributes and values. Each intersection in the tree represents an entity, each bifurcation path represents a potential attribute value, and each leaf intersection correlate with the entity value appear for by the direction from the root junction to the leaf junction. Although decision trees have a single output, multiple trees can be utilized to handle various outputs. This technology is commonly utilized in data mining [5].

In the field of liver cancer, decision tree models can be employed to categorize patients based on their symptoms and forecast the possibility of developing liver cancer or their prognosis post-diagnosis. Decision tree models can also be combined with other machine learning algorithms to enhance precision and credibility [6].

APRIORI algorithms like Random Forest and Generalized Boosting Machines are frequently utilized supervised models for liver cancer prediction [7]. Random Forest is a decision tree-based association learning technique that establish multiple decision

*Corresponding Author: Renhe Chi, 108356503@nccu.edu.tw

https://dx.doi.org/10.25046/aj080607

trees and returns the approach of the class predictions from individual trees [8]. On the other hand, Generalized Boosting Machines is an iterative algorithm that constructs a strong model by combining several weak models, with each weak model aiming to rectify the errors of the previous one [9].

2. Previous work

This section presents an overview of the main machine learning techniques utilized in the analysis of the Hepatitis dataset obtained from CARNEGIE-MELLON University in 1988, as part of the Statlog project. The outcomes of the analysis, performed with and without 10-fold cross-validation, are combined into a consolidated form for the purpose of comparison and assessment.

Table 1: The analysis outcome of hepatitis data provided major from Statlog project

Reference	Year	Method	Accuracy %	With 10 fold
Kemal Polat and Salih Güneş [10]	2007	PCA+AIRS	94.12%	Yes
Statlog project (KG) [8]	1994	21-NN, stand Manhattan	90.3	No
Statlog project (RA) [8]	1994	FSM	90	No
Statlog project (KG) [8]	1994	14-NN, stand. Euclid	89	No
Weiss & K [11]	1990	LDA	86.4	No
Weiss & K [11]	1990	CART (decision tree)	82.7	No
Weiss & K [11]	1990	MLP+backprop	82.1	No
Duch & Grudzinski [12]	1998	Weighted 9-NN	92.9± ?	Yes
Duch & Grudzinski [12]	1998	18-NN, stand. Manhattan	90.2±	Yes
Rafa Adamczak [13]	1995	FSM with rotations	89.7± ?	Yes
Karol Grudzinski [12]	1998	15-NN, stand. Euclidean	89.0±	Yes
Rafa Adamczak [13]	1995	FSM without rotations	88.5	Yes
Stern & Dobnikar [14]	1996	LDA, linear discriminant analysis	86.4	Yes
Stern & Dobnikar [14]	1996	Naive Bayes and Semi-NB	86.3	Yes
Norbert Jankowski [15]	1999	IncNet	86	Yes
Stern & Dobnikar [14]	1996	QDA, quadratic discriminant analysis	85.8	Yes
Stern & Dobnikar, std added by WD [14]	1996	1-NN	85.3± 5.4	Yes
Stern & Dobnikar [14]	1996	ASR	85	Yes
Stern & Dobnikar [14]	1996	Fisher discriminant analysis	84.5	Yes
Stern & Dobnikar [14]	1996	LVQ	83.2	Yes
Stern & Dobnikar [14]	1996	CART (decision tree)	82.7	Yes
Stern & Dobnikar [14]	1996	MLP with BP	82.1	Yes
Stern & Dobnikar [14]	1996	ASI	82	Yes
Stern & Dobnikar [14]	1996	LFC	81.9	Yes
Rafa Adamczak [12]	1995	RBF (Tooldiag)	79	Yes
Rafa Adamczak [12]	1995	MLP+BP (Tooldiag)	77.4	Yes

This study presents a comprehensive comparative analysis of machine learning methods conducted by various authors, including M. Ramassamy, S. Selvaraj, M. Mayilvaganan, and Bascil & Temurtas. Notable methodologies include PCA+AIRS with 94.12% accuracy rate by Kemal Polat and Salih Güneş [10]. Other accuracy rates including 21-NN (stand. Manhattan) with 90.3%, FSM with 90% and 14-NN with 89% by Statlog project, and LDA with 86.4%, CART (decision tree) with 82.7%, and MLP+backprop by Weiss & K with 82.1% [11]. Duch & Grudzinski applied Weighted 9-NN with 92.9%±?, 18-NN (stand. Manhattan) with 90.2±0.7, and 15-NN (stand. Euclidean) with 89.0±0.5% [12], while Rafa Adamczak employed FSM with rotations with 89.7±? and FSM without rotations with 88.5% [13]. Stern & Dobnikar utilized a diverse set of methods, including LDA (linear discriminant analysis) with 86.4% accuracy rate, Naive Bayes and Semi-NB with 86.3%, 1-NN (stand. added by WD) with 85.3%±5.4, ASR with 85%, Fisher discriminant analysis with 84.5%, LVQ with 83.2%, CART (decision tree) with 82.7%, MLP with BP with 82.1%, ASI with 82%, and LFC with 81.9% [14]. Norbert Jankowski implemented IncNet with 86% accuracy rate [15]. These findings collectively contribute valuable insights into the efficacy of distinct machine learning approaches for addressing statistical learning challenges. Within the framework of the Statlog project, machine learning methodologies have demonstrated substantial efficacy in analyzing Hepatitis data, with the PCA+AIRS model outperforming others, achieving an accuracy rate of 94.12%.

Data Mining is getting increasingly important for discovering association patterns for health service innovation and Customer Relationship Management (CRM) etc. Yet, there are deficits of existing data mining techniques. First of all, most of them perform a plain mining based on a predefined schemata through the data warehouse; however, a re-scan must be done whenever new attributes appear. Second, an association rule may be true on a certain granularity but fail on a smaller one and vise verse. Last but not least, they are usually designed to find either frequent or infrequent rules. In this paper, we are going to invent more efficient and accurate approach with novel data structure and multi-dimensional mining algorithm to explore association patterns on different granularities [16] [17].

The paper presents at first the categories of innovative healthcare services as well as the way to find new service patterns. Then, we propose a data mining approach based on Apriori Algorithm for managing such new healthcare services, including a novel data structure and an effective algorithm for multi-dimensional mining association rules on various granularities. It is proved to be very useful for discovering new service patterns, even in-frequent by considering a dimension in a flat level. The advantages of this approach over existing approaches include (1) more comprehensive and easy-to-use (2) more efficient with limited scans (3) more effective with finding rules hold in different granularity levels, e.g. Age={(1-10), (10-20)….} (4) capable of finding frequent patterns and infrequent patterns, for instant we use the algorithm in finding the blood platelet frequently used for the female with age over 60, while the blood platelet infrequently for all the patients. With this method, users can choose the full match and the relaxed match (5) low information loss rate (6) capable of incremental Mining.

3. Data pre-processing

3.1. Field attributes

The majority of the primary dataset comprises symptom information, and therefore, the values in the range are predominantly binary (i.e., negative or positive). The dataset comprises 6 numeric and 14 categorical attributes, amongst the Class attribute is ranked in accordance with the form presented in reference [18].

3.2 Data pre-processing

a. Attribute analysis

Upon importing the raw data, an intrinsic attribute analysis was conducted utilizing the WEKA software to scrutinize the data pertaining to each attribute. [19].

Table 2: Hepatitis symptoms selected by Carnegie Mellon University

	Attributes	Content	Attribute Type	Range
1	Class	Survive and Die	Nominal	(die and live)
2	Age	Age Division	Numeric	(10~80)
3	Sex	Gender Distinction	Nominal	(male and female)
4	Steroid	Steroid	Nominal	(no, yes)
5	Antivirals	Anti-Viral Drug	Nominal	(no, yes)
6	Fatigue	Fatigue	Nominal	(no, yes)
7	Malaise	Depressed	Nominal	(no, yes)
8	Anorexia	Anorexia	Nominal	(no, yes)
9	Liver Big	Enlarged Liver	Nominal	(no, yes)
10	Liver Firm	Liver Currhosis	Nominal	(no, yes)
11	Spleen palpable	Enlarged Spleen	Nominal	(no, yes)
12	Spiders	Arachnoid Membrane(Spider Nervus)	Nominal	(no, yes)
13	Ascites	Ascites	Nominal	(no, yes)
14	Varices	Venous Flexion	Nominal	(no, yes)
15	Bilirubin	Bilirubin	Numeric	0.39, 0.80, 1.20, 2.00, 3.00, 4.00
16	Alk phosphate	Alkaline Phosphatase	Numeric	33, 80, 120, 160, 200, 250
17	Sgot	Aminotransferase	Numeric	13, 100, 200, 300, 400, 500,
18	Albumin	Albumin	Numeri	2.1, 3.0, 3.8, 4.5, 5.0, 6.0

b. Data preprocessing

Prior to data analysis, data preparation is a necessary step which involves data preprocessing and data reduction. The primary goal of data preprocessing is to address impure, incomplete or inconsistent data within the original dataset. Meanwhile, data reduction aims to decrease the volume or dimensionality of the initial data, for the purpose of alleviate the burden of data exploration. The significance of data preparation is demonstrated in the following scenarios: Firstly, the data may contain noise, such as errors or outliers resulting from issues with data collection equipment, human or computer errors during data recording or transmission, etc. Secondly, the data may be incomplete, with some attribute values missing due to reasons such as unnecessary data being excluded during recording or inconsistent records being deleted. Finally, inconsistency may also arise when the same data has multiple conflicting conditions, for instance, when the data is integrated from various sources with different naming conventions.

Data conversion is a critical step in data preprocessing that seeks to transform missing or inaccurate data into a compatible format for the exploration process. This research utilized four distinct preprocessing techniques, namely data discretization, data extreme value handling, data standardization, and data normalization, to enhance the quality of the data.

- Discretization of data

In order to absolve impoverished classification quality, continuous data is discretized to reduce the numerical allocation of the information.

- Data standardization

To normalize attribute data values and bring them into a minor and consistent range with other attribute data, various techniques can be used, such as Min-Max standardization, z-score standardization, and decimal standardization. The diagram below illustrates the attribute analysis of the initial data after standardization.

- Data normalization

Normalization is a data processing technique used to adjust the data values to a common scale or range. This is done to make the data comparable and reduce the impact of different measurement units or scales on data analysis. For instance, when comparing the annual income of customers in Taiwan and the Philippines, it is not appropriate to directly compare the income levels in Taiwan dollars, as the average income in Taiwan is much higher than that in the Philippines. Therefore, normalization is used to redistribute the data into a small and specific range, which allows for objective and meaningful comparisons.

The aforementioned data processing was carried out utilizing the configurations provided by WEKA.

c. Data reduction

Data reduction is a crucial technique that involves reducing the size or dimensions of data without significantly impacting the exploration outcomes. The main object of data reduction is to ease the burden of data exploration, reduce computation time, improve prediction accuracy, and enhance exploration outcomes' quality by removing irrelevant or unnecessary data. Information Gain, Gini Index, and $\chi 2$ independence test are common characteristic selection criteria used in data reduction. In this research, Information Gain is used as the attribute selection standard to remove attributes with the lowest direction gain value to prepare for the J48 data classification method in WEKA (Waikato Environment for Knowledge Analysis). Information Gain measures the difference between the information quantity before

and after a test, represented by the entropy value of the sub-decision tree (Entropy), which is the entropy value of the set produced by a junction with a particular characteristic as the conclusion number. However, Information Gain-based attribute selection may be biased towards attributes with more attributes, resulting in biased decisions. To address this issue, the Gain Ratio method normalizes the Information Gain by dividing it by the number of possible attribute values, preventing bias towards attributes with more qualitative attributes.

By using the conducting analysis, it was observed that attribute 9 and attribute 10 exhibit the lowest information gain and gain ratio. Consequently, these two attributes are eliminated to diminish the data dimensionality. Subsequent to data reduction, the data preprocessing procedures, comprising data discretization, standardization, and regularization, are implemented anew to finalize the data preprocessing stage.

4. Data analysis:

4.1. Classification

4.1.1. Decision tree

In the realm of machine learning, a decision tree is an example used to predict a mapping connection between characteristic and their respective values. Each junction in the tree denotes a task, and every branching path indicates a feasible characteristic value. The terminal nodes correspond to the values of the objects represented by the paths from the root junction to the terminal junctions. A decision tree has a solitary output, and to address multiple outputs, distinct decision trees can be constructed. Decision trees are a frequently employed approach in data mining for the purpose of analyzing and predicting data.

- Categorical decision tree: target variable is categorical

Categorical decision tree examination is a machine learning tactic used when the target variable is categorical in nature, such as predicting the species of a plant or the likelihood of a customer to purchase a product. This approach is implemented using various algorithms, including ID3, C4.5 (J48), and C5.0.

- Regression decision tree: target variable is continuous

Regression decision tree analysis involves the use of decision trees to predict continuous numerical values, such as the temperature or stock price. It is a widely used technique in data analysis and machine learning. Several algorithms can be used to implement regression decision tree analysis, such as CART, CHAID (Chi-Square Test), MP (multivariate polynomial) and C4.5 (Gain Ratio).

a. J48 Algorithm

J48 is a decision tree algorithm that is based on the C4.5 implementation. The creator of C4.5 later upgraded the algorithm to C4.8, which was then implemented in Java by the creators of Weka and named J4.8. The ID3 algorithm must be introduced first because the C4.5 algorithm is an improved version of ID3.

During the construction of the decision tree, the ID3 algorithm uses Information Gain as the criterion to select the attribute with the highest information gain value as the classification attribute. This algorithm is based on the principle of Occam's razor, which states that the smaller the decision tree, the preferable the exhibition. However, the ID3 algorithm is a heuristic algorithm and may not always produce the smallest tree structure. Moreover, one of the issues with ID3 is its bias towards attributes with multiple values. For example, if there is a distinctive recognition characteristic such as an ID, ID3 may choose it as the splitting characteristic. Although this creates a sufficiently clean section, it is nearly futile for classification purposes. To address this problem, the C4.5 algorithm, which is the successor of ID3, employs the gain ratio information obtain extension to reduce this bias.

b. C4.5:

C4.5 is a set of algorithms frequently utilized in machine learning and data mining for classification tasks. Specifically, its purpose is to perform supervised learning, where a dataset contains tuples characterized by attribute values and each tuple belongs to one of several exclusive categories. The aim of C4.5 is to construct a mapping function from the attribute values to categories that can be used to classify new instances with unknown categories.

J. Ross Quinlan proposed C4.5 as an extension of the ID3 algorithm, which is used to construct decision trees. A decision tree is a tree-like structure similar to a flowchart, where each internal node presents an attribute exam, each branch presents an exam outcome, and each leaf node reserves a class label. After the decision tree is constructed, an unclassified tuple can be traversed from the root node to a leaf node, which stores the predicted class label for the tuple. Decision trees are advantageous because they do not postulate any prior estate expertise or guideline settings and are appropriate for investigative comprehension discovery.

C4.5 overcomes the problems of ID3 by adopting the gain ratio of attributes, which normalizes the information gain by computing the break knowledge value of the virtue. In the C4.5 algorithm, the break apart virtue selection process does not solely rely on the virtue with the supreme gain ratio. Instead, it searches for attributes that have a direction obtain higher than the standard level among the candidate separation virtue, and then choice the virtue with the supreme gain ratio. This is because gain ratio tends to favor attributes with smaller values compared to information gain.

C4.5 has several improvements over ID3. Firstly, it can handle continuous attributes. Secondly, it uses gain ratio to overcome ID3's bias towards attributes with many distinct values but little significance. This is because the guidance obtain measure used by ID3 inclines to select virtue with many distinct values, which can lead to the creation of suboptimal decision trees. For example, if

the algorithm divides the data based on a unique attribute like student ID, it would generate numerous branches, each with only one or a few instances, resulting in a high information gain value but a meaningless split.

Table 3: J48 Results Comparison Table

Attribute	Accuracy Rate
Whole samples	90.3226%
Cross Validation	84.5161%
66% Training data	81.1321%

4.1.2. The principle of CART algorithm

As previously stated, the CART algorithm comprises two stages, and in the first stage, a binary tree is constructed recursively. The question then arises: how is the data divided?

In the field of machine learning and data mining, the CART algorithm is often employed for classification tasks, where each data point is assigned to one of several exclusive categories based on a selected attribute. The algorithm divides the multidimensional space recursively into non-overlapping rectangular regions through a process that involves selecting independent variables and partitioning the space based on the values of the selected variable. The procedure is duplicated circularly on each of the resulting areas until the entire space is covered by non-overlapping regions.

The standard for dividing the space is an important consideration in the CART algorithm. For variable attributes, the dividing point is typically determined as the middle between a pair of endless variable virtue values. The amount of adulteration that can be reduced by dividing on each attribute is then calculated and used to sort the attributes. The decrease of adulteration is explicit as the aggregate of the amount of adulteration before separates minus the amount of adulteration at each node after division. The Gini index is routinely accustomed to as a method for measuring adulteration. Gini impurity measures the probability that a given node represents a certain class, and it is minimized when all samples in the node belong to the same class.

The core concept of the CART algorithm is to recursively classify data based on a minimum distance-based Niki index estimation function. One of the main benefits of the algorithm is its simple and easy-to-understand rule extraction process. Moreover, the CART algorithm is robust against issues such as missing values and a large number of variables, making it a widely used and effective tool in machine learning and data mining.

Algorithm limitations: attribute selection is restricted to generating only two child nodes; error rate may increase rapidly with a large number of categories.

Application domains: identification of information distortion, identification of potential customers in the telecommunications industry, prediction of loan risks, and others.

c. J48 VS CART

The fundamental distinction between CART and J48 algorithms lies in the criterion used to split the nodes. CART adopts the GINI index to measure the purity of data partitions or training datasets when choosing a splitting attribute. The GINI index quantifies the purity of a sample based on the likelihood of it belonging to a specific category. Consequently, the attribute that results in the minimum GINI index is selected for division.

Table 4: CART Results Comparison Table

Attribute	Accuracy Rate
All samples	90.3226%
Cross-Validation	84.5161%
66% of Samples	81.1321%

Table 5: Classification results analysis

Algorithm	Pre-process	Test mode	Accuracy Rate
J48	Normalization	Whole sample	87.0968%
J48	Normalization	Cross Validation	85.1613%
J48	Normalization	66% Training data	88.6792%
CART	Normalization	Whole sample	90.3226%
CART	Normalization	Cross Validation	94.5161%
CART	Normalization	66% Training Data	81.1321%

4.2. Association Law (APRIORI)

Within a vast bibliography, interrelationships among specific purposes exist, commonly referred to as Market Basket Analysis, which originated from analyzing the extent of conjunction of sizeable itemsets in merchandise case data. This analysis utilizes the law of association, frequently used in the study of shopping baskets, to examine the correlation between purchased products in customer acquire data recorded by the POS system. An exemplary illustration of the law of association is the well-known paradigm of the correlation between beer and diapers.

Association rules can be conveyed in the form of X => Y [Support, Confidence], where T={t1, t2, …, tm} represents the set of all items, X⊂T, Y⊂T, and X∩Y=Φ. Here, X and Y denote unique data item sets in the transaction set T, indicating that if X emerge, Y may also emerge concomitantly. The assist of an association rule X Y in T, performed by support (X Y) = P(X Y) = s, is the ratio of agreement including X∩Y to all agreement in T. The accreditation of an association rule X Y in T, served by

confidence (X Y) = P (Y|X) = c, is the ratio of agreements including X∩Y to agreements including X in T. The values of support and confidence range between 0 and 1.

An item set (itemset) refers to a collection of distinct items, such as {A, B, C} in a record, which can produce the item group {A}, {B}, {C}, {A, B}, {B, C}, {A, C}, {A, B, C}. If there are n items in the item set, the item group comprises 2n-1 items. Therefore, when managing a large number of items, the item group can be extensive.

The support (Support) of an item set in the database is the frequency of the item set in the database, typically denoted by Support (X), where X is itemset. For instance, if a database has 100 transaction records, and 40 of them indicate the purchase of milk, then the support of this item set is 40/100=40%. The higher the support, the more crucial the item set is for further exploration.

Confidence (Confidence) signifies the level of trust between two itemsets and is represented by the conditional probability that Y will appear under the probability of X appearing, usually expressed as Support (X∩Y) /Support (X), where X and Y are itemsets.

In the realm of data mining, a robust association rule is characterized by X => Y, a rule that can be established in the transaction set T if it satisfies two conditions: support (A => B) >= min_sup and confidence (A => B) >= min_conf, where min_sup and min_conf indicate the minimum thresholds for support and confidence, respectively. When both of these criteria are met, the rule X => Y is deemed a robust association rule within the transaction set T.

In evaluating association rules, two critical criteria must be met:

The rule should identify unanticipated and unintended associations.

The rule should be capable of making an impact.

One well-known algorithm for generating association rules is Apriori. It employs a bottom-up, iterative approach to identify high-frequency item sets by breading and examination applicant item sets. From these high-frequency item sets, the algorithm identifies useful association rules.

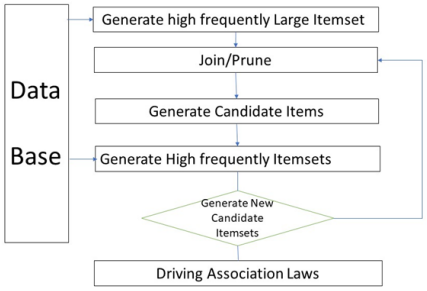


Figure 1: The Apriori algorithm

The Apriori algorithm involves two main steps:

Discovering Large itemsets from the transaction items in the database

The goal is to identify frequent Large itemsets, which requires repeated searches of the database. As Large itemsets have the property that all of their subsets are also frequent, the algorithm generates new sub-itemsets using join and prune operations.

Generating association rules based on the discovered Large itemsets

The Large itemsets obtained in step one are used to derive meaningful association rules. A rule is considered meaningful only if its confidence exceeds the minimum confidence threshold (Min Confidence).

Apriori algorithm process:

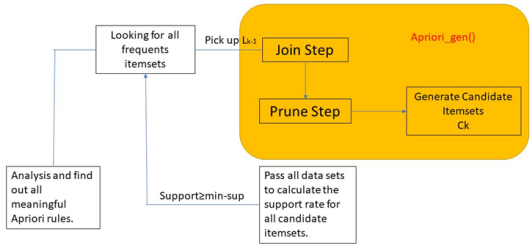


Figure 2: The Apriori process diagram

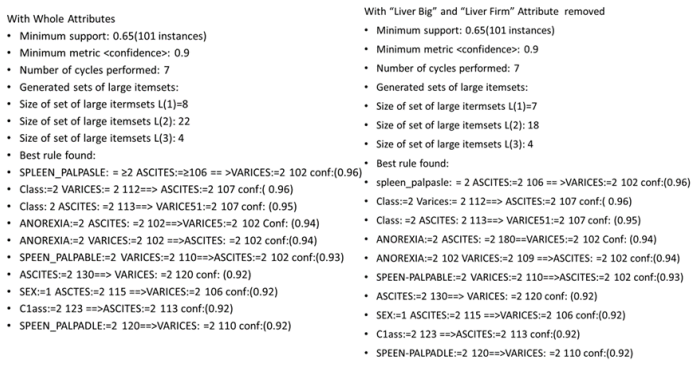


Figure 3: The Apriori result before and after "Liver big" and "Liver Firm" attribute removed.

In the APRIORI algorithm, the first pass through the database is employed to determine the Large 1-itemsets.

For subsequent passes, the algorithm is composed of two stages:

- In the first stage, the Apriori-gen function is utilized to generate new candidate itemsets Ck from the previously discovered Large itemsets Lk-1.

- In the second stage, the database is examined to calculate the Support value of the candidate itemsets in Ck.

The following is the result of the APRIORI algorithm based on our data, before removing “Liver Big” and “Liver Firm” in the APRIORI attribute.

Based on the two datasets provided and the outcomes of the association analysis, it is discernible that a substantive correlation between the "Liver Big" and "Liver Firm" attributes and other pertinent attributes appears to be lacking. The findings are expounded as follows:

In the initial dataset, encompassing both the "Liver Big" and "Liver Firm" attributes, the derived association analysis results are expounded as follows:

The cardinality of the generated large itemsets: L(1)=8, L(2)=22, L(3)=4

Optimal rules identified: Diverse rules, exemplified by instances such as spleen_palpable≥2, Ascites≥106 → Varices=2 conf:(0.96), and comparable formulations.

Conversely, upon the exclusion of the "Liver Big" and "Liver Firm" attributes from the dataset, the ensuing association analysis outcomes are delineated as follows:

The cardinality of the generated large itemsets: L(1)=7, L(2)=18, L(3)=4

Optimal rules identified: Analogous to those observed in the primary dataset, including instances like spleen_palpable=2, Ascites=2 → Varices=2 conf:(0.96), alongside other commensurate rules.

In light of these results, the following rationales can be adduced:

Scarcity of Substantive Rules: In both datasets, conspicuous absence of significant rules directly associating the "Liver Big" and "Liver Firm" attributes with other attributes is noticeable. This indicates a limited propensity for these two attributes to interact significantly with the remaining attributes in the datasets.

Attribute Sparse Occurrence: The rare occurrence of instances wherein the "Liver Big" and "Liver Firm" attributes co-occur with other attributes might be attributed to data scarcity. This scarcity may engender challenges in discerning robust associations between these attributes.

Threshold Specification: The stipulated thresholds for minimum support and confidence, set at 0.65 and 0.9 respectively, might inadvertently sift out associations characterized by lower frequencies and confidence levels. Given the presumed low-level associations of "Liver Big" and "Liver Firm" attributes, adherence to the specified thresholds could preclude their inclusion in the derived association rules.

Data Profile Dynamics: The outcomes are also liable to be influenced by data profile intricacies and distribution patterns. In instances where the "Liver Big" and "Liver Firm" attributes do not manifest as prominent co-occurring features within the dataset, the association analysis might struggle to identify substantial relationships.

In summation, predicated on the proffered datasets and the contextual framework of the association analysis, the dearth of observable significant associations between the "Liver Big" and "Liver Firm" attributes and other pertinent attributes is discernible. This, however, does not conclusively imply a universal lack of connection; rather, it underscores the paucity of apparent associations within the existing conditions and dataset parameters.

5. Discussion and future study

This investigation is fundamentally grounded in the amelioration of machine learning techniques, as opposed to adopting traditional statistical methods. Additionally, it has been observed that mixed methods generally yield higher accuracy levels, thereby substantiating the selection of J48 and the Gini index-based CART algorithm as apt methodologies for this particular study.

It is imperative to acknowledge that both machine learning and AI are continuously evolving fields, and with access to an augmented sample size and the elucidation of additional attributes, there is a potential for even more exemplary performance and a more meticulous analysis.

The Apriori analysis conducted revealed a low correlation between the attributes "Liver Big" and "Liver Firm," indicating that their removal does not impact the final results significantly. For analyzing relationships such as the variations in age groups, we recommend employing our Multi-dimensional Multi-granularities Data Mining based on the Apriori Algorithm. This approach enables the segmentation of patient ages into various granularities, specifically {(10-20), (20-30), …, (70-80)}. Subsequently, we can mine for association patterns within these defined segments, ensuring that phenomena pertinent to children do not get erroneously associated with adults. However, upon constructing data cubes for age ranges (10-20), (60-70), and (70-80), we may uncover associations within these specific segment combinations or granularities.

6. Conclusion

The consolidation of machine learning with the therapeutic realm presents numerous advantages, such as an improved understanding of disease characteristics and the potential to aid healthcare providers in developing more efficient treatment strategies for patients. Machine learning finds application in diverse areas within the medical sector, not just limited to the employment of qualitative and quantitative material categorization to draw inferences, and association rules to establish links between manifestation. For example, in the domain of oncology, machine learning is utilized in supervised therapeutic photo and quantitative data-based congregate to determine if a tumor is hostile. Furthermore, deep learning and computer vision technologies aid in detecting brain tumors. These advancements are indicative of the maturing machine learning

applications in medical treatment. With easily accessible tools, physicians and researchers can obtain precise results and prescribe appropriate medication for symptom management, while the principle population can adopt this knowledge to prevent and improve recognize diseases. The medical field anticipates the emergence of additional machine learning and data mining utilization in the future, extending beyond the treatment of hepatitis.

References

[1] J. K. Chiang and R. Chi, "Comparison of Decision Tree J48 and CART in Liver Cancer Symptom with CARNEGIE-MELLON UNIVERSITY Data," 2022 IEEE 4th Eurasia Conference on Biomedical Engineering, Healthcare and Sustainability (ECBIOS), Tainan, Taiwan, 28-31, 2022, doi: 10.1109/ECBIOS54627.2022.9945039.

[2] Liver cancer deaths in 2020 approaching incidence, https://www.cn-healthcare.com/articlewm/20210115/content-1180778.html.

[3] M. E. Cooley, "Symptoms in adults with lung cancer: A systematic research review," Jounal of Pain and Symptom Management, **19**(2), February, 2000.

[4] C. M. Lynch, "Prediction of lung cancer patient survival via supervised machine learning MARK classification techniques," International Journal of Medical Informatics 108, 1-8, 2017.

[5] Z. Mahmoodabai, S. S. Tabrizi, "A new ICA-Based algorithm for diagnosis of coronary artery disease," Intelligent Computing, Communication and Devices, **2**, 415-427, 2014.

[6] Datasets used for classification comparison of results. https://www.is.umk.pl/~duch/projects/projects/datasets.html#Hepatitis

[7] M. Hegland, The APRIORI Algorithm—A Tutorial, https://www.worldscientific.com/doi/abs/10.1142/9789812709066_0006

[8] D. Michie, D.J. Spiegelhalter, C.C. Taylor, "Machine Learning, Neural and Statistical Classification," Ellis Horwood Series in Artificial Intelligence: New York, NY, USA, **13**, 1994.

[9] S. Touzani, J. Granderson, S. Fernandes, "Gradient boosting machine for modeling the energy consumption of commercial buildings," Energy and Buildings, 158(1533-1543), 2018, doi: 10.1016/j.enbuild.2017.11.039

[10] K. Polat, S. Güneş, "Hybrid prediction model with missing value imputation for medical data, Expert Systems with Applications," **42**(13), 5621-5631, 2015

[11] S.M. Weiss, I. Kapouleas, "An empirical comparison of pattern recognition, neural nets and machine learning classification methods," Department of Computer Science, Rutgers University, New Brunswick, NJ 08903, 1989

[12] W. Duch, K. Grudzi´nski, "Weighting and selection of features," Intelligent Information Systems VIII, Proceedings of the Workshop held in Ustro´n, Poland, 1999

[13] N Jankowski, A Naud, R Adamczak, "Feature Space Mapping: a neurofuzzy network for system identification,", Department of Computer Methods, Nicholas Copernicus University, Poland, 1995

[14] B. Stern and A. Dobnikar, "Neural networks in medical diagnosis: Comparison with other methods," Proceedings of the International Conference EANN, **96**, 427-430, 1996.

[15] Norbert Jankowski, "Approximation and Classification in Medicine with IncNet Neural Networks," Department of Computer Methods Nicholas Copernicus University ul. Grudziądzka 5, 87-100, Toruń, Poland, 1999

[16] J. K. Chiang, C. C. Chu, "Multi-dimensional multi-granularities data mining for discovering innovative healthcare services," Journal of Biomedical Engineering and Medical Imaging, **1**(3), 214, DOI: 10.14738/jbemi.13.243

[17] J. K. Chiang, C. C. Chu, "Multidimensional multi-granularities data mining for discover association rule," Transactions on Machine Learning and Artificial Intelligence, **2**(3), 2014.

[18] Hepatitis Data Set. https://archive.ics.uci.edu/ml/datasets/Hepatitis

[19] Weka website. https://www.cs.waikato.ac.nz/~ml/weka/.

Advances in Science, Technology and Engineering Systems Journal Vol. 8, No. 6, 65-77 (2023)

www.astesj.com

ASTESJ

ISSN: 2415-6698

Design of Bio-Inspired Robot Hand Using Multiple Types of Actuators

Traithep Wimonrut, Jittaboon Trichada, Narongsak Tirasuntarakul*, Eakkachai Pengwang

Institute of Field Robotics, King Mongkut's University of Technology Thonburi, Bangkok, 10140, Thailand

ARTICLE INFO

Article history:
Received:14 August, 2023
Accepted:14 November, 2023
Online: 30 November, 2023

Keywords:
Robotics hand
Multiple types of actuators
Hand gestures

ABSTRACT

Many prosthetic hands are focused on appearance and grip strength, however, gestures are also one of the performances that users need for communicating with others as body language to express their feeling and intention. For this paper, the initial prototype of the gesturing robotics hand is presented by using multiple types of actuators concept to maintain its appearance while the number of degrees of freedom (DOFs) is increased. The gesture performance of this robotic hand is improved by designing 2 DOFs in each finger; therefore, the entire hand has 15 joints, 10 DOFs, and one controllable wrist joint. In the detail of the design, all actuating mechanisms of 3 joints for each finger are specifically designed to maintain the human limb appearance. The Distal Phalange joint (DIP) used a linkage mechanism to acquire the Proximal Phalange joint's (PIP) movement by a 1:0.961 ratio due to appearance designed. The PIP joint is built with a cable-drive mechanism powered by a digital servo motor installed in the forearm. The Metacarpal joint (MCP) is driven by a micro linear actuator in the hand palm. A micro linear actuator was also selected to drive the wrist of the robot. The hand can perform 10 hand gestures follow common emoji hand gestures and holding 12 objects in the hand. The design of this bio inspired robot hand can be downloaded for educational purpose.

1. Introduction

This paper has been developed from "Design of an Open-Source Anthropomorphic Robotic Finger for Telepresence Robot" [1] to become a hand and forearm. As a big picture of the project is to develop the telepresence robot that can present the human feeling between the operator who controls a robot and participant who interactives with robot. From the study and research of various types of robotic hands, it can be divided into two major developments. The first is a robotic hand that was developed for the articulate arms, which focus on the performance to pick up objects in different ways. Generally, a number of controllable hands joints is more or equal to the number of human hands. However, the appearance is not a focus point for this type, for example, "The DLR hand arm system" [2], "Shadow Dexterous Hand E1 Series" [3], and many of the robotics hands in "A Review of Anthropomorphic Robotic Hand Technology and Data Glove Based Control" paper [4]. The second is robotic hands used for disabilities people also known as prosthetic hands. Most prosthetic hands have appearances like human beings. However, the number of controllable joints that is reduced to 5 DOFs for 1 hand such as "Dextrus V2.0" [5], "Limbitless" [5], or even reduce the moveable joint such as "Michelangelo Hand" [6] in order to reduce the volume and suitable for users. In many cases, a hand gesture for the prosthetic hands can be created with just an open bare hand and the grip for the fist posture. Some prosthetic hand has 2 joints in each finger which is Metacarpo Phalangeal Joint (MCP) as a drive joint, Proximal Interphalangeal Joint (PIP) as an under actuated joint, and Distal Interphalangeal Joint (DIP) Joint as a fixed joint. Each finger can be controlled by 1 or 2 actuators like a "Prosthetic hand from Touch Bionics" [7], and "Bebionic Prosthetic Hand" [8] which has been developed up to present. Researchers intend to design a prototype of robotic hand that has an appearance like a prosthetic hand to keep the participant feeling like communicating with human while remaining a controllable joint as a robotics hand for the operator to have a controllable joint equally to the human hand joint. As a result, In the constrained appearance, the hand has more natural movement more than normal prosthetic hands with 2 actuated joint drives and 1 under actuated linkage joint. This hand can be used to communicate by using a common hand sign to express the meaning of the operator and also has the capacity to hold daily used objects. The prototype hand as shown in Figure 1. It is mostly built from a 3D printer. The researcher intends to share this 3D model with those who are interested in further development.

*Corresponding Author: N. Tirasuntarakul, KMUTT, Bangkok, 10140, Thailand, (+66)961462235 narongsak.tir@kmutt.ac.th

https://dx.doi.org/10.25046/aj080608

Figure 1: Hand and Forearm Compared Between Robot and Dorsal Side (Left) and Ventral Side (Right).

2. Design Methodology

Given the significance of appearance, the design prioritized size considerations. The hand, along with the forearm, was segmented into seven main components, namely the fingers, palm, metacarpal thumb, wrist, forearm, Dynamixel box, and cover plate, as shown in Figure 2. The dimensions and specifics of each part are detailed below.

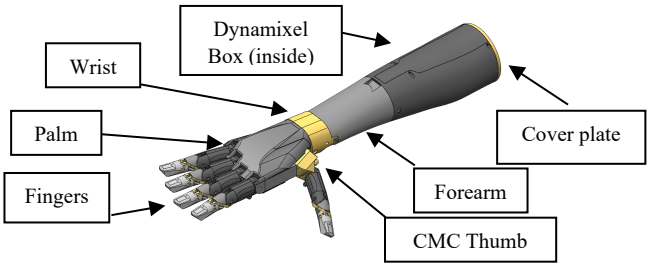


Figure 2: 3D Model of Robotics Hand and Forearm.

2.1. Fingers

The initial finger design utilized cables to control joint movement, with 10 rotary actuators located in the forearm, each dedicated to a specific joint. To flex or extend the PIP joint, tension is applied to the tendons linked to the DIP joint. This transmits force through the linkage, coordinating the movement of both joints. The tendon path from the actuator to the DIP joint passes through the PIP joint. The upper path extends the PIP joint, while the lower path flexes the PIP joint. However, for the tendon to pass through the upper part of the PIP joint, the linkage must have a cavity in its middle, potentially reducing its strength, as shown in Figure 3.

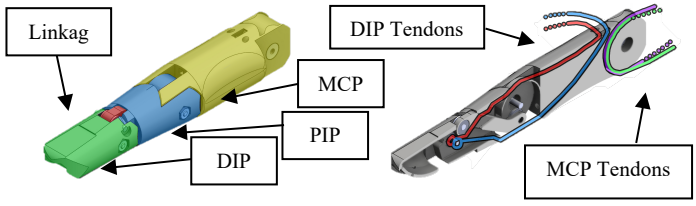


Figure 3: Initial Finger Design.

To improve the appearance of the forearm and create a more natural arm-like shape, modifications were made to the finger design. Specifically, the MCP joint was modified from a cable drive to support a linear actuator hinge drive. This refinement allowed for the preservation of five rotary actuators for cable drive, while the remaining five rotary actuators were replaced with linear actuators directly connected to their respective joints. Furthermore, the original 4-bar linkage system in the middle of the finger was reconfigured to a dual linkage system. In this design, the center axis of the Proximal Interphalangeal joint (PIP) is redesigned as a circular channel to support the tendon traction with a constant radius as shown in Figure 4.

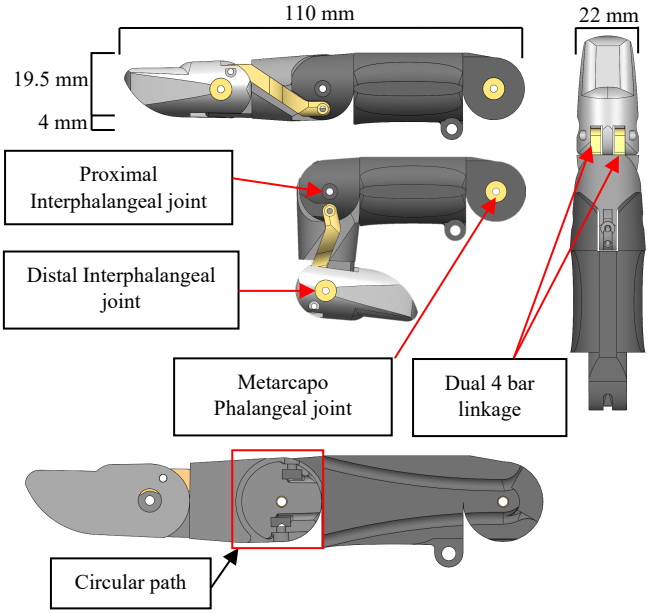


Figure 4: 3D Model Finger

Thumb, Index, Middle, Ring, and little fingers use the same models for convenience of maintenance and to reduce the time of printing parts. The MCP joints of the Index, Middle, Ring, and little fingers are attached with linear actuator PQ12-R 30:1 gear ratio with 20 mm stroke. When fully extended, these joints align with the palm, whereas when the linear actuator is completely retracted, the MCP joint flexes down to an angle of 77.59 degrees. This angle arises due to the position of the cylinder upon retraction. The linear actuator is designed to ensure that it fits as closely as possible to the palm, thus enabling convenient attachment via screwing. as shown in Figure 5.

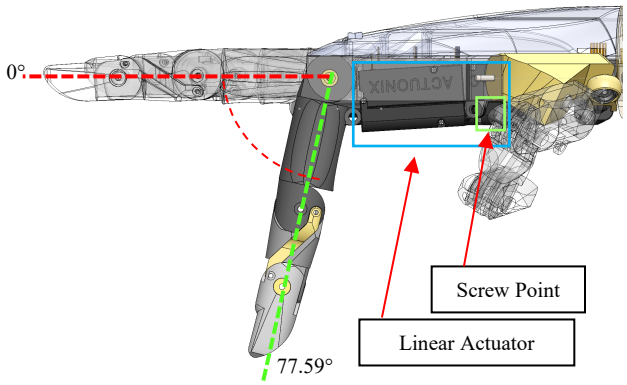


Figure 5: Range of Motion MCP joint.

The thrusting position of the linear actuator is perpendicular to the pivot point at a radius of 10.75 mm when the fingers are in the most folded position towards the palm. When the fingers are unfolded, the distance between the thrusting position and the pivot point is 14.11 mm as shown in Figure 6.

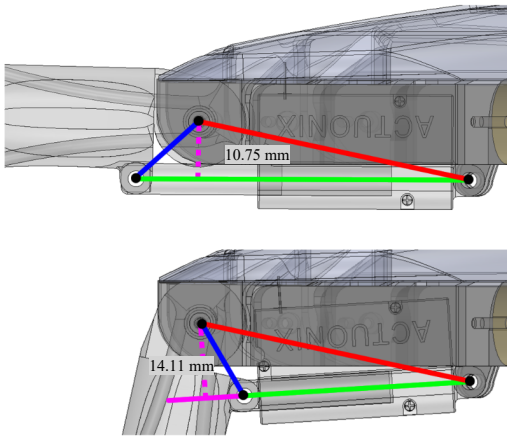


Figure 6: Extended MCP Joint (Top) and Flexed MCP Joint (Bottom)

The PIP joint is actuated by two of 4 braid PE fiber lines which have a thickness of 0.26 mm that provide flexibility in bending and can withstand a maximum tensile force of 13.6 KG. as tendons for flexion and extension, respectively. The metacarpal bone features two distinct paths for these tendons, namely the upper and lower paths. The flexion tendon travels through the lower path before turning up towards the top and securing with a screw, as illustrated in Figure 6. In contrast, the extension tendon travels through the upper path before turning down towards the bottom and fastening with a screw, as shown in Figure 7-8.

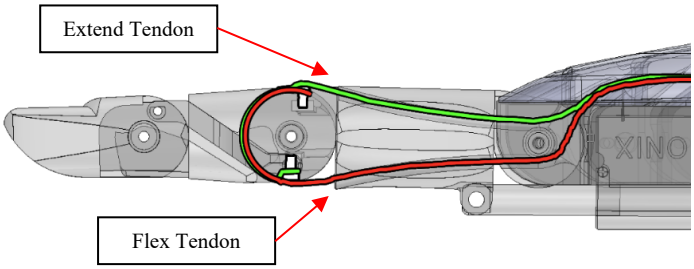


Figure 7: Flex Tendon (Bottom) and Extend Tendon (Top)

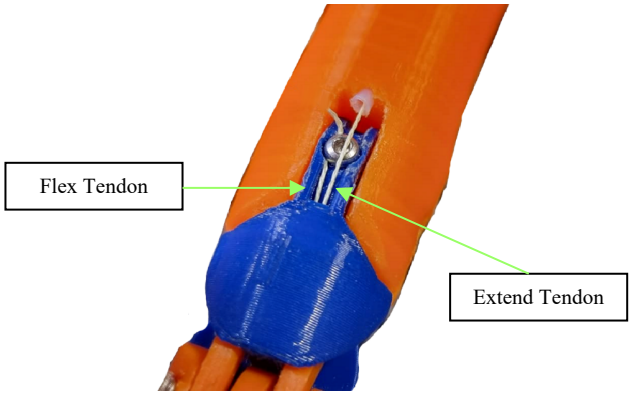
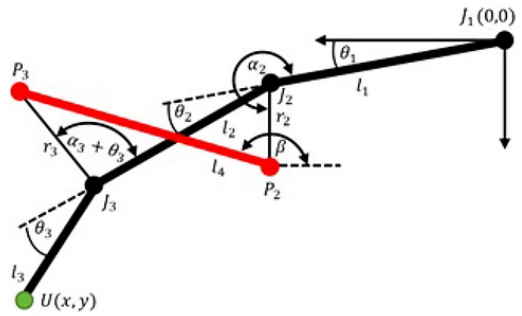


Figure 8: Flex Tendon Screw on Top of The PIP joint.

By focusing on the external appearance, the lengths of each joint are shown in Table 1. These values are substituted back in the equation to solve for the θ3. The result is the ratio of turning the PIP and DIP joints will be 1:0.961. While turning the PIP joint 90 degrees, the DIP joint will rotate 86.5 degrees as shown in Figure 9.

Table 1: Values of Finger

Finger Parts	Variable	Value	Unit
Middle Phalanx (Middle)	l_2	28	mm
Distal Phalanx (Distal)	l_3	26.5	mm
Proximal interphalangeal joint Four-bar radius	r_2	5.5	mm
Distal interphalangeal joint Four-bar radius	r_3	5.5	mm
Degree between Proximal Phalanx and Proximal inter phalangeal Four-bar	α_2	180	Degree
Standard degree between Middle Phalanx and Distal interphalangeal joint Four-bar	α_3	60	Degree
Moving degree of Proximal phalangeal joint	θ_2	90	Degree
Moving degree of Distal phalangeal joint	θ_3	Result	Degree



$$r_3 = \frac{-(l_2 r_2(\cos(\alpha_2) - \cos(\alpha_2 - \theta_2)))}{l_2\cos(\alpha_3+\theta_3) - l_2\cos(\alpha_3) + r_2\cos(\alpha_3 - \alpha_2 + \theta_2 + \theta_3) - r_2\cos(\alpha_2 - \alpha_3)} \quad (1)$$

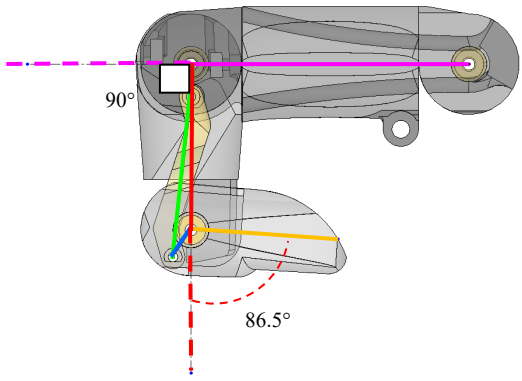


Figure 9: Annotations for Finger Dimension, Calculation, and the Relative Degree Between DIP and PIP.

2.2. Palm

The palmar side of the hand is equipped with five linear actuators, with the middle finger serving as the reference axis for the index and ring fingers. These fingers are separated at an angle of 5 degrees from the adjacent finger as shown in Figure 10. The thumb, however, requires special attention in order to mimic the

palm line pattern, as shown in Figure 10. To create a rotation axis for the Carpometacarpal joint (CMC), the axis of the Middle finger crossing over the edge of the wrist and the horizontal axis of the Little finger crossing the edge of the palm at the pointer finger side remains the same. A straight line is then drawn between these two points to create a rotation axis for the Carpometacarpal joint (CMC), as shown in Figure 11.

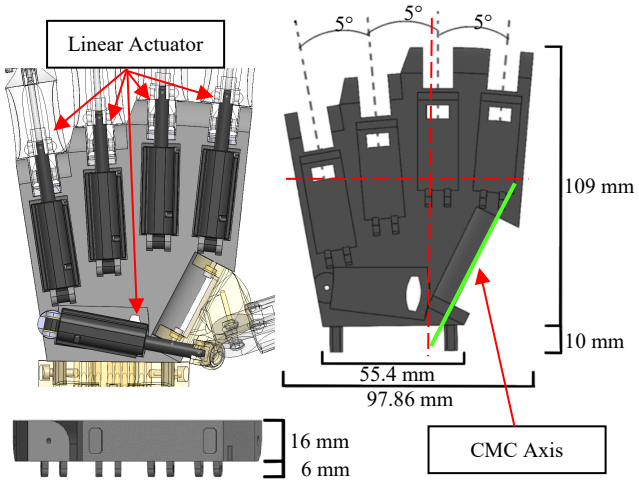


Figure 10: 3D Model of Palm

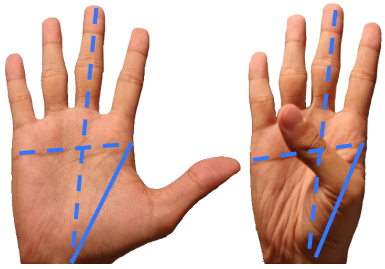


Figure 11: Reference for Palm Line Pattern.

The dorsal side of the hand is designed to accommodate the tendons and electric cables. The back of the palm is covered with a shell that has magnets, enabling quick removal for repair and maintenance, as shown in Figure 12.

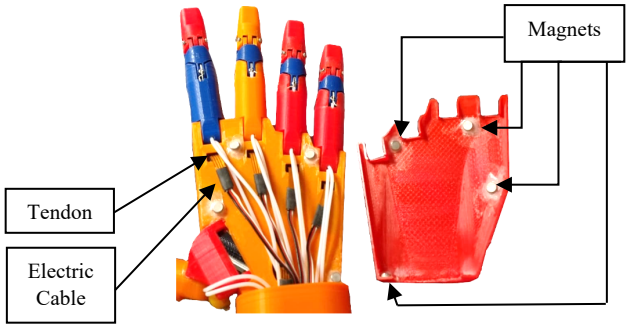


Figure 12: Dorsal Side of Palm

2.3. Carpometacarpal Joint

The Carpometacarpal (CMC) joint is the first joint of the thumb. It is driven by a single linear actuator for abduction. The extension is fixed at a 62.59° angle to improve grasping ability. This is capable of having 12° of pre-abduction and 42° of radial movement [9], [10], as shown in Figure 13.

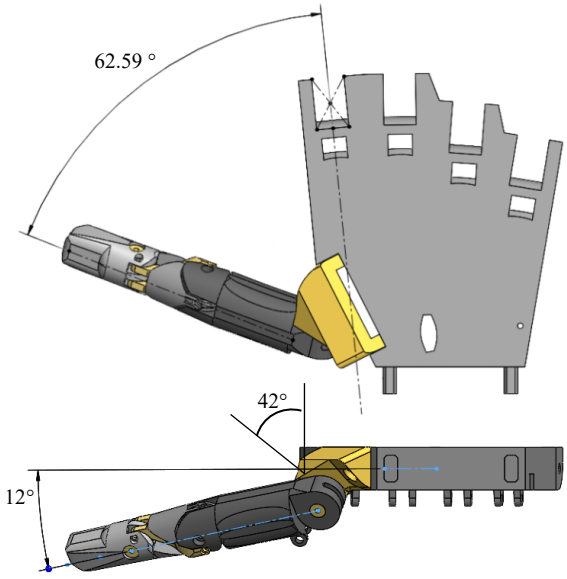


Figure 13: CMC Joint Extended Position Dorsal View (Top) and Wrist View (Bottom)

Since the space in the palm is limited by other MCP joints, the axis of CMC joints is not parallel to the linear actuator. To solve this problem, a ball joint is attached to convert the rotation axis of the CMC joint to the linear actuator axis as shown in Figure 14. The direction of force exerted by the linear actuator through the ball joint during both flexion and extension is indicated in Figure 15, with the arrow indicating the direction of force.

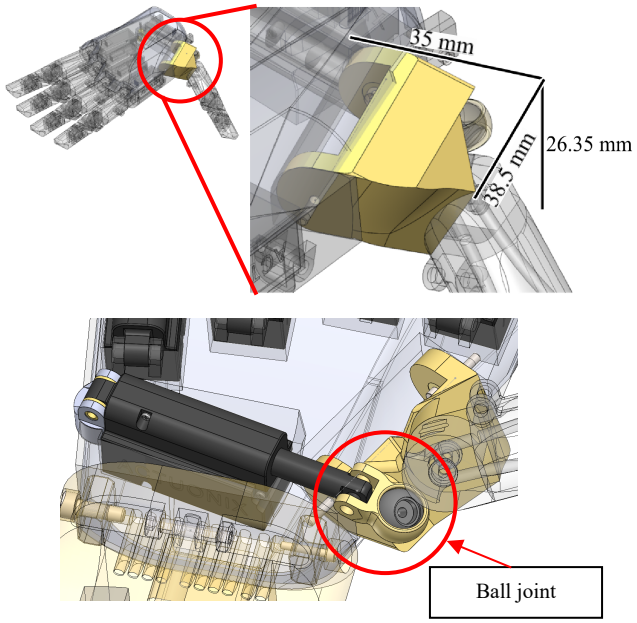


Figure 14: CMC Joint Normal Position

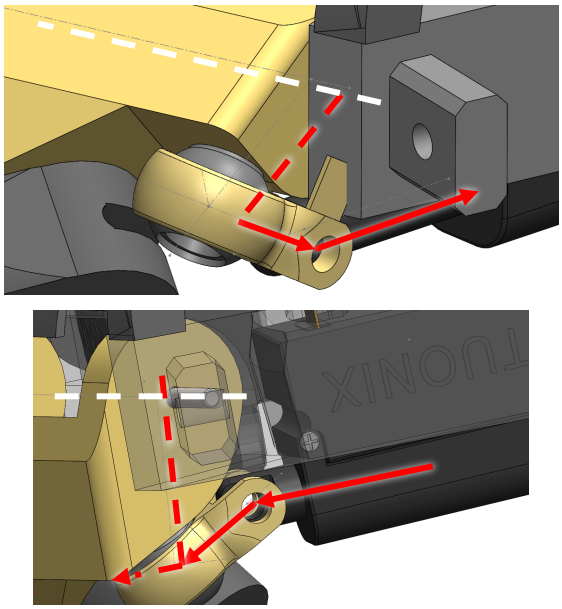


Figure 15: Extended CMC joint (Top) and Flexed CMC joint (Bottom)

The Carpometacarpal (CMC) joint, which cooperates with the ball joint, is responsible for the rotation angle of the non-parallel joint of the thumb. The rotation angle ranges from maximum extension to maximum flexion is 72 degrees, as shown in Figure 16.

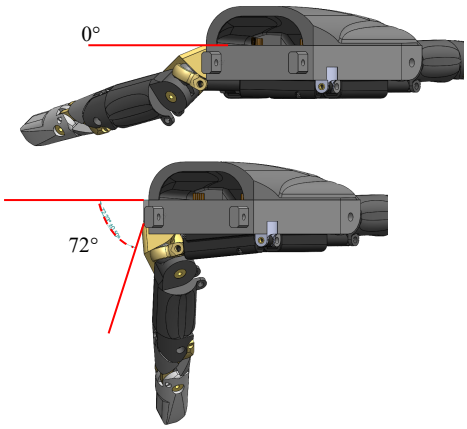


Figure 16: Range of Motion CMC joint

2.4. Wrist

The human wrist is not always in a straight position and requires mimicry to replicate natural postures. Additionally, the wrist is responsible for organizing tendons around the rotational axis to prevent any unnecessary stretch when it is flexed. The wrist itself has two distinct sides. The front side contains two sockets for attaching the hand to the bottom row, while the middle row has ten holes for tendon routing. The top row contains a single hole for the electric cable from the linear actuator. On the other side, the back side of the wrist has a rotation joint at the middle row, positioned at the same level as the tendons row, to prevent any tendon extension from the wrist's flexion and ensure smooth tendon movement as shown in Figure 17. A separate frictionless tube is used for each of the ten tendons as shown in Figure 18. The extension from the proximal finger to the tendon holder is within the proximal forearm. Finally, the bottom row contains a hinge for the linear actuator to actuate the wrist's flexion and extension. The design of the wrist is shown in Figure 19.

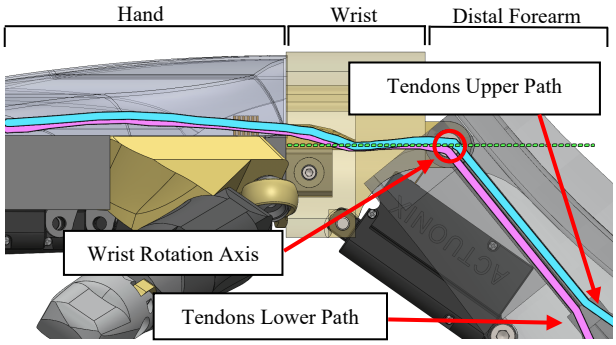
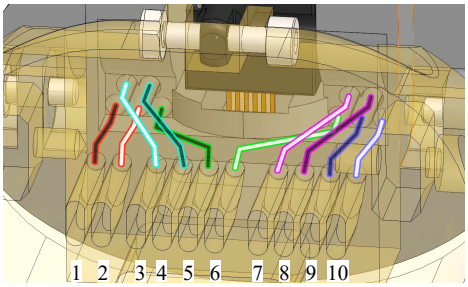


Figure 17: Tendons Path Side View



(1) Thumb Flex (2) Thumb Extend	(3) Pointer Extend (4) Pointer Flex (5) Middle Flex (6) Middle Extend	(7) Ring Extend (8) Ring Flex (9) Little Flex (10) Little

Figure 18: Tendons Path from Wrist to Forearm

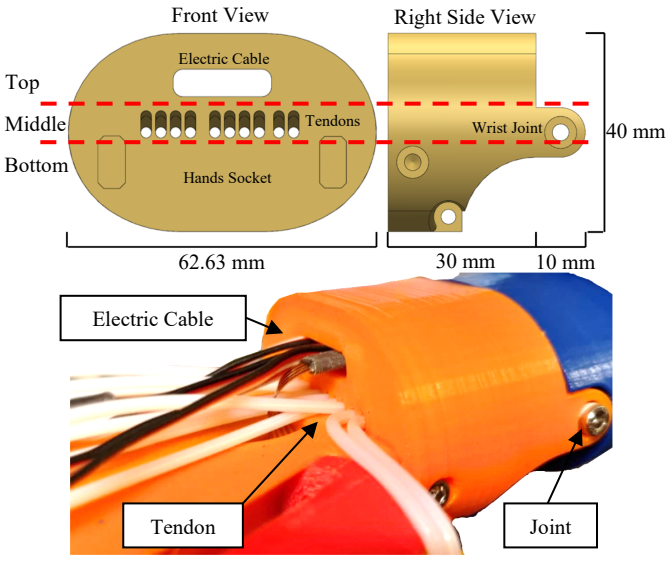


Figure 19: Wrist

The linear actuator is installed and aligned with the underarm area. The arm and wrist are designed to lie in parallel when it is fully extended. Conversely, when the linear actuator is fully retracted, the wrist is angled downwards by 50 degrees as shown in Figure 20-21. The technical specifications for linear actuators for all joints are shown in Table 2.

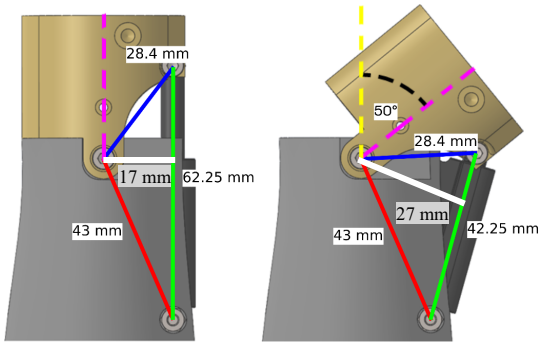


Figure 20: Wrist length parameter

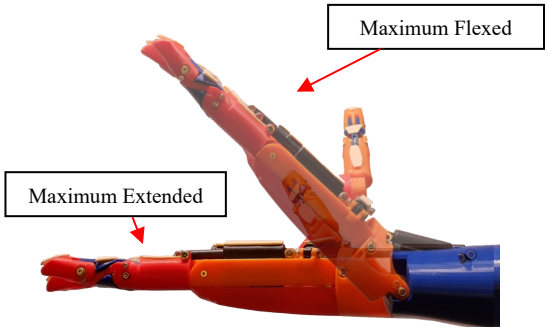


Figure 21: Robot Hand side view when flex and extend wrist.

Table 2: Specifications of Linear Actuator

Actuator	Actuonix PQ12-R 30:1	Actuonix PQ12-R 63:1
Joint	MCP/CMC	Wrist
Torque / Forces	18 N	45 N
Voltage	6 V	6 V
Stall Current	550 mA	550 mA
Dimensions (mm) (W × H × L)	21.5 × 15 × 48(+20)	

2.5. Forearm

The forearm is designed to resemble the anatomical structure of the human arm, with emphasis on its external appearance, as shown in Figure 22. The dimensions of the forearm are averaged values for an adult male forearm, measuring 263 mm in length, 97 mm in width at the elbow side, 64.75 mm in width at the wrist side, 75 mm in height at the elbow side, 40 mm in height at the wrist side [11].

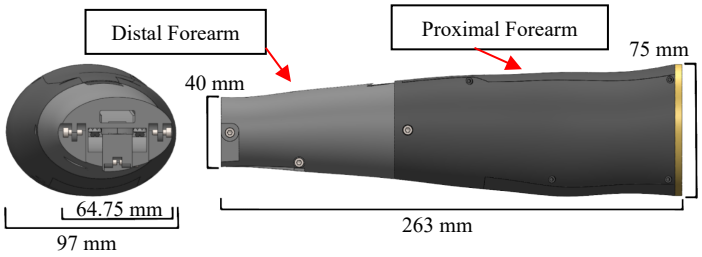


Figure 22: Forearm

The forearm is separated into two sections, namely the proximal and distal forearms as shown in Figure 23. The distal forearm is the location where the linear actuator for the wrist is attached, and it also provides a passage for wires from the internal to the external of the forearm. In addition, the distal forearm serves as the pathway for tendons to the proximal forearm, which contains the Dynamixel box as shown in Figure 23.

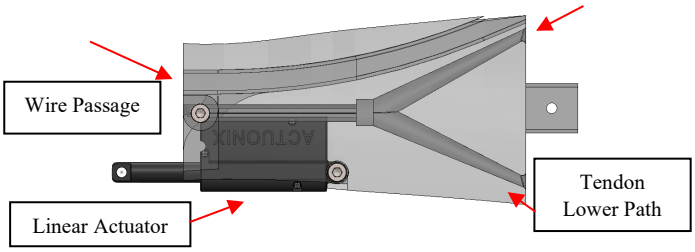


Figure 23: Distal Forearm

The Dynamixel box integrates all five Dynamixel XL430-W250-T with their tendon holders. The Dynamixel components are arranged in three rows, consisting of one unit, two units, and two units respectively. Rows 1 and 3 are oriented with heads up, while Row 2 is inverted to prevent tendons from overlapping with Row 3 as shown in Figure 24. At the end of the box, a base with a socket is installed for connection to the cover plate. The technical specifications for Dynamixel actuators for all joints are shown in Table 3.

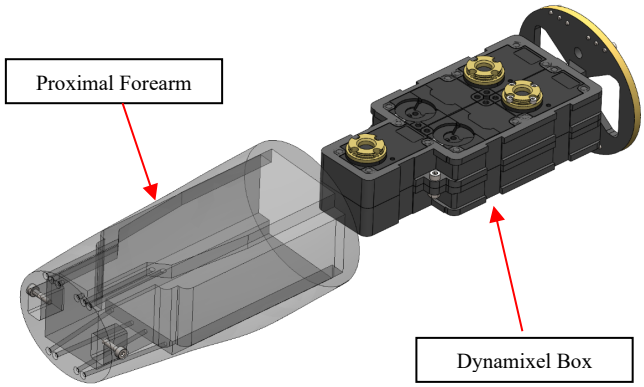


Figure 24: Proximal Forearm

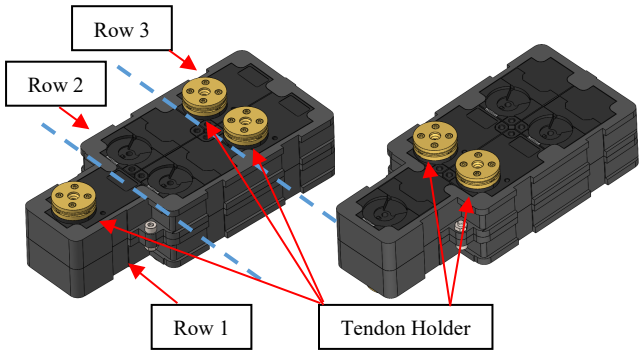


Figure 25: Dynamixel Box Upside (Left) and Downside (Right)

Table 3: Specifications of Linear Actuator.

Actuator	Dynamixel XL-430-W250-T
Joint	PIP
Torque / Forces	1.4 N·m
Voltage	11.1 V
Stall Current	1.3 A
Dimensions (mm) (W × H × L)	28.5 × 46.5 × 34

The tendon holder is composed of three parts, namely the top part, middle part, and bottom part. These parts are stacked into three layers to prevent binding between tendons. The bottom part is screwed to the Dynamixel flange, and the flex tendon is tied around it for 1 + 1/4 rounds counterclockwise. The middle part is used to extend the tendon and is tied clockwise around the part for 1 + 1/4 rounds. The top part is designed to prevent the extend tendon from coming off the circular and merging of the three parts together by using four screws as shown in Figure 26. When flex and extend tendons are tied around the tendon holder, they share the same binding point. As the Dynamixel rotates either clockwise or counterclockwise, one of the tendons will be released from the holder, while the other is wound around it at an equal distance. The radius of the tendon holder is designed to match that of the tendon binding around the proximal interphalangeal (PIP) joint. This design ensures that the rotation of the Dynamixel and the rotation of the PIP joint are synchronized and occur at the same rate. Ten tendons that have been threaded through the frictionless tube are responsible for pulling the Dynamixel box inward, ensuring that it remains securely in place within the arm as shown in Figure 27.

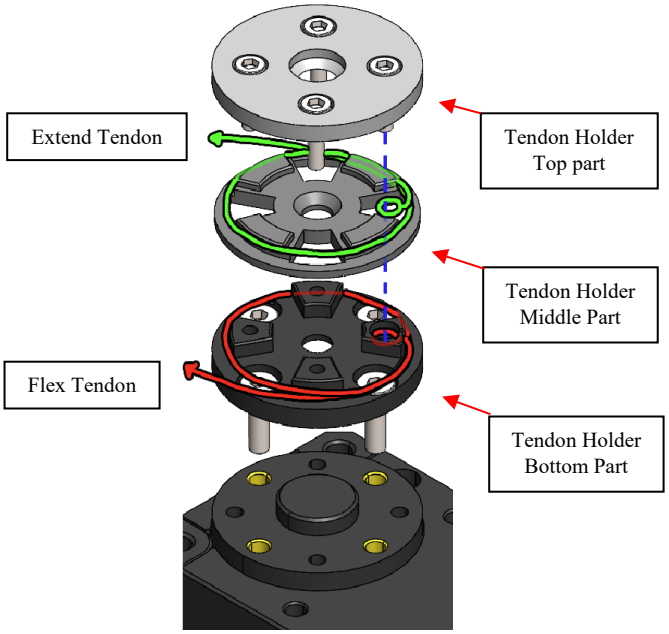


Figure 26: The layer of Tendon holder with flex tendon and extend tendon.

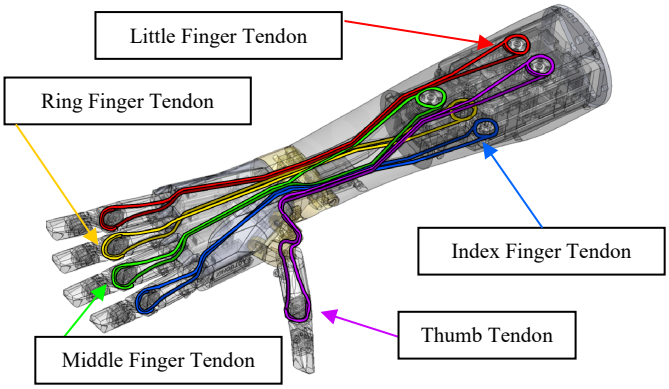


Figure 27: Overview of Tendons Routing.

Last, the cover plate encloses the proximal forearm and maintains tension in all ten tendons by securing it to the Dynamixel box. It is screwed in place to pull the Dynamixel box outward and straighten the tendons as shown in Figure 28.

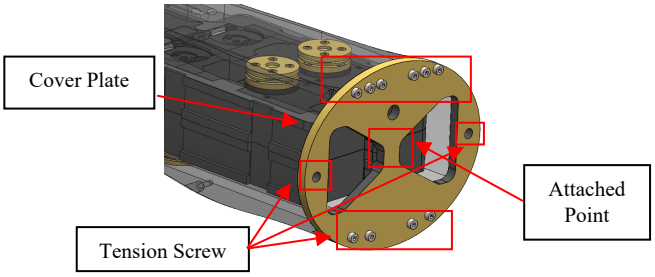


Figure 28: Cover plate.

To increase the degrees of freedom (DOFs) while maintaining the appearance of the hand and arm, multiple types of actuators were utilized within space constraints. Specifically, five linear actuators were implemented in the palm to control the MCP joints of the Index, Middle, Ring, and Little fingers, as well as the CMC joint of the thumb. The PIP joints of the Index, Middle, Ring, and Little fingers were controlled by Dynamixel digital servo motors through tendons, similar to the MCP joint of the thumb, which was also controlled by a servo motor connected through a tendon from the back of the forearm as illustrated in Figure 29. As a result of this design, the fingers can flex and extend the PIP, MCP, and CMC joints separately as shown in Figure 30.

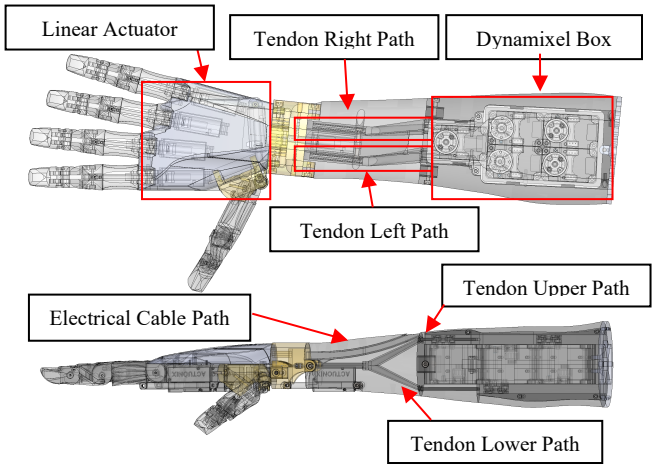


Figure 29: Inside the hand and arm.

Figure 30: Robot Hand flexing a MCP (Left) and PIP (Right) joint.

3. Evaluation

3.1. Generating Gestures

Basic perform of the hand is hand signs that are formed in many postures with different meanings. However, some hand signs are widely used, such as the emoji hand sign. The emoji hand sign is widely used in various social media. The meaning may deviate, depending on the context of communication between the speakers, but the hand sign has a stable shape. Having an independent DIP and PIP joint from the MCP and CMC joint. Hence, the posture that performs a straight finger can be more realistic than the fixed DIP finger. Ten emoji hands, as shown in Table 4 and Figure 31, are an emoji that uses one hand to perform.

Table 4: Hand Sign and Meaning

No.	Name	Meaning
1	Raised Hand	Stop, Hello (greeting), Hi-Five (greeting)
2	I Love You	Love or Affection
3	Sign of Horns	Rock Music Joy
4	Raised Fist	Unity Resistance
5	OK	It is fine.
6	Call Me	Call me via phone. Call me later. Take it easy
7	Thumbs Up	Like Yes Agree Understand
8	Backhand Index Pointing Right	Refer attention to the things that fingertip pointed.
9	Index Pointing Up	Contemplation Be careful
10	Victory	Victory Peace

More explanations for emoji and hand signs are discussed in the following section.

1) "Raised Hand" signifies that all fingers are maximum extended into a straight finger. It means "Stop", "Hello", or "Hi-five".
2) "I Love You Hand Sign" is a sign with the Little finger, Index finger, and Thumb extended straight and flexed Middle finger and Ring finger into the palm. It is used to express love to the interlocutor.
3) "Sign of the Horns" looks like the "I love you hand sign" but have a flexion of the Thumb in the palm. This sign has many meanings, but in common, it is known as "The symbol of rock music, and "joy"
4) "Raised Fist" is depicted by flexing of all fingers into the palm while leaving a flexed Thumb outside the Index finger. Performing the "Raised fist" with the back to the performer can mean "Unity" or "resistance". Front view of the fist emoji is called the "Fisted Hand Sign", which means punching somebody. While "Left-Facing Fist" and "Right-Facing Fist" are used together to depict a friendly greeting, like giving a High-Five.
5) "OK Sign" is the sign with a flexed thumb tip and index fingertip to touch each other and leave the Middle finger, Ring finger, and Little finger straight or in a neutral finger position. The meaning of "OK" is simply well-known as "It is fine." to the situation.
6) "Call Me" is the sign with an extended Thumb and Little finger straight and flexed Index finger, Middle finger, and Little finger into the palm. It is used to express the meaning of "Call me".
7) "Thumbs Up Sign" as the flex Index finger, Middle finger, Ring finger, and Little finger into the palm and extend the Thumb straight. The "Thumbs Up" gesture is popular on social media for a meaning of positive expression, such as "Like" when the person approves of the content in the post, meaning "Yes" when the person replies to a question about a situation of something which result is come out positive way, "Agree" when the person acknowledge on the mention, and “Understand” when the person realizes clearly. On the other hand, the "Thumbs Down sign" which have the same finger posture but rotates the arm to put the Thumb downward to the ground, which means "Dislike".
8) " Backhand Index Pointing Right" is the posture that flexes the Little finger, Ring finger, and Middle finger into the palm, leaving the Index finger extended straight. The Thumb is extended straight or flexed to the palm.
9) "Left Pointing.", "Down Pointing" and "Up Pointing" mean paying attention to something. Special for "Up Pointing" can be for "Think' and "Be careful".
10) "Victory Hand" is the sign with the Index finger and Middle finger extended straight and flexed the Little finger, Ring finger, and Thumb to the palm. and it can represent the Latin letter V which means "Victory".

3.2. Generation of grips for holding objects

In addition to expressing the meaning through the hand sign, holding objects is another way to tell the listener what the operator's intention is.

The objects that were selected to test are the daily use object, which comes in different shape, size, and weight [12] as shown in Table 5 and Figure 30. The object is put in the hand and the hand starts to grasp and hold still, before recording the picture. Various holding techniques are employed for different objects during grasping tasks. For instance, the Lateral Pinch grip, as demonstrated in Figure 32(1), is used for holding small flat objects like coins, card keys, and banknotes. The Tripod Pinch, depicted in Figure 32(2), is utilized for holding stick-type objects like pens and soldering irons, where three fingers are used to pin

the object in position. The Cylindrical Grip, shown in Figure 32(3-6), is used to entwine cylindrical objects like soda cans, water bottles, hand drills, cleaning sprays, and sanitizer sprays. The Sticky Tape grip, illustrated in Figure 32(7), is used for holding flat cylindrical and spherical objects. The Storage Box grip, as depicted in Figure 32(8), is achieved by using only the Proximal Interphalangeal (PIP) and Distal Interphalangeal (DIP) joints to grasp and hold objects such as document files and books. In contrast, the Claw grip, illustrated in Figure 32(12), is used for holding tote bags and is performed by pointing the hand toward the ground. The Platform Posture grip, as shown in Figure 32(9), involves extending the hand with the palm side up and placing the object on top, then flexing the fingers to support the object. Lastly, the Mouse grip, depicted in Figure 32(10), is a special grip for holding a computer mouse, where the thumb, ring finger, and palm are used to set the position, and the index and middle fingers are used for left and right-clicking, respectively.

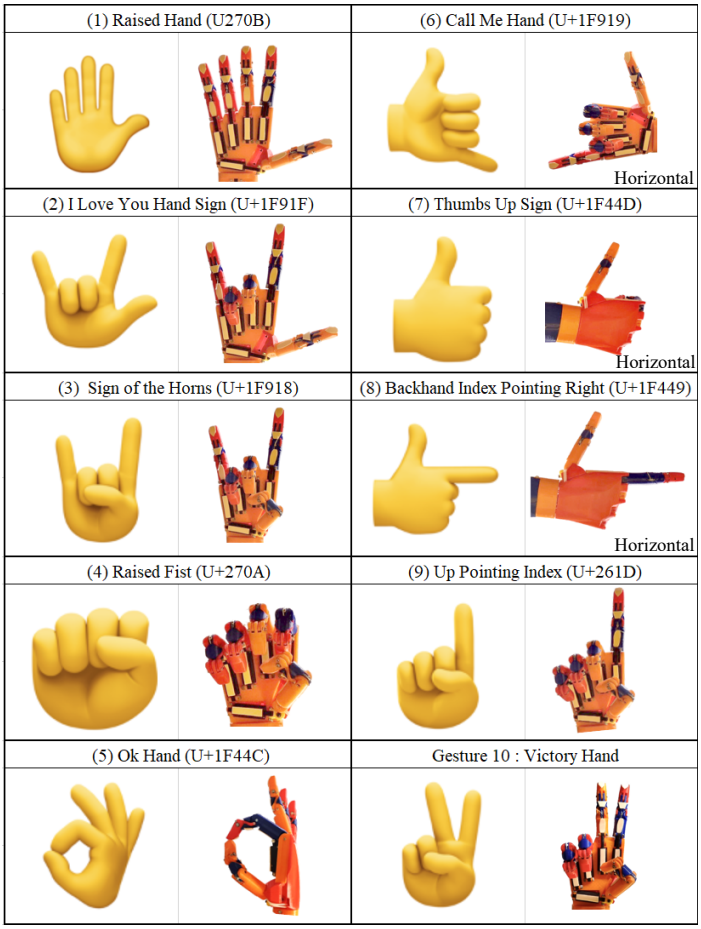


Figure 31: Robot Hand compared to the Facebook Emoji Hand.

Table 5: Object details for Figure 31.

No.	Object	Dimension (mm)	Weight (g)	Holding Type
1	Coin	1.8(h) × 24(Ø)	6	Lateral Pinch
2	Pen	124(h) × 12(Ø)	7	Tripod Pinch
3	Cleaning spray bottle	39(l) × 34(w) 57(l) × 34(w) (trigger)	60	Cylindrical Grip with Trigger
4	Sanitizer spray bottle	119(h) × 31(Ø)	23	Cylindrical with Extend Index Finger
5	Soda can	150(h) × 57(Ø)	13	Cylindrical Grip
6	Water bottle	177.5(h) × 57.4 (Ø)	193	Cylindrical Grip
7	Sticky tape	16(h) × 55.5(Ø)	24	Spherical Grip
8	Storage box	162.5(l) × 52(w) ×15.3(h)	48	Claw Grip
9	Plate	120 - 230(Ø) × 34(h)	176	Platform
10	Mouse	127(l) × 67(w) × 37(h)	73	Fingertip Grip
11	Hand	-	-	Handshake
12	Canvas Tote Bag	28(w) × 3(h) (handle)	129	Hook

Figure 32: Robot Hand when grasped and hold the objects.

Table 6: Equation of Linear actuator.

Fingers	Joint	Equation
Thumb	CMC	y = 0.07223 x – 72.23
Index	MCP	y = 0.07759 x – 77.59
Middle		
Ring		
Little		

For measuring the angle of a joint using a linear actuator, the actuator is driven by Pulse Width Modulation (PWM). A pulse width of 1000 µs results in the maximum retract stroke, while a

pulse width of 1500 µs results in a 10 mm stroke, and a pulse width of 2000 µs results in a maximum extended 20 mm stroke. A linear relationship between pulse width and stroke length can be observed. By mounting the linear actuator directly on the proximal part of the finger, the measurement of the joint angle can be obtained from the pulse width of the input, which is then compared to the angle of joint rotation. An equation for determining the angle of joint flexion is provided in Table 6.

For the Dynamixel joints, values of joints can be obtained from the sensors for each joint. Due to the transmission of power through tendons that may stretch or slack over time, the flex sensor 2.2-inch is used to measure the amount of voltage in digital to compare with the actual motion (Figure 33). The measurements were subdivided into 5-degree angles and the total value was recorded 20 times per angle by fixing the joints of the fingers with the angle measuring tools. and measure the resistance at the angle, as shown in Figure 34. Measurement begins by stabilizing the PIP joint and fixing the DIP joint at 0 degrees. Record the Sensor value, then increment the DIP lock point to 5 degrees. Continue this process until reaching 85 degrees, then return to the starting position at 0 degrees. Repeat this cycle 20 times for all five fingers. After obtaining the recording table, calculate the average value for each degree before creating a graph. The goal is to derive an equation suitable for the graph, as illustrated in Figure 35-39 and Table 9. Utilizing the Flex Sensor for feedback, the calculated reading value is employed in an equation to determine the degree of joint rotation. The accuracy of angle deviation is consistently maintained within an acceptable range of plus or minus 4 degrees, ensuring minimal deviation from normal postures. Flexible sensors exhibit various resistance ranges along different sensors. When used in a 5V pull-up circuit with 220k Ω resistor, the resistance readings decrease when the sensors are bent further specification of flex sensor are shown in Table 7. Dynamixel joint has an actual maximum movement only 85 degrees, because of the guide tube in this design interrupts the movement. The details of the equation are shown in Table 8.

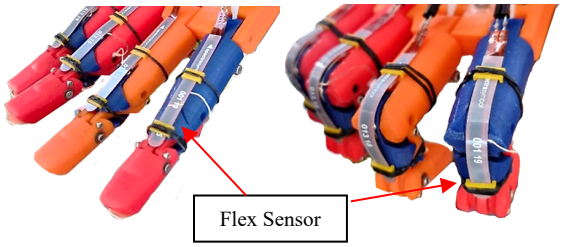


Figure 33: Flex Sensor on Fingers.

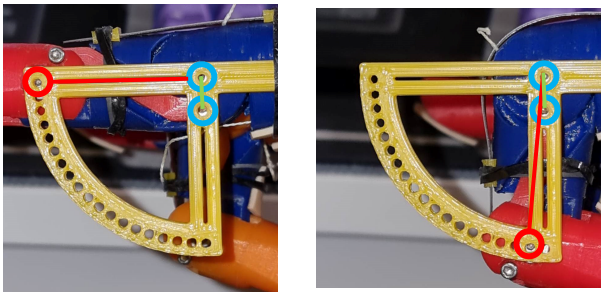


Figure 34: Measuring Tools When Not Applied Screw to Fix Angle.

Table 7: Flex Sensor Resistance Value.

Fingers	Minimum Resistance (kΩ)	Flat Resistance (kΩ)	Maximum Resistance (kΩ)
Thumb	40	440	720
Index	31	260	470
Middle	30	360	640
Ring	36	340	580
Little	43	560	970

Table 8: Equation of Dynamixel.

Fingers	Equation	R-Square	Residual SD
Thumb	$y = 0.0165x^2 – 3.4230x + 599.7518$	0.9900	5.6890
Index	$y = 0.0166x^2 – 3.1108x + 417.6042$	0.9912	4.5224
Middle	$y = 0.0165x^2 – 4.9180x + 502.2505$	0.9970	5.3356
Ring	$y = 0.0196x^2 – 4.5638x + 505.1175$	0.9993	2.1901
Little	$y = 0.0047x^2 – 3.4375x + 629.5187$	0.9977	4.0386

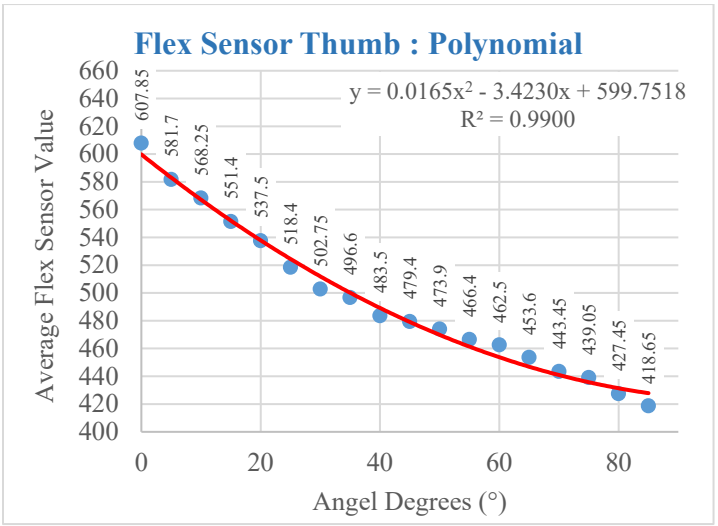


Figure 35: Flex Sensor on Thumb Finger.

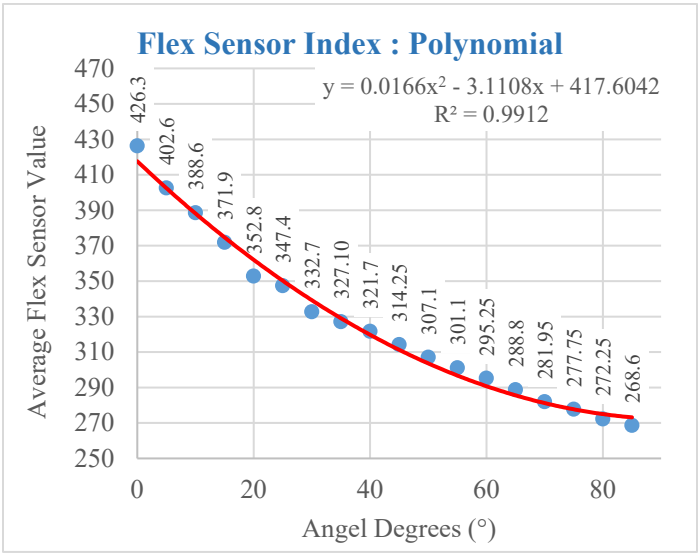


Figure 36: Flex Sensor on Index Finger.

Because of feedback from the sensor, gestures and object-holding positions can be recorded and utilized for subsequent replays without the need for the actual object to be present. This allows for the replication of movements, such as drinking water from a water can, in a simulated situation.

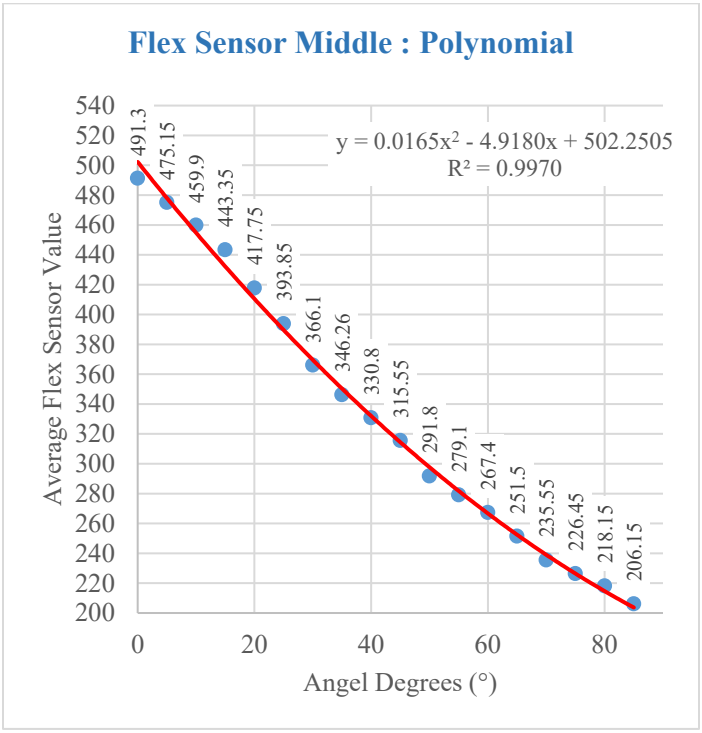


Figure 37: Flex Sensor on Middle Finger.

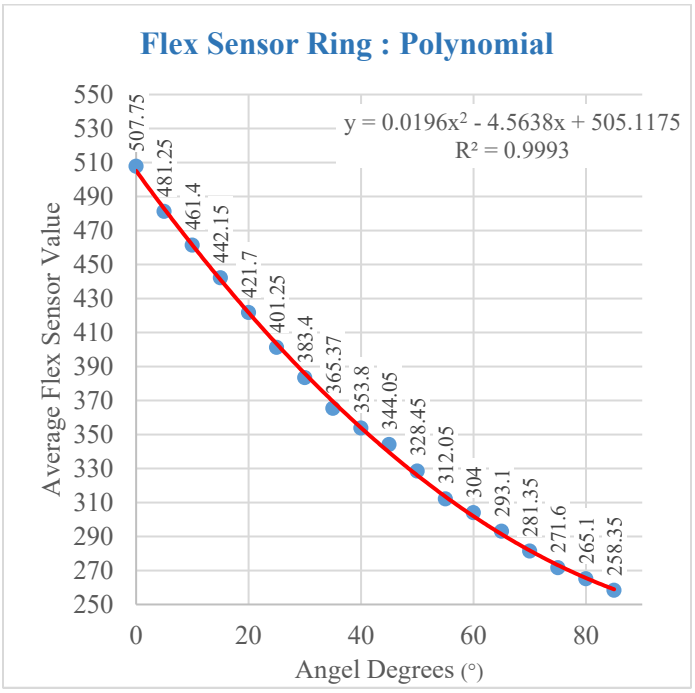


Figure 38: Flex Sensor on Ring Finger.

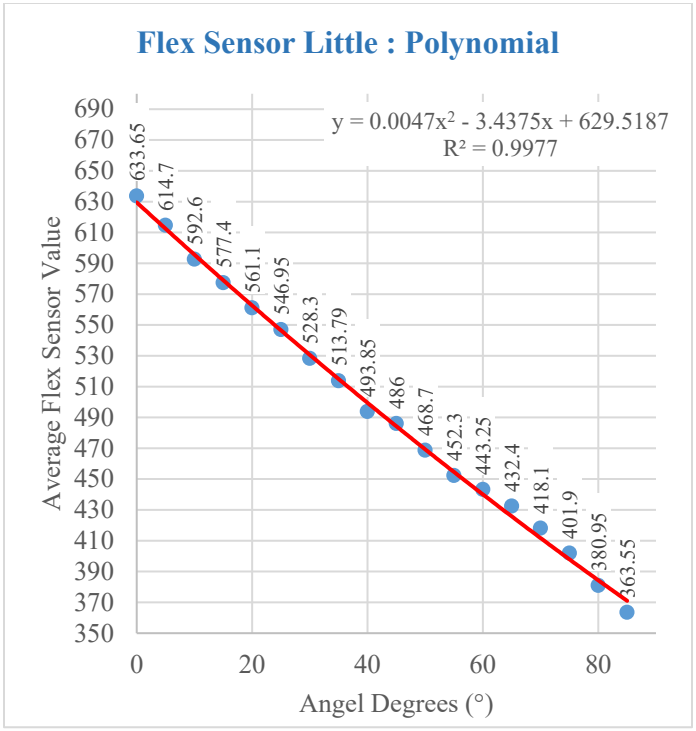


Figure 39: Flex Sensor on Little Finger.

Table 9: Flex Sensor Resistance Value.

Average Resistance Value										
Fingers /Deg	Thumb	SD	Pointer	SD	Middle	SD	Ring	SD	Little	SD
0	599.8	3.3	417.6	3.5	502.3	3.7	505.1	2.7	629.5	2.6
5	583.0	3.0	402.5	5.0	478.1	4.7	482.8	3.0	612.4	2.4
10	567.2	3.7	388.2	5.2	454.7	3.9	461.4	3.8	595.6	2.5
15	552.1	3.5	374.7	5.1	432.2	4.9	441.1	4.8	579.0	3.4
20	537.9	3.4	362.0	4.9	410.5	2.9	421.7	3.8	562.6	3.4
25	524.5	5.4	350.2	4.0	389.6	5.1	403.3	4.2	546.5	3.8
30	511.9	4.2	339.2	2.9	369.6	3.4	385.8	3.5	530.6	3.0
35	500.2	3.6	329.1	2.1	350.3	3.6	369.4	2.9	515.0	3.2
40	489.2	4.3	319.7	3.0	331.9	3.9	353.9	4.2	499.5	3.3
45	479.1	2.5	311.2	3.9	314.4	3.3	339.4	4.2	484.3	4.7
50	469.9	3.7	303.6	4.1	297.6	3.5	325.9	3.7	469.4	4.0
55	461.4	5.0	296.7	4.1	281.7	4.5	313.4	3.8	454.7	3.0
60	453.8	2.3	290.7	3.8	266.6	4.2	301.8	4.1	440.2	4.1
65	447.0	3.4	285.5	4.7	252.3	4.5	291.3	4.2	425.9	4.0
70	441.0	3.4	281.2	2.8	238.8	3.9	281.7	3.1	411.9	3.8
75	435.8	3.0	277.7	2.7	226.2	3.3	273.1	4.5	398.1	4.1
80	431.5	3.6	275.0	2.3	214.4	3.9	265.5	3.1	384.6	3.8
85	428.0	3.2	273.1	2.5	203.4	3.0	258.8	3.5	371.3	2.3
Std. Res.	5.7		4.5		5.3		2.2		4.0	

Force was quantified by assessing the pressure applied at the distal interphalangeal (DIP) fingertip, with the palm fixed in position and the finger held straight. Subsequently, the fingertips were placed on a weighing scale beneath the distal phalanx, as depicted in Figure 40. Each finger was then instructed to flex maximally, with measurements recorded in each cycle. The average force is illustrated in Figure 41. The tension in the tendon significantly influences the strength of finger flexion. Excessive tightness in the tendons can result in diminished flexion of the linear actuator. Additionally, the force produced by wrist flexion is measured using the middle finger.

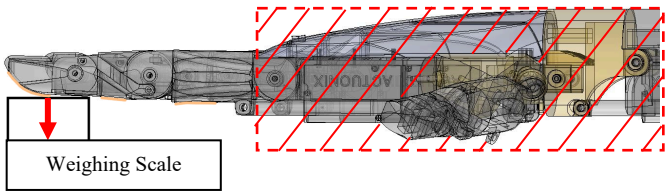


Figure 40: Setup of Force Measurement by Fixing the Palm in place.

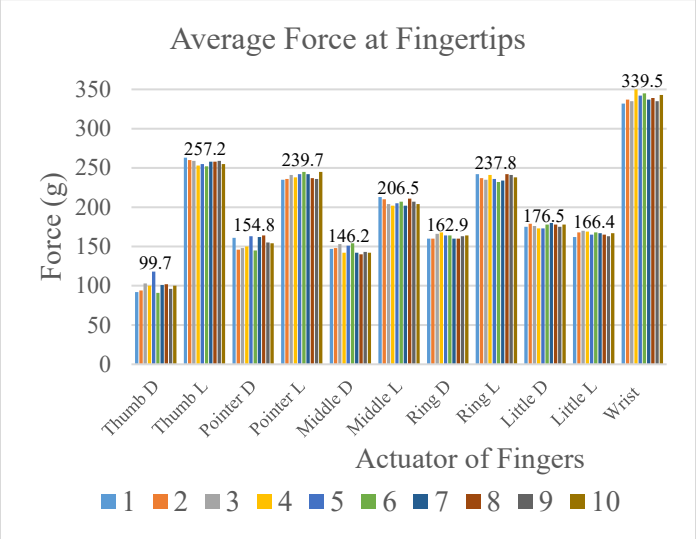


Figure 41: Flex Sensor on Little Finger.

4. Conclusion

The robot hand is designed to focus on the appearance of a human shape to represent as natural and friendly as a human form to a participant. The appearance is designed to be close to a human in shape as a prosthetic hand. Multiple types of actuators have been adopted in the transmission design to maintain performance in the limited space. The robot hand has 15 joints, 10 DOFs, and 1 wrist joint. While the linear actuator joint directly controls finger movement and utilizes Pulse Width Modulation (PWM) values for rotation measurement of MCP joint. For the PIP joint which is driven by Dynamixel by transmits power through the tendon, Flex sensors are strategically placed atop each finger, providing feedback on the angle of rotation to compensate for tendon degradation. Ensuring accuracy within plus or minus 4 degrees is achieved by applying an individual second-order polynomial curve fitting formula on each finger, derived from the calibration results. Recording the degree of rotation for each joint enables the hand to replicate hand gestures without needing physical objects. Furthermore, the hand has the capacity to hold objects and engage in communication through hand gestures. In gestures performed, 10 main hand signs can be performed. Designed within the given constraints to prioritize appearance, robotic hands can convey a wide range of gestures and symbols, including greetings, cessation signals, affection, joy, unity, resistance, agreement, distraction, contemplation, victory, and the OK hand sign. Moreover, these robotic hands can hold various daily objects, such as flat coins, stick objects like pens, cylindrical cans, or water bottles, trigger-operated spray bottles or hand sanitizers, and circular or flat cylindrical objects like sticky tape. They are even capable of engaging in handshakes for greetings, utilizing a fingertip grip for operating the computer mouse, and adopting a claw-like configuration to hold a box or document folder horizontally or to carry bag straps vertically. This hand is meticulously designed by eliminating the movement of abduction and adduction joints while maintaining a fixed angle for optimal expression of hand gestures with a suitable number of actuators in the design. Furthermore, the 3D model is accessible to any reader interested in further development at the link below. "https://github.com/Traithep-w/Robotic-Hand"

Conflict of Interest

The authors declare no conflict of interest.

Acknowledgment

The authors would like to thank the AI for All project and the Fundamental Fund for supporting tuition fees and research equipment. Also, the authors would like to thank the Institute of Field Robotics and the King Mongkut's University of Technology Thonburi, which is a source of knowledge and a place to develop this research.

References

[1] J. Trichada, T. Wimonrut, N. Tirasuntarakul, T. Choopojcharoen, B. Sakulkueakulsuk, “Design of an Open Source Anthropomophic Robotic Finger for Telepresence Robot,” ACM International Conference Proceeding Series, 62–66, 2021, doi:10.1145/3467691.3467704.

[2] M. Grebenstein, A. Albu-Schäffer, T. Bahis, et al. "The DLR hand arm system", Proceedings - IEEE International Conference on Robotics and Automation, 3175-3182, 2021, doi: 10.1109/ICRA.2011.5980371.

[3] Shadow Robot, "Shadow Dexterous Hand E1 Series (E1M3R, E1M3L, E1P1R, E1P1L)",2013.

[4] S. Powell, "A Review of Anthropomorphic Robotic Hand Technology and Data Glove Based Control", M.S. Thesis, Virginia Polytechnic Institute and State University, 2016.

[5] I. Llop-Harillo, A. Pérez-González, J. Andrés-Esperanza, "Grasping Ability and Motion Synergies in Affordable Tendon-Driven Prosthetic Hands Controlled by Able-Bodied Subjects", Frontiers in Neurorobotics, **14**(August), 1-15, 2020, doi:10.3389/fnbot.2020.00057.

[6] J. Belter, J. Segil, A. Dollar, R. Weir, "Mechanical design and performance specifications of anthropomorphic prosthetic hands: A review", Journal of Rehabilitation Research and Development, **50**(5), 599-618, 2013, doi:10.1682/JRRD.2011.10.0188.

[7] C. Connolly, "Prosthetic hands from Touch Bionics", Industrial Robot, **35**(4), 290-293, 2008, doi:10.1108/01439910810876364.

[8] C. Medynski, B. Rattray, "Bebionic Prosthetic Design", MEC 2011 Symposium MyoElectric Controls/Powered Prosthetics Symposium, 1-4,

2011.
[9] S. Gehrmann, J. Tang, Z. Li, R. Goitz, J. Windolf, R. Kaufmann, "Motion deficit of the thumb in CMC joint arthritis", Journal of Hand Surgery, **35**(9), 1449-1453, 2010, doi:10.1016/j.jhsa.2010.05.026.
[10] P.Lastayo, "Journal of Hand Therapy: Editor's note", Journal of and Therapy, **24**(2), 79, 2011, doi:10.1016/j.jht.2011.03.002.
[11] W. Chen, Y. Lin, Y. Chen, K. Chen, B. Kuo, P. Tsao, Y. Lee, W. Soong, M. Jeng, "Reference equations for predicting standing height of children by using arm span or forearm length as an idex", Journal of the Chinese Medical Association, **81**(7), 649-656, 2018, doi: 10.1016/j.jcma.2017.08.023.
[12] I. Llop-Harillo, A. Pérez-González, J. Starke, T. Asfour, "The Anthropomorphic Hand Assessment Protocol (AHAP)", Robotics and Autonomous Systems, **121**, 2019, doi:10.1016/j.robot.2019.103259.

ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 8, No. 6, 78-86 (2023)

www.astesj.com

Special Issue on Innovation in Computing, Engineering Science & Technology

ASTESJ

ISSN: 2415-6698

Implementation of a GAS Injection Type Prefabricated Lifting Device for Underwater Rescue Based on Location Tracking

Jong-Hwa Yoon[1], Dal-Hwan Yoon[2,*]

[1]*TheQuest Co. Ltd., Seoul, 05853, Korea*

[2]*Semyung University, Department of Electronic Engineering, Jecheon, 27136, Korea*

ARTICLE INFO

Article history:
Received:14 August, 2023
Accepted:15 October, 2023
Online: 30 November, 2023

Keywords:
Lifting fixture
Air cartridge
Marine disaster
Monitoring system
Underwater communication

ABSTRACT

In this paper, we have developed a gas injection-type prefabricated lifting device based on location tracking to efficiently lift the human body in the event of an accident that occurs underwater on the sea or land. The efficiency of the lifting system is very important to ensure the golden time of the rescue and the safety of divers in the event of casualties underwater. Divers performing underwater safety rescue operations must endure up to 30 minutes with two air vents, and always consider the safety accident environment due to difficulty in securing visibility or high flow rates due to underwater turbidity. Particularly, there are many cases where life is threatened by hypothermia in the water. Therefore, both divers and the deceased need location tracking connected to the lifting device, and a fast and efficient lifting system was studied in underwater activities. The monitoring device uses a communication speed of 115.2 kbps from the sensor to the monitoring, and a communication speed of 2.4 kbps from the controller to the receiving unit. The gas injection-type prefabricated lifting device with a high elastic structure is lightweight and portable, and which consists of a baggy bag with minimal components to increase usage and work efficiency based on the instinctive behavior of divers. Accordingly, the entrance element design combining a bow and hinge that maintains a moment of force with TPU-based materials, a balanced design using weight balancing technology of a network structure, an SMB linkage design that induces water surface rise through gas injection, and an underwater experiment.

1. Introduction

In the event of an accident in the water of the sea and land, it is very important to secure a golden time for saving lives. In addition, divers who search the human body underwater should also be accompanied by securing safety. The mobile navigation control system has been studied that tracks the position of the human body while lifting the human body and monitors the movement of the position [1]. These underwater communication devices are attached to rescue workers and the human body and serve to transmit location data. Figure 1 shows a location monitoring that transmits location data from underwater. J. H. Yoon, S. I. Kang, and D. H. Yoon developed a location monitoring device using underwater ultrasonic sensor signals and conducted research to transmit location tracking signals to mother ships or land control centers in LTE or Lora [2, 3].

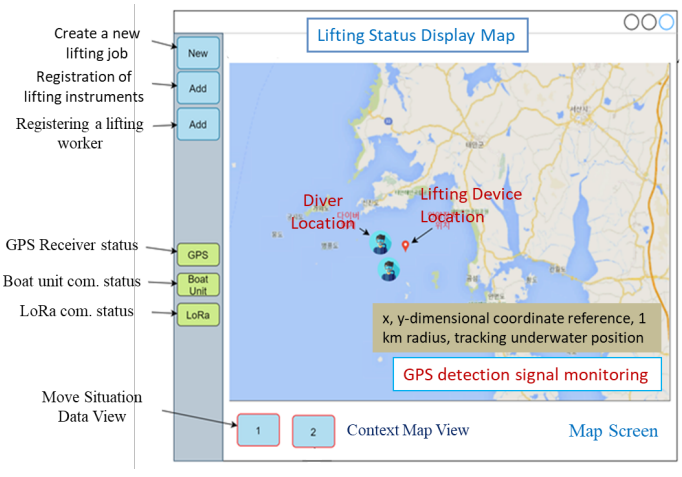


Figure 1: The surface location of ICT-based multi-communication system

Figure 2 shows a block diagram of the IoT injury motion monitoring system. The monitoring device may relay communication on a moving position and relay it to the land by

*Corresponding Author: Dal-Hwan Yoon, Semyung University, 65 Semyungro, Jecheon City, Chung-cheong Buk Do, 27136, Korea. E-mail: yoondh@semyung.ac.kr

LTE communication. The GPS data can then be used to track the location of the accident.

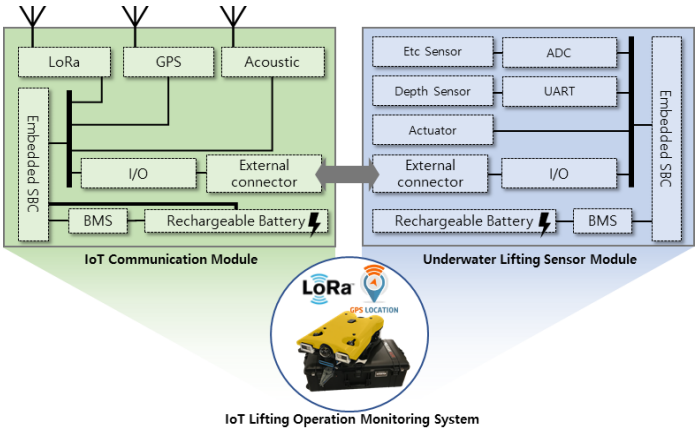


Figure 2: Block diagram of IoT behavior monitoring system

H. K. Min and D. H. Yoon studied a light diffusion device in which the information transmission system can float on the water surface and light is displayed [4]. It consists of a detection unit mounted on a lifting device underwater to detect a lifting situation and a control module that converts related information into an optical signal. This study includes an optical transmission line connected to transmit the optical signal of the control module to the optical diffusion mechanism.

D. H. Yoon and M. H. Park studied to provide a device and method for tracking the location of a target by continuously identifying the current location of a recovery object or rescue object such as a ship or drowning in the event of a water accident or emergency such as sinking, collision, subversion, fire, or drowning [5]. It consists of a hydraulic sensor that detects the water pressure applied to the object, a floating object separation function that separates the floating object from the object if the sensing water pressure exceeds the set value, a communication unit that communicates with the floating object, and a GPS receiver that calculates the current position.

Meanwhile, in [6] the author developed process fusion and production automation technology based on the infusion method to produce a boat with enhanced stability. Process fusion-based boat manufacturing devices to strengthen safety analyzed the balance and center of gravity of the boat in 3D (dimension), and studied the size of the bonding area, curvature of the bonding surface, and strength of the bonding surface. Particularly, the boat manufacturing device has the function of adjusting the mixing ratio of the resin and the curing agent and adjusting the discharge amount per unit time based on the results of the joint area analysis. This time, it includes controlling the manufacturing process, such as the width joint of the boat, makeup taping, accessory adhesion, and sealing by spraying adhesive at a set temperature according to 3D flow analysis.

Existing human lifting technology consists of zipping the instrument that holds the human body on the seabed, and most of the technologies are applied to raise the instrument by injecting air into a separate lift bag when lifting it to the surface [7, 8]. However, the integrated package set that combines roll-fold-based gas expansion technology does not show reliable performance for consumers [9]. Particularly, when diving into the water, it is subject to a lot of buoyancy resistance due to the weight and volume of the diver's equipment, and which complains of difficulties due to the time it takes to work underwater and the complexity of the work manual.

Technology for lifting the human body underwater should not miss Golden Time in the event of a marine accident, and the safety of divers should be secured first. It is very important not only to complete the work within 30 minutes of oxygen consumption time, but also to secure underwater turbidity, underwater flow rate, and visibility. To this end, various studies are needed, including durable materials, weight reduction, structure considering flow rates, and easy-to-handle manuals. In addition, since the marine area is wider than the land area, the cost of on-site helicopters, police patrol boats, diving personnel, and on-site command centers in the event of an accident is enormous [10]. Particularly, as seen in the Ferry Sewol incident in Korea, the underwater turbidity and flow rate were very severe, making it very difficult for divers to access the sunken ship, and it was also confirmed in cases where the safety of field workers could not be guaranteed.

In this study, we develop a package-type human lifting device system in which the lifting device rises to the surface through the quantity and flow rate flowing through the lifting device, renewable materials and durable designs, and underwater shooting of CO2 cartridges. In addition, the equipment is designed by applying an air cartridge method to minimize the time spent underwater through the convenience, weight reduction, and rapid operation of rescue workers. Through this, research is conducted on securing the reliability of the rapid lifting and lifting process.

2. Implementation of GAS Dispensing Human Lifting Device

2.1. Underwater Environment

The design of the lifting device is optimized based on various underwater environment data through prototype development. Korea's underwater environment has severe waves on the east coast, and it takes longer to darken than the bright time underwater between sunrise and sunset. In the case of the West Coast, the turbidity is so serious that it is difficult to check the front 1m, and there is a risk that everyone will be exposed to safety accidents [2]. Moreover, the difference between the tides, where the sea level changes vertically twice a day every 12 hours and 25 minutes, represents 9m from the coast in Incheon and 3m from Mokpo [9]. Compared to the tidal phenomenon in which the height of seawater changes vertically, algae move horizontally, and Korea's west coast is known to be the three most severe tidal regions in the world, along with Canada's Pun Dee Bay and France's Saint-Michel Bay. As such, if the vertical tidal phenomenon of seawater is severe, the horizontal tidal flow becomes fast, and marine accidents such as ship stranded occur frequently. Particularly, seawater cooled in winter begins to rise in temperature from the surface of the sea from April to May, and when seawater is mixed due to the temperature difference between the surface of the coast and the deep sea, the flow of algae increases. Frequent fog occurs due to the formation of electric wires, so caution is needed in ship navigation.

Another aspect of the underwater environment is that the bottom of the sea floor is piled up with light-type soil of tens of centimeters to tens of meters, and soil is pouring out of the Yellow River in China, making the sea foggy. Particularly, it is very

important to secure visibility in the event of a marine accident for the soil environment caused by severe turbidity and floating matter. Figure 3 shows diving activities in various underwater environments.

Figure 3: Diving activities in various underwater environments

In this study, depending on the worst underwater environment, the lifting device is implemented in consideration of the mesh structure, portability, weight reduction, and operability to reduce buoyancy in water. It is characterized by designing a lifting device in the form of an integrated lifting device and a surface marker Buoy (SMB), and firing a CO2 cartridge to quickly discharge it to the surface of the water. The 33g CO2 cartridge attaches two manipulators to attach two to the lifting mechanism. Until now, it is understood that no lifting net-integrated airbag has been developed yet.

The lifting mechanism utilizes the effect of rising to the surface of the water through the underwater bombardment of the CO2 cartridge. The air cartridge method was applied while requiring the portability and rapid operation of the lifting device. Therefore, research on securing the reliability of the rapid lifting and lifting process is continuing. Figure 4 compares the mesh-type lifting device designed as an early prototype with the lifting device used by the National Police Agency's scientific investigation unit.

2.2. Design of Lifting Instruments

The lifting device design is designed in consideration of mass production through portability, convenience and simplicity of use, production cost reduction, and mold improvement, and components are designed in consideration of the efficiency and convenience of underwater work. At this time, the flow rate and quantity are calculated by applying Boyle's law to secure the flexibility of the lifting mechanism in water. Figure 4 explains the Boyle law for the quantity and flow rate experiment flowing through the lifting mechanism. Here, d represents the length, A represents the cross-sectional area, Q represents the flow rate, t represents the time taken, and $\bar{v}$ is the average speed. We can explain the Figure 4 as follows an equation (1)

$$\mathrm{Q} = \frac{V}{t} = \frac{Ad}{t} = A\,\bar{v},\ \bar{v} = \frac{d}{t} \tag{1}$$

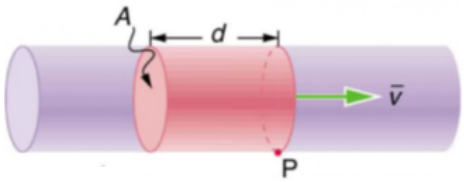


Figure 4: Designing the flow rate and quantity flowing through the lifting device

Lightweight is needed to minimize weight underwater and ease portability. The flow rate is calculated to secure flexibility as follows the equation (2).

$$\mathrm{Q} = \mathrm{Av},\ \ \mathrm{A} = \frac{Q}{v} = \frac{\pi}{4}\,d^2, d = \sqrt{\frac{4Q}{\pi v}} \tag{2}$$

Figure 5 uses TPU, a light and renewable durable material that taking account of the quantity and flow rate flowing through the lifting mechanism. The inlet of the lifting instrument plays an important role in underwater work. In addition, it is designed with a mesh structure so that the human body and water entering the entrance exit at a high speed.

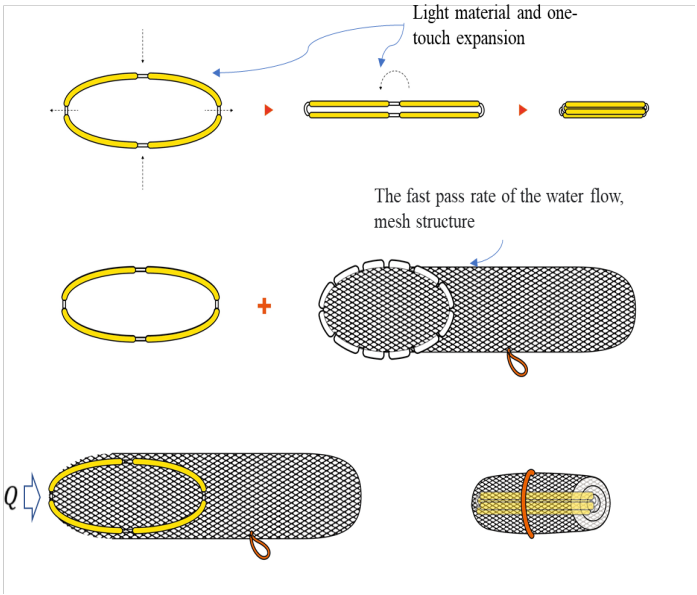


Figure 5: Detailed Design of Lifting Appliances

When the diver enters the water, the amount of oxygen in the oxygen tank is compressed, increasing the fatigue of the underwater worker. The deeper you get into the water, the more oxygen (within 30 minutes) shrinks, and the faster the work should be done in consideration of the falling time, working time, and rising time.

Figure 6 shows the operation of underwater using the designed lifting mechanism rule. Use the hook law for tensile stress and load during underwater operation. In equation (3), $\sigma(\mathrm{kg}/cm^2)$ is tensile stress, P is load (tension), E is cross-sectional area, and is elastic coefficient.

$$\sigma = \frac{P}{A} = E\epsilon = \frac{M}{Z} \tag{3}$$

here, ϵ is the coefficient, $M(cm.kg)$ is the silver bending moment, and $Z(cm^3)$ represents the cross-sectional coefficient. Use durable material TPU 80 and 95 for the bow.

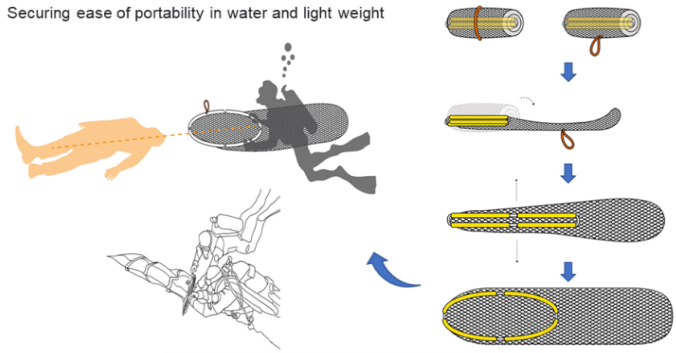


Figure 6: Underwater working behavior

In order to maintain extreme bending or the shape of the round part when combining the hinge and the bow, the occurrence of play due to elastic loss over time was minimized. The hinge connection was designed with a cross-shaped double support structure, but it was very difficult to maintain its shape due to tension loss. Therefore, it was designed with a support structure of thickness and width that gradually became thinner around the bow, and which developed into a two-piece one-stage structure. Figure 7 shows the double support structure and design for maintaining the roundness value and shape.

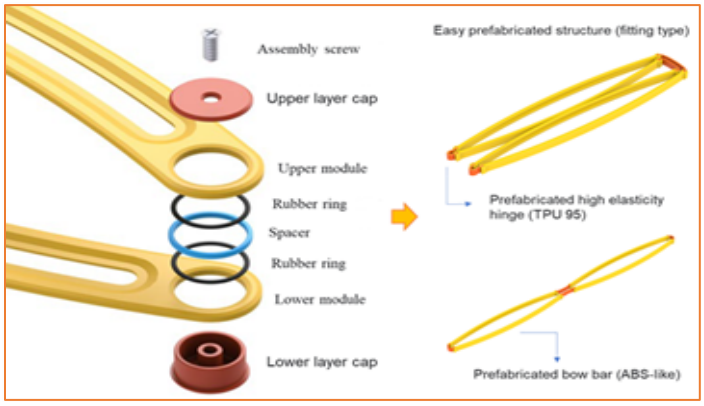


Figure 7: High elasticity hinge design and detailed schematic

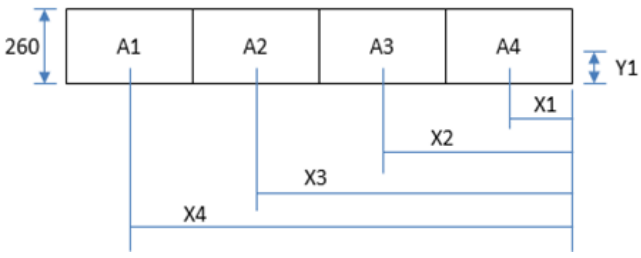


Figure 8: The lifting mechanism of network structure

When the human body is inserted into the lifting device and raised to the sea level, the weight balance technology of the network structure is applied to configure the head to face the sea level. The lifting mechanism uses a formula $h1 = h2 = h3 = h4 = h$ and $Y1 = Y2 = Y3 = Y4$ to design a weight-balanced algorithm for 2000x260mm SMB and network structures, which can calculate X1, X2, X3, and X4 differently. Figure 8 shows the weight balance algorithm of the lifting mechanism network structure. Figure 8 shows the lifting mechanism of network structure.

Figure 9 shows the weight balance algorithm of the lifting mechanism network structure based on figure 8.

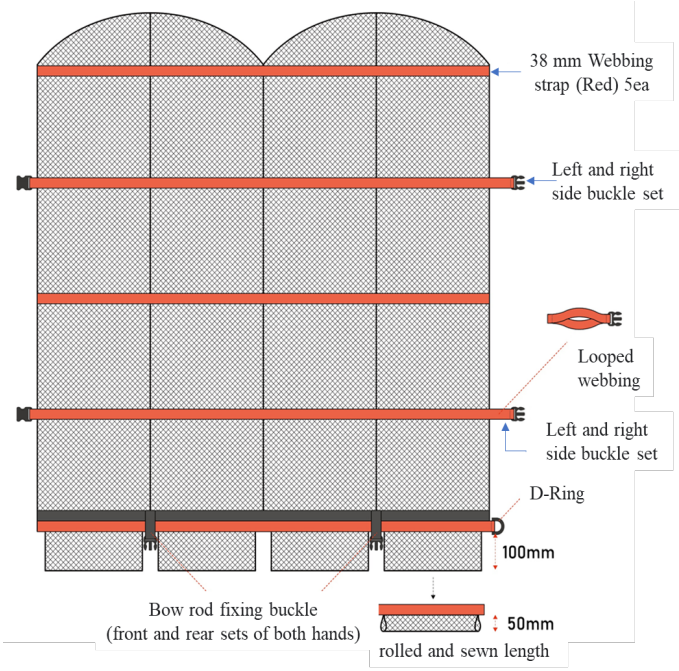


Figure 9: Weight balance algorithm of the lifting mechanism network structure

On the other hand, in water, SMB (Surface Marker Buoy) is designed in a form with a certain slope. The equation for volume and area S of SMB is as follows;

$$S = \frac{(a+b)}{2} h, \quad F_i = \rho V_i g \tag{4}$$

here, F_i is the buoyancy, ρ is the density of water and g is gravity acceleration. The scientific design of the lifting mechanism take into account for the weight held when underwater and the ease of work due to underwater internal force. Particularly, after inserting a dead body into a lifting device, weight balancing technology is applied to configure the head to face the sea level. Figure 10 shows the design cases according to the length of the SMB and mesh net with a certain slope.

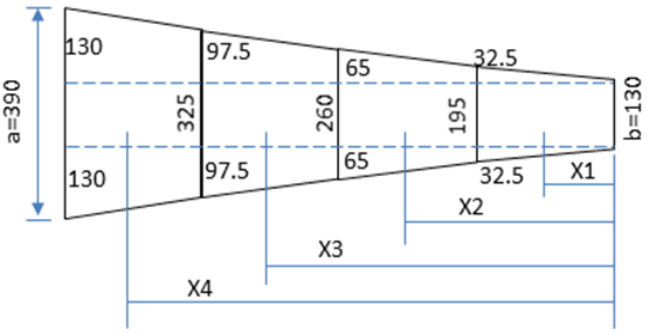


Figure 10: SMB and mesh gradient angle with constant gradient

Figure 11 shows the lifting mechanism packaged with the designed SMB and mesh network. Tightening devices were added to both sides in consideration of the expansion of the lifting mechanism. In the SMB header part, it has the pump valve, and the oral inflator are valves that take account of CO2 loss, and consist of an air inlet using the last CO2 cartridge.

Figure 11: Lifting device packaged with a mesh net

When working at a depth of 20 → 30 → 40m each, the worker's physical strength decreases severely due to securing time to the surface of the water and the difference in buoyancy of the human body [5]. When working in pairs, it is very important not to lose a team member. Considering that the maintenance time of the oxygen tank held by the underwater worker is 30 minutes, it takes more than 2 hours of sufficient rest time on the water surface. Figure 12 shows the folding method and size of the lifting device packaged with SMB and mesh net.

Figure 12: Folding method and size of lifting appliance packaged with SMB and mesh net

Figure 13 shows the monitoring tracking system and surrounding accessories. The monitoring system plays a very important role in securing the location of the lifting instrument and the location of underwater workers [2, 6]. The underwater ultrasonic sensor signal is supplied using a USB port, and the O/S is configured with Linux. In the commercialization stage of the lifting system, low-end type development is easy and compatibility is wide.

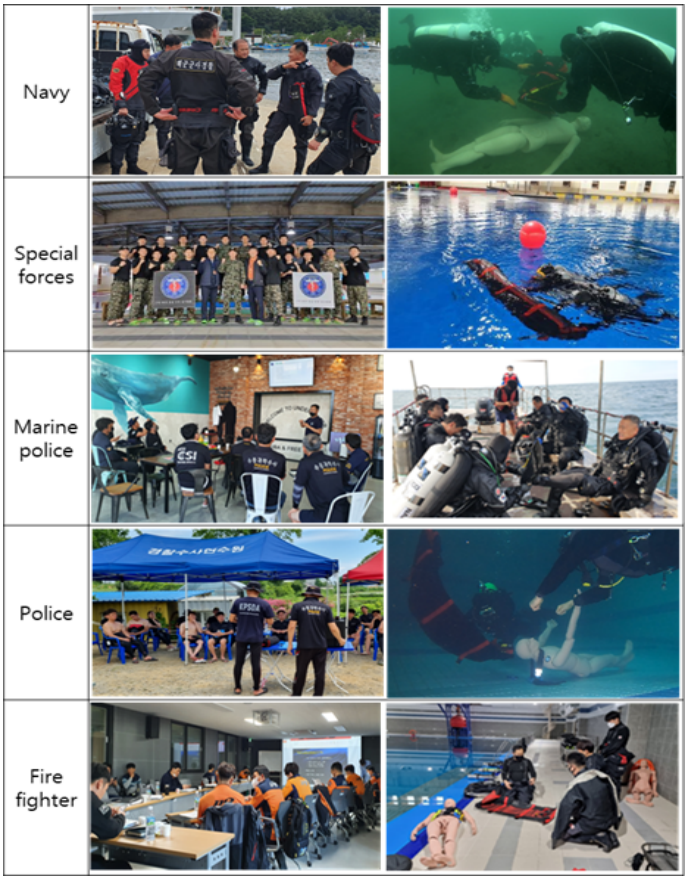


Figure 13. Monitoring position tracking system and peripheral accessories

3. Experimental Results

3.1. Experimental Scenarios

The design of the lifting device is optimized based on various underwater environment data through prototype development. Korea's underwater environment is characterized by severe waves on the east coast, and the water quickly darkens except between sunrise and sunset. In the case of the west coast, the turbidity is so severe that it is difficult to check 1m ahead, and there is a risk that everyone will be exposed to safety accidents. Particularly, despite the difficulty of the test environment due to the tangled waste and mud, this can be explained as the worst lifting condition in the event of an accident.

The quantity and flow rate flowing through the lifting mechanism, renewable materials, and durable designs were selected. Safety and efficiency are the top priorities of the package-type human lifting system in which the lifting device rises to the surface through the underwater shooting of the CO2 cartridge. Particularly, the GAS injection method SMB was packaged with a mesh network to minimize the time spent underwater through the convenience, weight reduction, and rapid

operation of rescue workers. Through this, an experiment was conducted on securing the reliability of the rapid lifting and lifting process.

When the depth of the water deepens, the diver's decompression limit time is 8 minutes for work above 40m, and the effective air capacity of the air tank is reduced by 1/4 by water pressure. After 20→30→40m of underwater entry work, the worker's physical strength is severely deteriorated due to the difference in buoyancy of the human body and securing time to come to the surface of the water. When working in pairs, it is very important not to lose the group due to underwater forgetting. Considering that the maintenance time of the oxygen tank held by the underwater worker is 30 minutes, it takes more than 2 hours of the sufficient rest time, Particularly, musculoskeletal diseases, mental diseases, and rheumatism that appear in divers are the reasons why sufficient rest and management are needed after underwater work. Figure 14 shows awareness of fatigue and stress that may appear after work.

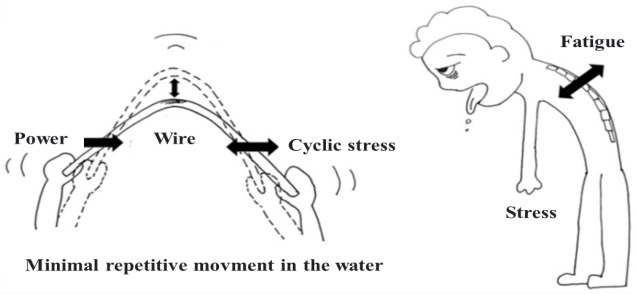


Figure 14: Awareness of fatigue and stress after work

The underwater communication test was conducted in real time from 6m to 40m in depth. The ultrasonic sound sensor is converted to 2,400bps and verifies the transmission error according to the binary. The communication speed from sensor to monitor is 115,200bps, and the communication speed from controller to receiver is 2,400bps.

Figure 15: Performing underwater work based on various environment

In order to gain the reliability of the experiment, public-private forces (Navy, Marine Police, Fire Department, and Public Safety Submersible Association) jointly conduct underwater human lifting training and experiments. Particularly, it was based on the experience of participating in Ferry Sewol events in Korea's West Sea (Korea Public Safety Submersible Association), and it was found that securing the safety of divers was also very important by conducting experiments based on various marine environment data. Figure 15 shows each participating organization that performs underwater work based on various environmental data, including the author. The organizations that participated in the study included naval special teams, maritime police, land police, firefighters and divers.

3.2. Lifting Appliances Experiment

Figure 16 compares the performance of each prototype with the proposal of a lifting mechanism of the rotary ring method, zipper and yelcro method, and ring cage method.

Figure 16. Comparison of the rotating ring method, zipper and Velcro method, and Linkage method

The rotating ring method of the initial prototype takes time to fasten in the rotating ring, and the weight is increased underwater using a mesh net made of plastic. In particular, it was difficult to dive more than 10m due to buoyancy when diving into the water. The zipper and Velcro method is a form of combining a straight SMB and fastening the inlet to a mesh net made of plastic with a zipper. When gas is injected into a straight SMB, it takes time because the body is not centered when it rises to the surface, and in the case of an old body, damage was feared. Lastly, the SMB integrated package bag type of the GAS injection method is a lightweight TPU 80 material and the entrance is designed for durability and flexibility.

The product used in the diving investigation department of the Korea Coast Guard requires rapid discharge due to the hops of the human body and the water accommodated through the entrance, and swells underwater, causing inconvenience in working. In order to protect the lifting device SMB, the relief valve provides a function of automatically maintaining a constant pressure by discharging air when the pressure inside the airbag increases. The water pressure corresponding to 5 atmospheric pressure is formed on the seabed surface of 40m deep, so the air capacity is reduced to 1/5 when the air cartridge is operated. When the water pressure decreases as the lifting mechanism rises, the air inside the lifting mechanism relatively increases. When the pressure or more is

formed in the lifting mechanism, air is discharged through the relief valve, and the pressure is controlled. Figure 17 shows the disassembly and assembly process of the relief valve.

Figure 17: Disassembly and assembly of relief valves

Figure 18 shows the water surface rise of the lifting mechanism according to buoyancy and weight after injecting CO2 gas into SMB. The lifting mechanism begins to tilt according to buoyancy and weight, tilting in the vertical direction such as 16.68° for S1, 22.78° for S2, 28.40° for S3, and 33.39, and rising to the surface of the water.

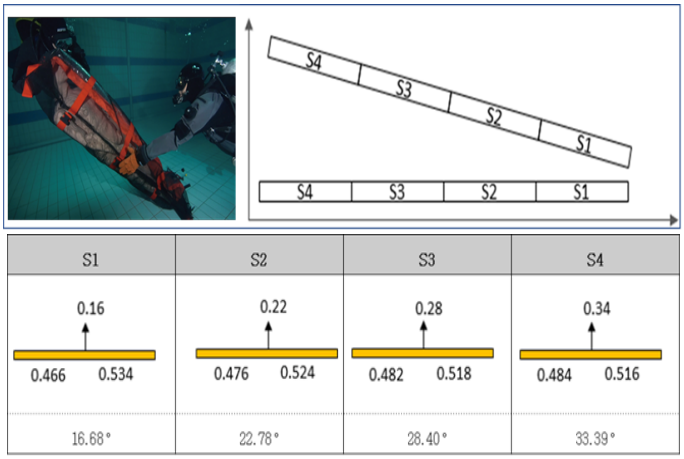


Figure 18: Water level rise of lifting equipment according to buoyancy and weight after CO2 gas injection into SMB

Table 1 shows the underwater characteristics according to diameter, length, weight, and burst pressure according to the CO2 cartridge specification.

Table 1: Underwater data according to CO2 cartridge specification

Vol.(cc)	Dia.(mm)	Length(mm)	weight (g)	Burst pressure (Bar)	Mouth Con.
18	22	88	70	450	No thread
25	25	95	90	450	3/8-24 UNF
32	25	107	105	450	1/2-20 UNF
42	22	160	117	450	No thread
45	22	248	225	450	No thread
60	30	120	155	450	1/2-20 UNF
61	22	248	225	450	No thread
95	40	138	275	450	5/8-18 UNF
110	40	150	450	245	M16 x 1.5

The buoyancy of the lifting instrument was 7-5, 9-5, rotary, and when folded, buoyancy and rising experiments were conducted. At this time, the measured weight = actual weight - was calculated as the weight of the substituted fluid, and the density / fluid density = weight / weight of the substituted fluid.

Table 2: Buoyancy of lifting instruments

Type	Trans. (m)	Length (m)	Height (m)	Volume (㎥)	Buoyancy (N)	Decision
7-5 type	2.00	0.70	0.05	0.070	686.70	rising
9-5 type	2.00	0.90	0.05	0.090	882.90	rising
Cir. Guide	6.00	3.14	0.03	0.00565	55.45	rising
Folded type	1.00	3.14	0.18	0.00565	55.45	rising

The lifting device uses a lifting device with a 4-link bridge structure as a group of two, but it was developed to enable rescue activities for one person. Particularly, the 4 -links inlet of the lifting device is designed to be easily handled by folding once after capturing the human body. In addition, a fastening device was installed to facilitate the expansion of the package that the human structures were simultaneously performed. Figure 19 shows cases such as SMB-integrated package type, SMB separation type, human lifting buoyancy experiment scene, and three-person expansion.

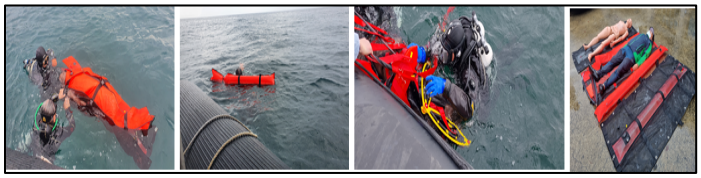


Figure 19: Experiments of SMB package, SMB detachable type, human lift buoyancy check.

Figure 20 shows that marine police and naval investigators are equipped with lifting instruments and conduct underwater experiments. Underwater gravity, underwater weight, weight of the lifting instrument, and total weight of the lifting instrument were measured for the total weight of 120 kg equipped with the equipment equipped with the diver and the lifting instrument package.

Figure 20: Underwater experiments of lifting instruments by maritime police and naval personnel

Gloves are worn to maintain the body temperature of underwater divers, but the working time may be extended due to a decrease in body temperature, and if the lifting device is complicated, it may take excessive working time.

Table 3: Total weight of underwater gravity, underwater and weight

Weight	Gravity of the lifting object	Weight of under water(kg)	Air lifting appliance	Appliance weight (kg)	Total weight (kg)	Gravity (N)
120.00	1.05	6.00	3.00	1.00	7.00	68.67
	1.10	12.00		1.00	13.00	127.53
	1.20	24.00		1.00	25.00	245.25

An example of experimenting is a lifting mechanism packaged with a GAS injection-type SMB and a mesh net at a depth of 40m.

At this time, the season was around May, and the experiment was conducted from 10 a.m. to 12 hours. To secure an underwater view, an LED lantern was equipped, and an experiment was conducted in an environment with a good wave of 2 to 3m. The experiment was completed in a short time as the oxygen supply was reduced to 20 to 25 minutes.

Figure 21 shows the buoyancy formation, acceptable weight, underwater pressure, air injection time and buoyancy, results of the lifting mechanism in accordance with the CO2 cartridge explosion in the experiments of Table 3.

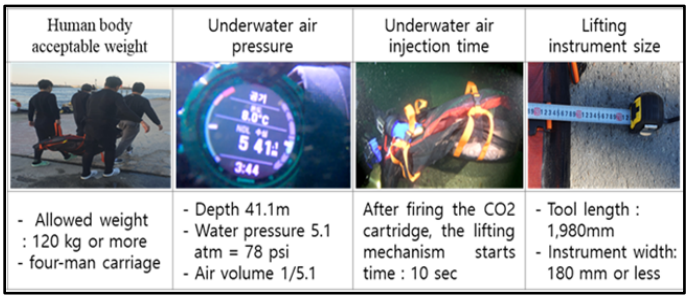


Figure 21: Flotation experiment according to CO2 GAS cartridge explosion at a depth of 40m

Underwater human lifting tests were conducted from 10:00 a.m. to 12:00 p.m. and 14:00 p.m. to 16:00 p.m. from November to December 2021, spring for a month between April and May 2022, and 30 to 40 experiments were conducted over four seasons from October to November 2022.

3.3. Experiment of a location tracking monitoring device

Figure 22 is the main screen of the monitoring device and shows the monitor layout in consideration of the environment of use, such as the lifting instrument state map, location information, and additional functions. The control system is a portable system that is convenient to move and receives sensor signals based on Linux O/S using a USB port. At this time, the temperature measurement data according to gyro, acceleration, and water depth are shown.

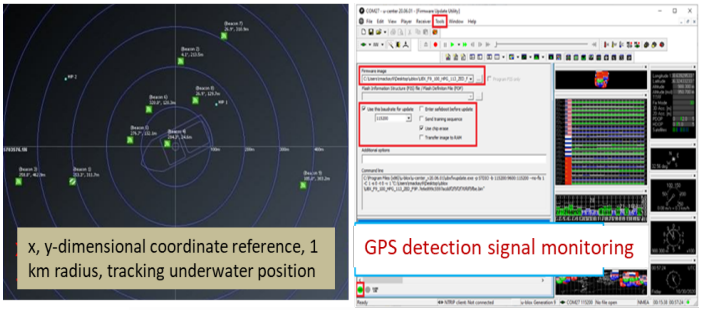


Figure 22: Lifting Status Map and Monitoring Display

Table 4: Measurement data according to gyro, acceleration, depth, and temperature

	Gyro			Acceleration			Depth of the water	Temperature
	yaw	pitch	roll	x-acc	y-acc	z-acc		
0m	130.31	-64.5	77.31	-8.85	-4.29	0.61	-0.11	23.29
-1m	38.13	-81.12	179.25	-9.66	-0.13	-1.4	0.85	23.38
-2m	191.44	-82.56	-172.13	-9.69	0.07	-1.36	1.94	23.49
-3m	97.56	-83.19	179.19	-9.71	-0.19	-1.15	2.96	23.54
-4m	10.81	-82.94	166.56	-9.75	-0.28	-1.03	3.93	23.58
-5m	87.69	-84.25	177.5	-9.78	-0.45	-0.9	4.93	23.63
-6m	252.63	0.37	-119.31	0.05	8.54	-4.61	5.63	23.63

Figure 23 shows the results of experiments on the communication distance and communication speed between the monitoring device and the underwater transmitter located on land and sea.

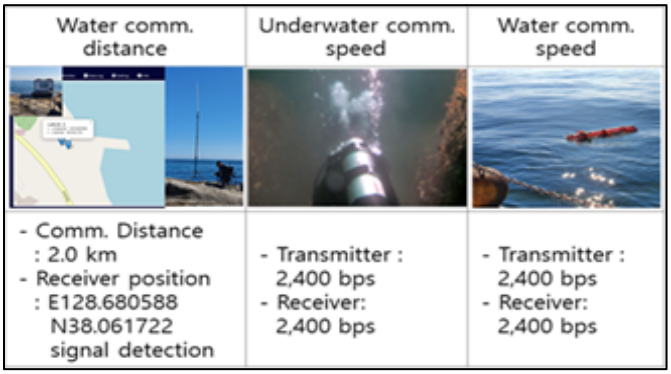


Figure 23: Experiments on the communication distance and speed of the monitoring device

The control monitoring device is portable and receives a sensor signal using a USB port. It can be configured with Linux O/S to provide a wide range of compatibility.

4. Conclusion

In the event of an underwater accident in the ocean or land, this study efficiently lifted the human body and implemented a gas injection-type prefabricated lifting device based on location tracking. To secure golden time and the safety of divers, the efficiency and safety of the lifting system were considered as the top priority for saving lives underwater.

At 40 m underwater, divers must endure up to 30 minutes with two air cylinders, and the worst underwater experimental environment conditions such as securing visibility and dangerous environments with high flow rates were selected due to underwater turbidity. Particularly, there are many cases where life is threatened by hypothermia in the water. Therefore, both divers and the deceased need location tracking connected to the lifting device, and a fast and efficient lifting system was studied in underwater activities.

The gas injection-type prefabricated lifting device with a high elastic structure is lightweight and portable, and a baggy bag is composed of minimal components to increase the use method and work efficiency based on the instinctive behavior of the diver. Accordingly, the entrance element design combining a bow and hinge that maintains a moment of force with TPU-based materials, the balance design using weight balancing technology of the network structure, the SMB linkage design that induces water

surface rise through gas injection, and the entire assembly were tested underwater.

Coast Guard, special investigators, and fire officials participated to improve reliability by using a situation where turbidity was very high and the flow rate of underwater sites was high as the worst field experiment conditions. Due to turbidity, the West Coast's two-person rescue experiment was also exposed to safety accidents, and the study was conducted in a way that auxiliary diving personnel performed guard duties in preparation for safety accidents.

As the water pressure increased by 1 atmosphere every 10m deep, the amount of air in the lifting appliance was compressed to 1/2 compared to the land, and it was found that using one CO_2 cartridge for 60kg underwater mannequin sufficiently reached the surface of the water.

When the water depth decreases in the process of the lifting instrument rising from the seabed to the surface of the water, the water pressure decreases at the same time. At this time, the air inside the lifting device expands and the pressure rises, as it reaches the water surface, the pressure control valve attached to the lifting device operates to discharge air and maintain constant pressure. When 38g of the CO_2 cartridge was injected at a depth of 40m, it took about 10 seconds for the water lift to start, and at the same time as lifting the human body, a manual for securing the safety of the diving source could be established.

At 40m underwater, water depth, water temperature, and direction angle were transmitted to rescue personnel on the water surface as a location detection signal through monitoring and the start of water rise of the lifting device. At a depth of 40m, the lifting test calculated the diving agent's acquisition time, working time, and time taken to get out, considering the oxygen content of about 30 minutes. At this time, the time available for work was as short as eight minutes.

The location tracking monitoring device of the lifting device was implemented in consideration of underwater lifting situation information storage, display, and waterproof functions. LTE technology for short-range and long-distance communication was applied to the acoustic sensors obtained underwater, and interface functions were expanded through USB ports. In the future, we will focus on portability, weight reduction, low battery power, and extended life time.

References

[1] J. H. Yoon, D. H. Yoon, “A Human Lifting and Navigation System Based on ICT for Underwater Rescue,” 2022 The 22nd International Conference on Control, Automation and Systems (ICCAS 2022) BEXCO, Busan, Korea, Nov. 27~Dec. 2022

[2] J. H. Yoon, S. I. Kang, D. H. Yoon, “Implementation of ICT-based Underwater Communication Monitoring Device for Underwater Lifting,” Institute of Korean Electrical and Electronics Engineers (IKEEE), **26**(3), 396~400, 2022

[3] D. H. Yoon, “Location Tracking Apparatus and Method in Water Accident or Emergency Situation,” Patents No.10-2020-0142370, Sept. 2020

[4] H. K. Min, D. H. Yoon et al, "Information Transmission System of Lifting Apparatus" Patents No.10-2020-0127360, 2020

[5] D. H. Yoon, M. H. Park, "Water Accident Emergency Response System and Method Thereof”, Patents 10-2020-0126397, 2020

[6] D. H. Yoon, “Boat Aerostat Production Apparatus and Method for Safety Strengthen Based on Manufacture Convergence,” Patents No.10-2020-0137878, 2020

[7] Science and Technology, “System Assessment and Validation for Emergency Responders (SAVER),” U.S. Department of Homeland Security, 2021

[8] Central Maritime Safety Tribuna, “Announcement of Maritime Accident Statistics in 2021”

[9] H. K. Min, N. H. Seong, et al, “Development of ICT-based human body lifting system for underwater structures”, Techinical Report, Ministry of SMEs and Startups, 2021

[10] J. G. Kim, “The Design and Implementation of Seabed Auto-interpretation System Using Ultrasonic Signal Processing”, 2001

ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 8, No. 6, 87-95 (2023)

www.astesj.com

Special Issue on Innovation in Computing, Engineering Science & Technology

ASTESJ

ISSN: 2415-6698

Towards Real-Time Multi-Class Object Detection and Tracking for the FLS Pattern Cutting Task

Koloud N. Alkhamaiseh[*,1], Janos L. Grantner[2], Ikhlas Abdel-Qader[2], Saad Shebrain[3]

[1]*Department of Computer Science, Michigan Technological University, Houghton, 49931, MI, USA*

[2]*Department of Electrical and Computer Engineering, Western Michigan University, Kalamazoo, 49008, MI, USA*

[3]*Western Michigan University Homer Stryker MD School of Medicine, Kalamazoo, 49008, MI, USA*

ARTICLE INFO

Article history:
Received:26 April, 2023
Accepted:08 October, 2023
Online: 30 November, 2023

Keywords:
Laparoscopic surgery
Object detection
Bag-of-freebies
FLS pattern cut

ABSTRACT

The advent of laparoscopic surgery has increased the need to incorporate simulator-based training into traditional training programs to improve resident training and feedback. However, current training methods rely on expert surgeons to evaluate the dexterity of trainees, a time-consuming and subjective process. Through this research, we aim to extend the use of object detection in laparoscopic training by detecting and tracking surgical tools and objects. In this project, we trained YOLOv7 object detection neural networks on Fundamentals of Laparoscopic Surgery pattern-cutting exercise videos using a trainable bag of freebies. Experiments show that YOLOv7 has a mAP score of 95.2, 95.3 precision, 94.1 Recall, and 78 accuracy for bounding boxes on a limited-size training dataset. This research clearly demonstrates the potential of using YOLOv7 as a single-stage real-time object detector in automated tool motion analysis for the assessment of the resident's performance during training.

1. Introduction

This paper is an extension of work originally presented in DICTA 2021 [1]. In this project, more data is collected and prepared to train YOLOv7 [2] as a real-time object detector of laparoscopic tools and objects in the Fundamentals of Laparoscopic Surgery (FLS) pattern-cutting exercise using a box trainer [3]. Laparoscopic procedures have become increasingly popular in operating rooms worldwide due to their numerous benefits, leading medical schools to incorporate this technique into their surgery curricula [4]. However, the one-on-one apprenticeship model is subjective and time-consuming. To address this issue, laparoscopic trainers and simulators have become well-accepted alternatives that allow for safe and harm-free training [5]. Although simulation systems offer objective measurements and remote training, expert surgeons are still required to assess surgical skills proficiency. Virtual Reality (VR) training provides a completely virtual environment with haptic feedback and complex software, but it is expensive and requires highly sophisticated mechanical design [6]. By improving the real-time object detection of laparoscopic tools and objects, this project aims to enhance the effectiveness and accessibility of laparoscopic training.

Box trainers and physical trainers provide a practical environment for using real laparoscopic instruments to improve basic skills such as knotting, handling objects, and cutting tissues. While time is currently the primary metric for evaluating a surgeon's performance using statistical tools, studies have shown that box trainers enhance trainee confidence and dexterity [7], [8]. However, objective assessments of laparoscopic skills still require experienced surgeon evaluations. To address this issue, hybrid trainers combine the benefits of simulators and physical trainers to recreate real-world conditions and provide objective assessments through integrated software. Hybrid trainers provide a comprehensive approach to evaluating real-world situations by merging both simulators and physical trainers.

The emergence of deep learning [9] has proven to be a highly effective machine learning approach for detecting and classifying objects from raw data by learning representations from the data. Its superior feature extraction and expression capability has surpassed other machine learning methods in many areas, especially when dealing with large data sets. Therefore, deep learning appears to be a very promising method for detecting tool presence [9].

[*]Corresponding Author: Koloud N Alkhamaiseh, +12695449311 & kalkhama@mtu.edu

The main contributions of this research are as follows:

- Contribution to the creation of the first laparoscopic box trainer custom dataset, i.e., the WMU's Laparoscopic Box-Trainer Dataset [10]. This custom dataset was developed through a research collaboration between Western Michigan University's Department of Electrical and Computer Engineering and the Department of General Surgery at Homer Stryker M.D. School of Medicine. Researchers are free to download the dataset at their convenience. This dataset was created specifically to aid research in the field of Laparoscopic Surgery Skill Assessment. It consists of videos showcasing four different tasks on the Laparoscopic Box-Trainer - two precision cutting tests, intracorporeal suturing, and peg transfer. These videos were recorded by surgeons, surgical residents, and OB/GYN residents at the Intelligent Fuzzy Controllers Laboratory at WMU. You can access the dataset at https://drive.google.com/drive/folders/1F97CvN3GnLj-rqg1tk2rHu8x0J740DpC. The dataset also contains labeled images with related labels for all tasks, and more files will be added as the research progresses.
- Proposing a robust real-time multi-class object detection and tracking module based on YOLOv7 as a single-stage real-time object detection neural network for surgical tools and objects in FLS pattern cutting test.

The adoption of YOLOv7 is a wise choice because of its superior network architecture, precise object detection, efficient label assignment, and resilient loss function and model training. Moreover, YOLOv7 is more cost-effective than other deep learning models [2] and is highly proficient in detecting and tracking surgical tools and objects within spatial boundaries.

In order to fully explain our proposed system, this paper is organized as follows: Section 2 gives a brief introduction to the methods used for evaluating the performance of laparoscopic surgery training. In Section 3, we present our methodology. Section 4 contains a summary of our experimental findings, and in Section 5, we outline our plans for future work.

2. Background

FLS tool is widely used for psychomotor skill training in surgery. The American College of Surgeons (ACS) has created didactic instructions and manual skills to improve the basic laparoscopic surgery skills of surgical residents and practicing surgeons using the FLS box trainer [3].

The FLS box trainer, along with didactic instructions and manual skills, can help surgical residents and practicing surgeons improve their basic surgical skills. Current assessment methods focus on detecting surgical tools and analyzing motion, but it's also crucial to track surgical instruments during operations or training to analyze operations and assess training.

In a previous study [5], computer vision algorithms were used to assess performance during surgical tool detection, categorization, and tracking in real-time FLS surgical videos. An artificial neural network learned from expert and non-expert behaviors and a web-based tool was created for uploading MIS training videos securely and receiving evaluation scores with trainee performance analysis over time. The assessment used a multi-dimensional vector consisting of smoothness of motion, proficiency of surgical gestures, and number of errors.

Another study [6] presented a trainer for assessing laparoscopic surgical skills using computer vision, augmented reality, and AI algorithms on a Raspberry Pi programmed in Python. The assessment method employs an artificial neural network based on a predetermined threshold for the peg transfer task. A simulation of pattern-cutting was used to track laparoscopic instruments, while computer vision libraries counted the number of transferred points during the transfer task.

Recent advancements in deep learning, specifically CNN networks, have shown remarkable progress in computer vision tasks [11]. Various studies have implemented deep learning architectures to detect surgical tool presence in laparoscopic videos [12], [13], [14], and phase recognition [15].

Some projects have created systems that can detect laparoscopic instruments in real-time during robotic surgery, using the real-time detection algorithm of the CNN network. These systems are based on the object detection systems YOLO [16] and YOLO9000 [17], with a mean average precision of 84.7 for all tools. They also have a speed of 38 frames per second (FPS).

The available skill assessment frameworks have some limitations when it comes to evaluating fundamental laparoscopic skills based on globally accepted standards and criteria. These frameworks only focus on tool motion and do not consider surgical objects and their manipulation during training. For instance, the Objective Structured Assessment of Technical Skills (OSATS) [16] and the Global Operational Assessment of Laparoscopic Skills (GOALS) [17] are examples of such frameworks. To address this limitation, a new system was developed using a deep learning algorithm called YOLACT [18]. This system tracks surgical tool motion and detects surgical objects, including their deformability, shapes, and geometries in the surgical field of view. The system was tested on a modified FLS peg transfer exercise and provided a more comprehensive evaluation of laparoscopic skills beyond tool motion alone.

To evaluate the abilities of those performing intricate intracorporeal suturing, automated systems have been suggested. One such system, developed by the authors in [19], uses the latest versions of One-Stage-Object-Detectors like YOLOv4, Scaled-YOLOv4, YOLOR, and YOLOX. A dataset of suturing tasks was used to train this system, which strikes a balance between cutting-edge architectures. In [20], the authors proposed a skill evaluation system that employs Scaled-YOLOv4 and a centroid tracking algorithm.

The authors presented a fuzzy logic supervisor system for assessing surgical skills in [21]. This system used multi-class detection and tracking of laparoscopic instruments during standard FLS pattern-cutting tests. However, the system had limitations when the instruments or objects were not within view of the camera. To address this issue, a new autonomous evaluation system was proposed by authors in [22], which utilized two cameras and multi-thread video processing to detect laparoscopic instruments.

In addition, two fuzzy logic systems were implemented in parallel to evaluate left and right-hand movement. The authors in [23] have improved the YOLOV7x algorithm significantly for detecting surgical instruments. These enhancements effectively address concerns about dense arrangements, mutual occlusion, difficulty in distinguishing similar instruments, and varying lighting conditions.

To provide a more comprehensive assessment of surgical quality, our approach includes examining circle shape deformability, as well as laparoscopic tool tracking and detection in box trainer pattern cut test recorded videos.

3. Methodology

The FLS box trainer boasts multiple exercises, but we've focused on perfecting a pattern-cutting exercise. Our system centers around two circles printed on artificial tissue, with a radius of 2.5 and 3.0 centimeters for the inner and outer circles respectively Figure 1. Keeping the scissors within these circles is essential for this exercise, as crossing either circumference will result in an incorrect cut.

- In this paper, we propose a system that works seamlessly with our intelligent FLS box trainer. This system utilizes two cameras placed inside the box to record videos, which are then used to train a deep-learning object detector and tracker. We have employed powerful deep learning algorithms YOLOv7, which have set a new standard in real-time object detection. Our model has been trained, validated, and tested using a custom data set to track three objects - the scissors, the clipper, and the circle - within the box trainer's surgical view. The circle is the object that needs to be cut out, and this is achieved using laparoscopic scissors and clippers.
- Figure 2 illustrates the complete workflow of our method. First, we divide the recorded videos into frames and preprocess them before training the YOLOv7 network. After successfully training the model, it can accurately detect and track intended objects in both tested videos and real-time videos. Lastly, we calculate the performance evaluation parameters and generate an output video that displays the labeled surgical objects.

3.1. Network Architecture

The YOLO family of models has a long-standing association with the Darknet framework [24], tracing back to its inception in 2015 [25].

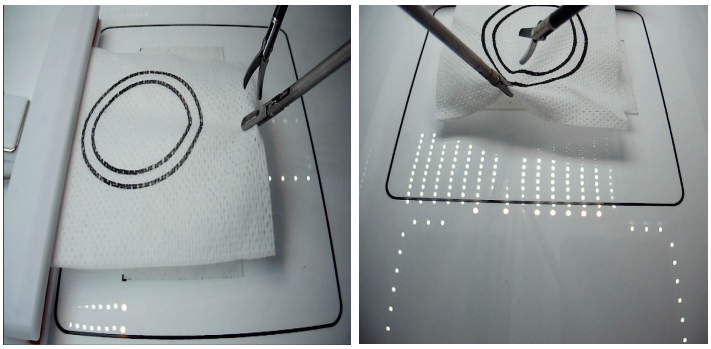


Figure 1: FLS Pattern cutting test setup views as captured by the two cameras.

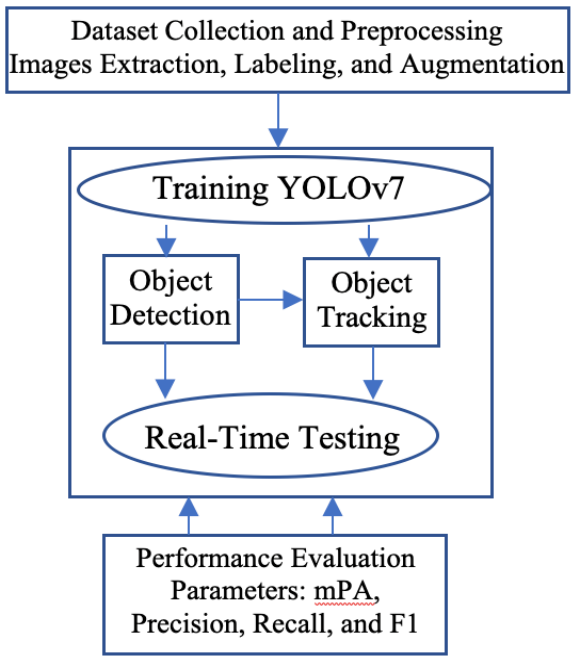


Figure 2: The proposed workflow chart.

The YOLO (You Only Look Once) detection layers rely on regression and classification optimizers to determine the necessary number of anchors. The image is divided into cells using a 19x19 grid, where each cell can predict up to five bounding boxes. However, some of these cells and boxes may not contain an object, so a probability of object presence (PC) is utilized to remove low-probability bounding boxes. Non-max suppression is subsequently used to select the bounding boxes with the highest shared area. YOLO has many versions and variants that enhance performance and efficiency.

The most recent official version, YOLOv7, was created by the original authors of the architecture. It is a single-stage real-time object detector and, according to the YOLOv7 paper [2], it is currently the fastest and most accurate real-time object detector available.

- E-ELAN (Extended Efficient Layer Aggregation Network): It is the computational block in the YOLOv7 backbone, in which the network learns faster by expanding, shuffling, and merging cards to continuously improve its ability to learn without destroying its gradient path.

- Concatenation-based model scaling allows the model to maintain the properties that it had at the initial design and thus maintain the optimal structure.
- To replace the convolutional layer or residual with re-parameterized convolution, planned re-parameterized convolution without an identity connection uses RepConv.
- Coarse for auxiliary and Fine for lead loss: As YOLOV7 includes multiple heads, the Lead Head is responsible for the final output, and the Auxiliary Head is used to train in the middle layers as illustrated in Figure 3 (a). Loss assists with updating the weights of these heads, allowing for Deep Supervision and better model learning. A Label Assigner mechanism was introduced to enhance deep network training, which considers the network prediction results and ground truth before assigning soft labels as shown in Figure 3 (b). Unlike traditional label assignment methods that generate hard labels based on given rules by directly referring to the ground truth, reliable soft labels use calculation and optimization methods that also consider the quality and distribution of prediction output together with the ground truth.

YOLOv7 introduces important reforms that significantly improve real-time object detection accuracy while keeping inference costs low. Compared to state-of-the-art real-time object detections, YOLOv7 reduces parameter and computation costs by about 40% and 50%, respectively, resulting in faster inference speeds and higher detection accuracy [2]. YOLOv7 has a fast and robust network architecture that integrates features, provides better object detection performance, and employs an efficient model training process with a robust loss function and label assignment. Overall, YOLOv7 represents the best option for optimizing real-time object detection.

3.2. Dataset

Our laparoscopic detection and tracking project requires a dataset annotated with spatial bounds for objects and tools. To achieve this, we extracted 1572 labeled images from 13 videos ofthe FLS pattern-cutting test, recorded by an expert surgeon and residents from the School of Medicine at Western Michigan University [26]. These videos have a resolution of 640x480 pixels and a frame rate of 30 frames per second and were carefully selected to accurately depict various instrument scenarios, lighting conditions, and angles. We resized the images to 416x416 pixels with auto orientation as a preprocessing step.

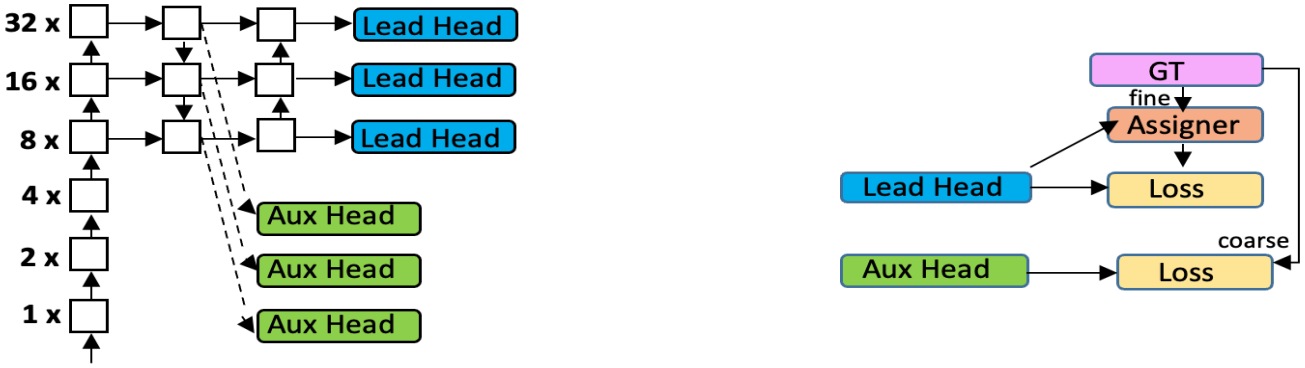
Figure 4 displays a ground-truth example utilizing a free preprocessing tool from Roboflow [27]. This tool manually labels the three intended objects- circle, clipper, and scissors in each frame. To augment our dataset's sample size, we employed various techniques, such as affine transformations, rotations, cropping, shearing, hue saturation, and blurs, as depicted in Figure 5. To ensure accuracy, new pixels were filled with the average RGB value of the corresponding image, which has proven to be highly reliable [28]. Our augmentation step yielded 3,458 images, with 87% designated for training, 8% for validation, and 5% for testing. The dataset's distribution of instruments and objects is outlined in Table 1.

3.3. Evaluation Criteria

To evaluate our work, we used box loss, objectness loss, classification loss, precision, recall, and mean Average Precision(mAP) as performance metrics. Figure 6 depicts these metrics. By measuring box loss, we were able to determine the algorithm's ability to accurately locate the center of an object and ensure that its bounding box adequately covers it. Objectness measures the probability that an object exists within a proposed region, serving as a confidence metric. High objectness indicates a greater likelihood that an object will be visible in the image window. Classification loss evaluates the algorithm's ability to predict the correct object class. Ground-truth intersection over union (GIoU) refers to the overlap between the ground-truth region and the detection result region. In the context of GIoU judgment, precision is the ratio of true positives to total detections. Meanwhile, recall is the ratio of successful detections to the total number of classes. The mAP, on the other hand, displays our bounding box predictions based on various GIoU thresholds set at mAP@0.5:0.95 and mAP@0.5 on average. To obtain the final estimate, the AP value is computed for each class across all GIoU thresholds, and the mAP is averaged for all classes.

Table 1: Details of the dataset: The number of instances for each instrument type is shown, distributed over 1572 images, and the resulting augmented sample size is included.

Object type	Instant samples	Augmented sample size
Scissors	1253	3759
Clipper	1289	3867
Circle	1432	4296
Total instances	3974	11922
Images	1572	3458



(a) The addition of an auxiliary head is included in the model. (b) Coarse-to-fine lead guide assigner.

Figure 3: YOLOV7 multiple heads and Label Assigner [2].

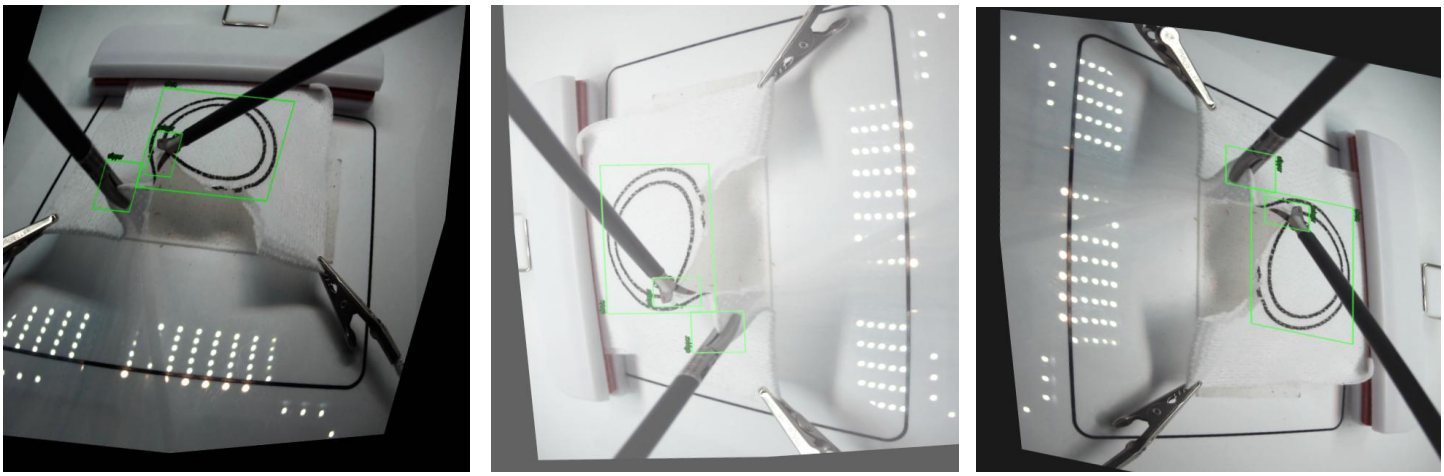


Figure 5: Some sample images for preprocessing using augmentation techniques.

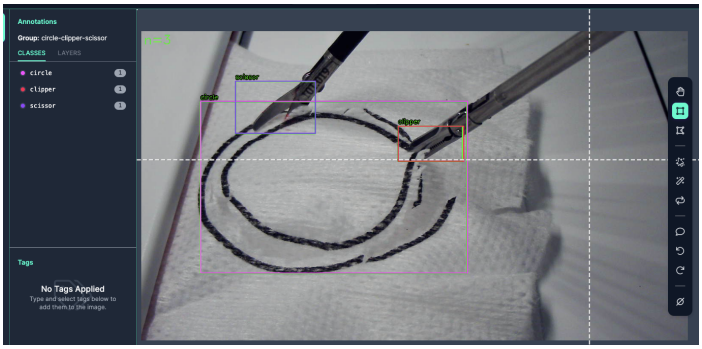


Figure 4: Image labeling process ground-truth example.

4. Experimental Results

This section outlines the setup used to train and evaluate CNN-based models for FLS trainer pattern-cutting test instrument recognition and tracking. We utilized a notebook developed by Roboflow.ai [29] to train YOLOv7 with our custom dataset and yolov7_training.pt pre-trained weights.

4.1 Training

To train YOLOv7, the proposed system used the Tesla P100-PCIE-16 GB GPUs with 56 processors and 16,280 MB of memory obtained from Google Colab [30]. To implement the process and validate the performance of the model scripts, several Python libraries were used (e.g., in [31] and [32]). The YOLOv7 model was trained with 416 x 416-pixel images, 16 batches, and 200 epochs. The training process took 3.357 hours with 10.6G of GPU memory.

4.1 Quantitative and Qualitative Results

In this subsection, we quantitatively and qualitatively evaluate the performance of our approach to detecting and tracking the FLS laparoscopic instruments and objects in the pattern-cutting test using YOLOv7.

The performance details during the training and validation phases are presented in Figure 6 and Table 2. Along with the losses, precision, recall, and mean average precision were calculated using GIoU thresholds of 50% and 50%:95% for up to 200 iterations. The model's precision, recall, and mean average precision exhibited rapid improvement, stabilizing after roughly 100 epochs with minor fluctuations at the start. Moreover, the validation data's classification loss decreased significantly until approximately epoch 50. To select weights, early stopping was employed.

Further, Figure 7 presents a precision-recall curve that provides a granular performance indicator for each class. The PR curve analysis indicated that the circle provided the highest performance (98.7%), followed by the clipper (95.9%), and the scissors (91.0%). It was expected since the scissors were not always clearly visible. They may be obscured by the gauze while cutting and exhibit different orientations as they move. Table 3 shows the precision, recall, and mean average precision values for each class.

Moreover, the F1 score measures the model accuracy by calculating the harmonic mean of precision and recall for the minority positive class. The harmonic mean emphasizes similar precision and recall values; the more precision and recall scores differ, the worse the harmonic mean. This score provides both recall and precision, which means that it captures both positive and negative cases. For all classes, the F1 score for the proposed model is 0.95 at a confidence level of 0.78 as shown in Figure 8.

Figure 6 showcases qualitative results for the suggested module. The top row displays the actual boxes, and the second row reveals the detection and classification outcomes obtained from YOLOv7. Despite the laparoscopic instruments and circles having deformities, varied orientations, locations, and some covering, the detection accuracy is quite high.

Moreover, this system has demonstrated an exceptional ability to detect and track targeted objects with a high degree of accuracy in pattern-cutting test videos, taking only 12.3 milliseconds per frame for processing. An example of a pattern-cutting test with active tracking and detection can be seen in Figure 9, which shows some selected frames from two videos recorded by two different cameras. The trained model can detect and track the scissors, graspers, and circles despite their varying orientations, locations, and coverage.

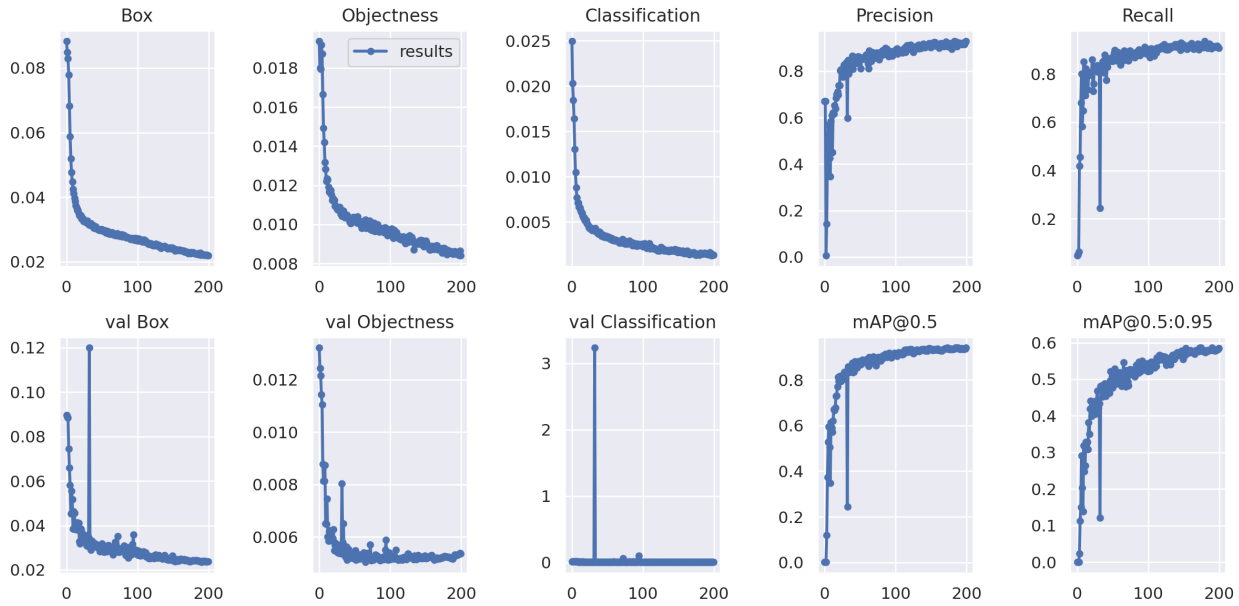


Figure 6: Plots of the box loss, objectness loss, classification loss, precision, recall, and mean average precision (mAP) for both the training and validation sets over the training epochs.

Table 2: Losses, mean average precision, precision, and recall final values.

Evaluation Criteria	Final Value
Box Loss	0.01391
Objectness	0.004788
Class. Loss	0.0003568
mAP@0.5	0.951
mAP@0.5:0.95	0.641
Precision	0.95
Recall	0.941

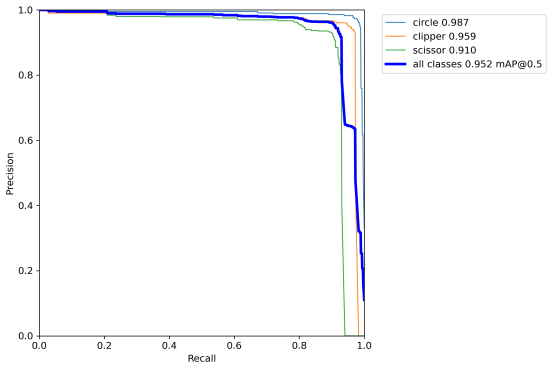


Figure 7: Precision-recall (PR) curves for all classes.

Table 3: Precision, recall, and mean average precision values for each class.

Evaluation Criteria	Circle	Clipper	Scissors
Precision	0.979	0.949	0.932
Recall	0.966	0.957	0.9
mAP@0.5	0.987	0.959	0.91
mAP@0.5:0.95	0.889	0.537	0.495

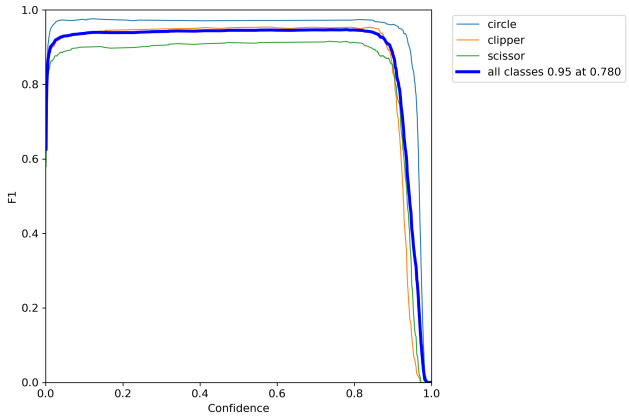


Figure 8: F1 score curves for all classes.

Afterward, testing was conducted on the lab's main workstation. This workstation is equipped with a 2.5GHz Intel(R) Xeon(R) CPU E5-1650 v4 and 32.0GB of RAM. With a delay of 1.67 seconds, the model can detect and track the circle, the grasper, and the scissors. In this case, the delay was caused by the time it took to capture and process frames. To conduct real-time assessments, more powerful hardware is required.

Our study proposes a new approach for detecting and tracking laparoscopic instruments, using deep-learning neural networks.

We have compared our approach with other methods reported in the literature, summarizing the number of extracted images, labeling tools, model built, and results in Table 4. Our proposed approach outperforms previously reported models, achieving an F1 score of 0.95 at a confidence level of 0.78, and a mAP score of 95.2, 95.3 precision, 94.1 Recall, and real-time processing speed of 83.3 FPS, despite the limited number of videos. The models in previous studies may differ in construction, which could explain the differences in results. Overall, our study presents a reliable and efficient method for assessing the performance of trainers in laparoscopic instrument use.

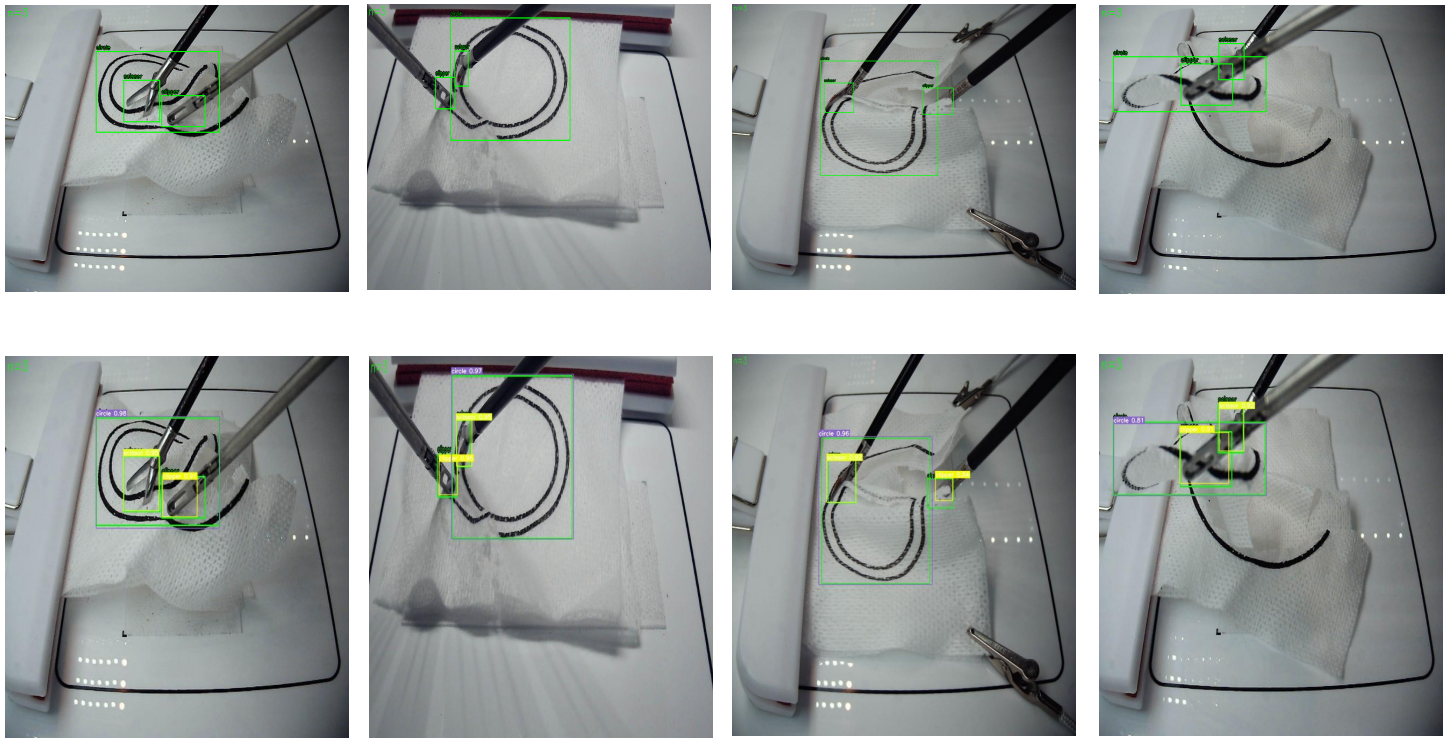
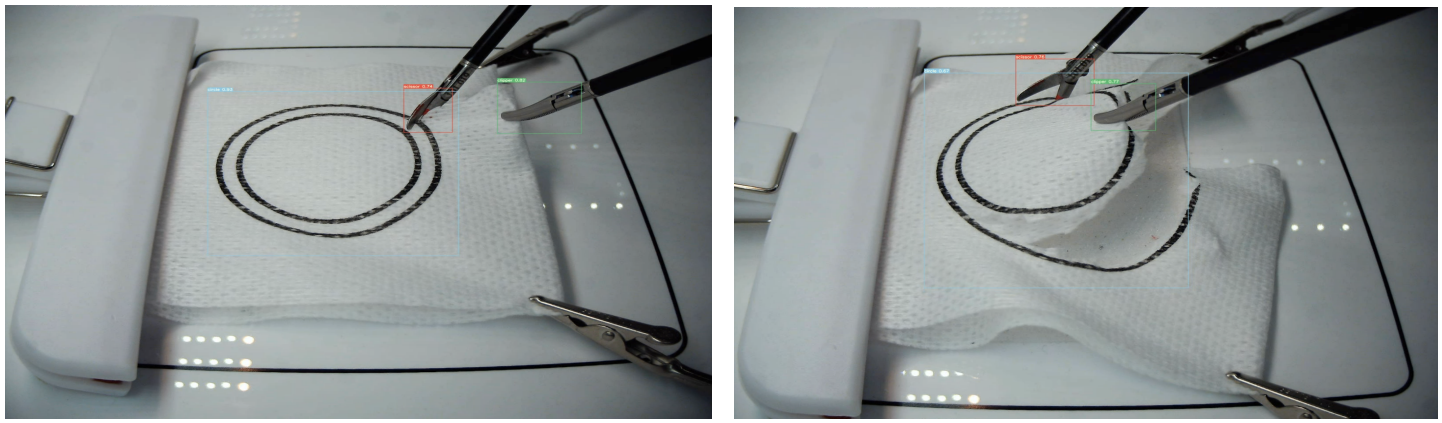
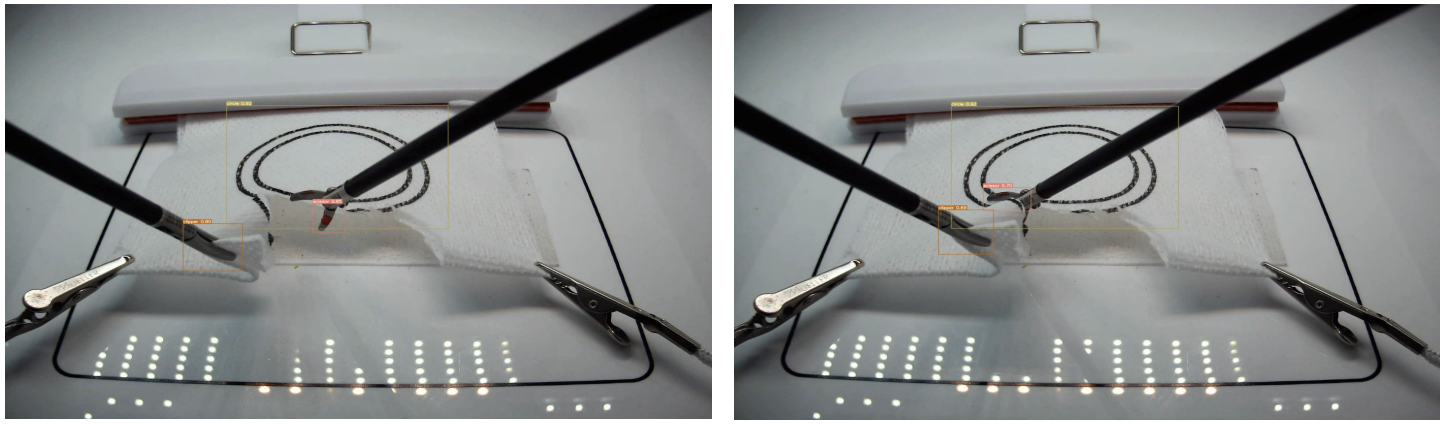


Figure 9: Qualitative results showing the detection of four test images.



(a) First camera tested video.



(b) Second camera tested video.

Figure 10: Qualitative results showing detection and tracking of laparoscopic instruments in two tested videos

One significant use of this model lies in the field of surgical education and performance evaluation. The output of the model, which includes images and videos, can serve as feedback for surgical performance or as a means of deliberate practice for cognitive behaviors during tests. Moreover, these results are accurate and can be utilized as input for further analysis.

5. Conclusions and Future Work

The aim of this study was to enhance laparoscopic surgical training and assessment by developing an extended dataset of instruments and objects for a box trainer pattern-cutting test and implementing a real-time object detection approach based on YOLOv7. Our findings demonstrate that our method effectively detects and tracks spatial tool and object movements and could be used to create a reliable real-time assessment system. Moving forward, we plan to integrate these results into a fuzzy logic decision support system to develop an automated GOALS assessment system.

Conflict of Interest

The authors declare no conflict of interest.

Acknowledgment

The authors acknowledge the Department of General Surgery at Western Michigan University Homer Stryker M.D. School of Medicine for their assistance in producing the dataset used in this work.

Table 4: A comparison summary of the proposed model with the related reported approaches in the literature.

Approach	Dataset	Labeling Tool	Model	Accuracy %	Precision %	Speed
The proposed model	1572 images extracted from our lab dataset [10]	Roboflow [27]	Yolov7	78	mAP 95.2	In real-time at 83.3 FPS
Surgical tools detection based on modulated anchoring network in laparoscopic videos [12]	5696 extracted from m2cai16-tool-locations and AJU-Set datasets	The data already labeled	Faster R-CNN	69.6% and 76.5% for each dataset	mAP 69.6% and 76.5% for each dataset	not reported
Real-Time Surgical Tool Detection in Minimally Invasive Surgery Based on Attention-Guided Convolutional Neural Network [13]	4011 extracted from EndoVis Challenge, ATLAS Dione, and Cholec80-locations datasets	not reported	ResNet50 with multi-scale pyramid pooling.	not reported	100, 94.05, and 91.65 for each dataset	In real-time at 55.5 FPS
Deep learning based multi-label classification for surgical tool presence detection in laparoscopic videos [14]	29478	Pixel Annotation Tool36	EndoNet	not reported	mAP 63.36	not reported
Identifying surgical instruments in laparoscopy using deep learning instance segmentation [15]	333	not reported	Mask R-CNN	not reported	AP 81	not reported
Surgical-tools detection based on convolutional neural network in laparoscopic robot-assisted surgery [17]	M2CAI 2016 Challenge videos	not reported	YOLO	not reported	mAP 72.26	48.9 FPS
Robust real-time detection of laparoscopic instruments in robot surgery using convolutional neural networks with motion vector prediction [18]	7492 extracted from m2cai16-tool-locations dataset	not reported	YOLO9000	not reported	mAP 84.7,	38 FPS
Instrument Detection for the Intracorporeal Suturing Task in the Laparoscopic Box Trainer Using Single-stage object detectors [19]	900 images extracted from our lab dataset [10]	Roboflow [27]	YOLOv4, Scaled-YOLOv4, YOLOR, and YOLOX	not reported	mAP50 0.708 0.969 0.976 0.922 for each model	not reported
Surgical Skill Assessment System Using Fuzzy Logic in a Multi-Class Detection of Laparoscopic Box-Trainer Instruments [21]	950 images extracted from our lab dataset [10]	not reported	SSD ResNet50 V1 FPN and SSD Mobilenet V2 FPN	not reported	65% and 80% reliability, 70 and 90 of fidelity for each architecture	not reported
Surgical Instrument Detection Algorithm Based on Improved YOLOv7x. [23]	452	LabelImg	Improved YOLOV7x algorithm based on RepLK Block and ODConv	94.7	not reported	not reported

References

[1] K. Alkhamaiseh, J. Grantner, S. Shebrain and I. Abdel–Oader, "Towards Automated Performance Assessment for Laparoscopic Box Trainer using Cross-Stage Partial Network," 2021 Digital Image Computing: Techniques and Applications (DICTA), 2021, 01-07, doi: 10.1109/DICTA52665.2021.9647393.

[2] Wang, Chien-Yao, A. Bochkovskiy, and H. Liao., " YOLOv7: Trainable bag-of-freebies sets new state-of-the-art for real-time object detectors," (2022), arXiv. https://doi.org/10.48550/arXiv.2207.02696

[3] "Fls homepage." [Online]. Available: https://www.flsprogram.org. ˜ Last accessed 2 Dec 2022.

[4] R. Aggarwal, T. Grantcharov, K. Moorthy, J. Hance, and A. Darzi, "A competency-based virtual reality training curriculum for the acquisition of laparoscopic psychomotor skill," American journal of surgery, **191**(1), 128—133, January 2006. [Online]. Available: https://doi.org/10.1016/j.amjsurg.2005.10.014

[5] G. Islam, K. Kahol, B. Li, M. Smith, and V. L. Patel, "Affordable, web-based surgical skill training and evaluation tool," Journal of Biomedical Informatics, **59**, 102–114, 2016. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1532046415002397

[6] G. A. Alonso-Silverio, F. P´erez-Escamirosa, R. Bruno-Sanchez, J. L. Ortiz-Simon, R. Mu˜noz-Guerrero, A. Minor-Martinez, and A. Alarc´on-Paredes, "Development of a laparoscopic box trainer based on open source hardware and artificial intelligence for objective assessment of surgical psychomotor skills," Surgical Innovation, **25**(4), 380–388, 2018, pMID: 29809097. [Online]. Available: https://doi.org/10.1177/1553350618777045

[7] N. J. Hogle, W. D. Widmann, A. O. Ude, M. A. Hardy, and D. L. Fowler, "Does training novices to criteria and does rapid acquisition of skills on laparoscopic simulators have predictive validity or are we just playing video games?" Journal of surgical education, **65**(6), 431–435, 2008.

[8] M. A. Zapf and M. B. Ujiki, "Surgical resident evaluations of portable laparoscopic box trainers incorporated into a simulation-based minimally invasive surgery curriculum," Surgical innovation, **22**(1), 83– 87, 2015.

[9] Y. LeCun, Y. Bengio, and G. Hinton, "Deep learning. nature 521 (7553), 436444," Google Scholar Google Scholar Cross Ref Cross Ref, 2015.

[10] https://drive.google.com/drive/folders/1F97CvN3GnLj-rqg1tk2rHu8x0J740DpC

[11] O. Russakovsky, J. Deng, H. Su, J. Krause, S. Satheesh, S. Ma, Z. Huang, A. Karpathy, A. Khosla, M. Bernstein et al., "Imagenet large scale visual recognition challenge," International journal of computer vision, **115**(3), 211–252, 2015.

[12] B. Zhang, S. Wang, L. Dong, and P. Chen, "Surgical tools detection based on modulated anchoring network in laparoscopic videos," IEEE Access, 8, 23 748–23 758, 2020.

[13] Shi, P., Zhao, Z., Hu, S. and Chang, F., "Real-Time Surgical Tool Detection in Minimally Invasive Surgery Based on Attention-Guided Convolutional Neural Network," IEEE Access **8**, 228853-228862, 2020.

[14] S. Wang, A. Raju, and J. Huang, "Deep learning based multi-label classification for surgical tool presence detection in laparoscopic videos," in 2017 IEEE 14th International Symposium on Biomedical Imaging. IEEE, 620–623, 2017.

[15] S. Kletz, K. Schoeffmann, J. Benois-Pineau, and H. Husslein, "Identifying surgical instruments in laparoscopy using deep learning instance segmentation," in 2019 International Conference on Content-Based Multimedia Indexing (CBMI). IEEE, 1–6, 2019.

[16] E. Kurian, J. J. Kizhakethottam, and J. Mathew, "Deep learning based surgical workflow recognition from laparoscopic videos," in 2020 5th International Conference on Communication and Electronics Systems (ICCES). IEEE, 928–931, 2020.

[17] B. Choi, K. Jo, S. Choi, and J. Choi, "Surgical-tools detection based on convolutional neural network in laparoscopic robot-assisted surgery," in 2017 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC). IEEE, 1756–1759, 2017.

[18] K. Jo, Y. Choi, J. Choi, and J. W. Chung, "Robust real-time detection of laparoscopic instruments in robot surgery using convolutional neural networks with motion vector prediction," Applied Sciences, **9**(14), 2865, 2019.

[19] M. Mohaidat, J.L. Grantner, S.A. Shebrain, and I. Abdel-Qader, " Mohaidat M, Grantner JL, Shebrain SA, Abdel-Qader I. Instrument detection for the intracorporeal suturing task in the laparoscopic box trainer using single-stage object detectors," In2022 IEEE International Conference on Electro Information Technology (eIT) May 19, 455-460, 2022.

[20] M. Mohaidat, J.L. Grantner, S.A. Shebrain, and I. Abdel-Qader, "Multi-Class Detection and Tracking of Intracorporeal SuturingInstruments in an FLS Laparoscopic Box Trainer Using Scaled-YOLOv4," In Proceedings of the Advances in Visual Computing:17th International Symposium, ISVC 2022, San Diego, CA, USA, 3–5 October 2022

[21] F.R. Fathabadi, J.L. Grantner, S.A. Shebrain, and I. Abdel-Qader, "Surgical skill assessment system using fuzzy logic in a multi-class detection of laparoscopic box-trainer instruments," In 2021 IEEE International Conference on Systems, Man, and Cybernetics (SMC), 1248-1253, 2021.

[22] F.R. Fathabadi, J.L. Grantner, S.A. Shebrain, and I. Abdel-Qader, "3D Autonomous Surgeon's Hand Movement Assessment Using a Cascaded Fuzzy Supervisor in Multi-Thread Video Processing," Sensors, 23, 2623, 2023. https://doi.org/10.3390/s23052623

[23] R. Boping, B. Huang, Sh. Liang, and Y. Hou, "Surgical Instrument Detection Algorithm Based on Improved YOLOv7x," Sensors (Basel, Switzerland) 23,11 5037. 24 May. 2023, doi:10.3390/s23115037

[24] https://pjreddie.com/darknet/

[25] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You only look once: Unified, real-time object detection," in Proceedings of the IEEE conference on computer vision and pattern recognition, 779–788, 2016.

[26] "School of medicine." [Online]. Available: https://med.wmich.edu/. ˜ Last accessed 2 Dec 2022.

[27] [Online]. Available: https://aroboflow.com/. Last accessed 2 Dec 2022.

[28] A. M. Obeso, J. Benois-Pineau, M. G. Vázquez, and A. R. Acosta, "Saliency-based selection of visual content for deep convolutional neural networks," Multimedia Tools and Applications, 78(8), 9553–9576, 2019.

[29] https://colab.research.google.com/drive/1X9A8odmK4k6l26NDviiT6dd6TgR-piOa#scrollTo=GD9gUQpaBxNa

[30] https://colab.research.google.com/signup\

[31] Keras image preprocessing. Available at: march 2015; accessed 3 november 2021.

[32] Googleresearch, "tensorflow: large-scale machine learning on heterogneous systems," google res., 2015.

ASTES

Advances in Science, Technology and Engineering Systems Journal
Vol. 8, No. 6, 96-106 (2023)
www.astesj.com
Special Issue on Innovation in Computing, Engineering Science & Technology

ASTES Journal
ISSN: 2415-6698

A Secure Medical History Card Powered by Blockchain Technology

Samiha Fairooz[1], Shakila Yeasmin Miti[2], Zihadul Islam[2], Meem Tasfia Zaman[*,2]

[1]*University of Adelaide, Faculty of Sciences, Engineering and Technology, Adelaide, South Australia*

[2]*North South University, Department of Electrical and Computer Engineering, Dhaka, Bangladesh*

ARTICLE INFO

Article history:
Received: 29 September, 2023
Accepted: 26 November, 2023
Online: 30 December, 2023

Keywords:
Medical history card
Web application
Blockchain
Decentralized database
Electronic medical records
Healthcare

ABSTRACT

A reliable healthcare system ensures that the population has access to top-notch medical services, ultimately enhancing their overall health most efficiently. At times, data are not secured or handled appropriately. Addressing these concerns, blockchain technology is projected to bring about a substantial revolution in the medical industry by assuring the confidentiality of electronic health information. This research not only seeks to rectify the shortcomings in Bangladesh's existing health system but also explores the potential of blockchain technology's decentralized database to fortify the entire healthcare framework. More importantly, it showcases a web-based application, particularly a medical history card that displays a patient's details, diagnoses,vaccines, medication records, investigation background, familial information, blood donation history, and many additional information starting from birth. Alongside, the paper emphasizes the transformative impact of implementing blockchain technology in the healthcare sector, paving the way for a more secure and efficient healthcare ecosystem. All in all, the array of medical information captured within the pack face of a single card could hasten medical decisions and ensure the effectiveness of any treatment.

1 Introduction

The health sector holds an exceedingly central position in safeguarding an overall sustainable socio-economic advancement. The health world is immensely diversified with the presence of several technical and biomedical analyses. The previous concepts of medical management are now found substituted over time. Currently, people are more focused on constituting a community of healthiness in which disease prevention outweighs the importance of the cure, unlike in the past. Notwithstanding that, the healthcare management system confronts the most critical challenges and barriers. Although technological and medicinal advancements are now quite prominent, no steps have yet been taken to incorporate the patient's medical history in a decentralized manner. The patients of private and public Healthcare Centers (HCs) are still found carrying the baggage of reports, diagnoses, and prescriptions while visiting a physician. Reports or prescriptions are either lost or misplaced, resulting in harassment and stress during emergencies. Medical health records are irreplaceable not only to patients but also to the hospital authorities themselves. A detailed history can put additional value to the current treatment by the medical consultants and physicians. The continuing development of the Internet of Medical Things (IoMT) could accelerate the maintenance of digital documents while offering greater convenient services to clients. Despite these precautions, healthcare frequently encounters virtual hacking incidents that end up resulting in the deletion and disclosure of personally identifiable information. Software vulnerabilities, security collapse, and human error are ordinarily the reasons behind this catastrophe. Amid such a situation, the data breach discloses many loopholes in the healthcare database system that can be encapsulated under three keynotes: 1) centralized aggregation of essential data, 2) unauthorized access to the public, and 3) disclosing confidential data purposely due to inadequate information security. Notable, health records need to be breach-proof as any data tampering can cause critical medical emergencies, including the death of patients. With the significance of medical history in mind, we are introducing a medical history card that would contain all a person's medical records under a platform. To explain, the patients will be emancipated from the burden of bearing all their medical history before visiting a physician. Furthermore, the likelihood of doctors encountering incorrect and deceptive information will decrease. The utilization of blockchain technology in the card ensures the decentralized accuracy of medical information, eliminating the need for third-party electronic storage. Blockchains are often referred to as distributed ledger technology (DLT) as blockchain records are immutable and cannot be modified, changed, or deleted.

[*]Corresponding Author: Meem Tasfia Zaman, North South University, Email: zaman.tasfia@northsouth.edu

2 Literature Review

Conventionally, the idea of digitally archiving medical information has traditionally been in development for a significant period of time. The current paper is dedicated to extending the paper entitled "A medical history card utilizing the Blockchain technology" which was published in the 2023 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA) [1]. In the past in 1973, The Regenstrief Medical Record System (RMR), a type of paper-based electronic record system has been utilized in outpatient healthcare facilities. The RMR obtained information about patients from a wide range of sources including physician chambers, forensic lab data, pharmacies, and others. It generated a summary report, surveillance report, and the Patient Encounter Form (PEF) to deliver protocol-based feedback to doctors about critical clinical conditions. It was extensively believed that the widespread use of EMRs had decreased surgical errors, boosted health, and decreased expenditures on healthcare. Likewise, the organizational processes have ensured excellent quality, effectiveness, and transparency through EHRs [2]. In order to create an integrated medical record between patients and medical professionals, the author of [3] (2008) established a patient portal called CONNECT (Care Online: Novel Networks to Enhance Communication and Treatment). The patients could easily access it from home, hospital, or doctor's office using the heterogeneous networks. CONNECT application was committed to improving patient-provider communication and assisting patients in understanding and managing their illnesses. In 2010, author of the paper [4] described that the use of EMRs in long-term care institutions at the time was neither widespread nor successful. The hospitals implementing EMRs were working on techniques to evaluate effectiveness; no statistical information was available on the efficacy of EMRs in the long-term care context. They opposed the widespread use of EMRs. Conversely, it was evident that when most patients carry their EHR, many chances were created for the industries. For instance, a "health record bank," proposed in [5], was a starting point for the enterprise's additional "value-added" services. An EHRs facilitates clinicians to view patients' data from numerous sources across a period for extensiveness and continuity of care. Research showed that the appropriate application of the EHRs could minimize medical errors, assist in diagnosing detrimental health events, facilitate the more appropriate use of healthcare services, and potentially reduce healthcare expenses [6]. An e-prescription system that assists mother and children with medicine data recording, retrieving, and reporting techniques have been developed by the author of [7]. Moreover, the possible medication errors were reduced by upgrading the prescribing process. In [8], the author claimed that the Implantable Device Cardiac Observation (IDCO) profile had been constructed at the Leiden University Medical Centre (LUMC) to integrate data from the external databases maintained by two device providers into the departmental Cardiology Information System. They continued by saying that the growing use of ICDs and remote monitoring at treatment stations will improve patient outcomes by lessening the burden of follow-up on clinics and personnel. From the patient's point of view, it was appealing due to better security and prevention of lengthy and time-consuming visits to the hospital. In particular, readmissions were minimized when patient history was viewed [9]. In the publication with reference [10], the author covered, The Internet of Things (IoT) and the digitization of medical records topics in a number of their presentations. They made portable web servers out of smart gadgets like smart discs and cards, making remote diagnostics record-keeping easier. The functional requirements call for a device-enabled system that could obtain and capture all the records with a backup on a few cloud-based platforms so that data is not lost, even though the device was lost. The system claimed to eliminate paper from patient transactions completely. Besides, storing patient reports, histories, visits, prescriptions, results, pharmacy bills, and emergency contact information was more straightforward. The patient had exclusive access to the gadget, and adequate verification was required for updating any information on the device. Additionally, in the same year, an advanced decentralized system, MedRec for managing Electronic Health Records (EHRs) through Blockchain technology was proposed. Their solution offered patients a comprehensive, tamper-proof log and easy access to their data [11]. In 2008, the basic concept of a distributed secure ledger was introduced. Blockchain technology is the approach to creating an immutable, secure, distributed database of transactions. Blockchains were trained to deliver a distributed ledger of financial transactions, not relying upon a central bank, credit company, or other financial institution. Additionally, it confirms a secure and permanent record of transactions. The significant progress in EMRs was the generation of a distributed ledger to productively transfer patients' records from the healthcare organization to the individual. One of the key features of blockchain technology is that it is way too transparent: transactions are processed by the network without requiring a single computer, database, or institution. Besides, the paper [12] offered insights into the use of blockchain in healthcare data management, with a specific focus on sharing EMRs among healthcare providers. Collaborating with Stony Brook University Hospital, a framework was developed for managing and sharing Electronic Medical Records (EMRs) of cancer patients. This framework involved connecting to the hospital's local database management system, which was specifically designed for storing oncology-related data. Patient data was then encrypted using each patient's unique key and stored on a cloud-based platform known as Varian Cloud. Additionally, a blockchain-based data-sharing system was proposed as part of this initiative. This system aimed to leverage the immutability and autonomy characteristics of blockchain technology to effectively address various medical challenges related to data security and sharing [13], [14]. In 2018, a blockchain-based data-sharing system called BPDS (Blockchain-based Privacy-Preserving Data Sharing) was introduced with the primary goal of safeguarding user privacy. By implementing BPDS, patients gained control over their Electronic Medical Records (EMRs), and both users and institutions could access this data without concerns about compromising patient privacy. In BPDS, the original EMRs were securely stored in the cloud-based BPDS system, while the indexes were maintained within a consortium that had stringent tamper-proof measures. This approach significantly reduced the risk of medical data leakage. During the same year, a novel method involving attribute-based signatures, with multiple authorities, was developed to ensure the authenticity of Electronic Health Records (EHRs) embedded within the blockchain. In this method, a patient could sign a message based on certain

attributes without revealing any additional personal information, thus providing proof of their attestation [15] [16]. To enhance privacy within the system, a method involving Personalized Radio Frequency Identification (RFID) cards was implemented. These RFID cards assigned unique IDs to different users, and modifications to these IDs could only be made by the relevant doctors using the medical database. This approach ensured the authentication of medical information, as only authorized personnel could manage and update the data. Furthermore, another blockchain-based approach was suggested to secure Electronic Medical Records (EMRs) for healthcare applications. In this approach, access control was patient-centric, meaning that patients would share the decryption key only with trusted doctors. These trusted doctors would then store the patient's encrypted electronic medical information securely on a blockchain, adding an additional layer of security to the handling of medical data. By utilizing the encryption technology, the authors of the publication [17] proposed a Sensitive and Energetic Access Control (SE-AC) mechanism for certifying fine-grained confidentiality of the patient's Electronic Health Record (EHR), wherein people given authorization could update or examine certain EHR. The authors emphasized that the security of EHRs seriously threatens the patient's privacy, and most third-party hosting platforms have some issues with data security and user privacy. Individuals having drug or alcohol addiction histories and HIV could request primary care physicians to access certain documents in the hospital [18] [19] [20]. The concept of remote healthcare was introduced with a focus on securing electronic records through encryption before they are transmitted to medical Blockchain networks. In this approach, the medical team members established a session key for authorized groups in a way that allowed authorized participants to decrypt and access patient information. Importantly, the content could only be deciphered using either the patient's private key or a group member's session key, and no personal identification password was involved in the entire process. In [21], the authors discussed the use of 'The InterPlanetary File System (IPFS)' for storing Electronic Medical Records (EMRs) and the Ethereum platform for replicating the blockchain. This proposed method enhanced the confidentiality of uploaded data, reduced the risk of errors due to data manipulation, and facilitated the secure digitization of medical records. The public key served as a universal identifier to segregate and maintain the complete medical record history for each patient [22]. In 2021, a comprehensive healthcare system was developed, encompassing an Android app, an iOS app, and a website, all designed to grant patients easy access to their medical records and history. Additionally, a novel feature was introduced: a health passport designed to compile and display patients' medical data from various healthcare providers. This encompassed a wide range of information, including medical images, clinical reports, lab results, dental records, and more. Users had the convenience of utilizing their smartphones to consolidate their medical history from diverse sources, including healthcare providers, imaging CDs, PDF notes, fitness trackers like Fitbit and Apple Watch, wellness forms, CDA Files, JPEG documents, and self-reported health records. Furthermore, they could maintain and update their health vitals such as Blood Pressure, Heart rate, height, weight, BMI, Body Temperature, Oxygen saturation, allergies, and BSA. Additionally, the application provided a user-friendly feature that enabled individuals to easily locate their nearest healthcare center and schedule appointments, making healthcare management more accessible and efficient [23]. A new architecture termed as Internet-of-Health-Care-Systems (IoHCS) was launched to supervise the EHRs accumulated from all partaking hospitals in a network; through Blockchain Technology developed on the Ethereum platform. Software agents via Message Queueing Telemetry Transport (MQTT) protocol were used to network the Health Information Systems (HIS) of all linked hospitals. A mobile app for accessing patient records using a Key Management System (KMS) and an Application Programming Interface (API) for reading and writing data for each hospital on the blockchain was also generated. Studies show that the prevailing HIS of 350 partaking hospitals was incorporated into the app. The EHRs of the patient have been formulated in 6 parts — personal information, visit information, laboratory test information, drug order information, and a hash value created by the encryption module. Amazon Key Management System and Amazon S3 (Simple Storage Service) guarantee data and process security. In 2022, a new web-based project was proposed with the aim of creating a centralized database to store patients' medical histories. The paper provided details about the software and technological architecture employed for this purpose. The project focused on enabling remote control and management of the integrity and documentation of medical histories, reports, and prescriptions. For the backend of the online application, PHP, AJAX, and jQuery were utilized, with MySQL serving as the database. On the frontend, HTML5, CSS, Bootstrap, and JavaScript were employed. Researchers developed a prototype platform that aimed to digitalize the healthcare system by offering digital appointments, artificial intelligence-driven recommendations, and a health-tracking blood bank. One notable challenge addressed in the context of the technological revolution was the storage of segmented Electronic Health Records (EHRs) in Healthcare Centers (HCs). To tackle this issue, a platform was introduced to establish a distributed electronic health record (EHR) ecosystem. This ecosystem aimed to integrate electronic medical reports securely within a private and permissioned blockchain, addressing the fragmentation of EHR data. The notable advantages of implementing the distributed network regarded clinical outcomes such as improved quality, and reduced medical errors; organizational outcomes like financial, and operational benefits; managerial outcomes, e.g., improved ability to conduct research, improved population health, and lower costs [24], [25]. To highlight, Blockchain is an emerging decentralized technology to validate and secure a patient's medical record efficiently. Several attempts were proposed to use Blockchain technology to address healthcare data privacy, security, and ownership issues. Blockchain-based digital platforms empower patients to communicate with their data providers, including healthcare providers, in a faultless, secure, and efficient approach [26], [27].

3 Features

Since the inception of the paper, the goal has been to deploy the history card for the comprehensive collection of an individual's crucial medical records to facilitate appropriate treatment

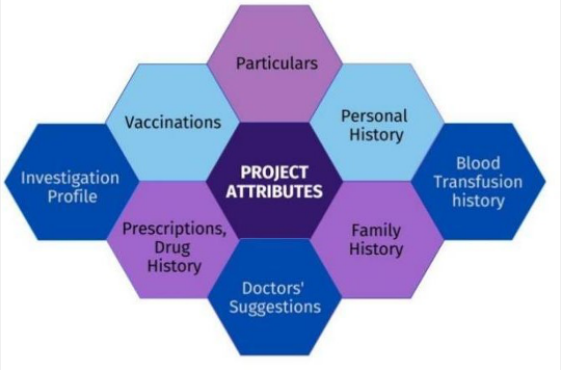


Figure 1: Features Diagram

To ensure the card's effective and optimized application, various features have been integrated, in Figure 1. Initially, 'Particulars' will contain the Name, Date of birth, blood group, parent's name and details, weight, height, classification of gender, address, and contact number. The 'Personal History' section provides comprehensive information concerning past allergies, sinusitis, any congenital anomalies, diabetes, Claustrophobia, thyroid conditions (hypothyroidism or hyperthyroidism), etc. Another vital segment is the 'Investigation Profile,' which grants access to all diagnostic reports, including cellular and chemical analyses (such as blood analysis, glucose tolerance test, serological test, enzyme analysis, kidney and liver function, protein-bound iodine test, gastric fluid analysis, and more); diagnostic imaging (such as mammography, ultrasonogram, brain scanning, and so forth); health examinations (like biopsy, laparoscopy, and others). Following that, the 'Vaccinations' section will contain a record of all vaccinations administered from birth onwards. Subsequently, the 'Drug History' segment provides a catalog of medication names, dosages, and the timing of each medication taken. In the 'Blood Transfusion History,' the record includes details about the quantity and blood type of blood donations made by the patient. Similarly, in the 'Prescriptions' section, all prescriptions provided by doctors are organized chronologically. Another essential component is the 'Family History,' which encompasses the genetic diseases present in the patient's family, such as Congenital deafness, Cancer, thyroid concerns, and so on. Finally, 'Doctors Suggestions' will outline the healthcare recommendations given by doctors regarding the patient's medical conditions.

4 Proposed Strategical Plan

The paper initially intends to use the health card to collect necessary information in order to eliminate the need for patients to repeatedly visit the history room next to the doctor's office. In summary, there are four sorts of users in this article's web application: patients, doctors, vaccine staff, and report staff. The priority of patient's health history has been analyzed as per the priority list of records in the card.

Following that, the attributes of the website such as Patients (Name, age, blood group, gender, etc..), Vaccination History, Personal History (Diabetics, High / Low blood pressure, thyroid, history of surgery, blood transfusion, allergy, congenital anomaly, Covid-19, etc.), Diagnosis Report, Prescriptions, Drug History, Family History (Kidney, Heart Disease, Cancer, Skin disease, etc.) and Doctors' Suggestions schemed.

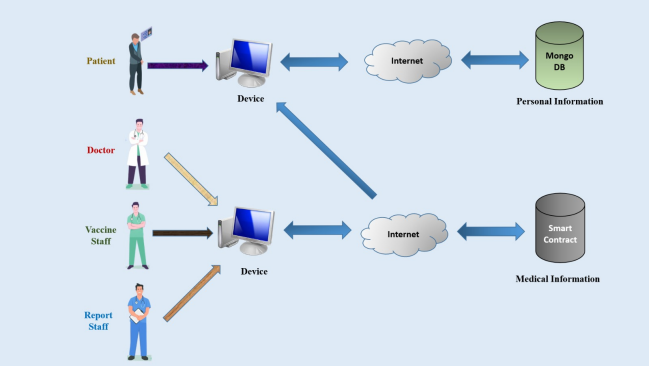


Figure 2: Network Diagram

The Network diagram depicts the fundamental work processes of the users for circumstances where accessibility to health records is prohibited for security reasons. (Figure 2). All of the patient's information can be read by both patients and doctors, but only they have the ability to make specific changes. The two more users, the vaccine and report staff are only permitted to look at the patient's personal background and relevant fields. Moreover, patients might view the automated EMR snapshots and update their personal information. Furthermore, MongoDB, a NoSQL database, was used to save the users' other traditional information, such as personal narratives, via the Internet, and the blockchain Smart Contract was chosen to store the medical data because there is always the risk of vital medical information being lost.

Smart Contract has been deployed as Blockchain Database to accommodate the patient's medical health history. To add, Smart Contract is a form of Ethereum account capable of sending transactions over the network. The agreement enables the execution of a contract between two parties through blockchain, without the involvement of any legal system.

5 Implementation

In this section, the web application's tools, frameworks and databases as well as the benefits of using these methods over more conventional methods. In addition, we shed light on the robust security measures and policies that have been put in place to safeguard the system.

5.1 Framework and Structural Design

The web application has been constructed using the MERN stack, which seamlessly combines four core technologies: React, and Node, MongoDB and Express. Furthermore, the application adheres to an architecture model that is built with 3-tier and it is characterized by three distinct layers: the front-end tier, represented by the web interface; the middle tier, composed of servers; and the back-end tier, covering the databases.

5.2 Approach to User Interface Development

To begin, the front-end infrastructure was constructed with HTML, CSS, React and JavaScript (JS). React is preferred for the project as it provides a front-end build pipeline making it useable with any back-end. Secondly, in order to develop dynamic HTML sites for taking user input into account and preserving permanent data using specialized objects, files, and relational databases, JS was utilized. Thirdly using CSS, the website's appearance and layout were updated.

5.3 Approach to Server-Side Development

The back-end server was developed with Node JS. In order to establish a connection between the front-end and the back-end, the Web3 application programming interface has been seamlessly integrated into the system.

During authentication, JSON Web Token (JWT) has been implemented for security purpose. JWT has been attached as "bearer" header on each login request to server. After that, it will be parsed by the server from header and the client identity will be verified. The JWT has been implemented because this authentication system is helpful to use for different type of users. To generate the JWT during every login HS256 signing algorithm has been used in the header that has been given below:

{
"alg": "HS256",
"typ": "JWT"
}

And the payload part of the JWT contains the claims of the particular users. The claims includes statements about the user and additional data which looks like this:

{
"hid": "123456789",
"exp": '5th June, 2023'
"iat": "2023-12:12 12:20:00"
}

Similarly, the refresh JWT is also being set as cookie so that, while the login access JWT will be invalidated the server could take set cookie of the refresh JWT and can generate a new refresh token for the logged in user. In the whole process, the expiration time of the access JWT has been set for 15 minutes and the refresh JWT has been set for 60 days.

In Figure 3, the displayed code snippet from our web application represents the implementation of the login process using JWT. As well as, specific validations has been incorporated to enhance security measures. Furthermore, to mitigate the risk of database injection, the use of the 'sanitize-html' package has been implemented.

5.4 Decentralized and Prominent Databases

The information will be stored in two separate databases. MongoDB will handle the orthodox data, while Smart Contract will store significant EMRs to enhance long-term protection. Additionally, MetaMask has been incorporated into the system as a wallet for overseeing and managing expenses related to ether.

```
// Login route to generate and return access and refresh tokens
app.post( path: '/clientLogin',
    handlers: (req :Request<P, ResBody, ReqBody, ReqQuery, LocalsObj>, res :Response<ResBody, LocalsObj> ) => {
    const { hid, password } = req.body;

    // Find the user based on the provided health ID and password
    const user = users.find((u :{...} ) => u.hid === hid && u.password === password);

    if (!user) {
        return res.status( code: 401).json( body: { message: 'Authentication failed' });
    }

    // Generate an access token with user information, exp, iat, and a secret key using HS256 algorithm
    const accessToken = jwt.sign( payload: {
        hid: user.hid,
        exp: Math.floor( x: Date.now() / 1000) + (15 * 60), // 15 minutes from now
        iat: Math.floor( x: Date.now() / 1000), // Issued at the current time
    }, secretKey,
        options: { algorithm: 'HS256' },
        callback: function(err, accessToken) {console.log(accessToken);});

    // Generate a refresh token with user information and a refresh secret key using HS256 algorithm
    const refreshToken = jwt.sign( payload: {
            hid: user.hid,
            exp: Math.floor( x: Date.now() / 1000) + (60 * 24 * 60 * 60), // 60 days from now
            iat: Math.floor( x: Date.now() / 1000),
        },
        refreshSecretKey,
        options: { expiresIn: '60d', algorithm: 'HS256' },
        callback: function(err, refreshToken) {console.log(refreshToken);});

    // Set the refresh token in a cookie with a secure flag and HttpOnly to make it more secure
    res.cookie( name: 'refreshToken', refreshToken, options: {
        maxAge: 60 * 24 * 60 * 60 * 1000, // 60 days
        httpOnly: true,
        secure: true,
        sameSite: 'none',
    });

    // Return the access token to the client
    res.json( body: {message: "Successfully Logged In", access_token : accessToken });
});
```

Figure 3: Code Snippet Illustrating User Authentication

```
ClientInfo.sol 1 ×   {} ClientInfo.json
contracts > ClientInfo.sol
1   // SPDX-License-Identifier: MIT
2   pragma solidity >=0.4.22 <0.9.0;
3
4   contract ClientInfo {
5       // Prescription Contract Start here.
6       uint256 public prescriptionCount = 0;
7
8       struct prescriptionStruct {
9           uint256 id;
10          string Dfirstname;
11          string Dlastname;
12          string Docregid;
13          string hospitalname;
14          string src;
15          string Time;
16          string hid;
17      }
18
```

Figure 4: Medical Information's Data Structure

Patient's medical data is kept in an Ethereum Smart Contract Database. Each specific category of medical information has its own data structure (Figure 3).

The patient's whole medical history was then entered into the smart contract using the set method. The data was lastly acquired using the get method (Figure 5). The EMRs are securely stored within a decentralized Blockchain database. The decision to implement blockchain technology was primarily driven by two key objectives: transparency and data integrity. Specifically, blockchain was chosen to ensure that both patients and doctors cannot conceal information and to prevent the falsification of critical medical data. The blockchain architecture operates as a decentralized digital ledger, recording distinct data or transactions across a network of computers in blocks. Each node within this network possesses a complete copy of the blockchain, ensuring security and transparency without reliance on a central authority. Characterized by decentralization

and distribution, blockchain networks facilitate secure peer-to-peer transactions. Blocks, comprised of validated transactions, contain a cryptographic hash of the preceding block. The database's security is enhanced through decentralization, immutability, consensus mechanisms, cryptographic security, transparency, redundancy, and controlled access.

```
function setPrescriptionData(
    string memory _Dfirstname,
    string memory _Dlastname,
    string memory _Docregid,
    string memory _hospitalname,
    string memory _src,
    string memory _Time,
    string memory _hid
) public {
    prescriptionCount++;
    newPrescriptionStruct[prescriptionCount] = prescriptionStruct(
        prescriptionCount,
        _Dfirstname,
        _Dlastname,
        _Docregid,
        _hospitalname,
        _src,
        _Time,
        _hid
    );
}

function getPrescriptionDataCount() public view returns (uint256) {
    return (prescriptionCount);
}

function getPrescriptionData(uint256 dataNum)
    public
    view
    returns (
        uint256,
        string memory,
        string memory,
        string memory,
        string memory,
        string memory,
        string memory,
        string memory
    )
{
    prescriptionStruct memory s = newPrescriptionStruct[dataNum];

    return (
        s.id,
        s.Dfirstname,
        s.Dlastname,
        s.Docregid,
        s.hospitalname,
        s.src,
        s.Time,
        s.hid
    );
}
```

Figure 5: Set and Get Method of Medical Information

An object-oriented, high-level Solidity language was used for implementing Smart Contracts. This language is designed to target the Ethereum Virtual Machine (EVM). Truffle, the development environment, asset pipeline, and testing framework for smart contracts was used for the framework. Smart contracts, functioning within these networks, execute agreements or transactions without intermediaries, using platform-specific languages like Solidity for Ethereum. Once deployed on the blockchain, Smart Contracts become immutable code, and decentralized verification prevents any single entity from controlling their execution. This technology holds transformative potential for revolutionizing medical history management by securely storing records, providing patient-controlled access, and triggering actions based on predefined conditions. The project utilized MetaMask as a wallet to purchase ether. To add, MetaMask is a free web crypto wallet that allows users to store and connect with the Ethereum blockchain ecosystem. Lastly, to host the Blockchain server locally Ganache was deployed to set up a local Ethereum blockchain to test the decentralized application in a safe environment. Additionally, the Blockchain design eliminates the risk of data loss through its distributed architecture, where each server on the network maintains a copy of the data, and no server has the capability to alter, amend, or delete any previously recorded information from the medical records. This combination of transparency and data immutability establishes a robust and secure foundation for the management and protection of sensitive medical information within the system.

6 Outcome and Prospects

In this section, the output of the web application has been demonstrated in order to get a clearer web experience. More especially, with the use of screenshots from the web application, the actions of the four different user types— doctors, patients, the vaccine team, and the reporting team—are elucidated.

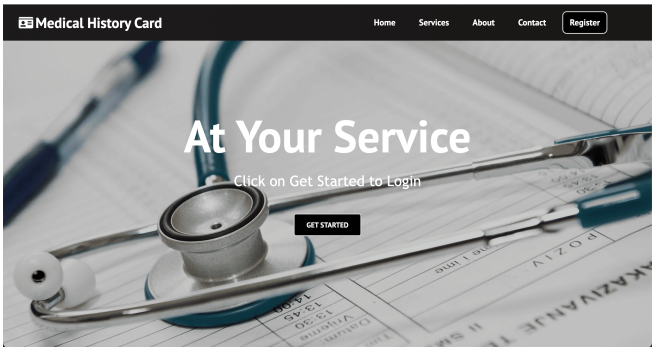


Figure 6: Home Page of the Website

The MHC starts with a Home page. This on boarding page will help the users learn how to get started and derive value from it (Figure 6). The home page contains a Navigation bar at the top to direct to a particular sector as per the user's requirements.

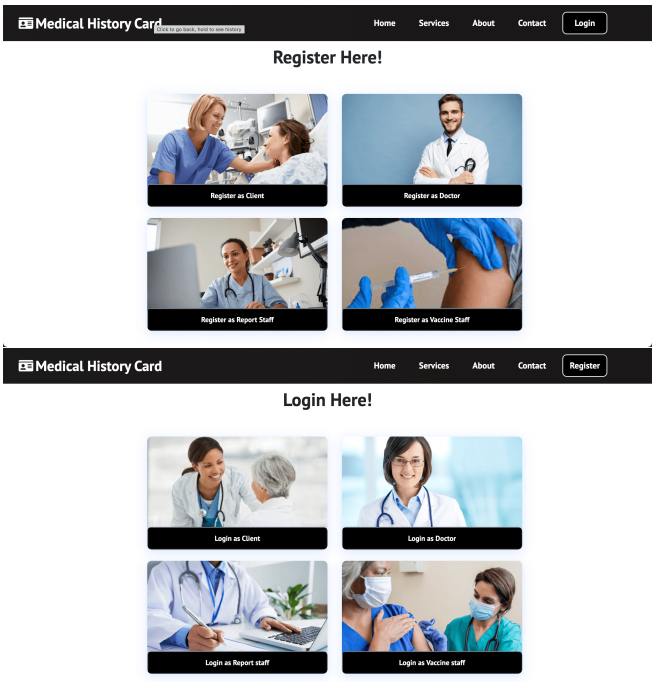


Figure 7: Registration and Login Dashboard

The registration and login pages contain four individual cards designed for each of our four users (Fig. 7). In the registration process, both the birth identity (BID) and national identification (NID) are collected as input, as the web application allows patients under the age of 18 to create accounts. In such cases, the BID becomes a mandatory requirement. After that, a success message will be received as well as the client could see the automatically generated HID in the message. Likewise, users can log in with the help of the login page after registration.

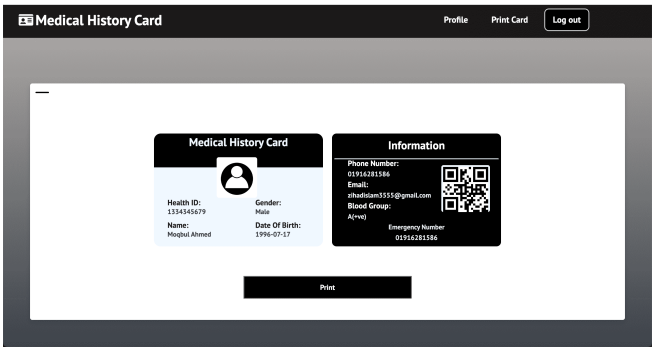


Figure 8: A Demo of the Medical History Card

The inclusion of a unique HID and QR code for each patient card adds an extra layer of convenience and security to the web application for both doctors and patients. It also adds an extra layer of security by ensuring that only authorized personnel (doctors and the respective patients) can access and view the associated medical records. Additionally, patients have the option to download and print their cards by clicking the ”Print” button within the website’s application, as illustrated in Figure 8.

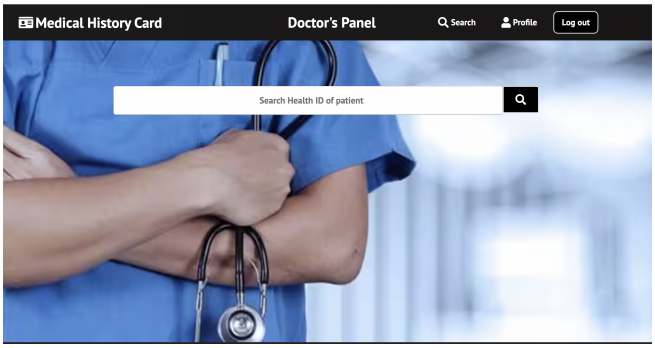


Figure 9: Doctor’s Searching Panel

The doctor can then search for a patient in the doctor searching panel by entering the patient’s HID and will be able to view his medical information (Figure 9). In a similar manner, the staff members who work with vaccines and reports have access to search. However, the patient’s medical information has been limited in accordance with the roles.

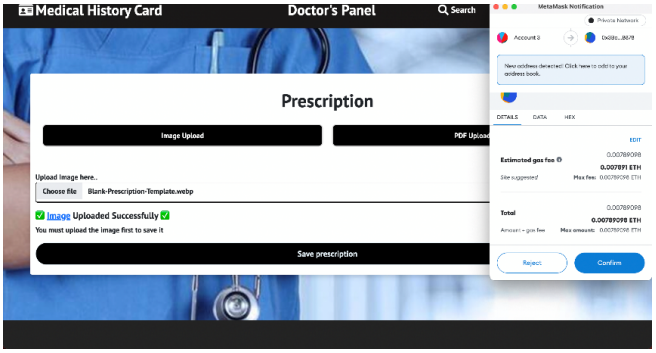


Figure 10: A Doctor Uploading a Patient’s Prescription

Doctors have the flexibility to upload patient prescriptions which prompts them to select the prescription file they want to upload. They can choose either an image file (e.g., JPG, PNG) or a PDF document, as shown in Figure 10.

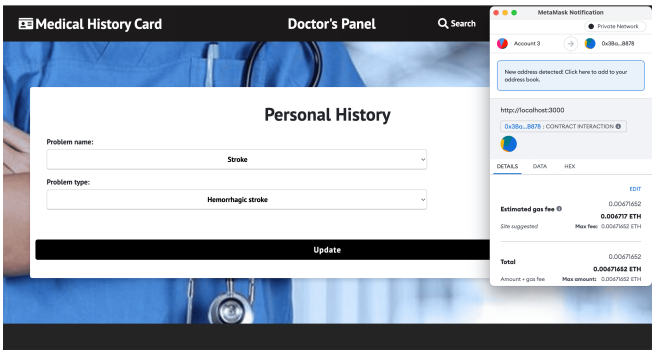


Figure 11: A Doctor Submitting Personal Health History of Patient

Moreover, they have the option to upload a patient’s personal medical background by picking the issue’s name and category from a drop-down menu, input familial medical histories by selecting the disease name and the family member’s relationship from a separate drop-down menu, and offer recommendations by entering information into a designated text field (Figure 11).

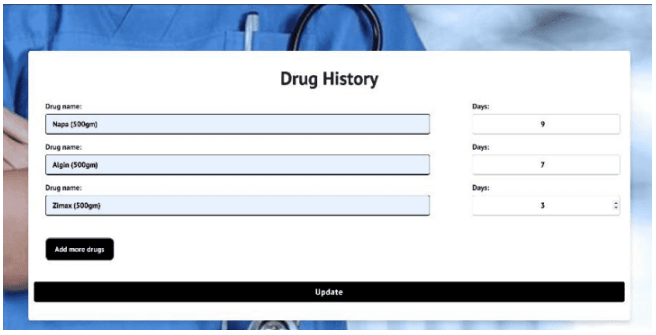


Figure 12: A Doctor Submitting a Patient’s Medication History

In the web application’s ’Drug History’ section, physicians can make updates to a patient’s prior medication record. To accomplish this, they need to enter the medication’s name manually into the text area and specify the duration of consumption by using the increment counter located on the right, as depicted in Figure 12.

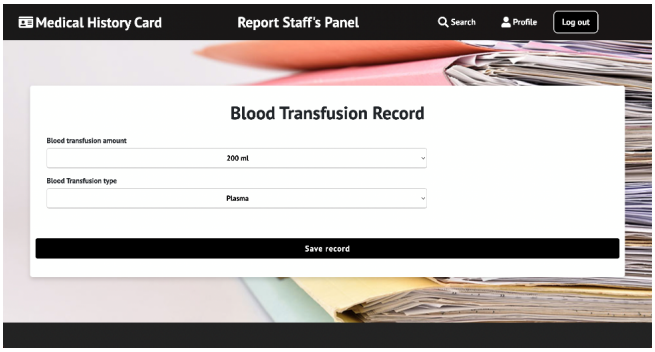


Figure 13: A Report Staff Uploading Blood Transfusion Record

On the other hand, the personnel responsible for managing vaccines and reports have the capability to not just review personal histories but also to make updates to vaccination histories and reports as needed. The "Blood Transfusion Record" might also be synced by the report staff, as shown in Figure 13. In this case, the drop-down boxes are utilized to choose the quantity and type of transfused blood.

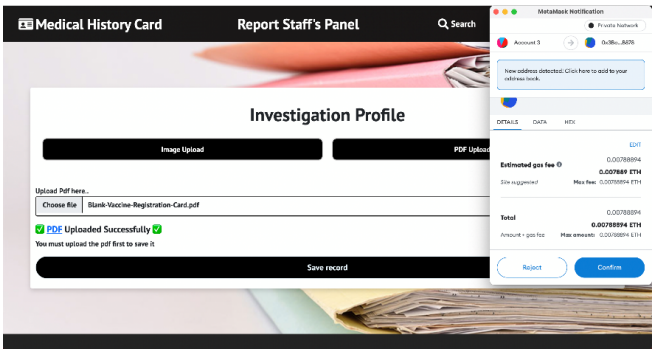


Figure 14: A Report Staff Uploading Patient's Investigation Profile

The report staff is also authorized to update a patient's "Investigation Profile," and the functionality for this task is similar to that of the prescription page. They have the ability to upload reports in both image and PDF file formats, providing flexibility in how medical information is recorded and shared.

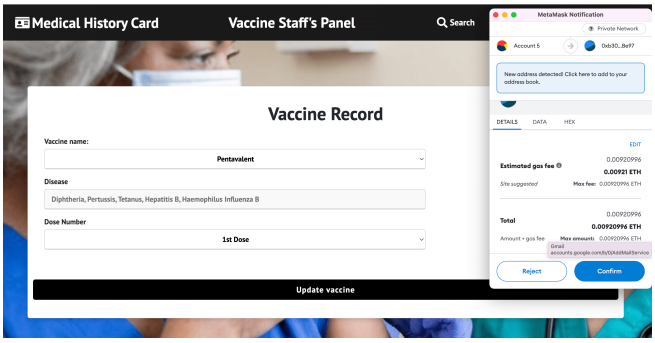


Figure 15: A Vaccine Staff Uploading Vaccination Record

It's also notable that, when updating vaccination histories, the vaccine staff will automatically see the name of the disease for which the vaccine is administered after selecting the vaccine's name from the drop-down box. Afterward, they must also select the quantity of vaccine doses (Figure 14).

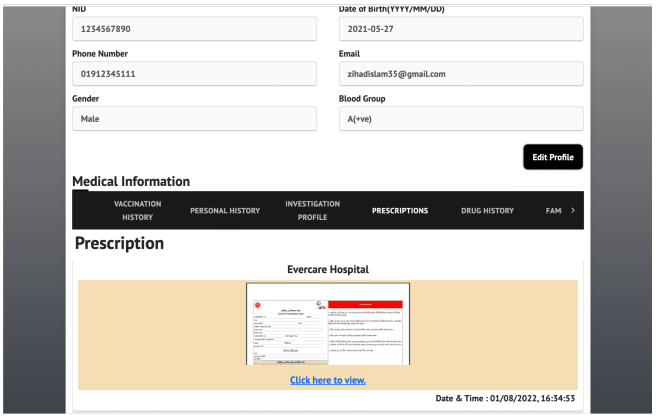


Figure 16: A Patient Viewing His Medical Information

Subsequently, patients are unable to upload their own data, but they can readily access their health-related information through the central navigation bar (as shown in Figure 15). Moreover, for enhanced monitoring, individuals have the option to download or print the medical reports and prescriptions, as well as capture screenshots of their medication history, personal health history, and vaccine history.

7 Contribution

The aforementioned card plays a crucial role in enhancing the security of patients' important medical data and preventing unauthorized access and manipulation of information. Along with preserving the authenticity of those high-priority data, this card can assist users during life-threatening conditions. The details enlisted in Personal History are of immense importance in the medical world. People with diabetes, high blood pressure, allergies, sinusitis, or asthma cannot afford every treatment or medicine. For this reason, doctors always ask these notable queries during consulting patients. If the patients are unaware of these facts, they are asked to undergo tests immediately. Besides, surgery history and thyroid (either hypothyroid or hyperthyroid) are also essential health indicators. During emergencies, the particulars provide essential information about a person. Specifically, the blood group and emergency contact number can significantly help during critical accidents. Concurrently, the investigation profile will remove the burden of carrying out reports, making diagnosis analysis easier for the doctors. They can glance through the reports to check whether the patient has any significant problems. To add, they can also check the severity of the disorder at that moment, which would instantly give them a more advanced view of the patient's present condition. They would understand if the present illness is somehow related to the previous history or not. Furthermore, people at a time tend to forget their vaccinations and the number of doses taken. This might create confusion in adulthood. Hence, this card can remove the hassle of memorizing all the vaccines. Drug history and prescriptions are the only ways to know about past treatments for any disease. With this card, the patients will no longer lose these valuable records while getting

treated. Consequently, they will get proper treatment on time. Congenital anomalies or birth defects develop prenatally or may be diagnosed later in life. These records help assess whether a disease is by birth. Afterward, the card will assist doctors in becoming familiar with the genetic disorders of a patient in such a way that they can recommend effective ways to reduce the risks. In the same way, blood transfusion history makes the task of knowing about the transfusion date and amount easier. So, patients can refrain from confirming any hypothetical dates to the medical officers.

It is worth mentioning that, Blockchain technology addresses healthcare security challenges in a broader range through its decentralized and tamper-resistant nature. Advanced encryption techniques and hash functions contribute to securing data within each block. The decentralized structure, distributed across a network of nodes, minimizes the risk of unauthorized manipulation. Smart contracts automate and enforce security protocols, reducing reliance on centralized databases and enhancing overall data protection. Above all, Blockchain presents a comprehensive solution to healthcare security by combining transparency, integrity, and patient-centric control in the management of sensitive health data.

Finally, advice given by doctors will be enlisted in this card. Suppose any patient has consulted two doctors for any particular disease over a time interval, and the former doctor has suggested something. Viewing the records allows the latter to analyze if it worked for the patient. Besides, he can also add his suggestions for future reference.

8 Observation

Between 1973 and 2023, there has been a significant evolution in the field of medical records. In the past, people relied on paper-based records, which were susceptible to data loss and damage, including the risk of being destroyed by fire or other accidents. As in [28] (2011) the authors have pointed out, EMRs have the potential to reduce diagnostic errors through various mechanisms. In a similar vein, we have structured our EMR system by categorizing information, aiming to create a more allocated, reliable, and information-rich system while maintaining brevity and efficiency. Furthermore, our web application is designed to alleviate the workload of hospital medical professionals and support staff.

Later, in 2016, the authors of the paper as refered [10] shed light on different aspects concerning the IoT and the digitalization of healthcare data. They emphasized that IoT mobile devices faced numerous challenges, including problems with integrating data, ensuring security and privacy, handling large volumes of data, maintaining performance, offering flexibility, dealing with the abundance of applications, and managing device diversity and interoperability. On the other hand, Blockchain databases were recognized for their flexibility and security. Additionally, our web application based on card technology was considered more convenient than relying on a device-oriented server.

Subsequently, we encountered web software which is stored information within a central database. However, in today's digital landscape, privacy issues have become prevalent, and concerns regarding hacking and data tampering with centralized databases have grown. Consequently, to enhance safety and visibility, we made the decision to adopt a decentralized database, specifically utilizing Blockchain technology. Moreover, we came across numerous applications that allowed patients to input their reports and other healthcare records. Nevertheless, on MHC, this information is automatically kept up to date by healthcare professionals and other affiliated staff members.

Following that, in [12] the authors provided valuable insights into the management of healthcare data utilizing blockchain technology, with a particular emphasis on sharing EMRs among medical providers. These researchers developed a prototype framework that aimed to guarantee privacy, security, availability, and precise access control over EMR data. It should be noted, however, that their framework had limitations, as it was designed exclusively for managing data related to cancer patients. In contrast, our paper extends this concept to encompass all patients, providing a more comprehensive approach to healthcare data management.

Next, in 2018, the researchers in [15] introduced an innovative attribute-based signature system that involved the participation of multiple authorities to authenticate the validity of EMRs integrated into the Blockchain. In this method, a patient signs a message using a specific attribute, revealing no extra information except for the verification that they have indeed endorsed it. It's important to emphasize that this signature method is rather complex and involves a higher associated cost. Conversely, our project is designed to be cost-effective, ensuring that it remains affordable for every citizen of a nation.

In summary, the Blockchain-based MHC system offers a solution where neither patients nor doctors can conceal or manipulate information, as records cannot be removed or altered. This innovative approach ensures the immutability of data, effectively putting an end to unreliable and erroneous information. The decentralized and distributed nature of Blockchain introduces a substantial level of complexity when it comes to any efforts to manipulate stored data, although it is not entirely impervious to such attempts. Moreover, the risk of data loss is eradicated because the servers of the network preserve a copy of the data.

Blockchain-based medical records systems in live healthcare environments face challenges such as user adoption, infrastructure integration, and regulatory compliance. These include complexity, resistance to change, compatibility with legacy systems, scalability, and compliance with data standards. Healthcare systems are highly regulated, and adhering to these regulations is crucial for patient data security. Additionally, ensuring interoperability and compliance with data standards across different healthcare providers' systems is essential. Initial investment in infrastructure, development, and training can be challenging, and resource allocation can be ongoing. To address these challenges, collaboration and education, pilot projects, interoperability standards, partnerships, and continuous evaluation and improvement are essential. A strategic approach, collaboration between stakeholders, and a clear understanding of technical and regulatory landscapes are necessary for successful implementation in a live healthcare environment.

The MHC system is not only cost-free but also more optimized than relying on any gadget-based server. Moreover, it is readily accessible to every citizen which makes it a valuable addition to the tech improvements of the medical field.

9 Upcoming Work

The medical history card is dedicated to advancing healthcare technology through the utilization of Blockchain technology. Its ultimate objective is to guarantee the safety and credibility of medical data. To enhance its use during emergencies, microchips will be incorporated in the future. This electronic, intelligent microchip-based card will store all patient data, enabling doctors to quickly access medical histories by scanning the card. Additionally, the implementation of biometric fingerprints will further enhance user authentication, providing significant benefits even for unconscious patients who may not have a physical card. Furthermore, MHC could serve as evidence of health insurance by storing records within a decentralized database. Medical history is essential in medical insurance, guiding risk assessment, underwriting, and claim validation. It informs insurers about health risks, aids policy customization, and verifies the legitimacy of treatments. Customizing policies based on health profiles and using medical history in actuarial analysis enhances overall insurance efficiency, ensuring tailored coverage and effective resource management. In essence, MHC is a cornerstone in shaping informed decisions throughout the insurance process.

In terms of family history, it would automatically establish a family history by cross-referencing an individual's HID with that of their parents. That said, the card that collects a patient's thorough history from birth will become inundated with a substantial amount of information, posing challenges and requiring a significant amount of time for doctors to navigate through. Therefore, several AI recommendations for assisting doctors would be added. When a patient visits a doctor, the system will prioritize displaying relevant information about the doctor's field of specialization. As an example, a cardiologist will be able to go through the patient's analysis reports, prescribed medicines, and diagnosis results of other consulted cardiologists first. This will not only optimize time and energy but also help in identifying the underlying causes more efficiently. The website will incorporate a search bar to simplify the process of searching for specific patient medical information by entering relevant keywords. In addition to this, it will introduce a filtering feature that allows doctors to search a patient's EMRs based on the year. The website will utilize AI to examine all the vital criteria provided by the client. If any potential risk factors are identified, the site will display a warning message and offer recommendations for the appropriate specialists. The integration of automated recommendation represents a paradigm shift in healthcare, employing AI, ML, and data analytics to offer personalized guidance to healthcare professionals and patients. These systems analyze patient data, create personalized treatment plans, predict health risks, monitor health remotely, prescribe medications, optimize resource allocation, and contribute to clinical trials. By leveraging extensive datasets, these automated recommendations enhance patient outcomes and streamline healthcare delivery, showcasing a substantial leap in utilizing data for improved medical practices. It also aspires to utilize AI to analyze user-provided information about their current health issues and provide recommendations for appropriate first-aid measures and relevant specialists. Besides, the users will be able to submit their urgent needs and preferred location for blood through a new section on the website. Anyone in the vicinity who is willing to donate blood will be promptly notified by the application.

10 Conclusion

The current paper implements a multi-functional history card system to be the best companion in one's healthcare world. In other words, it terminates the conventional papered system of preserving patients' medical history by introducing a portable card; that accumulates every tiny detail such as personal narrative, prescriptions, reports, drugs, vaccine history, etc. The card serves the dual purpose of consolidating Electronic Medical Records (EMRs) into a unified system and ensuring that users have controlled access to protect their privacy. Crucially, a brief review of the history card provides doctors with a more concise overview of the patient's medical background. Moreover, it makes it easy for the users to search for and get an auto-update of their required medical information within a trouble-free go. Besides, the understandable user interface can assist people in avoiding any last-minute stress while visiting doctors. Conversely, doctors and medical officers can also track patients' diagnoses properly. They can view, read, and update medical data as per their need and avoid the hassles of handling lots of reports and papers, eventually protecting their goodwill in the long run. Hence, the medical history card comes into the picture in every scenario of contributing to the flourishment of the healthcare world. All in all, Blockchain technology can revolutionize healthcare with secure, interoperable, and patient-centric data management. Research priorities include improving security, ensuring interoperability, implementing consent management, addressing legal challenges, and enhancing user experience and adoption. Continued research and development efforts have the potential to significantly elevate the capabilities and reliability of blockchain-based systems for medical records, transforming the healthcare industry.

References

[1] S. Fairooz, S. Y. Miti, Z. Islam, M. T. Zaman, "A medical history card utilizing the Blockchain technology," in 2023 5th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA), 1–6, 2023, doi:10.1109/HORA58378.2023.10156689.

[2] R. Hillestad, J. Bigelow, A. Bower, F. Girosi, R. Meili, R. Scoville, R. Taylor, "Can Electronic Medical Record Systems Transform Health Care? potential health benefits, savings, and costs," Health Affairs, **24**(5), 1103–1117, 2005, doi:10.1377/hlthaff.24.5.1103.

[3] C. M. Ruland, H. Bryhni, R. Andersen, T. Bryhni, "Developing a Shared Electronic Health Record for Patients and Clinicians," Studies in health technology and informatics, **136**, 57–62, 2008.

[4] K. Phillips, C. Wheeler, J. Campbell, A. Coustasse, "Electronic medical records in long-term care," J. Hosp. Mark. Public Relations, **20**(2), 131–142, 2010.

[5] M. Gomi, Y. Nakayama, Y. Sakurai, R. Oyama, K. Iwasaki, M. Doi, Y. Liu, M. Hori, H. Watanabe, K. Hashimoto, H. Tanaka, K. Tange, Y. Nakai, H. Akita, "Tolerogenic lipid nanoparticles for delivering self-antigen mRNA for the treatment of experimental autoimmune encephalomyelitis," Pharmaceuticals (Basel), **16**(9), 1270, 2023.

[6] Y. C. Li, P. S. Lee, W. S. Jian, C. H. Kuo, "Electronic health record goes personal world-wide," Yearb. Med. Inform., **18**(01), 40–43, 2009.

[7] S. Soegijoko, I. Puspitasari, A. Aridarma, I. Jani, "e-health for improving community healthcare: Encouraging clinical experience of simple e-prescription system and m-health system development for mother and childcare," in 2011 IEEE 13th International Conference on e-Health Networking, Applications and Services, 102–105, 2011, doi:10.1109/HEALTH.2011.6026722.

[8] E. T. van der Velde, H. Foeken, T. A. Witteman, L. van Erven, M. J. Schalij, "Integration of data from remote monitoring systems and programmers into the hospital electronic health record system based on international standards," Neth. Heart J., **20**(2), 66–70, 2012.

[9] O. Ben-Assuli, I. Shabtai, M. Leshno, "Using electronic health record systems to optimize admission decisions: the Creatinine case study," Health Informatics J., **21**(1), 73–88, 2015.

[10] A. Chhatlani, A. Dadlani, M. Gidwani, M. Keswani, P. Kanade, "Portable Medical Records Using Internet of Things for Medical Devices," in 2016 8th International Conference on Computational Intelligence and Communication Networks (CICN), 446–451, 2016, doi:10.1109/CICN.2016.93.

[11] A. Ekblaw, A. Azaria, J. Halamka, A. Lippman, "A case study for blockchain in healthcare:"MedRec" prototype for electronic health records and medical research data. White Paper," Retrievedfrom https://static1. squarespace. com/static/59aae5e9a803bb10bedeb03e, **5**, 1517278000381, 2016.

[12] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, F. Wang, "Secure and trustable electronic medical records sharing using blockchain," in AMIA annual symposium proceedings, volume 2017, 650, American Medical Informatics Association, 2017.

[13] "Why Blockchain Technology Is Important for Healthcare Professionals — Mendeley," https://www.mendeley.com/search/?page=1&query=Why%20Blockchain%20Technology%20Is%20Important%20for%20Healthcare%20Professionals&sortBy=relevance, (Accessed on 11/30/2023).

[14] A. F. Hussein, N. ArunKumar, G. Ramirez-Gonzalez, E. Abdulhay, J. M. R. Tavares, V. H. C. de Albuquerque, "A medical records managing and securing blockchain based system supported by a Genetic Algorithm and Discrete Wavelet Transform," Cognitive Systems Research, **52**, 1–11, 2018, doi: https://doi.org/10.1016/j.cogsys.2018.05.004.

[15] R. Guo, H. Shi, Q. Zhao, D. Zheng, "Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems," IEEE Access, **6**, 11676–11686, 2018, doi:10.1109/ACCESS.2018.2801266.

[16] J. Liu, X. Li, L. Ye, H. Zhang, X. Du, M. Guizani, "BPDS: A Blockchain Based Privacy-Preserving Data Sharing for Electronic Medical Records," in 2018 IEEE Global Communications Conference (GLOBECOM), 1–6, 2018, doi:10.1109/GLOCOM.2018.8647713.

[17] K. Riad, R. Hamza, H. Yan, "Sensitive and Energetic IoT Access Control for Managing Cloud Electronic Health Records," IEEE Access, **7**, 86384–86393, 2019, doi:10.1109/ACCESS.2019.2926354.

[18] Y. Zhao, M. Cui, L. Zheng, R. Zhang, L. Meng, D. Gao, Y. Zhang, "Research on electronic medical record access control based on blockchain," International Journal of Distributed Sensor Networks, **15**(11), 1550147719889330, 2019.

[19] V. Mehra, P. Sarvari, N. Ruban, "RFID Based Secured, Remotely Accessible Personal Medical Data Base Including the Medicinal History," in 2018 4th International Conference on Computing Communication and Automation (ICCCA), 1–4, 2018, doi:10.1109/CCAA.2018.8777617.

[20] M. T. de Oliveira, L. H. A. Reis, R. C. Carrano, F. L. Seixas, D. C. M. Saade, C. V. Albuquerque, N. C. Fernandes, S. D. Olabarriaga, D. S. V. Medeiros, D. M. F. Mattos, "Towards a Blockchain-Based Secure Electronic Medical Record for Healthcare Applications," in ICC 2019 - 2019 IEEE International Conference on Communications (ICC), 1–6, 2019, doi: 10.1109/ICC.2019.8761307.

[21] S. Siva Rama Krishnan, M. Manoj, T. R. Gadekallu, N. Kumar, P. K. R. Maddikunta, S. Bhattacharya, D. Y. Suh, M. J. Piran, "A Blockchain-Based Credibility Scoring Framework for Electronic Medical Records," in 2020 IEEE Globecom Workshops (GC Wkshps, 1–6, 2020, doi:10.1109/GCWkshps50303.2020.9367459.

[22] C.-T. Li, D.-H. Shih, C.-C. Wang, C.-L. Chen, C.-C. Lee, "A Blockchain Based Data Aggregation and Group Authentication Scheme for Electronic Medical System," IEEE Access, **8**, 173904–173917, 2020, doi:10.1109/ACCESS.2020.3025898.

[23] M. T. Mahmud, F. Soroni, M. M. Khan, "Development of a Mobile Application for Patient's Medical Record and History," in 2021 IEEE World AI IoT Congress (AIIoT), 0081–0085, 2021, doi:10.1109/AIIoT52608.2021.9454227.

[24] M. Nasim, S. Abdullah-Al-Noman, A. Ragib Hasan, A. Sattar, "Digitalization and Centralization of Medical Information and Patient History in Bangladesh," in 2022 6th International Conference on Computing Methodologies and Communication (ICCMC), 153–158, 2022, doi:10.1109/ICCMC53470.2022.9753690.

[25] R. Cerchione, P. Centobelli, E. Riccio, S. Abbate, E. Oropallo, "Blockchain's coming to hospital to digitalize healthcare services: Designing a distributed electronic health record ecosystem," Technovation, **120**, 102480, 2023, doi: https://doi.org/10.1016/j.technovation.2022.102480.

[26] S. Singh, S. Kumar Sharma, P. Mehrotra, P. Bhatt, M. Kaurav, "Blockchain technology for efficient data management in healthcare system: Opportunity, challenges and future perspectives," Materials Today: Proceedings, **62**, 5042–5046, 2022, doi:https://doi.org/10.1016/j.matpr.2022.04.998, international Conference on Innovative Technology for Sustainable Development.

[27] M. Haidar, S. Kumar, "Smart Healthcare System for Biomedical and Health Care Applications using Aadhaar and Blockchain," in 2021 5th International Conference on Information Systems and Computer Networks (ISCON), 1–5, 2021, doi:10.1109/ISCON52037.2021.9702306.

[28] N. Malhotra, M. Lassiter, et al., "The coming age of electronic medical records: From paper to electronic," International Journal of Management & Information Systems (IJMIS), **18**(2), 117–122, 2014.

ASTES

Advances in Science, Technology and Engineering Systems Journal
Vol. 8, No. 6, 107-119 (2023)
www.astesj.com
Special Issue on Innovation in Computing, Engineering Science & Technology

ASTES Journal
ISSN: 2415-6698

Enhancing Cloud Security: A Comprehensive Framework for Real-Time Detection, Analysis and Cyber Threat Intelligence Sharing

Fazalur Rehman[*,1], Safwan Hashmi[2]

[1]*Department of Cybersecurity, Air University, PAF Complex, E-9, Islamabad, Pakistan*

[2]*Department of Cybersecurity, Riphah International University, Evacuee Trust Complex, F-5, Islamabad, Pakistan*

ARTICLE INFO

Article history:
Received: 30 September, 2023
Accepted: 05 December, 2023
Online: 30 December, 2023

Keywords:
Cloud Security
Virtual Machine Introspection
Cloud Computing
Incident Management
Cyber Threat Intelligence
Incident Response
Threat Sharing
Cloud Infrastructure Security

ABSTRACT

Cloud computing has emerged as a pivotal component of contemporary IT systems, affording organizations the agility and scalability required to meet the ever-changing demands of business. However, this technological evolution has introduced a new era of cybersecurity challenges, as attackers employ increasingly sophisticated strategies to breach cloud networks. Such breaches can have far-reaching consequences, including data loss, financial repercussions, reputational damage, and legal liabilities. In response to these challenges, developing a robust security framework is imperative for effectively safeguarding cloud infrastructure. This paper proposes a novel Hypervisor-based Virtual Machine Introspection (HVMI) for real-time detection and runtime forensic analysis of cyberattacks targeting cloud platforms. The framework proposed comprises several essential components, including a forensic application empowered by Virtual Machine Introspection (VMI) for real-time memory analysis, a centralized Cloud Forensic Tool (CFT) portal for streamlined incident management, and a data transmission and integration web service. Notably, this framework is founded upon a commitment to continuous optimization and enhancement. This iterative process is facilitated through a collaboration approach. It involves fine-tuning various aspects of the framework, such as adjusting settings for VMI, refining criteria for classifying incidents, and updating security controls. Enhancing the forensic application represents a proactive measure aimed at improving the efficiency and effectiveness of VMI and forensic analysis capabilities. The iterative refinement process integrates incident analysis, threat intelligence infusion, and collaborative efforts to adapt to emerging challenges. This dynamic approach fosters a flexible security posture capable of detecting, analyzing, and responding to emerging attacks within cloud platforms. In summary, the proposed framework embodies a comprehensive approach to cloud security, integrating advanced technology with continuous refinement to protect cloud infrastructure, mitigate risks, and navigate the ever-evolving cybersecurity threat landscape effectively.

1 Introduction

Cloud computing has emerged as a fundamental element within modern computing systems, providing organizations with the capacity for on-demand resources and adaptable scalability. It is the on-demand delivery of IT resources. Organizations instead of buying or owning their physical data centers and servers depend on cloud service providers. Securing IT infrastructure is a major challenge nowadays. Within the domain of cloud computing, cybersecurity is a critical concern, given that data breaches have far-reaching impacts on organizations. This paper presents a novel technique and framework based on virtual machine introspection to detect and perform runtime forensic analysis of attacks on cloud platforms. This paper is an extension of the work originally presented at the IEEE 3rd International Conference on Artificial Intelligence (ICAI) 2023 [1].

With the expansion of cloud infrastructure adoption, there has been a corresponding amplification in the array of techniques and approaches employed by malicious entities to initiate attacks targeting these network environments [2]. Such attacks present a substantial threat to the confidentiality, integrity, and availability of cloud-based systems, and can have significant consequences for organizations depending on these systems for their operational functions [3]. These breaches can lead to the exposure of sensitive information, financial

[*]Corresponding Author: Fazalur Rehman, Air University, PAF Complex, E-9, Islamabad, Pakistan, 181219@students.au.edu.pk

losses, harm to an organization's reputation, and legal consequences [4]. To mitigate these risks, organizations need to implement effective cybersecurity measures to ensure the security of their cloud infrastructure [5].

Conventional methods employed for securing cloud infrastructures, such as virtual-level segregation, intrusion detection prevention systems (IDS/IPS), cloud access and security brokers (CASB), and endpoint detection & response, frequently prove inadequate in countering the progressively sophisticated techniques deployed by attackers targeting cloud networks [6]. Even when efforts are made to analyze or thwart these attacks, attackers often exhibit adaptability, which enables them to resist detection and mitigation. Furthermore, these protective measures often operate within virtualized environments shared across interconnected networks, rendering them susceptible to deceptive tactics, insider threats, and network-level attacks [7, 8].

In the event of a security breach, the proposed HVMI solution notifies the cloud service provider while concurrently initiating a forensic analysis to identify the root cause and extent of the breach. This real-time detection and analysis capability inherent in the HVMI tool represents a pivotal enhancement to cloud system security, offering substantial protection against the adverse consequences stemming from data breaches. Furthermore, by incorporating this solution within a web service framework, it attains cross-platform compatibility, irrespective of the underlying hardware and software infrastructure. In a bid to maximize the utility of this research, we have conceptualized a web portal where instances of attack patterns can be uploaded. This portal serves as a means to disseminate information to security organizations and cloud service providers globally, effectively notifying them of prevailing cloud-based attack trends and facilitating the formulation of defensive strategies against such threats. This research endeavor not only contributes to the collective knowledge in the field but also holds practical significance for industry stakeholders, security professionals, and cloud service providers. It offers a novel and real-time approach to detect and analyze attacks within cloud environments, with the overall objective of minimizing their adverse impact on the confidentiality, integrity, and availability of cloud systems.

1.1 Research Contributions

1. The HVMI solution comprises a client application, specifically a forensic application, that operates on the cloud service provider's host. Its primary function is to identify and mitigate the impact of security breaches, making it a valuable resource for organizations seeking to shield themselves from the cyberattacks.

2. Within this framework, malicious artifacts are systematically gathered from virtual machines (VMs), yielding critical insights into the techniques and methods employed by attackers. These artifacts are subsequently transformed into a comprehensible, organized, and shareable format. HVMI adopts the Structured Threat Information eXpression (STIX) standard [9] to generate consistent threat details. These standardized threat details are invaluable to security organizations as they facilitate the development of defensive strategies against specific types of cyberattacks in the cloud, thereby enhancing the overall security posture of cloud systems.

3. The integration of a web service framework ensures cross-platform compatibility, rendering the HVMI solution independent of the underlying hardware and software. Additionally, the accompanying web portal serves as a dedicated platform for the dissemination of cyber threat intelligence. It caters to the needs of both security organizations and cloud service providers, facilitating the exchange of vital information to bolster cybersecurity efforts in cloud environments.

1.2 Organization of the paper

The paper is organized as: section 2 provides literature review. Section 3 provides details of the proposed framework. Section 4 provides details of results, and attack simulations. Section 5 is conclusion & future directions.

2 Review of the Literature

This section offers a comprehensive summary of the existing research within the selected domain. It serves to elucidate the present state of knowledge regarding the subject matter, encapsulating the key findings and insights derived from prior studies. Furthermore, it identifies gaps in existing research or areas where current research falls short, signifying opportunities for further investigation and research.

Virtualization stands as a pivotal element within the IT industry, greatly augmenting management capabilities and unlocking the full potential of hardware infrastructure. In essence, Virtualization provides the capability to the impression of multiple physical systems of a single system. It provides a virtual version of the underlying hardware platform, storage media, network devices etc. Virtualization has numerous advantages over traditional physical system architectures, encompassing cost-efficiency, reduced hardware resource requirements, and optimal utilization of available hardware resources. It enables the utilization of hardware to its maximum potential, a feat unattainable within the confines of conventional infrastructure [10]. A hypervisor, also referred to as a virtual machine manager (VMM), is a software application designed to facilitate the creation and administration of virtual machines (VMs) on a physical host. These hypervisors introduce a layer of abstraction between the physical hardware and the virtual machines, enabling multiple VMs to efficiently utilize the resources of a single physical machine. Hypervisors are of paramount importance in cloud computing settings, as they assume a central role in the establishment and supervision of numerous virtual machines (VMs) on a single physical host. This functionality endows organizations with the flexibility to dynamically adjust their computational resources in tandem with fluctuations in demand, thereby optimizing resource allocation in the cloud environment. There are two primary categories of hypervisors:

Type I (or native or bare metal) hypervisors: These hypervisors operate directly on the host's hardware, creating a virtualization layer that interfaces between the hardware and the operating sys-

tem [11]. Prominent examples of Type 1 hypervisors encompass VMware ESXi, KVM, Microsoft Hyper-V, and Xen.

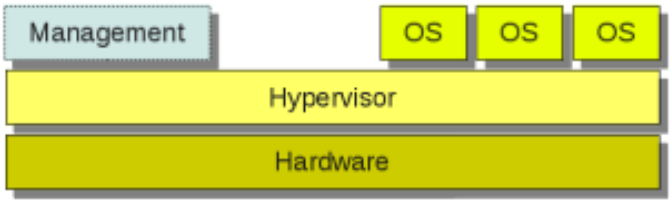


Figure 1: VMM Type I [12]

Type II (or hosted) hypervisors: These hypervisors run atop a host operating system, delivering virtualization capabilities for guest operating systems. Well-known instances of Type 2 hypervisors include VMware and VirtualBox.

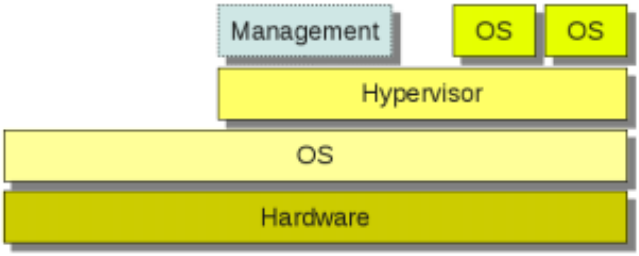


Figure 2: VMM Type II [12]

There has been a growing interest in the adoption of hypervisor-based introspection techniques for the identification and analysis of security breaches within cloud platforms. Notable contributions in this field include the work of Brian [13] have developed a toolbox known as Virtual Contemplation for Xen (VIX). This toolbox has demonstrated its capacity to conduct live examinations and gather volatile data from virtual machines. Their approach involves pausing the virtual machine, extracting the necessary data, and then resuming the virtual machine. In a similar vein, another toolset akin to VIX is XenAccess, created and maintained in [14]. XenAccess is designed to offer a library of functions for constructing a monitoring architecture. This includes employing virtual memory introspection to monitor applications and access the memory state of the virtual machine. This architecture has been leveraged to implement Virtual Machine Introspection (VMI), enabling forensic investigations within virtual machine environments.

In [15], the author introduced Memory Forensics Analysis (MFA). They achieved this by deploying an in-guest agent within the virtual machine (VM) to collect detailed information regarding the processes running on that VM. In a similar vein [16], the author proposed a comprehensive security framework that encompasses both a network-based intrusion detection system (NIDS) and a virtual machine introspection-based intrusion detection system (VMIIDS). The NIDS acts as the initial line of defense, monitoring network traffic before it reaches the virtualization layer. Meanwhile, the VMI-IDS operates at the hypervisor level, where it focuses on detecting intrusions occurring within the VMs themselves. This dual-layered approach enhances the security posture of cloud environments by addressing threats at different levels of the infrastructure.

In [17], the author introduced an anomaly-based detection system designed for the detection of malware at the hypervisor level. Nonetheless, the effectiveness of this approach is circumscribed, and it may not prove sufficiently robust against highly sophisticated and complex attacks. In [18], the author advocated for the utilization of hypervisor-based introspection to identify malware by analyzing information gathered from guest machines and network-level devices. Although this approach achieved a detection accuracy of approximately 90 percent under optimal conditions, its performance declined when confronted with more complicated and advanced attack vectors.

In [19], the author introduced an innovative hardware-based monitoring system named HyperMon, designed for the detection and surveillance of attacks within cloud platforms. HyperMon was implemented within the Xen hypervisor and used machine learning techniques to inspect low-level hardware data at the virtual machine manager (VMM) layer. This process was employed to construct statistical models for programs. In [20], the author put forward a Virtual Machine Introspection (VMI) approach, focusing on anomaly-based detection of keyloggers. This approach accomplished by tracking a spectrum of events, including memory reads and writes, interrupts, and network logs. Subsequently, the collected data underwent analysis employing an artificial immune system (AIS)-based intrusion detection system (IDS) to identify anomalies. However, it's noteworthy that this approach has limitations as it is primarily applicable to Linux-based systems and virtual machines.

In [21], the author proposed a security framework for cloud environments, centered around Virtual Machine Introspection (VMI). This framework is geared towards monitoring the active processes within virtual machines (VMs) by tracking system call traces. The method employs Nitro, a hardware-based tool, to capture these system call traces, which are subsequently relayed to a centralized analyzer. This analyzer utilizes a classification model to distinguish between legitimate and malicious processes. If a process is classified as malicious, an alert is generated. In alignment with the notion that security and monitoring should be implemented at the hypervisor level. In [22], the author proposed a malware analysis technique employing VMI. Their research, however, predominantly focuses on the domain of malware analysis, virtualization techniques, and specific malware families.

The existing solutions discussed in the literature review, while effective at detecting certain types of attacks like rootkits, keyloggers, or malware, exhibit limitations in their capacity to defend against emerging cybersecurity threats. These limitations arise due to their inability to comprehensively address the evolving tactics, techniques, and procedures employed by sophisticated attackers. Furthermore, many of these solutions lack a specific focus on the unique challenges posed by the cloud environment, thus constraining their effectiveness in safeguarding against cloud-based attacks. Traditional methods for analyzing virtual machine (VM) memory and conducting forensic investigations are becoming increasingly very complicated and resource-intensive, rendering them impractical for everyday use. There is a pressing need for an automated solution capable of handling the concurrent security of numerous

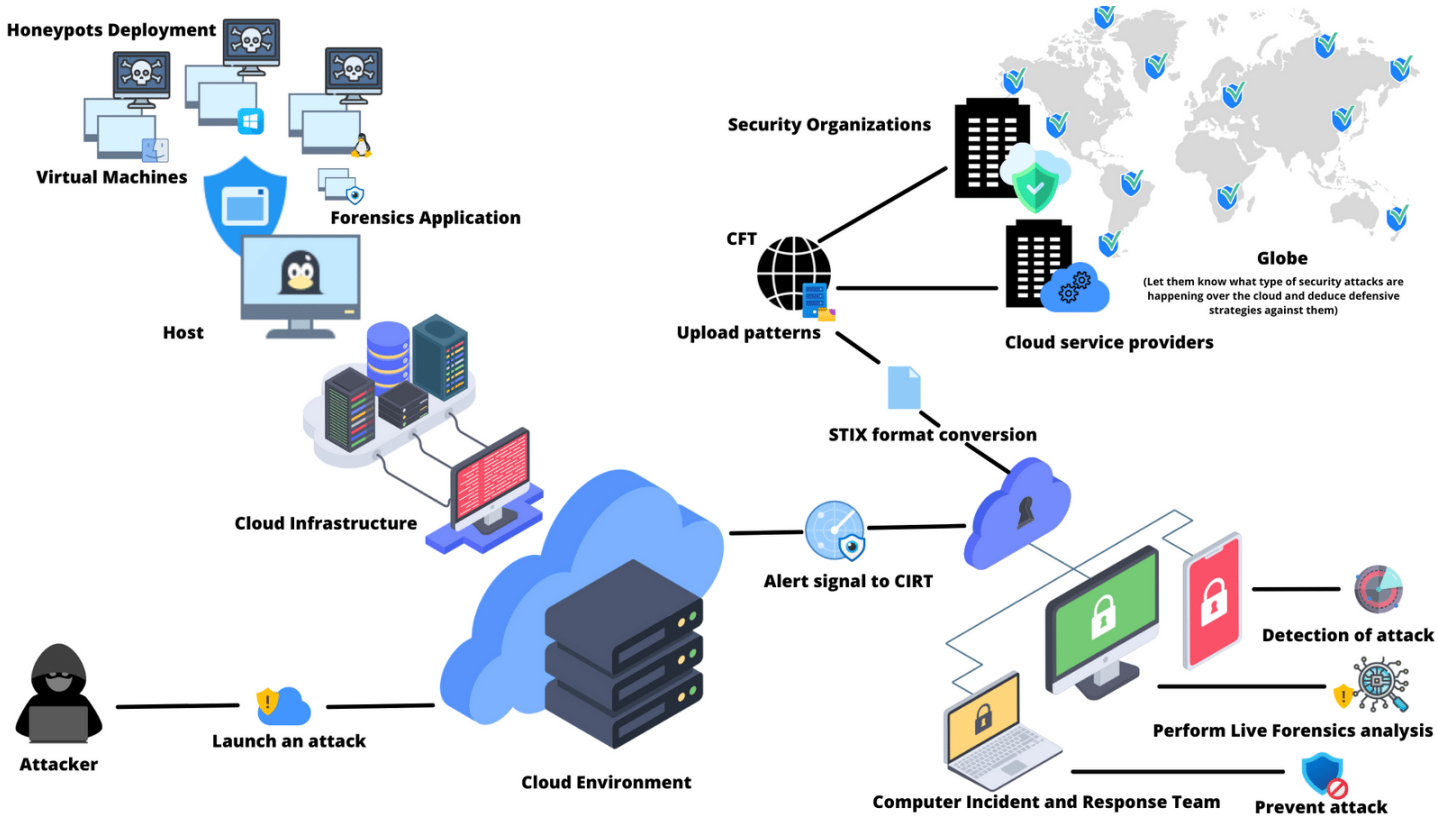


Figure 3: Provides a comprehensive overview of the proposed framework.

VMs, effectively guarding against a broad spectrum of emerging cyber threats, and possessing the scalability required to meet the demands of extensive cloud environments.

3 Proposed Framework: Design and Architecture

Our proposed framework for detecting and analyzing attacks on cloud platforms adopts a proactive monitoring approach encompassing both the host and virtual machine (VM) levels. Within this framework, a dedicated forensic application is deployed to inspect VM memory for valuable artifacts and to execute forensic analysis in response to potential attacks on VMs. In the event of a security breach, the system generates alerts, which are promptly disseminated to a Computer Incident Response Team (CIRT) portal. At the CIRT portal, an in-depth forensic analysis is initiated to identify the specific tactics, techniques, and procedures employed in the attack. The findings from this analysis are subsequently translated into a structured threat information expression (STIX) format, enabling their integration into the realm of cyber threat intelligence. Importantly, this framework emphasizes rapid incident reporting, ensuring that security incidents are communicated as soon as they are detected and thoroughly analyzed.

The CIRT possesses access to an extensive knowledge repository comprising analytical reports, procedural guidelines, service records, security logs, and applications installed within the targeted virtual machine (VM). This repository serves as a pivotal resource for identifying any indicators of malicious activity during forensic analysis. Furthermore, the forensic application integrated into the framework exhibits continuous operational verification by dispatching SYN (synchronize) messages to the user interface, thereby confirming its operational status and ensuring the continued activity of the VM. This application also generates diverse types of alerts that are duly documented within the activity log featured on the dashboard. The underlying objective of our proposed framework is to deliver a holistic approach for the detection and analysis of security breaches within cloud platforms. This entails facilitating the exchange of threat intelligence, enriching the knowledge base, and generating alerts, all while maintaining cross-platform compatibility—a facet often absent in traditional solutions. The fundamental aim is to mitigate the repercussions of security incidents and empower the formulation of effective defensive strategies [23].

Fig. 3 offers a comprehensive schematic representation of our proposed framework, providing a holistic view of its operational dynamics. The diagram illustrates the combination of (VMs) operating within the host machine, located in the upper left corner. Concurrently, it offers an illustrative depiction of an attack scenario orchestrated by an aggressor. On the right-hand side of the diagram, the visualized attack scenario seamlessly transitions into the stages of detection, forensic analysis, and the subsequent generation of attack patterns. Notably, these attack patterns are made accessible to the public domain, facilitating proactive measures for defense against forthcoming cyber threats. This visual representation encapsulates the essence of our proposed framework's operation clearly and concisely, offering a cohesive understanding of its functionali-

ties.

In the realm of cybersecurity, the acquisition and utilization of information hold paramount importance. The contemporary surge in cyberattacks has given rise to an encyclopedia of data related to these attacks, effectively constituting a comprehensive repository of information-gathering assaults. Safeguarding systems and IT infrastructure necessitates a two-fold approach. Firstly, a thorough understanding of system vulnerabilities and weaknesses is imperative. Simultaneously, it is crucial to possess insights into the tactics and techniques employed by malicious actors to conduct attacks. This dual comprehension forms the base for making informed decisions geared towards fortifying system defenses. Acknowledging the critical need for robust information exchange within the cybersecurity community, a standardized language has been devised to share threat indicators. This standardization provides flexible and effective dissemination of vital information among cybersecurity stakeholders. In tandem, it complements the proactive stance of gathering comprehensive knowledge about cybersecurity threats, thereby fortifying our capacity to defend against adversarial actions targeted at IT and digital infrastructure. Facilitating this information sharing and knowledge enrichment is done by the Structured Threat Information eXpression (STIX). STIX is an industry-standard programming initiative, developed from the collaborative efforts of multiple organizations, tailored to cater to the need of cyber threat intelligence. This standardized framework is designed to enable the most effective, flexible, and uniform exchange of information in the realm of cybersecurity. The data sharing encompassed within this framework covers threat indicators, incident reports, cyberattack campaigns, profiles of threat actors, courses of action, cyber observables, adversary Tactics, Techniques, and Procedures (TTPs), and exploited targets.

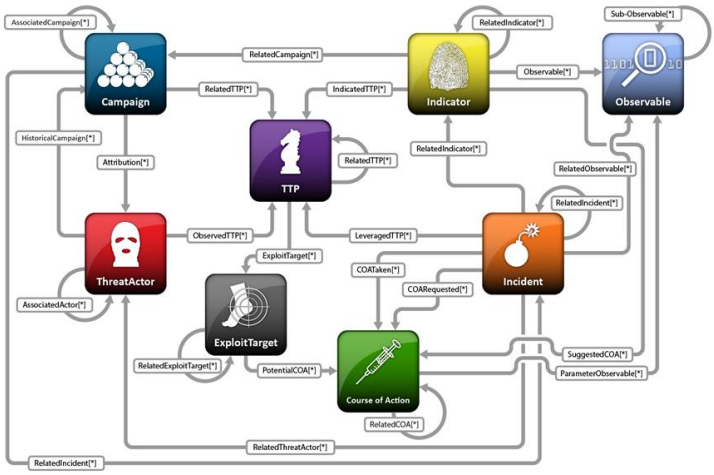


Figure 4: Figure 4 outlines STIX's architecture [24] for human-machine cyber threat understanding.

Fig. 4 provides a brief and basic overview of STIX's architecture consisting of cyber threat information which enables human and machine understandable format. Furthermore, our proactive approach extends to the development of a web portal that invites collaborative contributions from Computer Incident Response Teams (CIRTs), cloud service providers, and security organizations. This collaborative endeavor is predicated on the principle that sharing knowledge and expertise is instrumental in enhancing cybersecurity measures. In the aftermath of successfully mitigating an attack, the resulting attack patterns are transmuted into the STIX format and uploaded onto this web portal. This affirms the pivotal role played by STIX in the domain of cyber threat intelligence, as an indispensable tool for strengthening cybersecurity measures and fostering collective resilience against evolving threats.

Within this solution, we have strategically integrated the NIST 800-53 security control families, with particular emphasis on the following key elements: **Audit and Accountability (3.3):** This component is vital for maintaining comprehensive records of system activity to facilitate effective monitoring and analysis. **Assessment, Authorization, and Monitoring (3.4):** This aspect encompasses the critical phases of assessing, authorizing, and continually monitoring system security. **Vulnerability Monitoring and Scanning (3.16 RA-5):** The solution places significant focus on continuously monitoring and scanning for vulnerabilities, ensuring proactive threat mitigation. **Technical Surveillance Countermeasures Survey (3.16 RA-6):** This control addresses the imperative task of conducting technical surveillance countermeasures surveys to safeguard against potential threats. **Incident Response (3.8):** Incident response is a core facet, with particular emphasis on IR-4, which encompasses incident handling. This includes detection, analysis, containment, and eradication of security incidents. These NIST 800-53 control families are integral to the comprehensive complete solution, contributing to its robust security posture by addressing various aspects of security control, monitoring, and incident response, thereby fortifying the overall cybersecurity framework.

3.1 Deployment and Simulation

The proposed framework for the detection and analysis of attacks on cloud platforms is adaptable to diverse cloud environments. Its flexibility is exemplified by the ability to deploy the forensic application both on the host and within virtual machines (VMs). Furthermore, the CIRT portal is designed to be accessible remotely, permitting authorized users to engage with it from a distance. To enhance the efficacy of the proposed framework, rigorous testing can be conducted through the execution of simulated attack scenarios encompassing various attack types and security contexts. The outcomes derived from these simulations serve as a means to comprehensively assess the framework's performance. Subsequently, any identified areas for potential enhancement or improvement can be systematically addressed, ensuring that the framework attains optimal effectiveness in real-world deployments. This iterative process of testing and refinement contributes to the continual evolution and robustness of the framework, aligning it with the dynamic landscape of cybersecurity in cloud environments.

To illustrate, the forensic application within the framework is amenable to configuration for the emulation of diverse attack types, encompassing scenarios involving malware, rootkits, and keyloggers. Subsequently, the CIRT can conduct an in-depth analysis of the data generated by these simulated attacks to assess the framework's efficacy in both detection and analysis. The outcomes of these simulations serve a dual purpose. Firstly, they enable the fine-tuning of the forensic application's configuration and the optimization of

the CIRT portal's functionality, enhancing their performance in the context of attack detection and analysis. Secondly, the simulation results can illuminate potential vulnerabilities or deficiencies within the framework, thereby providing critical insights for further enhancement. By utilizing the power of simulations, the proposed framework stands to undergo iterative refinement, resulting in an elevated level of effectiveness in the detection and analysis of attacks within cloud platforms. This iterative process, rooted in empirical testing and analysis, lends itself to the continuous improvement of the framework's capabilities, ensuring its relevance and robustness in an ever-evolving cybersecurity landscape within the cloud. To facilitate comprehension, an illustrative workflow is presented in Fig. 5, providing a simplified depiction of the sequential steps inherent to the outlined rational approach. This provides a clear and accessible representation of the procedural sequence.

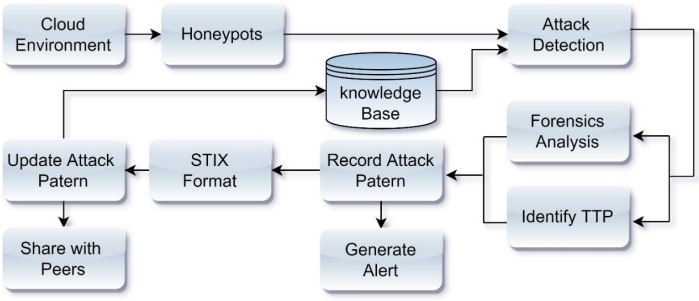


Figure 5: A visual representation of the attack detection workflow process.

The establishment of a cloud system entails the configuration of multiple virtual machines (VMs), each equipped with distinct honeypots designed to entice potential attackers into initiating attacks. Upon activation of these honeypots, they initiate a signaling process that notifies the Computer Incident Response Team via the dedicated CIRT portal. This orchestration allows the framework to conduct forensic analysis of the attack stealthily, rendering the attacker unaware of the ongoing detection, monitoring, and analysis. This stealthy approach is instrumental in uncovering the Tactics, Techniques, and Procedures (TTP) deployed by the attacker during the course of the attack. By surreptitiously observing and dissecting the attack, the framework can glean critical insights into the attacker's modus operandi, thereby enhancing our understanding of cyber threats and fortifying our defenses. Detailed information regarding the subcomponents, essential features, and functional domains is elaborated upon in the subsequent sections.

3.1.1 *Forensic application*

The core functionality of the forensic application encompasses the critical task of executing virtual machine introspection (VMI) and subsequently transmitting the acquired data to the web service [25]. It is important to highlight that the forensic application is designed to function flawlessly on both the host and the virtual machines (VMs), highlighting its critical function in enhancing cloud infrastructure security against persistent cyber threats. To ensure the distinct identity and traceability of each instance of the forensic application, a unique identification (ID) is assigned to every running instance, whether on the host or VMs. This rigorous identification system serves as a base for precise command execution during VMI operations. Notably, the framework's inherent cross-platform compatibility enables the seamless implementation of updates and patches for the forensic application, thereby ensuring its continual alignment with evolving security requirements. It is crucial to keep the forensic application hidden from possible attackers. It is safeguarded through an array of comprehensive countermeasures that are meticulously enforced to preserve the application's integrity. Furthermore, the forensic application, seamlessly integrated within the framework, maintains continuous operational verification. This is achieved through the systematic dispatch of SYN messages to the user interface, thereby affirming its operational status and ensuring the sustained functionality of the associated VM.

3.1.2 *Web services*

The web service plays a pivotal role within the architecture, serving as a vital intermediary between the forensic application and a centralized database repository. This repository houses an extensive range of data, which is subsequently made accessible through a dedicated cloud forensic tool (CFT) or portal. The primary function of the web service revolves around the seamless transmission of data from the forensic application to the database, a process executed in real-time upon data reception. The data collected by the forensic application is rich and multifaceted, encompassing crucial system information such as operating system details, processor specifications, core configurations, RAM allocations, storage characteristics (both hard drive and solid-state drive attributes), serial identification markers, geographical location data, active processes, system services, security logs, and a comprehensive list of installed applications. Before integration into the database, this collected data undergoes rigorous parsing procedures to ensure its uniformity and compatibility. Once parsed, the data is methodically inserted into the database, subsequently becoming readily accessible through the designated portal. The incorporation of the web service stands as a fundamental component within this framework, endowing the proposed solution with cross-platform compatibility. This strategic architecture ensures that the core infrastructure remains consistent, with adaptations made solely to the forensic application running on the host and VMs to align with the specific programming languages and hardware of the underlying systems. Consequently, the framework boasts versatility, capable of accommodating diverse operating environments ranging from UNIX, Linux, MAC, and IOS, to Android, among others. This cross-platform compatibility underscores the framework's adaptability and applicability across a wide spectrum of technology ecosystems.

3.1.3 *Cloud Forensic Tool/Portal (CFT)*

Cloud Forensic Tool (CFT) is a special portal designed to make it easier for Cloud Service Providers (CSPs) to interact with the framework. Through this site, CSPs can easily register both their host machines and virtual machines (VMs). Furthermore, the CFT operates as a centralized hub for receiving real-time security breach alerts, a critical function that underpins the framework's proactive stance in cybersecurity. Integral to the CFT's functionality is its role as the platform for orchestrating Virtual Machine Introspec-

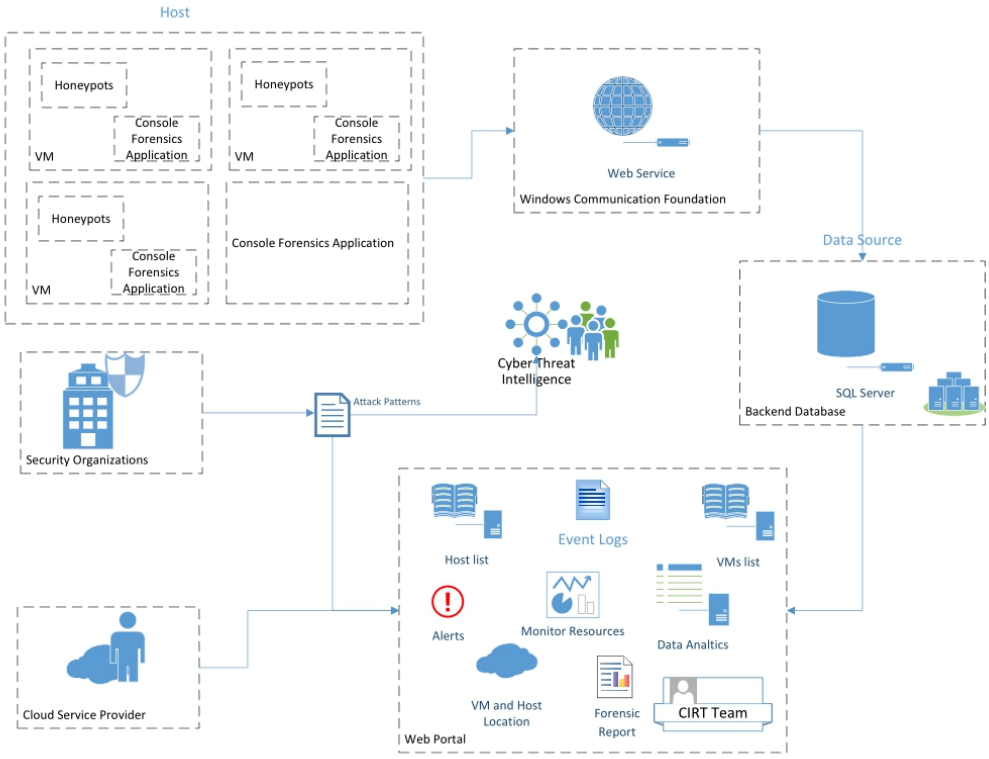


Figure 6: Provides a complete system architecture overview of the proposed framework.

tion (VMI). This capability empowers the framework to conduct deep and real-time examinations of VMs, enhancing its capacity to swiftly detect and analyze security breaches. Additionally, the CFT is the medium through which attack patterns are uploaded in a structured threat information expression (STIX) format after an attack has been effectively contained. This mechanism facilitates the dissemination of vital cyber threat intelligence, thereby bolstering the collective knowledge base and enhancing preparedness against future threats. Fig 7 offers a glimpse into the CFT's user interface, providing an insightful single-screen overview encompassing all integral components of the framework. This visual representation serves as an invaluable tool, affording users a consolidated perspective of the framework's operations, enhancing user experience, and streamlining administrative functions.

Figure 7: A dashboard screen snapshot offering a comprehensive overview of CFT components.

The CFT dashboard screen serves as a pivotal control center within the framework, offering a comprehensive array of critical information and functionalities. It serves as a dynamic repository of indispensable data, including reported cybersecurity incidents, real-time threat alerts, updates regarding newly onboarded Cloud Service Provider (CSP) members, resource utilization metrics pertaining to host machines, and geospatial location data pinpointing the whereabouts of both host machines and their hosted virtual machines (VMs). Notably, CSPs are endowed with the versatile capability to access and extract data in various formats, including the option to download data in CSV files or generate hardcopy printouts. This flexibility extends to encompass data retrieval from host machines, VMs, as well as comprehensive logs and process records.

In terms of incident management and response, both CSPs and administrators wield the authority to initiate alert transmissions to the Computer Incident Response Team (CIRT). This role complements the foundational commitment of the framework to prompt and efficient incident response and plays a crucial role in launching forensic investigations. Furthermore, the dashboard's functionality extends to the systematic dispatch of SYN (synchronize) messages from VMs to validate the operational status of the forensic application and affirm the active state of the VM. Together with the various alert types found in the activity log, these messages help to strengthen the dashboard's real-time monitoring and notification features.

Optimizing the framework is a crucial aspect of maintaining a robust security posture in cloud environments. The optimization process involves identifying vulnerabilities or weaknesses in the framework's configuration. This can be achieved through rigorous testing, incident simulations, and real-world incident analysis. The primary goals of optimizing the framework are to enhance its resilience against emerging cyber threats, improve its efficiency in detecting and analyzing attacks, and minimize false positives. During the optimization process, cloud service providers (CSPs) and administrators collaborate to fine-tune various components of the framework. This may include adjusting settings for Virtual Machine Introspection (VMI), refining incident classification criteria, and updating security controls. By continually optimizing the framework, organizations can adapt to evolving threat landscapes and ensure that their cloud infrastructure remains secure and resilient. Enhancing the forensic application is a proactive measure aimed at improving the effectiveness of virtual machine introspection (VMI) and forensic analysis capabilities. Enhancements to the forensic application may encompass several aspects for example performance improvement, feature updates, security enhancement, and cross-platform compatibility. Regular updates and enhancements to the framework help to stay ahead of emerging cyber attacks.

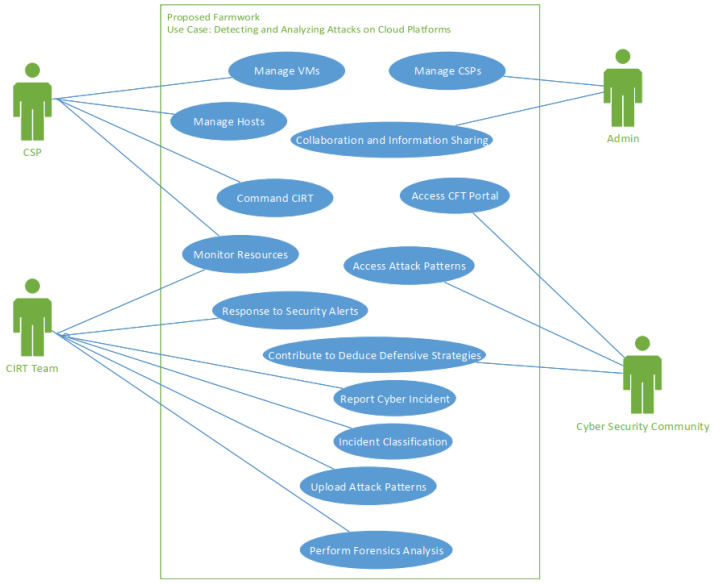


Figure 8: Provides a concise overview of use case modeling.

Fig 8 provides a very brief and precise use case modeling encompassing the proposed framework, and Fig 6 depicts the system architecture implemented within the proposed framework.

4 Results

The outcomes derived from the utilization of our proposed Hypervisor-based Virtual Machine Introspection (HVMI) tool exhibited promising results in detecting and analyzing attacks on cloud platforms. Rigorous testing was conducted through a series of simulations to comprehensively evaluate HVMI's efficacy in detecting a spectrum of attack types and dissecting the complexity of their tactics, techniques, and procedures (TTPs).

In the initial simulation, our evaluation focused on assessing HVMI's capability to identify a straightforward brute-force attack directed toward a virtual machine. The findings from this simulation revealed that HVMI exhibited prompt and effective detection of the attack, transmitting timely notifications to the CSP mere seconds after the attack's commencement. Furthermore, HVMI furnished a detailed and comprehensive analysis of the attack's Tactics, Techniques, and Procedures (TTPs). This encompassed an in-depth examination of the attack's nature, its originating source, and the specific system that was the subject of the attack.

Within the scope of the second simulation, our assessment aimed to evaluate HVMI's proficiency in detecting and analyzing a complicated and highly sophisticated malware attack targeted at a virtual machine. The findings from this simulation affirmed HVMI's adeptness in not only promptly identifying the attack but also in conducting a comprehensive analysis of the attack's intricacies. This analysis culminated in the generation of an exhaustive report detailing the Tactics, Techniques, and Procedures (TTPs) employed by the attack. Furthermore, the report delved into the potential ramifications of the attack, particularly in terms of its potential impact on the confidentiality, integrity, and availability of the system. To facilitate a holistic understanding of the entire process, we have included a detailed case study within this context.

4.1 Case Study: Launching a reverse TCP attack

Conducting the case study necessitated the initial setup of a Kali Linux machine, designated as the attacker entity. This machine underwent meticulous configuration to enable the initiation of a reverse TCP attack against a virtual machine (VM) hosted within the cloud infrastructure, ultimately aiming to illicitly establish reverse shell access. For the execution of this attack, the utility was employed to craft a payload tailored to facilitate the invasion into the VM. A pivotal component of this payload was an executable (Exe) file, meticulously constructed to be delivered to the target VM. Upon execution of this payload, a chain of events was set into motion. It prompted the VM to initiate the opening of a reverse shell, thus enabling the attacker to gain remote access through reverse TCP connectivity. Within the payload's configuration, crucial details such as the IP address and port on which the attacker's machine would be listening were meticulously specified. This case study served as a practical exercise to comprehensively assess HVMI's capabilities in detecting and analyzing an incursion of this nature, ultimately yielding valuable insights into the attack's methodologies and potential impact on the targeted system's security and integrity.

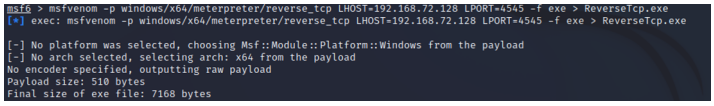


Figure 9: A Snapshot of an Exe payload generation for targeted VM.

Upon configuring the requisite parameters, the exploit was executed. This initiation prompted the attacker's machine to transition into a listening state, awaiting the incoming reverse TCP connection

from the target virtual machine (VM). This allowed an attacker to gain unauthorized access to the victim machine's shell, thereby affording an array of capabilities for potentially malicious activities. Within the scope of this gained access, activities encompassed the potential for privilege escalations and the execution of DLL injection, thereby underscoring the severity and breadth of the security breach. Fig 10 shows a snapshot of the reverse shell from the attack simulation.

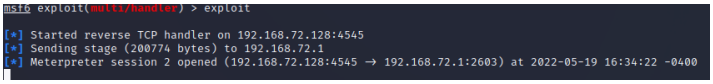


Figure 10: A snapshot of the accessed reverse TCP shell in the attack simulation.

Following the successful execution of the attack, our subsequent actions encompassed the installation of remote access software with the intent of securing persistent access while simultaneously deleting all traces within the event logs to obfuscate our activities and minimize detection. However, as soon as this attack occurred, our forensic application sprang into action. It promptly transmitted a series of alerts to the designated web portal and initiated the critical forensic analysis procedure. Fig 11 provides a comprehensive insight into the detailed real-time alerts generated as part of this incident response mechanism, emphasizing the real-time nature of our detection and analysis capabilities.

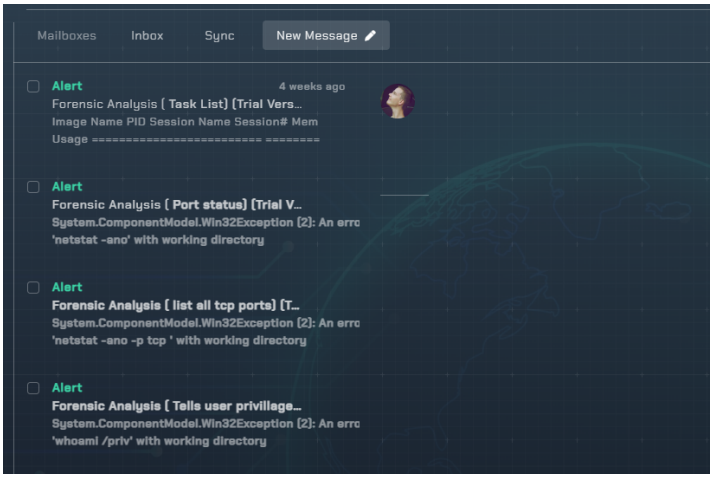


Figure 11: A snapshot of real-time alert prompts displayed on the portal.

This point underscores the pivotal role played by HVMI in resolving these security challenges. The proactive security and monitoring functionalities embodied within HVMI serve as a potent deterrent against such malicious incursions.

Before embarking on the identification of anomalous entities within VM's memory, several key inquiries come to the forefront. These include: Process Legitimacy: Are there any indications of suspicious processes deviating from their expected execution paths? Is the suspicious process running in tandem with its legitimate parent, or does it originate from an unrelated source? Temporal Aspects: What is the temporal profile of the process in question? When did it commence and conclude its execution? What are the implications of its execution timeline, and do they align with the expected behavior? Behavioral Profiling: What behavioral advantages can be attributed to the observed process? Does its behavior conform to the anticipated outcomes, or does it exhibit aberrant characteristics that warrant scrutiny? Process Name Variance: Does the process name exhibit any anomalies? Is it masquerading as a valid Windows process, thus evading detection? Comprehensive Analysis: Beyond process name scrutiny, an exhaustive analysis extends to threads, mutexes, Dynamic Link Libraries (DLLs), process-to-file mappings, Resident Memory (RAM) sections, and any associated sockets and open ports attributed to the process. These attributes are critical in discerning the origin of connections and the entities initiating them, as well as their associated dependencies. Our proposed solution (HVMI) empowers cybersecurity professionals with a potent arsenal of capabilities, enabling a proactive stance in countering, identifying, and comprehensively analyzing security threats.

HandleCount	Name	Priority	ProcessId	ThreadCount	WorkingSe
0	System Idle Process	0	0	8	8192
4139	System	8	4	115	57344
0	Registry	8	124	4	79228928
60	smss.exe	11	352	2	573440
645	csrss.exe	13	452	11	2678784
161	wininit.exe	13	540	3	1728512
169	csrss.exe	13	548	10	2392064
214	winlogon.exe	13	640	3	4018176
644	services.exe	9	684	9	8208384
4304	lsass.exe	9	704	8	19484672
1033	svchost.exe	8	824	11	15077376
33	fontdrvhost.exe	8	852	5	1613824
33	fontdrvhost.exe	8	860	5	1523712
1232	svchost.exe	8	936	10	20365312
1911	svchost.exe	8	988	5	9269248
2881	svchost.exe	8	500	127	33820672
503	LogonUI.exe	13	440	9	45416448
752	dwm.exe	13	552	14	21630976
211	svchost.exe	8	984	1	2277376
340	svchost.exe	8	1080	1	4386816
611	svchost.exe	8	1152	6	30240768
158	svchost.exe	8	1272	3	3686400
138	svchost.exe	8	1300	2	3866624
213	svchost.exe	8	1364	2	7499776
179	svchost.exe	8	1372	3	2637824

Figure 12: A snapshot of real-time processes running on VM.

The forensic application, as part of its operational protocol, diligently transmitted an array of pertinent information regarding the processes actively running within the targeted virtual machine (VM). This comprehensive data set encompassed critical attributes such as process priority, unique process identification (PID), thread counts, and resource consumption metrics, among other relevant parameters. For more clarity and reference, Fig 12 provides a visual representation of the enumerated processes actively executing within the targeted VM, thereby affording a comprehensive overview of the system's operational state.

sethc.exe	12800		2	720 K
TabTip.exe	13360		2	9,588 K
TabTip32.exe	14272		2	1,376 K
svchost.exe	12740	Services	0	5,996 K
SecurityHealthService.exe	12572	Services	0	9,932 K
msedge.exe	2816		2	86,100 K
msedge.exe	6444		2	9,116 K
msedge.exe	8892		2	31,396 K
msedge.exe	5396		2	35,784 K
msedge.exe	6552		2	19,728 K
msedge.exe	12692		2	72,888 K
TabTip.exe	11060	Console	1	13,500 K
msedge.exe	9140		2	134,240 K
MusNotifyIcon.exe	11844		2	3,420 K
w3wp.exe	8252	Services	0	322,612 K
Ssms.exe	6084		2	306,216 K
WmiPrvSE.exe	11760	Services	0	20,896 K
sppsvc.exe	11236	Services	0	12,688 K
devenv.exe	11052		2	1,257,808 K
ReverseTcp.exe	11056	Services	2	9,924 K
PerfWatson2.exe	8160		2	77,848 K
Microsoft.ServiceHub.Cont	10704		2	73,008 K
ServiceHub.VSDetouredHost	14648		2	101,360 K
ServiceHub.IdentityHost.e	14548		2	71,900 K
ServiceHub.ThreadedWaitDi	15692		2	80,312 K
ServiceHub.RoslynCodeAnal	700		2	434,764 K
ServiceHub.Host.CLR.x86.e	9676		2	73,828 K
ServiceHub.SettingsHost.e	14584		2	76,404 K
ServiceHub.Host.CLR.x64.e	12860		2	827,164 K
ServiceHub.Host.CLR.exe	6148		2	117,212 K
ServiceHub.TestWindowStor	14172		2	80,300 K
Microsoft.Alm.Shared.Remo	15284		2	70,808 K
Microsoft.VisualStudio.We	12324		2	90,512 K
ServiceHub.DataWarehouseH	5580		2	105,408 K
WebViewHost.exe	13668		2	55,956 K
conhost.exe	2940		2	11,576 K
msedgewebview2.exe	10308		2	103,552 K
msedgewebview2.exe	12492		2	8,880 K
msedgewebview2.exe	7936		2	45,892 K
msedgewebview2.exe	9396		2	29,668 K
msedgewebview2.exe	4420		2	19,160 K
msedgewebview2.exe	4344		2	68,864 K
msedgewebview2.exe	1088		2	52,956 K
ServiceHub.Host.CLR.x86.e	8560		2	86,092 K
node.exe	10212		2	43,752 K
node.exe	4576		2	44,092 K
conhost.exe	5488		2	11,744 K
conhost.exe	6980		2	11,752 K
node.exe	5384		2	38,636 K
VsDebugConsole.exe	8460		2	6,200 K
conhost.exe	11936		2	22,984 K

Figure 13: A snapshot of real-time identification of ”ReverseTcp.exe” by the forensic application on the VM.

Attackers employ diverse methodologies for delivering malicious payloads to victim machines. Given our primary emphasis on defensive measures, we have confined our analysis to two prominent attack vectors. The first scenario involves an attacker uploading a payload to a server hosting a service accessible via a specific port. Alternatively, attackers may disseminate the payload by incorporating it into a website or server. In such instances, unsuspecting users who attempt to access the compromised server or website inadvertently trigger the download of the payload. Additionally, attackers may resort to deception by disguising the payload as a Trojan horse. In response to any of these scenarios, the Computer Incident Response Team (CIRT) wields the capability to issue commands to the forensic application, thereby facilitating the retrieval of a comprehensive list of installed applications within the target virtual machine (VM). This scrutiny serves as a crucial component in the quest to identify any suspicious software installations or potential security breaches. Fig 13 provides an inclusive catalog encompassing active services and applications hosted within the VM. This exhaustive compilation of applications is readily accessible through the Computer Incident Response Team (CIRT) portal, thereby offering a streamlined reference point for cybersecurity professionals and facilitating in-depth investigative analysis. Of noteworthy significance within this list is the presence of the ”Reverse TCP Exe” application. This particular application bears significance as it was generated by the attacker with the explicit intent of establishing remote access to the virtual machine, thereby highlighting a critical security concern warranting further investigation and remediation.

Fig 14 provides a brief overview of the activity log within the CIRT portal. This log serves a dual purpose: first, it offers operational verification of both the Virtual Machine (VM) and the forensic applications throughout the simulation, ensuring their continuous activity and functionality. Secondly, it highlights the availability of the forensic analysis report on the portal, presenting a real-time and chronological account of activities and alerts generated during the simulation.

Figure 14: A snapshot of the activity log within the CIRT portal.

The HVMI tool demonstrated its capability to access and retrieve a comprehensive analysis report pertaining to the targeted virtual machine (VM). This encompassed a thorough examination of the VM's operational facets, encompassing active processes, running services, security logs, and the catalog of installed applications. Furthermore, the Cloud Service Provider (CSP) was equipped with the remote accessibility to monitor processes and network connections, allowing for the identification of the processes responsible for initiating and sustaining these connections. At a broader analytical spectrum, the HVMI tool extends two primary reporting avenues, specifically the Forensic Report and the Incident Report. The Forensic Report serves as a document that presents the results of forensic investigation. Fig 15 provides a snapshot of the interface, showcasing the automated forensic reports that have been systematically generated and made accessible through the portal.

Figure 15: A snapshot of available forensic reports on the portal.

Fig 16 provides a visual representation of the logs that have been systematically generated and recorded throughout the entire operational process. These logs are pivotal in facilitating comprehensive documentation of the actions, events, and activities undertaken within the cloud platform, rendering them invaluable for analytical and investigative purposes within the academic and technical domains.

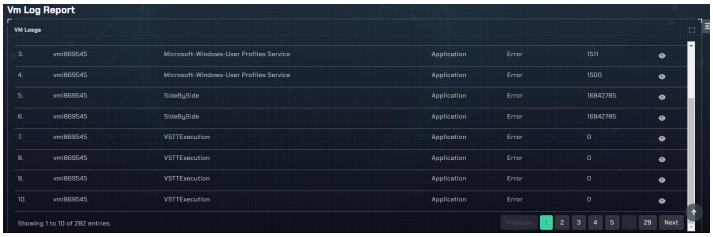


Figure 16: A visualization of VM logs generated during the entire process.

The Computer Incident Response Team (CIRT) portal offers the capability to export event logs in digital format, specifically in Comma-Separated Values (CSV) format for electronic use, or in hardcopy format for physical documentation purposes. This functionality allows for the efficient dissemination and preservation of critical event data for further analysis and reference in the context of incident response and cybersecurity management.

Within the context of cloud service providers (CSPs), the establishment of a robust cyber threat intelligence capability is of paramount importance. A pivotal facet of such a capability lies in the practice of sharing critical information with trusted partners, peers, and relevant stakeholders. This collaborative approach to cyber threat intelligence serves as a vital means of streamlining and comprehending the vast and very complicated landscape of cybersecurity data that CSPs encounter. By engaging in cyber threat intelligence and data sharing endeavors, organizations can effectively distill and prioritize the overwhelming volume of complicated cybersecurity data they encounter. This process involves gaining insight into the vulnerabilities and flaws within their information systems, as well as an understanding of the complicated tactics, techniques, and procedures (TTPs) employed by cyber adversaries. Additionally, it encompasses the identification and analysis of attack patterns. For the purpose of global accessibility and ease of comprehension, the results of cyber incidents, intelligence data, and attack patterns are systematically generated in the standardized Structured Threat Information Expression (STIX) format. This format facilitates the seamless exchange of cyber threat intelligence and enhances the collaborative efforts aimed at fortifying information systems against cyberattacks. Fig 17 provides a sample code snippet that serves as an illustrative for comprehending the visualization of Structured Threat Information Expression (STIX).

```
<stix:Threat_Actors>
    <stix:Threat_Actor id="trojan:threatactor-9b371afe-ddfd-4954-abaf-8abb357ac78e" xsi:type="ta:ThreatActorType" version="1.2">
        <threat-actor:Title>Trojan Horse backdoor</threat-actor:Title>
        <threat-actor:Type>
            <stixCommon:Value>APT</stixCommon:Value>
        </threat-actor:Type>
    </stix:Threat_Actor>
    <threat-actor:Observed_TTPs>
        <threat-actor:Observed_TTP>
            <stixCommon:Relationship>Use</stixCommon:Relationship>
            <stixCommon:TTP idref="trojan:ttp-649b70a0-0158-4cc6-a8d5-cf8a441dc290"/>
        </threat-actor:Observed_TTP>
    </threat-actor:Observed_TTPs>
</stix:Threat_Actors>
```

Figure 17: A sample code for visualization of patterns and syntax within STIX code.

STIX serves as a standardized language designed to convey comprehensive information concerning cyber threats. This encompassing data includes indicators of compromise (IOCs), which are distinctive attributes or artifacts linked to a cyberattack, such as specific IP addresses, domain names, file hashes, and other pertinent information instrumental in identifying or tracing an attack's origins. The strategic collection and analysis of IOCs empower organizations to pinpoint ongoing or past attacks, subsequently enabling them to initiate pertinent countermeasures and proactively deter future assaults. STIX plays a pivotal role in streamlining the aggregation, organization, and dissemination of IOCs, ensuring consistency and structure in the process. Fig 18 provides a visual representation of the relationship between the extracted IOCs during the attack simulation.

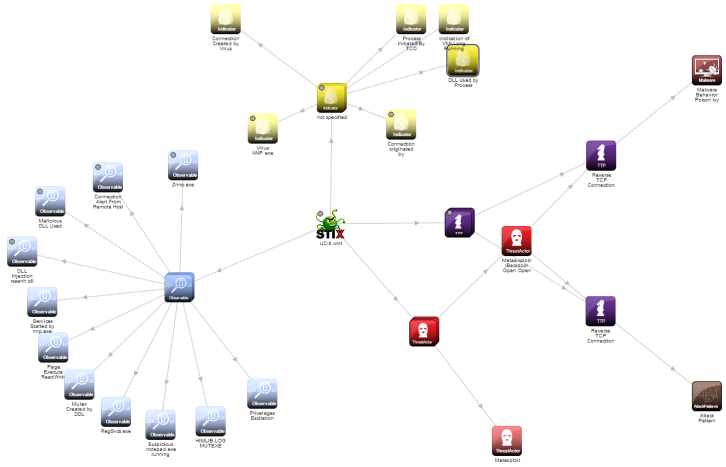


Figure 18: Provides a visual representation of the relation between the extracted IOCs.

In the cloud environment organizations frequently operate within shared infrastructure and resource environments, which inherently pose challenges in terms of tracking and detecting cyberattacks. The integration of STIX and IOCs into their cybersecurity framework equips organizations with a standardized mechanism to enhance their ability to recognize and respond to attacks more efficiently. This is achieved by facilitating the systematic collection and sharing of critical threat-related information and indicators of compromise, ultimately enhancing their cyber defense capabilities.

As an illustration, consider an organization that strategically incorporates STIX and IOCs into its cloud security framework. In this context, the organization leverages various sources of threat intelligence feeds or other pertinent information repositories to proactively identify potential indicators of compromise (IOCs). These IOCs might encompass entities like IP addresses or domains that are linked to previously documented malicious activities. Subsequently, the organization uses this invaluable information to configure its suite of security tools and policies. These configurations serve to either block or trigger alerts in response to these identified IOCs, thereby fortifying their capacity to avert or detect cyberattacks at an early stage, consequently reducing the potential for substantial damage.

Upon the completion of the comprehensive forensic analysis, the prevention of the cyber attack, and the documentation of attack patterns, the subsequent crucial step involves the formal reporting of the incident. An incident report serves as comprehensive documentation encompassing everything about the cyber attack incident that has occurred. These details encompass temporal information such as the precise timing of the incident, location, and a thorough narrative outlining the nature of the occurrence. Additionally, the report encapsulates actions taken in direct response to the incident.

Fig 19 provides a snapshot of the cyber incident report available on the portal.

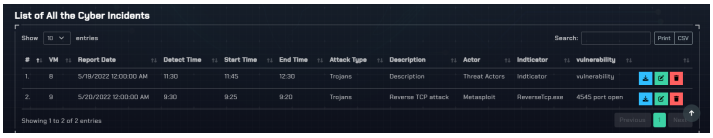


Figure 19: A snapshot of a comprehensive cyber incident report accessible via the portal.

The cyber incident report serves as a repository of critical insights into the security breach, exploring various facets and aspects of the incident from different angles. This comprehensive report encompasses pivotal details such as the attack vectors employed, the specific vulnerability that was exploited, the identity of the threat actor or actors involved, the classification of the attack type, and a detailed narrative about the attack's modus operandi. Moreover, the report incorporates a comprehensive analysis of attack pattern vectors and indicators, facilitating in understanding of the incident's intricacies. Additionally, it features a graphical STIX format, providing a visual overview of the incident's characteristics. Notably, the report also offers insights into recommended patches and fixes for the vulnerabilities that were exploited to compromise the system, thus contributing to the post-incident remediation process.

In summary, the outcomes of our simulation exercises demonstrate the efficacy of HVMI in detecting and analyzing cyberattacks within cloud infrastructures. HVMI emerges as a potent instrument, providing cloud service providers and cybersecurity practitioners with a robust means to safeguard cloud environments and mitigate the repercussions of security breaches. These results underscore the significance of HVMI as a proactive and potent tool in the arsenal against cloud-based cyber threats, offering valuable insights and capabilities to enhance the security posture of cloud systems.

5 Conclusion and Future Work

In conclusion, the ever-expanding realm of cloud computing necessitates a robust and adaptive security framework to combat the growing sophistication of cyber threats. The proposed HVMI solution, comprised of core components like the VMI-enabled forensic application, CFT portal, and data transmission web service, offers a comprehensive and promising strategy for detecting and analyzing attacks in real-time. Its commitment to iterative optimization and enhancement, coupled with proactive measures such as fortifying the forensic application, ensures that organizations can effectively safeguard their cloud infrastructure. By continually refining their security posture through HVMI, organizations can stay resilient against emerging threats and minimize the impact on the confidentiality, integrity, and availability of their cloud systems in this dynamic cybersecurity landscape. Nonetheless, here are several areas for future research that hold potential for enhancing HVMI's efficacy.

To ensure the effectiveness of HVMI in safeguarding large-scale cloud systems, optimizing its scalability is paramount. This endeavor entails devising techniques capable of efficiently processing substantial data volumes while fine-tuning HVMI's performance under heavy loads. The scalability enhancements will enable HVMI to protect expansive cloud infrastructures effectively, even as they evolve and expand. Future research can delve into advanced techniques for detecting and analyzing cyberattacks within cloud environments. Notably, machine learning-based approaches can be explored to elevate HVMI's capacity to identify and respond to increasingly sophisticated threats. By integrating machine learning models for anomaly detection, the framework can discern novel attack patterns and adapt dynamically to emerging threats.

Moreover, future work could explore intriguing intersections with emerging technologies such as blockchain and virtual reality. Integrating blockchain technology into HVMI has the potential to enhance the security and traceability of its forensic analyses. This innovation would instill greater confidence in the integrity of HVMI's findings, as they would be anchored in an immutable blockchain ledger. Meanwhile, integrating virtual reality could revolutionize forensic analysis, creating immersive and interactive experiences that empower investigators to explore attack scenarios in unprecedented depth. Lastly, synergizing HVMI with cloud tools represents a compelling roadmap for further research. This integration could automate security processes, providing rapid responses to emerging threats. Additionally, it would facilitate the swift deployment of security measures across cloud systems, bolstering their overall security posture. These directions mark a new exciting frontier in the ongoing effort to strengthen cloud security against ever-evolving and persistent cyber threats.

Resources For source code and further references, see the GitHub repository.

References

[1] F. Rehman, Z. Muhammad, S. Asif, H. Rahman, "The next generation of cloud security through hypervisor-based virtual machine introspection," in 2023 3rd International Conference on Artificial Intelligence (ICAI), 116–121, 2023, doi:10.1109/ICAI58407.2023.10136655.

[2] N. S. Shaikh, A. Yasin, R. Fatima, "Ontologies as Building Blocks of Cloud Security," International Journal of Information Technology and Computer Science (IJITCS), **14**(3), 52–61, 2022.

[3] J. Shahid, Z. Muhammad, Z. Iqbal, A. S. Almadhor, A. R. Javed, "Cellular automata trust-based energy drainage attack detection and prevention in Wireless Sensor Networks," Computer Communications, **191**, 360–367, 2022.

[4] M. Fatima, H. Abbas, T. Yaqoob, N. Shafqat, Z. Ahmad, R. Zeeshan, Z. Muhammad, T. Rana, S. Mussiraliyeva, "A survey on common criteria (CC) evaluating schemes for security assessment of IT products," PeerJ Computer Science, **7**, e701, 2021.

[5] S. Asif, M. Ambreen, Z. Muhammad, H. ur Rahman, S. Iqbal, "Cloud Computing in Healthcare-Investigation of Threats, Vulnerabilities, Future Challenges and Counter Measure," LC International Journal of STEM (ISSN: 2708-7123), **3**(1), 63–74, 2022.

[6] W. R. Simpson, K. E. Foltz, "Network Segmentation and Zero Trust Architectures," in Lecture Notes in Engineering and Computer Science, Proceedings of the World Congress on Engineering (WCE), 201–206, 2021.

[7] P. Purnaye, V. Kulkarni, "A comprehensive study of cloud forensics," Archives of Computational Methods in Engineering, **29**(1), 33–46, 2022.

[8] Z. Muhammad, F. Amjad, Z. Iqbal, A. R. Javed, T. R. Gadekallu, "Circumventing Google Play vetting policies: a stealthy cyberattack that uses incremental updates to breach privacy," Journal of Ambient Intelligence and Humanized Computing, 1–10, 2023.

[9] "Structured threat information expression (STIX™) 1.x archive website," .

[10] D. Barrett, G. Kipper, "2 - Server Virtualization," in D. Barrett, G. Kipper, editors, Virtualization and Forensics, 25–36, Syngress, Boston, 2010, doi: https://doi.org/10.1016/B978-1-59749-557-8.00002-3.

[11] Z. Aalam, V. Kumar, S. Gour, "A review paper on hypervisor and virtual machine security," in Journal of Physics: Conference Series, volume 1950, 012027, IOP Publishing, 2021.

[12] N. R. Nasab, "Security functions for virtual machines via introspection," 2012.

[13] B. Hay, K. Nance, "Forensics examination of volatile system data using virtual introspection," ACM SIGOPS Operating Systems Review, **42**(3), 74–82, 2008.

[14] B. D. Payne, D. d. A. Martim, W. Lee, "Secure and flexible monitoring of virtual machines," in Twenty-Third Annual Computer Security Applications Conference (ACSAC 2007), 385–397, IEEE, 2007.

[15] M. A. Kumara, C. Jaidhar, "Leveraging virtual machine introspection with memory forensics to detect and characterize unknown malware using machine learning techniques at hypervisor," Digital Investigation, **23**, 99–123, 2017.

[16] P. Mishra, E. S. Pilli, V. Varadharajan, U. Tupakula, "Intrusion detection techniques in cloud environment: A survey," Journal of Network and Computer Applications, **77**, 18–47, 2017.

[17] M. R. Watson, A. K. Marnerides, A. Mauthe, D. Hutchison, et al., "Malware detection in cloud computing infrastructures," IEEE Transactions on Dependable and Secure Computing, **13**(2), 192–205, 2015.

[18] A. K. Marnerides, P. Spachos, P. Chatzimisios, A. U. Mauthe, "Malware detection in the cloud under ensemble empirical mode decomposition," in 2015 international conference on computing, networking and communications (iCNC), 82–88, IEEE, 2015.

[19] H. Zhou, H. Ba, Y. Wang, T. Hong, "On the Detection of Malicious Behaviors against Introspection Using Hardware Architectural Events," IEICE TRANSACTIONS on Information and Systems, **103**(1), 177–180, 2020.

[20] H. Huseynov, K. Kourai, T. Saadawi, O. Igbe, "Virtual Machine Introspection for Anomaly-Based Keylogger Detection," in 2020 IEEE 21st International Conference on High Performance Switching and Routing (HPSR), 1–6, IEEE, 2020.

[21] B. Borisaniya, D. Patel, "Towards virtual machine introspection based security framework for cloud," Sādhanā, **44**(2), 1–15, 2019.

[22] S. Paakkola, "Assessing performance overhead of Virtual Machine Introspection and its suitability for malware analysis," 2020.

[23] Z. Muhammad, Z. Anwar, B. Saleem, J. Shahid, "Emerging Cybersecurity and Privacy Threats to Electric Vehicles and Their Impact on Human and Environmental Sustainability," Energies, **16**(3), 1113, 2023.

[24] S. Barnum, "Standardizing cyber threat intelligence information with the ... - stix," 2014.

[25] J. Shahid, Z. Muhammad, Z. Iqbal, M. S. Khan, Y. Amer, W. Si, "SAT: Integrated Multi-agent Blackbox Security Assessment Tool using Machine Learning," in 2022 2nd International Conference on Artificial Intelligence (ICAI), 105–111, IEEE, 2022.

ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 8, No. 6, 120-143 (2023)

www.astesj.com

Special Issue on Innovation in Computing, Engineering Science & Technology

ASTESJ

ISSN: 2415-6698

Dual Mode Control of an Inverted Pendulum: Design, Analysis and Experimental Evaluation

Laura Álvarez-Hidalgo, Ian S. Howard*

School of Engineering, Computing & Mathematics, University of Plymouth, Plymouth, PL4 8AA UK

ARTICLE INFO

Article history:
Received: 14 November, 2023
Accepted: 13 December, 2023
Online: 30 December, 2023

Keywords:
Inverted pendulum
State space control
Luenberger observer
3D printing
LQR

ABSTRACT

We present an inverted pendulum design using readily available V-slot rail components and 3D printing to construct custom parts. To enable the examination of different pendulum characteristics, we constructed three pendulum poles of different lengths. We implemented a brake mechanism to modify sliding friction resistance and built a paddle that can be attached to the ends of the pendulum poles. A testing rig was also developed to consistently apply disturbances by tapping the pendulum pole, characterizing balancing performance. We perform a comprehensive analysis of the behavior and control of the pendulum. This begins by considering its dynamics, including the nonlinear differential equation that describes the system, its linearization, and its representation in the s-domain. The primary focus of this work is the development of two distinct control modes for the pendulum: a velocity control mode, designed to balance the pendulum while the cart is in motion, and a position control mode, aimed at maintaining the pendulum cart at a specific location. For this, we derived two different state space models: one for implementing the velocity control mode and another for the position control mode. In the position control mode, integral action applied to the cart position ensures that the inverted pendulum remains balanced and maintains its desired position on the rail. For both models, linear observer-based state feedback controllers were implemented. The control laws are designed as linear quadratic regulators (LQR), and the systems are simulated in MATLAB. To actuate the physical pendulum system, a stepper motor was used, and its controller was assembled in a DIN rail panel to simplify the integration of all necessary components. We examined how the optimized performance, achieved with the medium-length pendulum pole, translates to poles of other lengths. Our findings reveal distinct behavioral differences between the control modes.

1. Introduction

1.1. Declaration

This paper represents a substantial extension of work originally presented at the 2022 International Conference on System Science and Engineering (ICSSE) [1]. The differences with the previous publication are that here we now include the ability to change the physical pendulum's mechanical characteristics, provide a more rigorous system analysis, build a custom testing rig, and improve upon previous system identification and testing procedures.

1.2. Overview

An inverted pendulum is a mechanical system comprising a rigid pole, with a pivot at one end that is located on a mobile cart. The challenge of building an inverted pendulum is that, in its inverted upright configuration, it represents a marginally an unstable system. The task is to maintain the system in this inherently unstable upright position, even in the presence of minor disturbances such as a gentle tap. Achieving this balance requires the implementation of a control strategy. The control mechanism must continuously measure the angular displacement of the pendulum from the vertical and correspondingly manipulate the cart's position to counteract any deviations.

1.3. Previous work

The inverted pendulum is widely recognized as one of several classical problems in the field of control engineering that is enlightening to study [2]. It has been used as a benchmark in robotics and control theory for almost the last 100 years and is often chosen to test and evaluate new control methods [3]. This preference arises because pendulum balancing represents behavior

*Corresponding Author: Ian S. Howard, ian.howard@plymouth.ac.uk

relevant to a wide range of theoretical challenges and practical applications [4,5].

One prominent example of these behaviors is the inverted pendulum's manifestation as a simple non-linear dynamic system, characterized by stable and unstable equilibrium points. During the dynamic transition from a downward to an upright position, the pendulum exhibits nonlinearity, primarily arising from how the pendulum angle affects the applied torque due to the pendulum's weight [6]. In addition, it represents a system for which it is crucial to achieve stability at the upright position in the presence of disturbances, which can only be achieved by moving the cart appropriately along its rail [7].

James Kerr Roberge was one of the first researchers to describe an inverted pendulum [6]. Since then, many inverted pendulum designs and their variants have been constructed and studied, including ones aimed at teaching and research [8,9], mobile designs [10,11], pendulums mounted on drones [12], as well as rotary designs [13,14].

Derivations of the dynamics of inverted pendulums and their simulation have been carried out by many researchers, for example [15]. Many different approaches to control have also been investigated. These include PID and classical approaches to control in the s-domain [16,17], state feedback control [1,18], and Lyapunov-based controller design [19], and comparisons have been made between different controllers [20]. Machine Learning (ML) approaches are becoming an increasingly successful way to deal with hard control problems. They mark a change from designing controllers based on explicit mathematical models derived from physics to more empirical methodologies that are essentially data driven [21]. ML approaches make use of reinforcement learning (RL) based on Q-Learning [22], Policy Iteration [23], and Deep Q-Networks [24]. The PILCO RL algorithm is especially data efficient, since it builds and makes use of a probabilistic model of the task dynamics as it learns to balance the pendulum [25]. Further ML approaches involve neural networks [26,27] and genetic algorithms [28,29]. Hybrid methods using control engineering approaches and neural network techniques have also been investigated [30]. Researchers often compare different control approaches [31]. More complex two-link inverted pendulums have also been studied by several researchers and implemented using a range of control techniques [32]. Other researchers have even investigated the use of reinforcement learning to control a pendulum with three links [33].

The inverted pendulum also forms a basis for understanding simple balancing robots [34–36]. There is also increasing interest in the construction of legged and humanoid robots[37,38], in which control of balance plays an important role [39–41].

Falls in the elderly are a common health issue worldwide and consequently understanding the mechanisms of how humans maintain balance whilst standing is an area of much research [42–45]. The inverted pendulum has also been used to model and understand this process [44–52]. More recent work has also included the use of experiments with robotic manipulanda to investigate how humans can balance items with their hands [53–56].

Given the significance of the inverted pendulum in the field of control engineering, inverted pendulum theory finds extensive applications across diverse fields, including robotics, aerospace systems, marine systems, flexible systems, mobile systems, and locomotive systems [57–59]. The characteristics of the inverted pendulum make it well-suited for modelling a multitude of practical scenarios, highlighting its significance and profound influence across various industries.

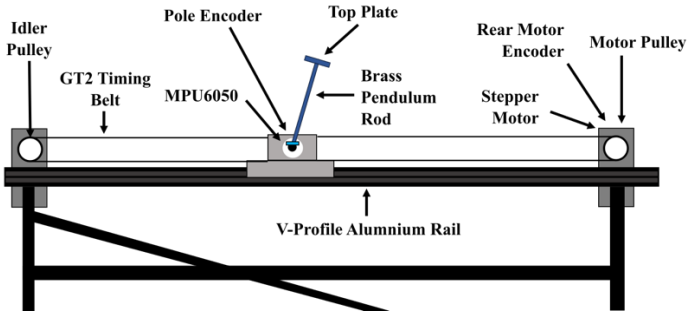


Figure 1: Schematic diagram showing main pendulum components.

2. Mechanical design of the Inverted Pendulum

2.1. Extension of previous work

The current inverted pendulum design expands upon our previous publication [1], in several important ways. We made modifications to the mechanical components of the pendulum system, enabling us to alter its physical characteristics and now utilize a range of pendulum configurations, with changes in pendulum length (635mm, 335mm, 233mm), viscous damping (adding a paddle to the pole), and friction (compression of a brake on the pendulum pole).

2.2. Inverted pendulum components

Here we build an inverted pendulum system consisting of a pole pivoted at one end on a cart that moves on a linear track actuated by a stepper motor, which can be balanced in its inverted position by observing the pole angle and controlling cart movement. Our design comprises several distinct component parts, illustrated in Figure 1.

The pendulum assembly is composed of several distinct components. These include a v-groove aluminum profile track and a cart unit that supports the inverted pendulum, moving along the track on a wheeled cart. Additionally, a stepper motor unit propels the cart via a timing belt from one end of the track, while a passive idler pulley supports the belt at the opposite end. The motor and pulley mechanisms are securely affixed to the aluminum profile structure using T-nuts. This design not only offers the flexibility to easily remove and replace these parts with similar components but also simplifies the process of tensioning the drive belt.

2.3. Track

The mechanical design integrated a V-slot profile to realize the pendulum track. This streamlined construction since it enabled the use of readily available accessories. These included a stepper motor mounting plate, an idler pulley mechanism, as well as gantry plates.

2.4. Cart

A 4-wheeled gantry plate formed the basis of the cart mechanism. During balancing operation, it traversed the V-slot aluminum track along its sides as needed to balance the pendulum pole. Wheel clearances were adjusted so the cart remained securely on the track without excessive wobbling, while also avoiding undue friction.

A thick flat PLA+ 3D-printed rectangular sheet with mounting holes was affixed to the gantry plate. This served as the support for both a ball bearing race and an encoder unit, which held and facilitated the rotation of a shaft. This shaft, in turn, held the pendulum pole, allowing it to swing freely. The incremental encoder measured the pole's angular deviation from the vertical position, as depicted in Figure 2.

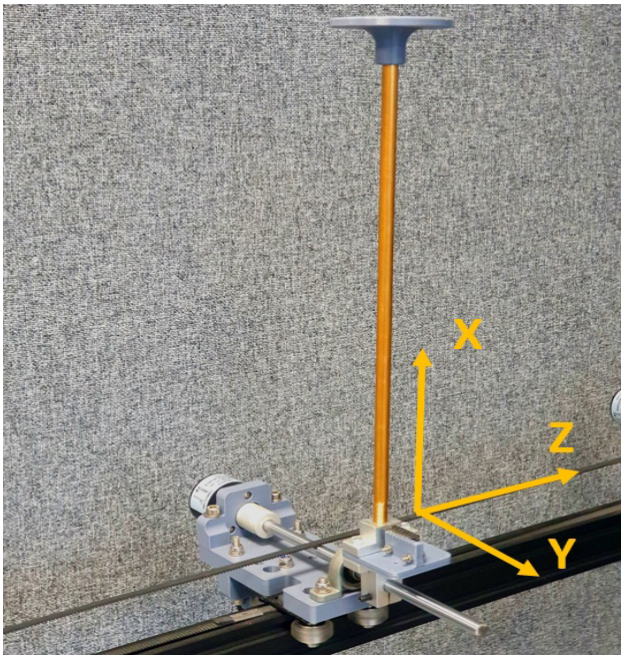


Figure 2: 3D-printed pendulum cart incorporating an encoder and an inertial measurement unit (IMU). A flat-topped table can be attached to the end of the pendulum to support objects on its surface.

2.5. Shaft friction adjustment

Normally, the rotation of the pendulum shaft is resisted by a low level of friction, arising from the bearing and the incremental encoder. To increase the amount of friction and examine its effect on pendulum behavior, a spring-loaded braking assembly was constructed (Figure 3). This consisted of a semicircular brake pad section made of PLA+ that could be pressed against the pendulum rotary shaft using a compression spring, thereby hindering its rotation. By fully withdrawing the brake, it was also possible to remove its effect completely.

2.6. Standard pendulum pole

The standard pendulum pole consists of a pole crafted from a brass segment, selected for its easy machinability and high density. One end of the pole was threaded to securely screw into an attachment component connected to the main shaft, ensuring a sturdy attachment as depicted in Figure 2. This led to an overall pendulum length of 335mm. While a relatively short pole increases the balancing challenge, necessitating quicker cart reactions due to the system's elevated natural frequency, it yields several benefits. A compact pole is not only more manageable but also ensures increased safety by minimizing accidental impact risks. Moreover, it provides characteristics that better match other systems, like smaller balancing robots [60].

2.7. Additional pendulum poles

An easy way to alter the fundamental characteristics of the pendulum is to change the length of the pole. To do so, two additional pendulum poles were built (Figure 4). These poles consisted of 8mm diameter stainless steel poles, leading to pendulum lengths of 222mm and 635mm. Since they were only required for intermittent use, no screw attachment was used, thereby facilitating construction. Instead, they were simply clamped at their endpoint into another attachment component connected to the main shaft.

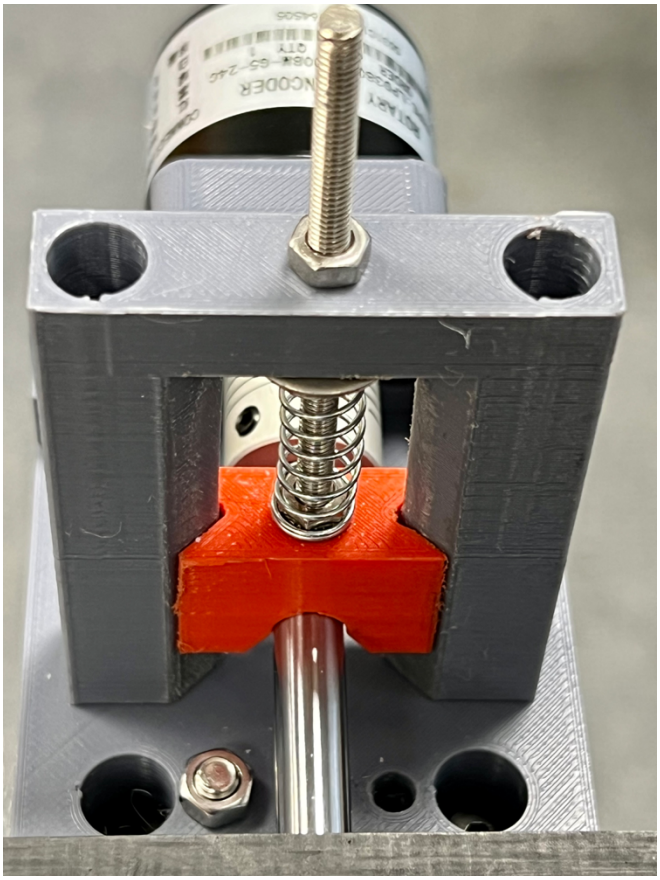


Figure 3: Shaft friction adjustment mechanism for the pendulum cart, designed to alter the sliding friction around the pendulum's rotational axis.

2.8. Pendulum pole end attachments

To provide a platform for placing objects, and to shield its endpoint for safety reasons, a round disc was 3D printed from PLA+ and slid onto the end of the pendulum pole, where it was held in place by friction.

To offer a means to change the viscous air resistance experienced by the pendulum pole as it swung, the round disc at the endpoint of the pole could be replaced with a paddle (Figure 5). The paddle consisted of a 5mm thick square measuring 100mm

by 100mm and was 3D printed from PLA+. It slid onto the end of the pole via a central mounting hole and was again held in place by friction. By rotating the paddle 90°, it was possible to adjust the amount of viscous resistance the pendulum pole experienced from a low to a high value.

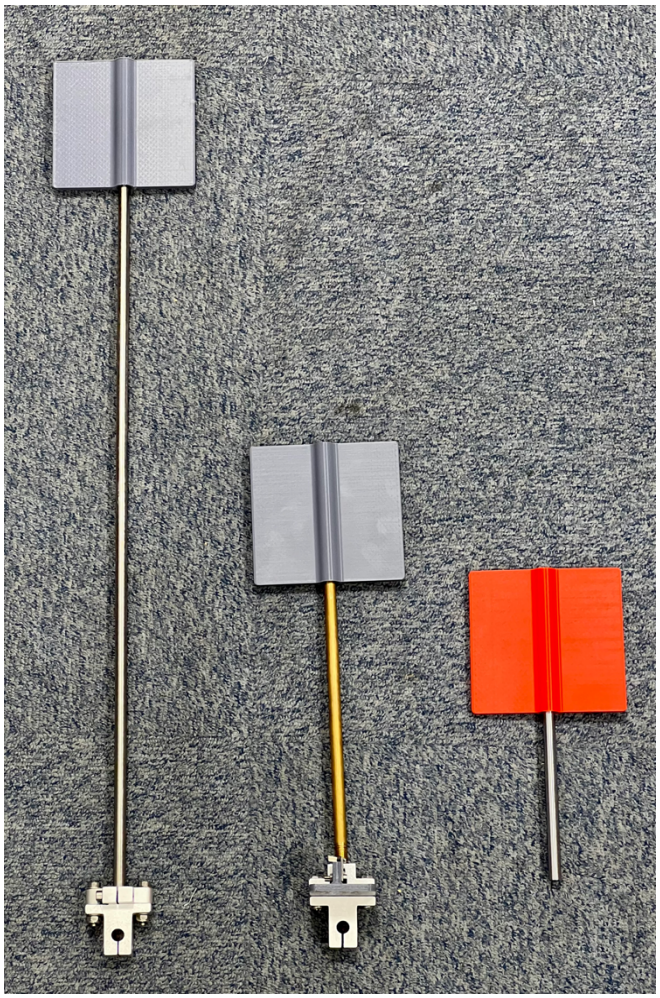


Figure 4: Three different pendulum poles were utilized to evaluate the controller's sensitivity to changes in pendulum length.

2.9. Stepper motor actuation

The motor drive assembly includes an aluminum plate, situated on the profile rail, which serves as firm support for a NEMA23 stepper motor. The motor is securely affixed to the plate using bolts. The motor is connected to a drive pulley at its front, and an encoder is mounted on the rear end of its shaft. This enables accurate measurement of the cart's position, although it is only needed to analyze the pendulum's behavior and is not involved in the balancing process (see Figure 6).

To operate the stepper motor, an A4988 stepper controller is employed, driven from an Arduino Mega 2560 R3 Microcontroller. The latter is programmed in C++ and provides precise control of the pendulum cart along the linear rail.

2.10. Belt

A pulley and belt mechanism are used to convert the motor's rotary motion into linear movement, thereby appropriately driving the cart along its rail. The cart traverses its designated rails using a GT2 timing belt, which is typically used in 3D printers. The belt, affixed to the cart using steel clamps, spans almost the entire length of the track. The stepper motor, located at one end of the track, has a 60-tooth GT2 motor pulley secured to its shaft. A passive idler pulley is situated at the opposite end of the track. Ball bearings, integrated into the idler pulley, minimize frictional resistance, ensuring smooth operation even under the stress of high belt tension. Adjusting the precise location of the idler provides an easy means to modify belt tension.

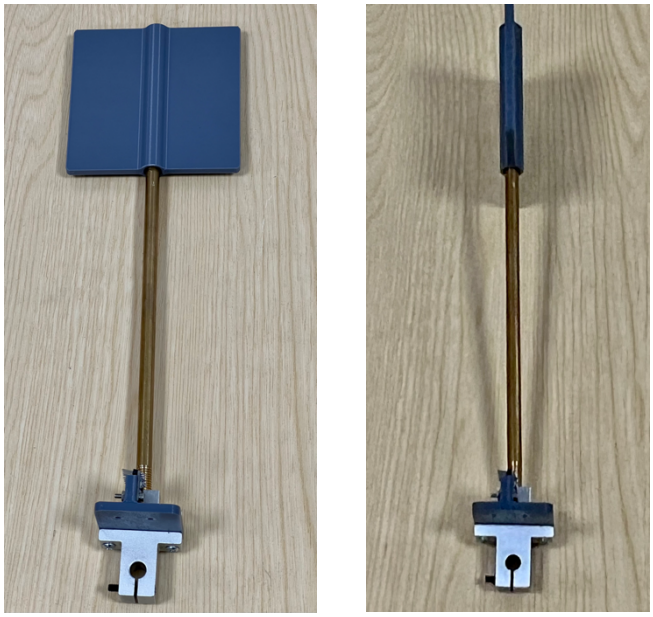


Figure 5: The pendulum paddle can be rotated, thus adjusting the viscous drag due to air resistance from low to high values.

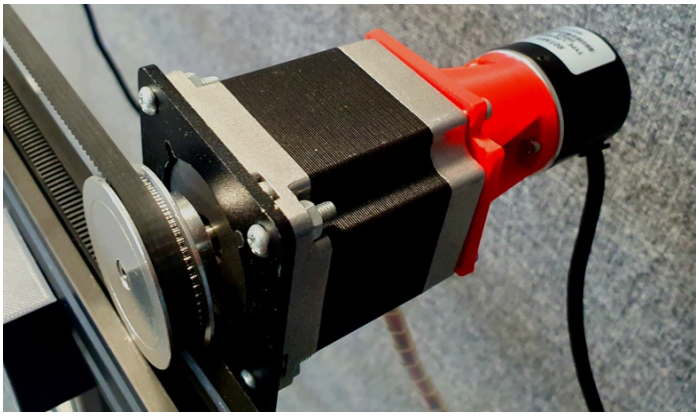


Figure 6: Stepper motor actuation, showing the drive pulley and a custom-made 3D-printed encoder mount at the motor's rear.

2.11. Inertial Measurement Unit

To support future developments of the pendulum system, a cost-effective 6-DOF accelerometer/gyro (MPU-6050) was strategically mounted to a 3D-printed support on the pendulum pole, aligning it with the pendulum shaft's rotational axis. This configuration presents an alternative method to measure the pole's angular displacement. The pendulum shaft's rotation revolves around the MPU-6050's y-axis. When in the inverted

configuration, its x-axis points downward, and the pole points upwards along its negative x-axis, with its z-axis horizontal (Figure 2).

2.12. Modular adjustable pendulum design

The utilization of modular construction within the system ensures that the parameters governing the behavior of the inverted pendulum can easily be adjusted or reconfigured. Such adaptability can prove useful in educational contexts. With minimal adjustments to the apparatus, diverse tasks can be allocated to distinct student cohorts, each tackling a specific control problem. For instance, the pole's length, an essential aspect of the system's dynamics, can be altered by substituting the pole with another of a different length. Adaptability extends further to the motor unit. For example, stepper motor drive could be exchanged with actuation employing a BLDC motor, a modification that would support force control, as opposed to velocity control, of the pendulum system.

2.13. 3D printing

The components for the pendulum cart were designed using AutoCAD Fusion 360. This software also facilitated the conversion of the designs into STL format files, which is a critical step for additive manufacturing. The mechanical parts were then fabricated using PLA+ material on a Creality 6SE 3D printer. It is noteworthy to mention that although tougher plastics could further enhance the durability of the design, PLA+ was chosen for its ease of printing and cost-effectiveness.

2.14. Pendulum Stand

Operating the pendulum necessitates mounting the track at an elevation that ensures unobstructed swinging of the pole. We designed a custom-engineered support stand using aluminum profiles to secure the pendulum system (refer to Figure 7). This stand offers a robust yet lightweight construction that facilitates easy transportation.

The support stand comprises two support pillars, fabricated from aluminum profile. These pillars are anchored at their base with additional lengths of aluminum profile, and 3D printed feet are used at each end to provide stable support. The top of each pillar is fitted with a 3D-printed bracket, tailor-made to accommodate the aluminum v-rail. To enhance the rigidity of the structure and to increase its resistance to mechanical stress, diagonal aluminum profile sections are incorporated, to brace the assembly. This results in a rigid structure, minimizing potential vibrations or displacements that could affect the system's performance.

3. Mechanical tapper for performance evaluation

3.1. Testing balancing systems

Monteleone and his team [61] presented a methodology to evaluate the balance resilience of robots, utilizing unique performance indicators and a custom-made testbed. Through extensive testing on a humanoid robot, their study demonstrated the method's effectiveness in designing more robust robotic systems.

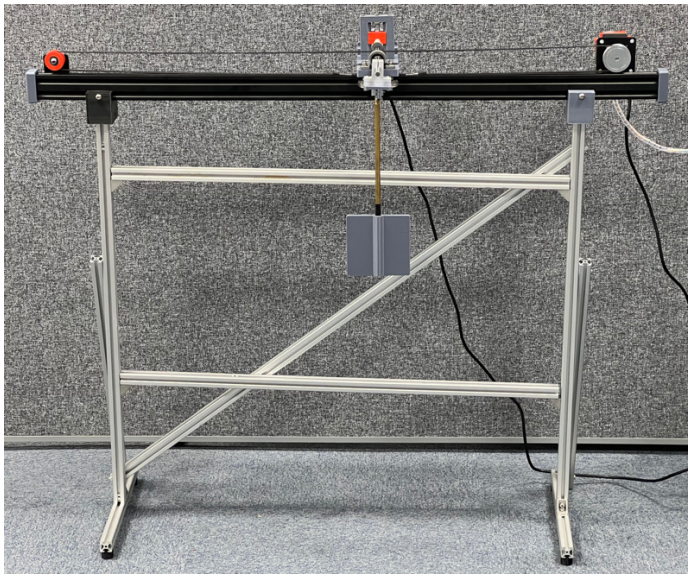


Figure 7: Pendulum mounted on its stand: The structure uses diagonal bracing to increase its rigidity.

3.2. Tapper components

In the same vein, to conduct tests across various pendulum conditions, including different pendulum lengths, friction, and damping levels, as well as different control laws, and to compare the results, it was necessary to disturb the pendulum pole consistently. To achieve this, a tapping mechanism was constructed (Figure 8).

We built and used a testing rig to deliver repeatable disturbances to the pendulum pole whilst balancing, to examine the recovery and robustness of control. This could be carried out during balancing whilst the cart was either static or moving.

3.3. Finger-spring mechanism

The primary component of this tapping mechanism is the 'tapper finger,' which is mounted onto a baseplate. This mounting baseplate for the tapping mechanism is attached to a cart that can be maneuvered up and down a V-groove rail track by means of a stepper motor.

The finger is composed of a stainless-steel pole inserted in a PLA+ holder, which pivots around a rotary axis located 3 cm from its lower end. Two sets of springs are connected at the endpoint of the holder and at the base on either side, pulling in opposite directions. When the finger is in its undisturbed equilibrium position, these springs ensure that it maintains a 0° orientation.

This finger-spring assembly forms an underdamped second-order system. Its behavior, particularly the overshoot following appropriate excitation, serves as an effective method to strike the pendulum pole. To generate a movement suitable for producing a tap, it is necessary to displace the lower end of the finger from its equilibrium position around its pivot and then release it suddenly. This action results in a rapid movement: the finger travels back through its equilibrium position and out the other side, which enables it to impact the pendulum pole and then quickly withdraw.

Using this tapping mechanism, it is important to note that the pendulum pole must be positioned at an appropriate distance from

the tapping finger before operation commences, to prevent multiple impacts. At the tap, energy is transferred from the finger to the pendulum pole, and if the distance to the target pendulum pole is set correctly, it ensures that the finger only strikes once and then retreats without making further contact.

3.4. Finger actuation

Although it would be possible to manually displace the lower end of the tapping pole and release it by hand, we incorporated an RC servomechanism into the design to achieve this action automatically and more consistently. The RC servo first displaces the finger from its equilibrium position. Then, owing to the cam mechanism's design, it releases the finger suddenly as it passes the end point. This action consequently results in a rapid underdamped second-order trajectory of the end of the tapper finger, ideal for exciting the pendulum pole.

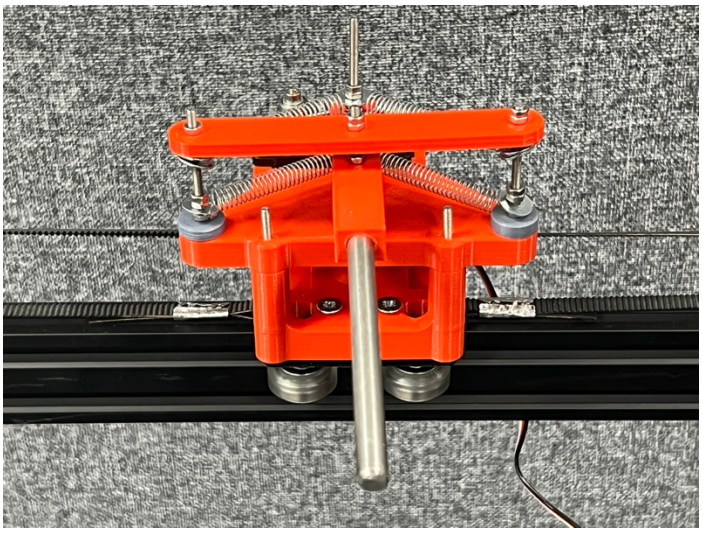


Figure 8: 3D-printed tapping mechanism. Two sets of springs are configured to pull the bottom of the tapping pole to the left and right, thereby establishing a neutral equilibrium position at 0° as depicted. An RC servo is positioned to travel 180°, engaging and then releasing the rear of the tapping mechanism. This action, assisted by the tension of simultaneously contracted springs, causes the pole to swing in an under-damped motion, with overshoot delivering an appropriate tap to the pendulum pole. All custom parts were designed using AutoCAD Fusion 360 and printed with PLA+ material.

To achieve a consistent tap, it is essential to maintain a constant distance between the tapping pole and the pendulum pole and to ensure that the tap occurs at the same location during each trial. This consistency is achieved by visually aligning the tapping finger with the pendulum pole before a tap is initiated.

3.5. Tapper cart

In the inverted pendulum position control mode, the pendulum cart remains stationary, simplifying the process of tapping its pole. However, in the velocity control mode, the cart moves along the rail while balancing. The goal was to create a tapping mechanism suitable for both velocity and position modes, necessitating the ability of the tapping mechanism to track the pendulum cart's movement by employing an additional cart. This capability ensures taps can be delivered effectively, even while the pendulum cart is in motion. To achieve necessary synchronization, the tapping mechanism's cart is propelled along a separate V-groove aluminum profile track, using a stepper motor that receives the same control signal as the pendulum cart's stepper motor.

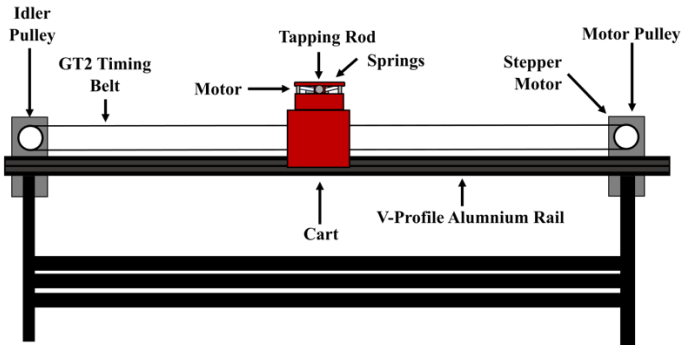


Figure 9: Schematic of the tapping mechanism mounted on its adjustable stand, showing all its main components.

3.6. Adjustable height tapper stand

The upper track of the tapper mechanism was mounted to the side of the support pillars, allowing for adjustable height of the tapper, as illustrated in Figures 9 and 10.

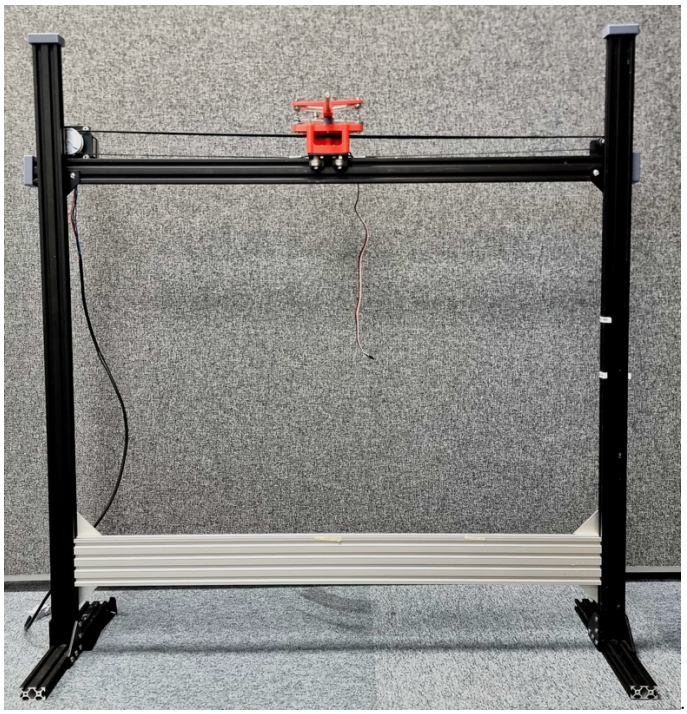


Figure 10: Side view of the adjustable mechanical tapper assembly. The cart supporting the tapping mechanism can be driven left and right to synchronize with the pendulum cart. The cart is mounted on a rail that can be slid up and down the outer stand legs, and then fastened firmly in place with screws, enabling adjustment of the height at which tapping occurs.

4. Analysis of pendulum dynamics

4.1. Mathematical analysis

We performed a comprehensive analysis of the pendulum's dynamics, including the nonlinear differential equation, its linearization, and s-domain representation. This provided a theoretical foundation for our practical implementation.

4.2. Equilibrium positions

A pendulum exhibits two distinct equilibrium points. In the stable equilibrium state, the pendulum hangs downward, functioning like a traditional pendulum, similar to those in pendulum clocks. At this stable equilibrium point, if the pendulum is slightly displaced, it will begin to oscillate back and forth with a characteristic frequency determined by its dynamic properties. Factors such as damping in the joints and air resistance lead to a gradual decrease in oscillation amplitude over time. Eventually, the pendulum will stop moving and return to a stationary state at its equilibrium position. In contrast, an unstable equilibrium occurs when the pendulum is delicately balanced upright on its pivot point.

4.3. Analysis of non-linear pendulum dynamics

If sliding friction is neglected, the kinematics of an inverted pendulum can be characterized by the following non-linear differential equation:

$$(I + ml^2)\frac{d^2\theta}{dt^2} + \mu\frac{d\theta}{dt} = mgl\sin\theta + ml\frac{d^2x_P}{dt^2}\cos\theta \quad (1)$$

Here, the terms represent the following:

θ: Angle of the pendulum pole to the vertical axis

μ: Coefficient of viscosity

m: Mass of the pendulum

I: The Moment of Inertia (MoI) of the pendulum pole about its center of mass

l: Distance from the pivot point to the pendulum pole's center of mass (typically half the length of the pole)

x_p: Displacement of the pivot

Although exponential decay due to viscous resistance is often assumed to be the primary cause of oscillatory decay in second-order systems like the pendulum, it is known that sliding friction leads to a linear decay of oscillatory amplitude [62–65]. To account for sliding friction, we can also write

$$(I + ml^2)\frac{d^2\theta}{dt^2} + \mu\frac{d\theta}{dt} + fsign\left(\frac{d\theta}{dt}\right) = mgl\sin\theta + ml\frac{d^2x_P}{dt^2}\cos\theta \quad (2)$$

In this context, an additional friction term exists, scaled by the coefficient f, which is dependent on the sign of the angular velocity. The presence of this sign term complicates formal analysis; therefore, we initially disregard the effects of friction.

We observe that the provided kinematic description suffices for deriving control, assuming reliance solely on the cart's velocity as the control input. Additionally, it's worth noting that force control, a common approach in numerous inverted pendulum implementations [66], would necessitate an extra equation to accurately capture the dynamics of the cart's force.

Refactoring Eqn. (1) with the highest-order differential term on the left-hand side, yields:

$$\frac{d^2\theta}{dt^2} = -\frac{\mu}{(I+ml^2)}\frac{d\theta}{dt} + \frac{mgl}{(I+ml^2)}\sin\theta + \frac{ml}{(I+ml^2)}\frac{d^2x_P}{dt^2}\cos\theta \quad (3)$$

we now write:

$$\frac{d^2x_P}{dt^2} = \frac{dv_c}{dt} \quad (4)$$

We will now represent the constant terms using coefficients as follows:

$$a_1 = \frac{\mu}{(I+ml^2)} \quad (5)$$

$$a_2 = \frac{-mgl}{(I+ml^2)} \quad (6)$$

$$b_0 = \frac{ml}{(I+ml^2)} \quad (7)$$

This leads to the equation for dynamics:

$$\frac{d^2\theta}{dt^2} = -a_1\frac{d\theta}{dt} - a_2\sin\theta + b_0\frac{dv_c}{dt}\cos\theta \quad (8)$$

To express the system in state space form as two first-order differential equations, selecting the first state x_1 is straightforward since it represents the pendulum angle, denoted as θ:

$$x_1 = \theta \quad (9)$$

$$\Rightarrow \dot{x}_1 = \frac{d\theta}{dt} \quad (10)$$

We now write the second state variable x_2 as:

$$x_2 = \frac{d\theta}{dt} - b_0 v_c\cos\theta \quad (11)$$

Re-arranging Eqn. (11) gives:

$$\Rightarrow \frac{d\theta}{dt} = x_2 + b_0 v_c\cos\theta \quad (12)$$

$$\Rightarrow \dot{x}_1 = x_2 + b_0 v_c\cos x_1 \quad (13)$$

Differentiating Eqn. (12) with respect to time and using the product rule to the right-hand side terms

$$\Rightarrow \frac{d^2\theta}{dt^2} = \dot{x}_2 + b_0\frac{dv_c}{dt}\cos\theta - b_0 v_c\sin\theta \quad (14)$$

$$\Rightarrow \frac{d^2\theta}{dt^2} = \dot{x}_2 + b_0\frac{dv_c}{dt}\cos x_1 - b_0 v_c\sin x_1 \quad (15)$$

Substituting the Equations (12, 15) into Eqn. (8) and replacing angle terms with state variables

$$\Rightarrow \dot{x}_2 + b_0\frac{dv_c}{dt}\cos x_1 - b_0 v_c\sin x_1 = -a_1(x_2 + b_0 v_c\cos x_1) - a_2\sin x_1 + b_0\frac{dv_c}{dt}\cos x_1 \quad (16)$$

$$\Rightarrow \dot{x}_2 - b_0 v_c\sin x_1 = -a_1(x_2 + b_0 v_c\cos x_1) - a_2\sin x_1 \quad (17)$$

$$\Rightarrow \dot{x}_2 = -a_1(x_2 + b_0 v_c\cos x_1) - a_2\sin x_1 + b_0 v_c\sin x_1 \quad (18)$$

This leads to the following expression:

$$\Rightarrow \dot{x}_2 = -a_1 x_2 - a_2 \sin x_1 + (b_0 \sin x_1 - a_1 b_0 \cos x_1) v_c \quad (19)$$

The two equations (13) and (19) can be used in a non-linear simulation of the pendulum system.

5. Linearizing the non-linear system

5.1. Equilibrium

We now extend the mathematical analysis to derive the linearized state space model by calculating and evaluating the system's Jacobian around equilibrium positions. To linearize the nonlinear differential equation description of the pendulum around its equilibrium points, we first need to identify their locations. Equilibrium occurs when the control input is zero, and the state derivatives are also zero. That is

$$\dot{x}_1 = x_2 + b_0 v_c \cos x_1 = 0 \quad (20)$$

$$\dot{x}_2 = -a_1 x_2 - a_2 \sin x_1 + (b_0 \sin x_1 - a_1 b_0 \cos x_1) v_c = 0 \quad (21)$$

Since control velocity is zero at the equilibrium points, we see that $x_2 = 0$ and:

$$\dot{x}_2 = -a_1 x_2 - a_2 \sin x_1 = 0 \quad (22)$$

From Eqn. (22) we see that:

$$-a_2 \sin x_1 = 0 \quad (23)$$

$$\Rightarrow x_1 = \{0, \pi\} \quad (24)$$

Thus, the system has an equilibrium in an inverted configuration at 0 radians and a non-inverted configuration at π radians. To linearize the system at these equilibrium points, we need to calculate the Jacobian of the system, denoted as J_A, with respect to the system state, and evaluate it at those points. We first express the two state equations as functions:

$$f_1 = x_2 + b_0 v_c \cos x_1 \quad (25)$$

$$f_2 = -a_1 x_2 - a_2 \sin x_1 + (b_0 \sin x_1 - a_1 b_0 \cos x_1) v_c \quad (26)$$

We then calculate the partial derivatives of these two functions with respect to the state variables:

$$\frac{\partial f_1}{\partial x_1} = -b_0 v_c \sin x_1 \quad (27)$$

$$\frac{\partial f_1}{\partial x_2} = 1 \quad (28)$$

$$\frac{\partial f_2}{\partial x_1} = -a_2 \cos x_1 + (b_0 \cos x_1 + a_1 b_0 \sin x_1) v_c \quad (29)$$

$$\frac{\partial f_2}{\partial x_2} = -a_1 + (b_0 \cos x_1 + a_1 b_0 \sin x_1) v_c \quad (30)$$

5.2. Jacobian in matrix form

This leads to the Jacobian matrix:

$$J_A = \begin{bmatrix} -b_0 v_c \sin x_1 & 1 \\ -a_2 \cos x_1 + (b_0 \cos x_1 + a_1 b_0 \sin x_1) v_c & -a_1 + (b_0 \cos x_1 + a_1 b_0 \sin x_1) v_c \end{bmatrix} \quad (31)$$

We now evaluate this matrix at the equilibria points when control is zero. For the inverted configuration equilibrium at 0 radians, we have

$$J_A[x_1 = 0] = \begin{bmatrix} 0 & 1 \\ -a_2 & -a_1 \end{bmatrix} \quad (32)$$

For the non-inverted configuration equilibrium at π radians we have

$$J_A[x_1 = \pi] = \begin{bmatrix} 0 & 1 \\ a_2 & -a_1 \end{bmatrix} \quad (33)$$

We now need to linearize the control of the system. To do so, we calculate the Jacobian of the control, denoted as J_B, with respect to the control input. This involves calculating the partial derivatives of the two system functions with respect to the control input.

$$\frac{\partial f_1}{\partial v_c} = b_0 \cos x_1 \quad (34)$$

$$\frac{\partial f_2}{\partial v_c} = b_0 \sin x_1 - a_1 b_0 \cos x_1 \quad (35)$$

$$\Rightarrow J_B = \begin{bmatrix} b_0 \cos x_1 \\ b_0 \sin x_1 - a_1 b_0 \cos x_1 \end{bmatrix} \quad (36)$$

Evaluating this matrix for the equilibrium at 0 and π radians we have

$$J_B[x_1 = 0] = \begin{bmatrix} b_0 \\ -a_1 b_0 \end{bmatrix} \quad (37)$$

$$J_B[x_1 = \pi] = \begin{bmatrix} -b_0 \\ a_1 b_0 \end{bmatrix} \quad (38)$$

The linearized system in state space notation takes the form:

$$\dot{X} = AX + BU \quad (39)$$

$$Y = CX + DU \quad (40)$$

From Equations (33, 37), we can write the linearized system for the inverted configuration at 0 radians in matrix form as:

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ -a_2 & -a_1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} b_0 \\ -a_1 b_0 \end{bmatrix} v_c \quad (41)$$

Since we require the state space model to generate an output corresponding to the pendulum angle θ, its output equation is therefore:

$$Y = [1 \quad 0]\begin{bmatrix} x_1 \\ x_2 \end{bmatrix} \tag{42}$$

5.3. Linearized ODE

Multiplying out the matrix Equations (41, 42), we see that we have two linear equations. For the first state, we have:

$$\dot{x}_1 = x_2 + b_0 v_c \tag{43}$$

$$\Longrightarrow x_2 = \dot{x}_1 - b_0 v_c \tag{44}$$

$$\Longrightarrow \dot{x_2} = \ddot{x}_1 - b_0 \frac{dv_c}{dt} \tag{45}$$

For the second state, we have:

$$\dot{x}_2 = -a_2 x_1 - a_1 x_2 - a_1 b_0 v_c \tag{46}$$

$$\Longrightarrow \ddot{x}_1 - b_0 \frac{dv_c}{dt} = -a_2 x_1 - a_1 x_2 - a_1 b_0 v_c \tag{47}$$

Substituting back in x_1, $\dot{x}_1$, $\ddot{x}_1$ and x_2 from Eqn. (12)

$$\Longrightarrow \frac{d^2\theta}{dt^2} - b_0 \frac{dv_c}{dt} = -a_2\theta - a_1\left(\frac{d\theta}{dt} - b_0 v_c\right) - a_1 b_0 v_c \tag{48}$$

$$\Longrightarrow \frac{d^2\theta}{dt^2} = -a_2\theta - a_1 \frac{d\theta}{dt} + b_0 \frac{dv_c}{dt} \tag{49}$$

5.4. System eigenvalues and stability

The eigenvalues (λ) of the system matrix A represent the behavior of the pendulum system. These eigenvalues are related to the poles in the transfer function. The eigenvalues, denoted as λ, of matrix A can be determined by solving the following matrix equation, involving the calculation of the determinant, where I is the identity matrix:

$$|(A - \lambda I)| = 0 \tag{50}$$

If all eigenvalues have a negative real part, the system will be stable. Conversely, if any eigenvalue has a positive real part, the system will be unstable. It is also important to note that if the real part of an eigenvalue is zero, then the system is marginally stable, existing on the boundary of stability, neither conclusively stable nor unstable. Complex eigenvalues typically lead to oscillatory behavior, especially if they have a non-zero real part.

To incorporate feedback control into this system, the system must use a feedback mechanism. One approach involves utilizing full state feedback, as depicted in Figure 11. In this figure, the matrix K represents the gain of the state feedback, while R(t) denotes a reference input. If the reference input is zero, the state feedback can be described by the following expression:

$$U = -KX \tag{51}$$

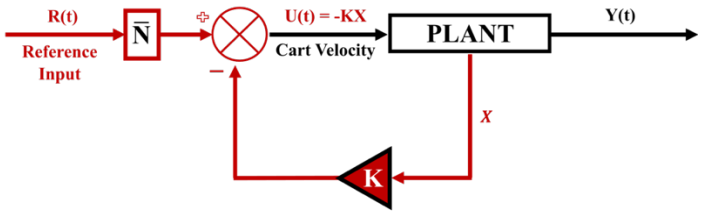


Figure 11: Signal flow graph of a plant under direct full-state feedback control: The red line delineates the feedback path, which includes multiplication by the feedback gain, denoted by K. Additionally, a feedforward gain term, represented by $\bar{N}$, is introduced to improve tracking of the reference input.

Substituting the state space system equations (39) and (40) into this expression leads to the modified state space equations, which represent the system dynamics under the influence of the feedback mechanism.

$$\dot{X} = AX + BU = (A - BK)X \tag{52}$$

$$Y = CX + DU = (C - DK)X \tag{53}$$

Implementing state feedback alters the system dynamics leading to a new expression for the state derivative. This alteration involves not just multiplying the state by matrix A, but rather by (A−BK). Consequently, the eigenvalues (λ) of the full state feedback system can be determined by solving the updated characteristic equation:

$$|(A - BK - \lambda I)| = 0 \tag{54}$$

Consequently, by modifying the gain matrix K, we can manipulate the location of the system's eigenvalues. The method for calculating K is discussed in Section 7.

5.5. Using a Luenberger observer

Many procedures in control design assume that the full state vector is available. However, this is often not the case, as in our pendulum design. In such circumstances, we can use an observer to estimate the full state using a linear plant model. The Luenberger observer computes the state estimate according to the differential equation:

$$\dot{\hat{X}} = A\hat{X} + BU + L(Y - C\hat{X}) \tag{55}$$

The observer uses the state space matrices A and B to provide a linear model of the plant. In our case, we determine the observer gains, denoted as L, using MATLAB. Similar to the state feedback gain, the Luenberger observer gain vector L must be chosen such that all the eigenvalues of the observer system, as solutions to the characteristic equation, possess appropriate negative real values. The signal flow graph for the Luenberger observer is shown in Figure 12. The system's eigenvalues satisfy the following characteristic equation:

$$|(A - LC - \lambda I)| = 0 \tag{56}$$

The calculation of L is discussed in Section 7.

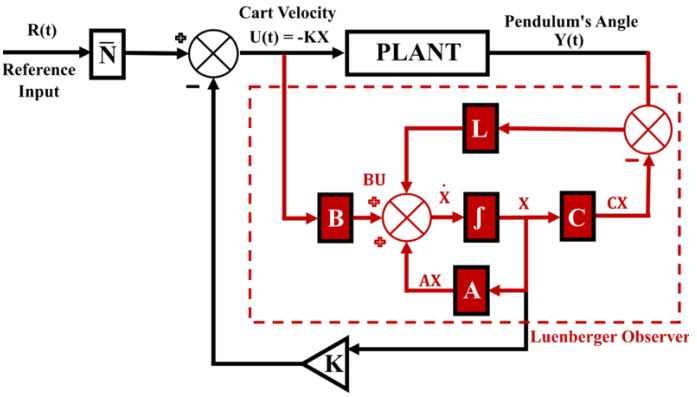


Figure 12: Estimation of plant state using a Luenberger observer. The observer, which simulates the real dynamics of the inverted pendulum, generates an estimated state, denoted as $\bar{X}$. This estimated state serves as a proxy for the actual system state, labeled X, some of which may be unobservable. The signal Y(t) is employed to correct the state estimate.

6. Augmenting the state space model

6.1. Adding cart positional state

To enable control of both the cart's position and the balancing of the pole, we introduce an additional state variable x_3 to explicitly represent the cart's position. We can relate the cart position to the control velocity input, since:

$$\dot{x}_3 = v_c \tag{57}$$

The linearized system dynamics are then represented by a 3x3 matrix, that includes the new positional state variable. The updated matrix equation is:

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 \\ -a_2 & -a_1 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} + \begin{bmatrix} b_0 \\ -a_1 b_0 \\ 1 \end{bmatrix} v_c \tag{58}$$

The output equation remains similar to before, but with an appended coefficient of zero in the C matrix:

$$\Rightarrow Y = [1 \quad 0 \quad 0] \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \tag{59}$$

We can compute the numeric values of the matrices using MATLAB. See Figure 13 for the udpated state feedback controller signal flow graph schematic.

6.2. Adding integral action

We can further improve cart position performance and reduce its steady-state error by adding integral action on the cart position (see Figure 14). To incorporate integral action, a state is devised within the controller to compute the integral of the positional error signal. This is then used as a feedback term, as denoted by the red path on the schematic. Therefore, to achieve integral feedback, we simply augment a state-space system by adding another state Z, whereby the state Z is the integral of the error between the desired output ref_p (representing a reference input for cart position) and actual output Y. Thus, the standard state-space equation:

$$[\dot{X}] = [AX + BU] \tag{60}$$

Becomes:

$$\begin{bmatrix} \dot{X} \\ \dot{Z} \end{bmatrix} = \begin{bmatrix} AX + BU \\ Y - \text{refp} \end{bmatrix} \tag{61}$$

Where the output is given by:

$$\text{Y} = \text{CX} + \text{DU} \tag{62}$$

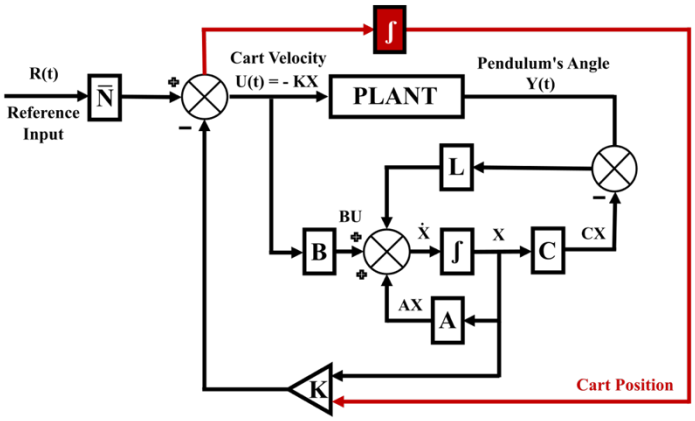


Figure 13: Adding a state for cart position provides a means to control cart position.

State feedback control is now generated from the state X and also from the state Z. That is:

$$\text{U} = -\text{KX} - \text{K}_Z\text{Z} \tag{63}$$

Thus, to add integral action to the state-space model of the cart position-augmented pendulum, and use the cart position to generate error integrated over time, we further augment the system matrices given in Eq. (58). We add a fourth state, x_4, to represent the integrated cart position error.

$$\begin{bmatrix} \dot{x}_1 \\ \dot{x}_2 \\ \dot{x}_3 \\ \dot{x}_4 \end{bmatrix} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ -a_2 & -a_1 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} + \begin{bmatrix} b_0 \\ -a_1 b_0 \\ 1 \\ 0 \end{bmatrix} v_c \tag{64}$$

$$\text{y} = [1 \quad 0 \quad 0 \quad 0] \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} \tag{65}$$

Notice that here we update the integral state by selecting the position state x_3 to generate the $(Y - ref_p)$ term used for integral action. For this model, we assume the reference position, ref_p, is zero.

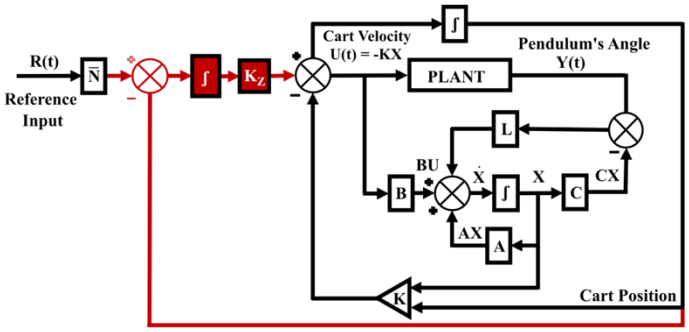


Figure 14: Illustration of integral error feedback within the system. This mechanism reduces steady-state positional error of the cart by comparing the reference setpoint with the estimated cart position, integrating the positional error, and using it in the feedback path.

7. Designing state feedback controllers

7.1. Determining feedback gain

In our pendulum design, a linear full state feedback controller is employed to balance the inverted pendulum. This method enables the maintenance of balance, even in the presence of noise and disturbances. Implementing this controller requires obtaining K, the feedback gain vector.

Various strategies can be used to find K. One method is to use pole placement, whereby we calculate K in order to achieve what we consider to be a good choice of poles for the system when it is operating under full state feedback control. Alternatively, the gain K can be found by formulating gain calculation as an optimization problem, where we specify an objective function indicative of what we consider desirable performance should be. In this work, we adopted the latter optimal control approach. Specifically, we find the gain K utilizing the MATLAB lqr command (which designs a linear quadratic regulator).

7.2. Velocity control mode

To design an optimal controller to balance the inverted pendulum using velocity as the control input, we need to consider the linear 2 state model given by the equations (41) and (42). To build an appropriate cost function for the optimization, suitable values were implemented along the leading diagonal of the 2x2 Q matrix to penalize non-zero system states. In addition, a suitable value is used in the 1x1 R matrix to penalize the control input.

Penalization of the state serves a crucial function: It ensures that the system approaches its target value. Within the scope of this design, it assists in keeping the pendulum's angle close to zero, facilitating effective balancing. In contrast, penalizing control with R serves to reduce the speed of the cart. The penalization values were determined through experimentation.

$$Q = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \tag{66}$$

$$R = 1 \tag{67}$$

7.3. Position control mode

To implement the control of the cart position as well as balancing the pendulum pole, we make use of the 4-state system that incorporates integral action. The linear state space system is described by equations (64) and (65). The diagonal entries of the 4x4 Q matrix, along with the single scalar value in the R matrix, were defined to aptly penalize state and control. The penalization values in Q and R were found by trial and error.

$$Q = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 20 \end{bmatrix} \tag{68}$$

$$R = 1 \tag{69}$$

To concurrently accomplish pendulum balancing as well as control of the cart position, we applied a larger penalty on state x_4 (which represents the integral of positional error), whereas state x_3 (which represents cart position) received a penalty term of zero.

7.4. Designing the Luenberger observer

To determine the Luenberger gain L, we again employed the MATLAB lqr command. We refrained from using the observer to predict the cart's velocity or position since estimating these is straightforward, given that velocity is directly used as the control signal.

As with the determination of state feedback controller gains, the leading diagonal entries of the 2x2 Q matrix and the single value in the R matrix were selected to penalize the system states and the control action, respectively. Suitable parameter values for these matrices were ascertained through trial and error.

$$Q = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \tag{70}$$

$$R = 1 \tag{71}$$

7.5. Gain scheduling

Transitioning between velocity control of the pendulum and position control of the pendulum was realized by selecting their respective system gain K and pre-processing term $\bar{N}$ (as discussed later and presented in Table 2). We note that resetting the integral error state to zero was necessary each time the controller was switched from velocity to position mode, to ensure processing started with a zero positional error.

In position control mode, we make use of integral action. In this case, the reference position input can have a zero value to preserve the cart's current position on the track.

During the velocity control of the cart, the velocity of the cart is required to track the reference input. To ensure this takes place

the controller requires an appropriate feedforward pre-emphasis term, denoted as $\bar{N}$:

$$\bar{N} = -[\mathrm{C}(\mathrm{A} - \mathrm{BK})^{-1}\,\mathrm{B}]^{-1} \tag{72}$$

For velocity control, we note that $\bar{N}$ has a value of 1 (that is, a gain of unity). Thus, the reference input directly sets the cart velocity. This is achieved by a slight update to the calculation of the control signal, which now incorporates a non-zero reference input, referred to as 'ref':

$$\mathrm{U} = -\mathrm{KX} + \bar{N}\mathrm{ref} \tag{73}$$

8. Laplace Analysis of the Inverted Pendulum Dynamics

8.1. System transfer function

Laplace analysis can provide useful insights into system behaviour. Neglecting the non-linear effect of friction, the linearized differential equation that describes the pendulum can be expressed as:

$$(I + ml^2)\frac{d^2\theta}{dt^2} + \mu\frac{d\theta}{dt} = mgl\theta + ml\frac{d^2x_P}{dt^2} \tag{74}$$

Applying the Laplace transform, and assuming initial conditions of zero we have:

$$(I + ml^2)s^2\Phi(s) + \mu s\Phi(s) = mgl\Phi(s) + mls^2X_P(s) \tag{75}$$

$$\Longrightarrow \big((I + ml^2)s^2 + \mu s - mgl\big)\Phi(s) = mls^2X_P(s) \tag{76}$$

This leads to the s-domain transfer function relating output pole angle $\Phi(s)$ to cart position $X_P(s)$:

$$\Longrightarrow \frac{\Phi(s)}{X_P(s)} = \frac{s^2ml}{\big((I + ml^2)s^2 + \mu s - mgl\big)} \tag{77}$$

We now rearrange terms in the denominator and use the relationship $\mathrm{V}(s) = sX_P(s)$. This leads to the expression relating output pole angle $\Phi(s)$ to cart velocity $\mathrm{V}(s)$:

$$\Longrightarrow \frac{\Phi(s)}{\mathrm{V}(s)} = \frac{\dfrac{sml}{(I + ml^2)}}{\left(s^2 + s\dfrac{\mu}{(I + ml^2)} - \dfrac{mgl}{(I + ml^2)}\right)} \tag{78}$$

8.2. 2nd order canonical form

Comparing the expression with the second-order canonical form, we can identify the coefficients and characteristics of the system. This comparison allows us to further analyze the dynamics of the inverted pendulum and gain deeper insights into its behavior and control requirements.

$$\frac{sk}{(s^2 + 2\xi\omega_n s - \omega_n^2)} \Leftrightarrow \frac{\dfrac{sml}{(I + ml^2)}}{\left(s^2 + s\dfrac{\mu}{(I + ml^2)} - \dfrac{mgl}{(I + ml^2)}\right)} \tag{79}$$

Here, k represents a simple gain factor. Upon examining the given expression, we find that it allows us to determine the natural frequency of the system as follows:

$$\omega_{n=}\sqrt{\frac{mgl}{(I + ml^2)}} \tag{80}$$

Given that angular frequency (ω_n) is related to frequency (f_n) in cycles per second through the relationship $\omega_n = 2\pi f_n$ we can write the expression:

$$f_{n=}\frac{1}{2\pi}\sqrt{\frac{mgl}{(I + ml^2)}} \tag{81}$$

Similarly, by inspection, we can write down an expression for the damping ratio of the system:

$$\xi = \frac{\dfrac{\mu}{(I + ml^2)}}{2\omega_n} \tag{82}$$

9. Numeric integration to implement real-time control

9.1. Euler integration

To implement real-time state feedback control, some form of numerical integration is needed. Such integration can often be carried out satisfactorily on a digital computer using Euler's methods. Forward Euler integration works by incrementally calculating contributions to the integral that arise from the differential term.

The basic idea is as follows. Consider a function y=f(x) such that when $x=x_0$ then $y=y_0$. This is illustrated in Figure 15. As we increase the value of x by Δx we reach a point where $x_1=x_0+\Delta x$ and similarly this increases y by Δy reaching the value $y_1=y_0+\Delta y$. Therefore:

$$(x_1, y_1) = (x_0 + \Delta x,\ y_0 + \Delta y) \tag{83}$$

The gradient of the curve at (x_0, y_0) is the tangent at this point. From Figure 15, it is seen that the gradient at this point can be approximated by the ratio of a small change in y divided by a small change in x:

$$\frac{dy}{dx}|(x_0, y_0) \approx \frac{\Delta y}{\Delta x} \tag{84}$$

This is only strictly true in the limit where Δx tends to zero. In practical numerical methods, this limit is approximated by choosing a sufficiently small Δx. We also see that we can use this relationship to iteratively estimate y_1 from y_0 by replacing the Δy term by two very close and successive y values:

$$\frac{dy}{dx}|(x_0, y_0) \approx \frac{(y_1 - y_0)}{\Delta x} \tag{85}$$

Re-arranging this equation and writing Δx as step size *h* gives:

$$y_1 = y_0 + h\frac{dy}{dx}|(x_0, y_0) \quad (86)$$

Writing the x-axis in terms of a time variable t, the gradient is given by:

$$\frac{dy}{dt} = f(t, y) \quad (87)$$

And initial conditions are given by:

$$f(t_0, y) = y_0 \quad (88)$$

We then obtain the recurrence relation for step n:

$$y_{n+1} = y_n + hf(t_n, y_n) \quad (89)$$

Where t is time, at initial time to the output is y_0, at future time $t_{(n+1)}$ the output is $y_{(n+1)}$, and h is the step size. This expression can be used to iteratively find the next estimate of y_1 if we know x_o and the gradient at (x_0, y_0). This approach provides a method for integrating the differential term, which is generally satisfactory if a sufficiently small temporal step size, h, is used. This method is easily extended to vector form to perform the integration stage needed in state space models.

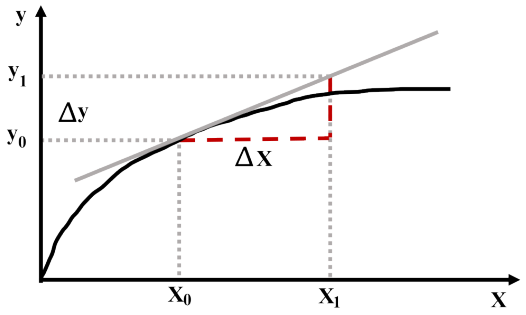


Figure 15: The gradient dy/dx of a curve y=f(x) can be locally approximated at the point (x_0,y_0) as the ratio of a small change in the value of y to a corresponding small change in the value of x.

9.2. Higher order numerical integration

Euler integration is the simplest fixed-step numerical method that can be adopted. However, other more complex integration rules can also be used. These include the midpoint, trapezoidal, and Runge-Kutta methods, which, though requiring more computational steps in the estimation of the integral, offer higher accuracy. Additional methods utilize dynamic selection of step size, such as the ode45 function in MATLAB. See [67] for a discussion of these methods.

Here, we use MATLAB's ode45 for simulations of the uncontrolled stable pendulum configuration. We use Euler Integration to model the controlled pendulum because of the method's simplicity and its ease of implementation on a microcontroller, especially considering its low computational requirements.

10. System identification

10.1. Large angle pendulum oscillatory behavior

Approximately estimating observable parameters of a pendulum, such as length and weight, can be done with relative ease. However, assessing other parameters is considerably more challenging, and in some cases, impossible, solely based on observations of the static mechanical system. To accurately determine values for viscous and sliding friction, it is necessary to conduct measurements during pendulum movement.

To examine the large-angle oscillatory behavior of the pendulum, we raised it from its resting, vertically hanging (non-inverted) position to a horizontal alignment, corresponding to an angle of approximately 90°, before releasing it. The pendulum then oscillated until viscous damping and friction gradually brought it to a standstill in its vertical, non-inverted position.

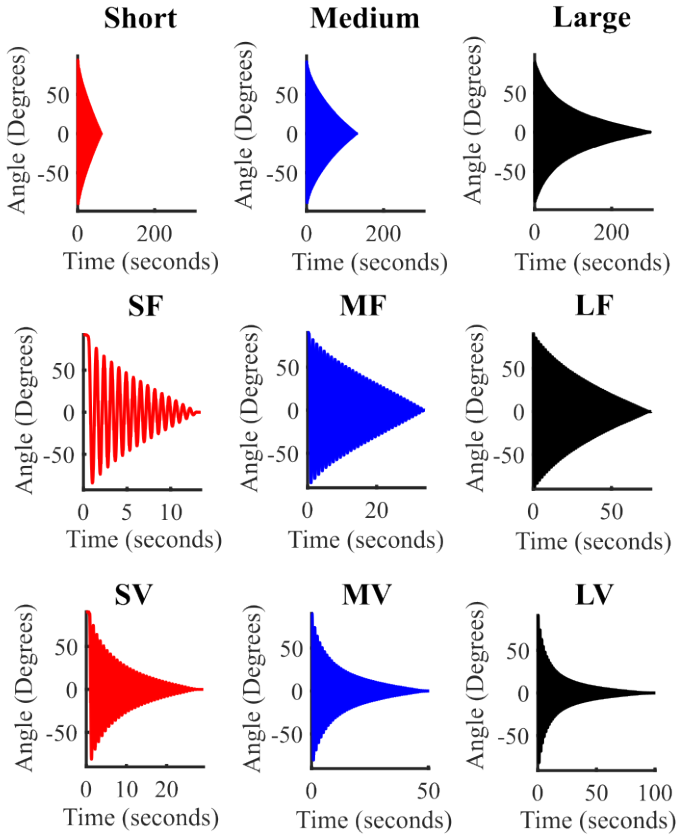


Figure 16: Pendulum large angle oscillation decay over time for three pendulum lengths. Data captured using an incremental encoder. Top row: No added viscosity or friction for short, medium, and long pole lengths. Middle row: Effect of added friction for short, medium, and long pole lengths (SF, MF, and LF, respectively). Lower row: Effect of added viscosity for short, medium, and long pole lengths (SV, MV, and LV, respectively).

10.2. Data logging

To examine the pendulum's oscillation decay over time, we collected time-stamped pole angle data from its shaft encoder as the pendulum swung. In addition, the pendulum cart position was recorded using readings from the encoder mounted on the rear of the cart drive stepper motor. The data were gathered using a program running on an Arduino Mega, which transmitted the time and angular measurements to a host PC equipped with Microsoft Excel. The Excel program was used to record the data at a 25Hz rate and save it to the hard disk in Excel file format. Subsequently, the data were imported into MATLAB for analysis. This allowed

for the generation of a plot depicting the pendulum's decaying oscillations under various conditions, as well as further analyses.

The mechanical pendulum system features three interchangeable poles, and for each pole, the level of friction could be adjusted from low to high. Similarly, the viscous damping could be altered from low to high by manipulating the wind resistance experienced by the paddle mechanism. This configuration led to a total of 9 different experimental conditions.

Figure 16 top row shows the temporal response waveforms for the undamped cases with no added friction for all three pendulum lengths, plotted on the same scale. It is observed that a longer pendulum length significantly increases the time required for the pendulum angle to decay to zero. Figure 16 middle and lower rows illustrate the responses of pendulums of three different lengths with additional friction and additional viscosity introduced, respectively. It is apparent that incorporating viscosity into the system accentuates the exponential decay. However, it is noteworthy that when friction is the dominant factor, the decay is linear rather than exponential.

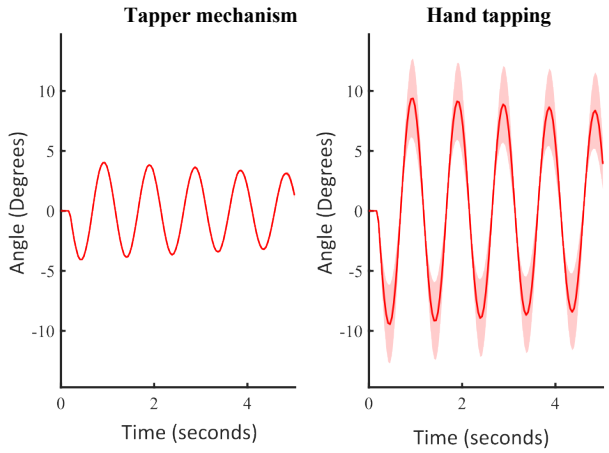


Figure 17: Testing the consistency of the tapping mechanism. Mean and standard deviation of the pendulum angular response averaged over 8 trials are shown using the tapper mechanism and hand excitations of the pendulum pole.

10.3. Small angle pendulum oscillatory behavior

The primary interest of this study is the examination of the balancing behavior of the pendulum system in its inverted configuration; therefore, large angle behavior is not of particular relevance. In a balancing configuration, the pendulum pole is maintained close to its unstable equilibrium position by the controller. In this case, the angular deviation from the 0° position is small, which is also essential for the validity of the linear approximation made in the observer model. Therefore, to estimate the parameters of the linear model accurately, it is necessary to examine the pendulum operation at small angles of deflection and to perform system identification for all pendulum parameters under these conditions. To generate consistent excitation to the pendulum, we utilized a mechanical RC servo tapping mechanism.

11. Using the tapping mechanism

11.1. Evaluating tapper consistency

To evaluate the consistency of the tapping mechanism's operation, we conducted tests on the medium pendulum pole without added friction or viscosity. Figure 17 illustrates that the tapper provides very consistent excitation of the pendulum, particularly when compared to the variability typically observed with manual tapping by hand.

11.2. Excitation of non-inverted pendulums

We examined the pendulums in their normal, stable, hanging-down mode to characterize the effects of the tapping. Figure 18 illustrate the responses of pendulums of different lengths driven by the tapper mechanism, both with and without added friction and viscosity. In comparison to the large angle oscillation tests, it is noteworthy that at small angles, the paddle has only a minor effect, and additional friction more rapidly damps out pendulum oscillation.

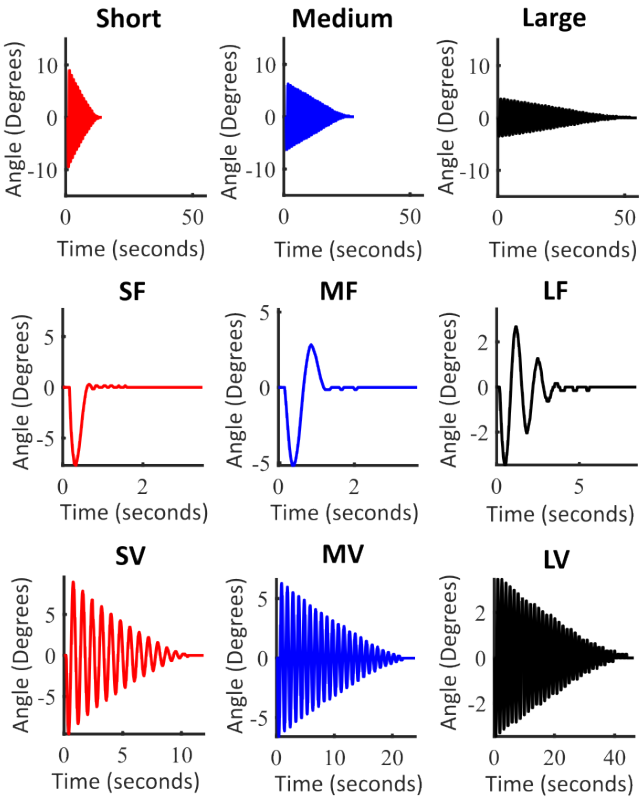


Figure 18: Pendulum small angle oscillation decay over time. Top row: No added viscosity or friction. Middle row: Effect of added friction for short, medium, and long pole lengths (SF, MF, and LF, respectively). Lower row: Effect of added viscosity for short, medium, and long pole lengths (SV, MV, and LV, respectively).

11.3. Estimating pendulum parameters

We performed grey-box system identification of the physical pendulum mechanism to identify parameters of viscous and static friction, and to fine-tune others, including pendulum length, weight, and moment of inertia.

To fit the small angle pendulum response data, we focused on six of the nine configurations: the three pole lengths both with and without added viscosity. This fitting was accomplished with a simulation of its nonlinear dynamics, employing an optimization procedure using the MATLAB fmincon function. We discarded the configurations with extra friction due to the dramatic impact it had on the system's behavior, which resulted in a limited amount of useful temporal data. This procedure optimized the mass,

effective pole length, pole moment of inertia, sliding friction, and viscous friction parameters of the pendulum system.

We designed an objective function that minimized the sum of squared distances between the predicted oscillations and the measured data. To align the simulation with the measured data for comparison, we first trimmed the measured data to begin at its first positive peak in the pendulum's oscillation. The pendulum's angular velocity at this point is zero, and its corresponding angle was used to set the initial angular state in the non-linear simulation of the pendulum, based on Eqn. (2), that includes both viscosity and friction. This was carried out using the MATLAB ode45 solve.

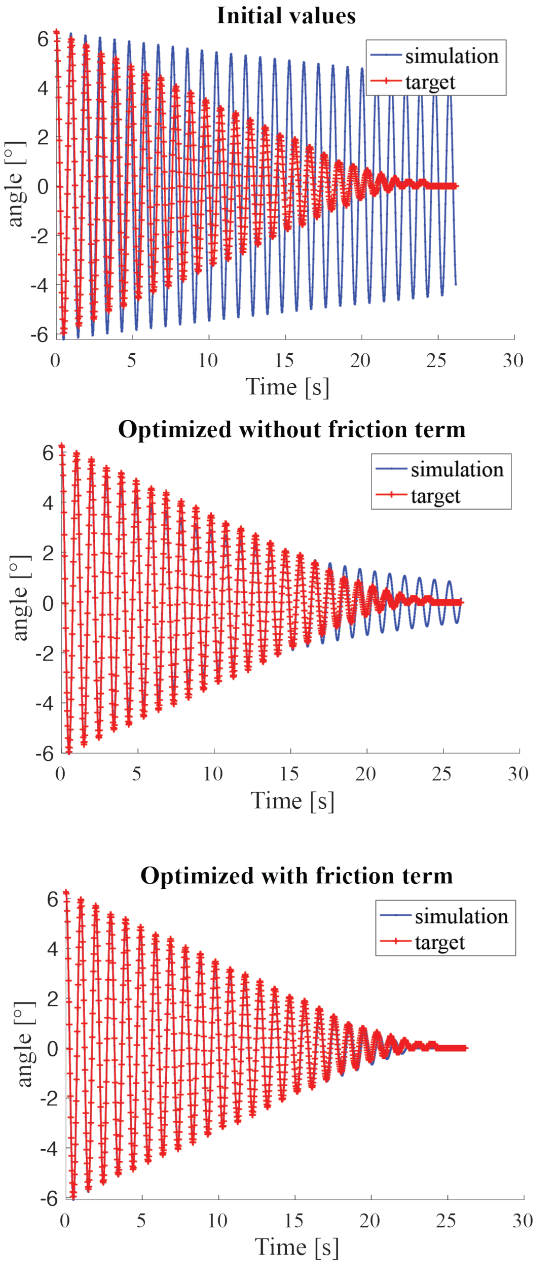


Figure 19: Running optimization to fit the measured response of the medium-length non-inverted pendulum without additional viscosity or friction. Top plot shows the predicted response based on an initial rough guess. Middle plot shows the estimated response after running the optimization algorithm without including the friction term. Lower plot shows the estimated response when the friction term is present. It is evident that accounting for friction leads to a significantly better fit.

We initialized the simulation parameters based on direct measurements of pendulum pole length and mass. Initially, we estimated the values of the friction and viscosity parameters through a process of trial and error, which was aided by careful observation of the simulated responses. During the fitting procedure, we allowed the optimization algorithm to refine all parameter values. However, it was necessary to constrain the parameter solutions to prevent fits that deviated substantially from the known ground truth values for mass and pendulum length. To this end, the mass and length were constrained to values between 0.9 and 1.1 times their measured values. The other parameters, for which we had less grounded certainty, were allowed to vary from 0.1 to 10 times their initial estimated values.

Table 1: Physical Measurements of the three different pendulums and estimated values found by system identification. Values marked with 'F' represent estimates with friction included in the second-order nonlinear differential equation model of the pendulum. The bold values represent estimates made when only a viscous damping term is present.

	Short Pendulum		Medium Pendulum		Long Pendulum	
	Normal	Viscous	Normal	Viscous	Normal	Viscous
Measured Length to CoG [m]	0.233/2 = **0.117**		0.335/2 = **0.168**		0.635/2 = **0.318**	
Measured Weight [Kg]	**0.174**		**0.226**		**0.336**	
Estimated Half-length to CoG [m]	0.116(F) **0.106**	0.117(F) **0.105**	0.167(F) **0.149**	0.164(F) **0.149**	0.322(F) **0.317**	0.308(F) **0.316**
Estimated Weight [Kg]	0.178(F) **0.158**	0.174(F) **0.157**	0.207(F) **0.207**	0.202(F) **0.207**	0.341(F) **0.338**	0.327(F)x **0.338**
Estimated MoI [Kg-m2]	8.97e-04(F) **9.02e-04**	8.47e-04(F) **8.83e-04**	0.0024v **0.0027**	0.0024(F) **0.0027**	0.0142(F) **0.0144**	0.0147(F) **0.0146**
Estimated Viscosity [N-m-s/rad]	2.21e-04(F) **9.90e-04**	2.22e-04(F) **1.00e-03**	3.36e-04(F) **1.00e-04**	2.35e-04(F) **1.00e-04**	2.22e-04(F) **0.0038**	5.20e-04(F) **0.0048**
Estimated Friction [N/Rads-1]	5.05e-04(F) **n/a**	6.16e-04(F) **n/a**	3.07e-04(F) **n/a**	3.87e-04(F) **n/a**	3.87e-04(F) **n/a**	5.46e-04(F) **n/a**

Figure 19 shows the results of using system identification to fit model parameters to the measured data for the medium-length, low-friction, low-viscosity pendulum condition. The initial guess, which incorporated insufficient damping, is shown in Figure 19 top plot. A reasonably good fit is achieved by fitting the model with only viscous damping, as demonstrated in Figure 19 middle

plot. An even better fit is obtained when the model also includes sliding friction, depicted in Figure 19 1ower plot.

For each pendulum length, measured and estimated values were obtained, both with and without friction, leading to a total of six conditions. These conditions are presented in Table 1. The corresponding (no-friction) state space matrices and Luenberger gain L are shown in Table 2. The computed state feedback controller system gains K and reference pre-scaling factor $\bar{N}$, are shown in Table 3.

11.4. Reality check using canonical form

To provide a ballpark estimate of the main parameters of the three pendulums in their low-damping modes, each pendulum was first nudged using the tapper mechanism and then allowed to sway freely, eventually settling into its stable position, as depicted in Figure 20. Measured values are shown in Table 4.

Table 2: Values of the state-space matrix and Luenberger observer gain, presented in MATLAB syntax.

Parameter	Value
A	[0 1 0 0; 41.4440 −0.1692 0 0; 0 0 0 0; 0 0 1 0;]
B	[44.2247; −0.7147; 1; 0;]
C	[1 0 0 0]
L	[12.7461 80.7319]

Table 3: Computed state feedback control K gains and $\bar{N}$ values used for the two control mode (in MATLAB syntax).

Control 1zModes	K Gain	$\bar{N}$
Position Control	[5.0514 0.7587; −4.4412; −4.4721;]	*0*
Velocity Control	[3.2478; 0.4734; 0; 0;]	*1*

Table 4: Measured decay and nearest integer number of cycles as a function of time for all three pendulum lengths in undamped conditions. The values in brackets were found by the system identification procedure.

	Short Pendulum	Medium Pendulum	Long Pendulum
Measured Maximum Time [s]	13.50	27.0	54.8
Measured 50% Decay Time [s]	5.99	12.15	26.2
Measured 50% Decay Cycles [integer count]	7	12	19
Observable frequency of oscillation f_d [Hz]	1.17 Hz **(1.25 Hz)**	0.99 Hz **(1.03)**	0.73 Hz **(0.74 Hz)**
Estimated damping ratio ζ	0.016 **(0.024)**	0.0091 **(0.011)**	0.0057 **(0.0084)**

We used Equations (80 and 81) to calculate the corresponding natural frequencies, which were essentially the same as the damped frequencies due to the very small damping ratio. These values aligned well (within 10%) with those obtained through system identification, confirming the appropriateness of the values found by the fitting procedure. We calculated the damping ratio from the decay to 50% in a time t_{50} using the equation:

$$\zeta = \frac{-\ln(0.5)}{\omega_n t_{50}} \tag{90}$$

From Table 4 it can be seen that the system identification yielded similar values.

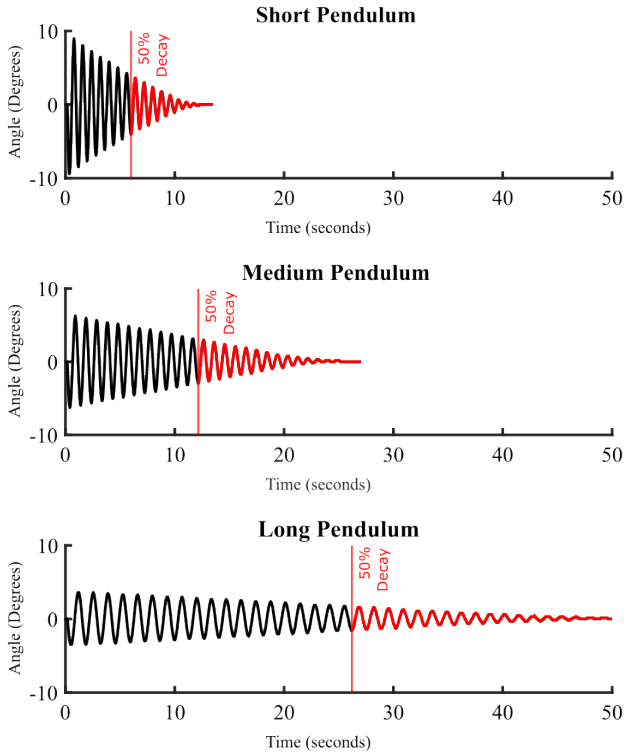


Figure 20: Approximate estimation of the canonical parameters for the pendulum system by observing the frequency of oscillation and the amplitude decay to 50% of the initial value. Plots are shown here for the short, medium, and long-length pendulums (with no extra damping), respectively.

12. MATLAB SFC controller simulations

12.1. Simulating the pendulum

In MATLAB, we simulated the pendulum balancing using both velocity and position controllers. This involved the deployment of a non-linear state space model to simulate the pendulum plant. Additionally, a linear model was implemented for Luenberger observer full state feedback control.

Following initial design of the two inverted pendulum controllers, they underwent iterative tuning and testing within MATLAB simulations. This methodology included assessing the behavior and stability of the inverted pendulum in response to cart movement and simulated impacts to the pole while it was balanced in its inverted position. Simulations carried out in both velocity control and position control modes, also involve modifying the reference input to maneuver the cart velocity or position.

12.2. Reference tracking

Simulated results of velocity tracking are shown in Figure 21 left column. The cart nearly achieved the reference velocity using

a feedforward velocity command applied directly to it. In this scenario, feedback control of the cart's velocity was not utilized. As a result, the tracking was not entirely accurate; this is partly because the feedback control required for stabilizing the balance tends to counteract the cart's movement.

Simulated results of position tracking are presented in Figure 21 right column. Utilizing integral action to correct the cart's position error proved effective for tracking the desired cart position. However, the response to the target location was not immediate, with a noticeable delay before the cart aligned with the desired position.

12.3. Recovery from impulsive disturbance

To simulate kick disturbances, we manipulated the state of the pendulum to mimic the effect of an elastic collision with another hard object. This involved setting the pendulum's angular state (x_1) to zero and its second state (x_2), which comprises an angular velocity component and a control input term, to a small positive value. The results of this simulation are shown in Figure 22.

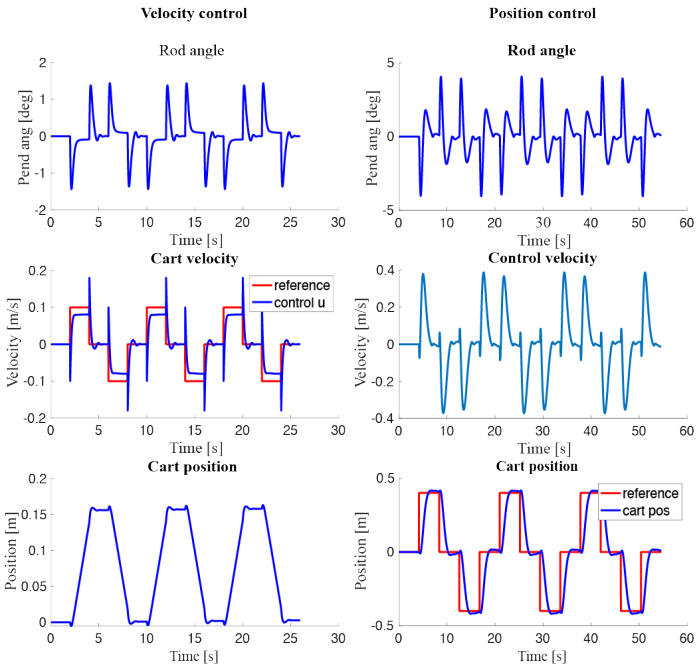


Figure 21: The pendulum angle and cart position are depicted in response to the cart movement, driven by changes in the cart position reference setpoint. Left column: MATLAB simulation of the pendulum with velocity control. The pendulum angle and cart position are shown in response to moving the cart, driven by changes in the velocity reference input. Right column: MATLAB simulation of the pendulum under position control of the cart with integral action on cart positional error.

The left column of Figure 22 shows the response of the inverted pendulum to an impulsive disturbance while operating in velocity control mode. It demonstrates a successful recovery to the initial pole deviation from the vertical position. However, it is notable that the cart position shifts and does not return to its initial starting position.

The right column of Figure 22 shows the behavior of the inverted pendulum to the same disturbance while operating in position control mode. Again it can be seen that a good recovery to the initial pole deviation from the vertical orientation is achieved. However, although the cart initially drives away from its initial location, is slowly moves back after a few seconds.

13. DIN Rail Panel Construction

13.1. Connections to controller

A DIN rail panel was tailor-made to control the inverted pendulum system. Figures 23 and 24 show the connectors and their corresponding wiring diagrams. The controller interface, located at the top of the panel enclosure, features a female USB-B port. This port connects the Arduino Mega 2560, located inside the controller assembly, to an external computer, which is used for software development and relaying control commands.

The panel features seven female D-connectors. The interfaces are configured to connect with four stepper motors, an I²C device, an SPI device, and two encoders. The use of these D-connectors allows for easy and quick connection of the panel to the inverted pendulum apparatus or other equipment.

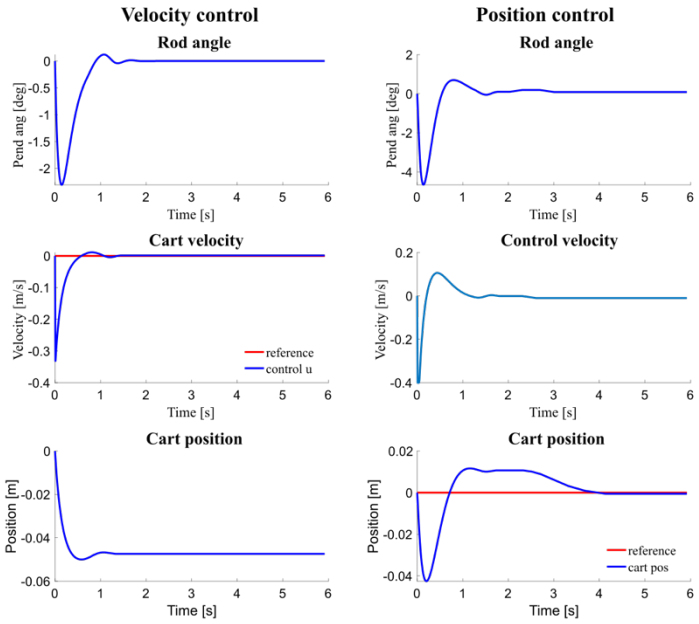


Figure 22: The pendulum angle and cart position are depicted in response to a simulated tap. Left column: MATLAB simulation of the pendulum with velocity control. The pendulum angle and cart position are shown in response to a 40 deg/s initial velocity disturbance. Right column: MATLAB simulation of the pendulum under position control of the cart, with integral action on cart positional error.

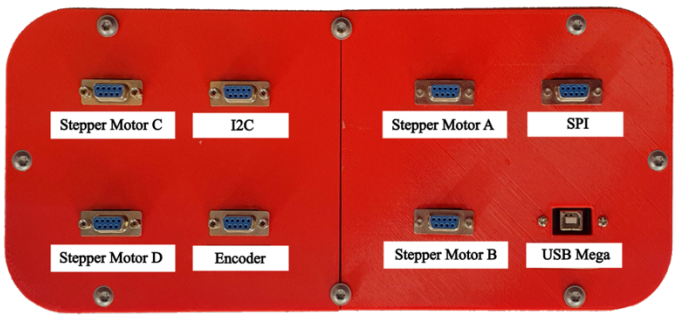


Figure 23: View of the actual controller panel cover, which was designed in Autodesk Fusion 360 and then 3D printed.

Special care was taken in the wiring of the plugs for each attached component, and they were configured with a unique connection pattern. This design feature serves to prevent accidental inappropriate connections that could result in electrical damage. The primary focus was on the power pin assignments, ensuring their isolation from other signal inputs and outputs. This safeguard ensures that potential connection errors will not result in component damage.

13.2. Panel internal layout

The controller panel's internal layout comprises three specific DIN rails, as depicted in Figure 25, which shows a photograph of the assembled unit. It consists of a microcontroller rail, a rail for motor drivers and power converters, and a power supply rail. Additionally, wiring conduit was strategically placed to manage the cabling in a tidy manner. This arrangement not only enhanced the orderly appearance but also reduced the risk of unintended cable contact with other components or causing interference.

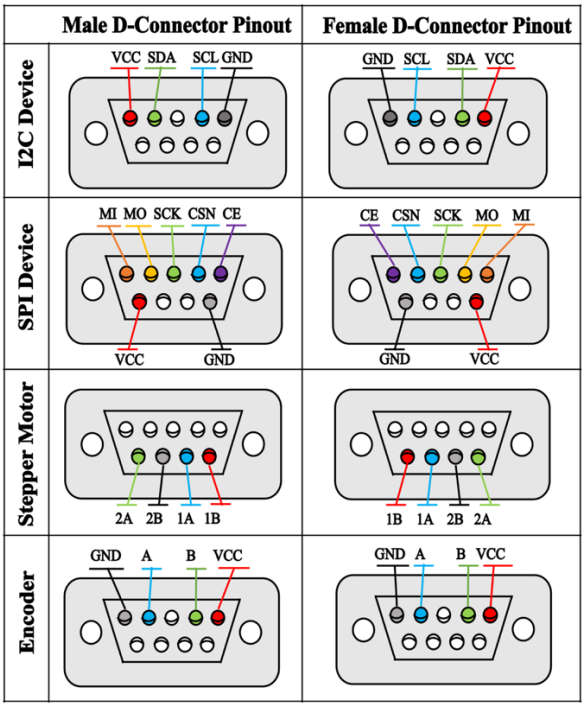


Figure 24: Rear view of soldered D-Sub connections on the male plugs (left-hand column) and the female sockets (right-hand column) mounted on the panel. The top row shows the Inter-Integrated Circuit (I²C) pinout, the second row is for Serial Peripheral Interface (SPI), the third row is dedicated to stepper motors, and the bottom row is configured for encoders

13.3. Panel DIN rail components

In the selection of panel components, preference was given to components equipped with rear mounts for DIN rail attachment. For other components, custom 3D printed support structures were made and fitted with clips to attach them to the DIN rails. The power rail within the controller panel was compartmentalized into three principal sections:

1. An AC circuit breaker section that is responsible for regulating overcurrent conditions and interrupting the main supply.
2. A region featuring a PULS Dimension DIN rail power supply, which delivers 24 volts at 5A, and meets the voltage and current prerequisites of the system.
3. A region containing three discrete DC circuit breakers, to permit individual disconnection of each control component. This feature provides additional protection against potential damage due to short circuits.

13.4. Stepper motor drivers

The power converter and motor driver rails were engineered to facilitate the operation of up to four stepper motors, each capable of being directly interfaced with the control panel's motor driver rail. The motor driver rail featured two 3D-printed carriers, each housing a pair of A4988 stepper motor drivers. These motor drivers were powered by a 24-volt supply operating on mains power.

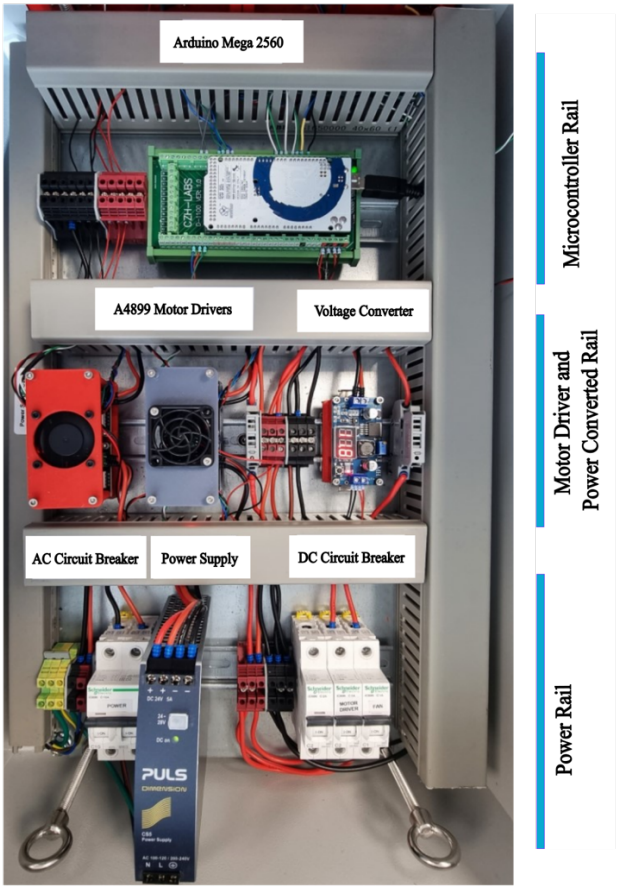


Figure 25: View displaying the internal layout of the controller panel, which is partitioned into distinct sections for power management, motor control, and microcontroller functions.

The A4988 driver offers eight distinct micro-stepping resolutions, providing flexibility in stepper motor control. For this project, we employed a one-fourth step resolution for all motors. To realize the one-fourth step resolution setting on the expansion board, the DIL switches were configured appropriately. The A4988 driver can operate within a voltage range of 8V to 35V and can deliver a current ranging from 1.5A to 2.2A. A potentiometer is incorporated into the driver breakout board, enabling hands-on fine-tuning of the current supplied to the stepper motor. To

determine the current limit, I_{lim}, it's essential to gauge the reference voltage (V_{ref}) on the potentiometer and apply the given formula to compute its desired value:

$$I_{lim} = 2V_{ref} \tag{90}$$

This facilitates precise control over the motor current, optimizing performance and efficiency. Our adjustment of the current limit was a critical step to ensure the proper functioning of our NEMA23 stepper motors. A current limit of 1.5A was determined to be ideal for this specific application. Exceeding this current threshold may damage both the motors and the drivers. Conversely, setting the current below 1.5A could compromise the motors' operation, raising the likelihood of stalling. Thus, appropriate calibration is paramount to ensure good performance while safeguarding the components from potential harm.

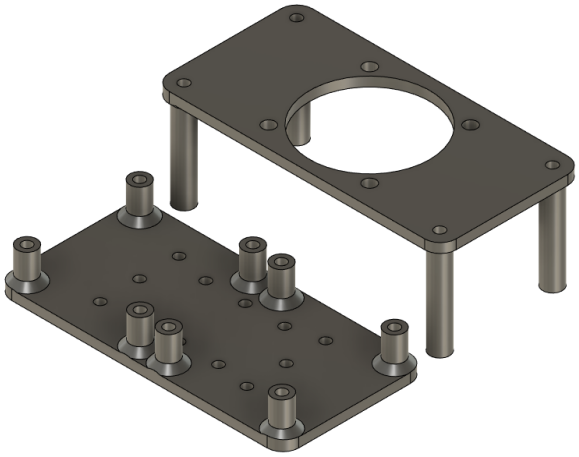


Figure 26: DIN Rail holder for the A4988 Driver Module. This setup mounts two stepper motor controller breakout boards onto a DIN rail. Notably, it includes a cooling fan to ensure the controllers remain at optimal temperatures and prevent overheating.

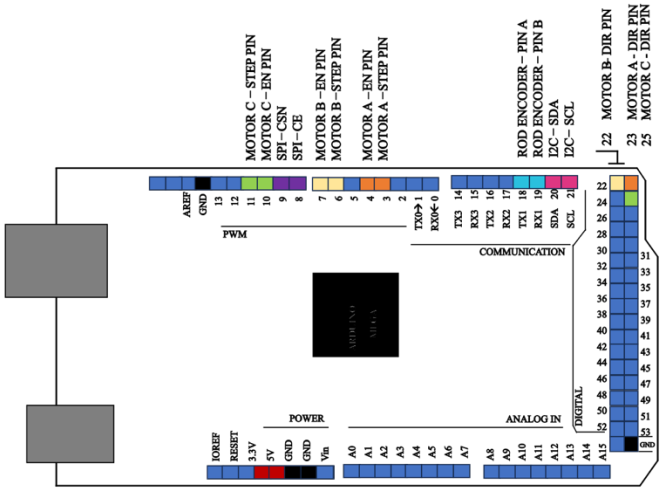


Figure 27: Pinouts for the Arduino Mega 2560. The connections are configured to control up to three stepper motors and communicate with peripherals via the I²C and SPI data buses.

To prevent overheating of the motor drivers, the incorporation of a cooling solution was essential. A pair of compact DC axial fans were positioned above them to prevent thermal damage to the chips. These fans required a supply voltage of 12V, which was furnished through a Buck converter operating from the 24V power line (refer to Figure 26). This setup ensured that the motor drivers stayed at a safe temperature during operation, enhancing both their performance and longevity.

At the heart of the controller panel, on the microcontroller rail, the Arduino Mega 2560 is prominently featured. Selected for its robust I/O capabilities, it offers 54 digital input/output pins, including 15 suitable for PWM, 256KB of flash memory, and a clock speed of 16MHz (refer to Figures 27 and 28). The Arduino Mega facilitates seamless communication with the host PC, aligning perfectly with the project's requirements.

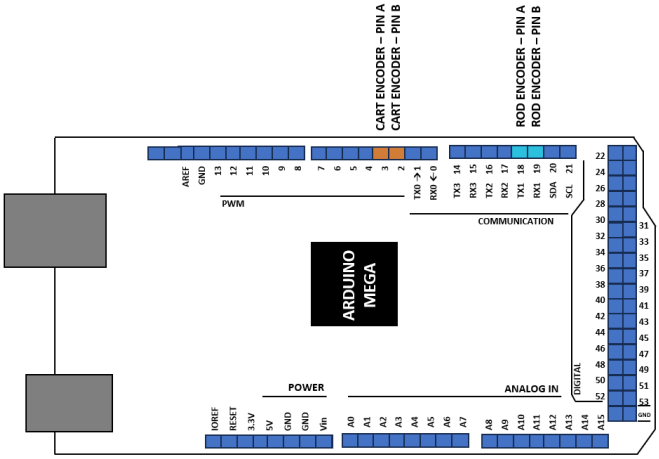


Figure 28: Arduino Mega 2560 pinout connections used for reading the system's two encoders.

14. Software Implementation in Arduino

14.1. Arduino software overview

Control over the pendulum was overseen by the Arduino Mega, which was employed to implement a state feedback controller function within its primary polling loop. During the polling operation, the control process begins by reading the encoder to ascertain the pendulum pole's angle relative to the vertical. For the state feedback controller to operate, it required the pendulum system's full state. Since only the angle was directly available, the second state was estimated using a Luenberger observer. Using the full state estimate, the control command was generated by multiplying it with the specified feedback gain. Based on the measured angle, the feedback controller then calculated the stepper motor velocity control signal. This signal produced an output pulse train, driving the stepper motor and allowing the cart to move at the ideal speed to maintain balance. State updates were computed utilizing Euler integration.

14.2. Arduino command menu

Within the polling cycle, the system processes and interprets incoming commands received through the serial interface. The suite of accessible commands encompasses the following:

- Activate control: Starts balancing when the pendulum is brought up to an inverted configuration.
- Deactivate control.
- Display help menu: View controller parameters.

14.3. Main Arduino loop pseudocode

The pseudocode for the main Arduino poll loop is shown below. This makes use of function calls the can reset the encoder, calculate the motor command, and drive the stepper motor. The loop is continuously run to control the system, ensuring that the pendulum maintains its desired position or follows a certain trajectory. In addition, there are command responses from calls to the menu system so that the program can be operated from a serial monitor over a USB connection.

Main Arduino Poll loop

Result: Balances pendulum on track

Initialization of SFC parameters and flags

while *program running* **do**

Call the menu object for input commands, act accordingly

Read time

Read pendulum pole angle

Read reference value

Call SFC function to compute control u

Generate stepper control pulses to

Drive stepper motor

end

14.4. Pseudocode to implement SFC

The state feedback controller is implemented as a C++ class. Its constructor sets up the parameters for the state space model, as well as the SFC gain K and the Luenberger gain L. A SFC function is called with the current time and the measured pendulum pole position. It returns the control value U, which is subsequently used to set the rotational velocity of the stepper motor and drive the pendulum cart.

State Feedback Controller

Result: state feedback control variable u

Initialization state space matrices A, B, C
Initialization SFC gain K
Initialization Luenberger gain L
Initialization state estimate; $\hat{X}$ = [0; 0; 0; 0];

while *balancing pendulum* **do**

Read reference value ref

Read pendulum output angle y

Calculate time step: h. = time - lastTime

Update last time: lastTime = time

Calculate control: u = - K$\hat{X}$ + ref * $\bar{N}$

Calculate Output prediction error: yErr = y – C$\hat{X}$

Calculate 1st pendulum state derivative:
$\dot{\hat{X}}(0)$ = A[0][0] * $\hat{X}$[0] + A[0][1] * $\hat{X}$[1] + B[0] * u + L[0] * yErr

Calculate 2nd pendulum state derivative:
$\dot{\hat{X}}(1)$ = A[1][0] * $\hat{X}$[0] + A[1][1] * $\hat{X}$[1] + B[1] * u + L[1] * yErr

Calculate 3rd cart position state derivative:
$\dot{\hat{X}}(2)$ = B[2] * u

Calculate 4th integral position error state derivative:
$\dot{\hat{X}}(3)$ = $\hat{X}(2)$ = B[2] – ref

Perform Euler integration:
$\hat{X}$ = $\hat{X}$ + h$\dot{\hat{X}}$

Return u

end

15. Experimental results

15.1. Online demonstration videos

Viewers can watch the inverted pendulum operations, including various tests, on the YouTube channel 'Robotics, Control and Machine Learning'. All related videos are grouped under the 'ASTESJ Inverted Pendulum' playlist. Please follow the provided link for direct access to these videos:

https://youtu.be/pvF0Zhs501U?si=P7vknbwL11tvBksE

15.2. Perturbation tests

We use a straightforward approach to assess control law performance by simultaneously monitoring the cart's position and the pendulum's angle during minor system disturbances. We obtain these measurements using encoders on the cart's stepper motor and at the pendulum's axis for angle measurement. During the balance test, disturbances are introduced by systematically applying an impulse to the pendulum using a tapping mechanism.

Experiments were conducted in both position and velocity control modes, varying the pole length from shorter to longer dimensions. These tests demonstrated the system's ability to maintain stability, even when subjected to additional loads altering its dynamic characteristics. Video demonstrations of these experiments can be found on YouTube, as per the link provided above.

15.3. Position mode results

Figure 29 shows the results of the test conducted in position control mode. The pendulum was initially stabilized and held stationary in a balanced position. Following the disturbance, immediate and noticeable changes occurred in both the pendulum angle and the cart's position. The pendulum angle plot showed minor fluctuations around zero. The motor encoder data revealed that the cart moved quickly to restore balance in the system and then gradually returned to its original position. This behavior, referring to the cart's movement and pendulum stabilization, is also evident in the YouTube videos.

During tests with the long-length pole, we observed a small oscillation of the cart, even in the absence of disturbance. This oscillation likely stems from a significant mismatch between the long-length pole's parameters and those of the medium-length pole, for which the controller was originally designed. Based on these observations, modifying the control law appears necessary to effectively manage the pendulum's behavior with its increased length.

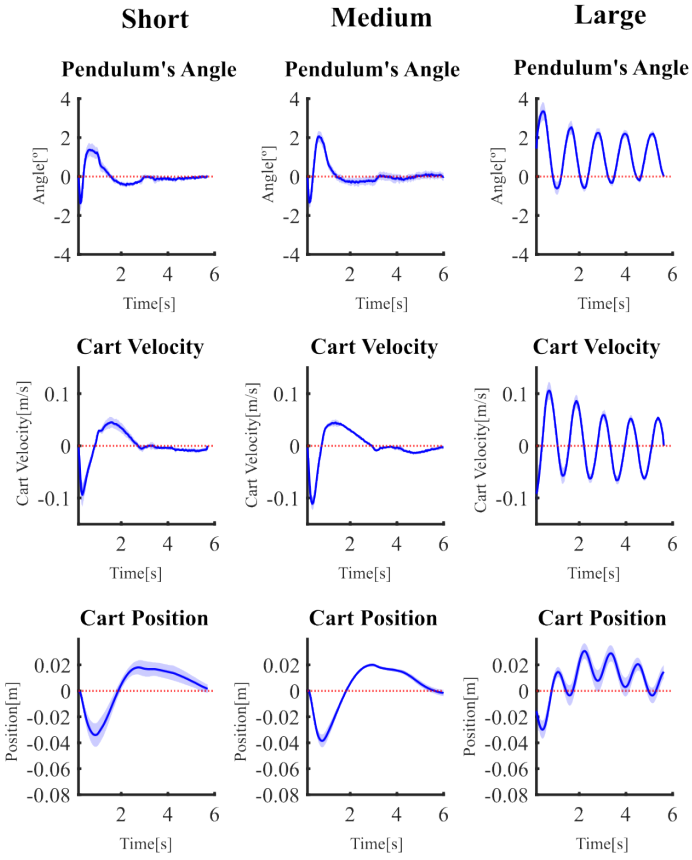


Figure 29: Responses of real, physically position-controlled inverted pendulums (using integral action on cart position) to impulsive disturbances delivered by the tapping mechanism. Results are for all three pendulum lengths in their low damping configurations. The solid blue line represents the mean response averaged across eight aligned recordings, and the light blue shading indicates the corresponding standard deviation.

15.4. Velocity mode results

The pendulum's performance was closely examined while operating under velocity control, as illustrated in Figure 30. The velocity control operation was initiated via the keyboard on the main PC. Users could select a cart velocity, resulting in the cart moving as specified in both left and right directions.

To further evaluate the system's resilience against knocks, representing impulsive disturbances, we conducted an additional test. In this test, the pole was gently tapped while the velocity was set to zero. In all instances, the pendulum system demonstrated notable stability and effectiveness in mitigating the disturbance. Compared to the position control mode, disturbances in the velocity control mode led to uncompensated cart movements, particularly for the short pendulum, as shown in the lowest row of Figure 30. Again, this behavior is also apparent in the YouTube videos. This is also worth noting that using a longer pole again resulted in a modest reduction in performance in velocity control mode, with some cart oscillations observed after the impulsive disturbance. However, this effect was less pronounced than in position control mode.

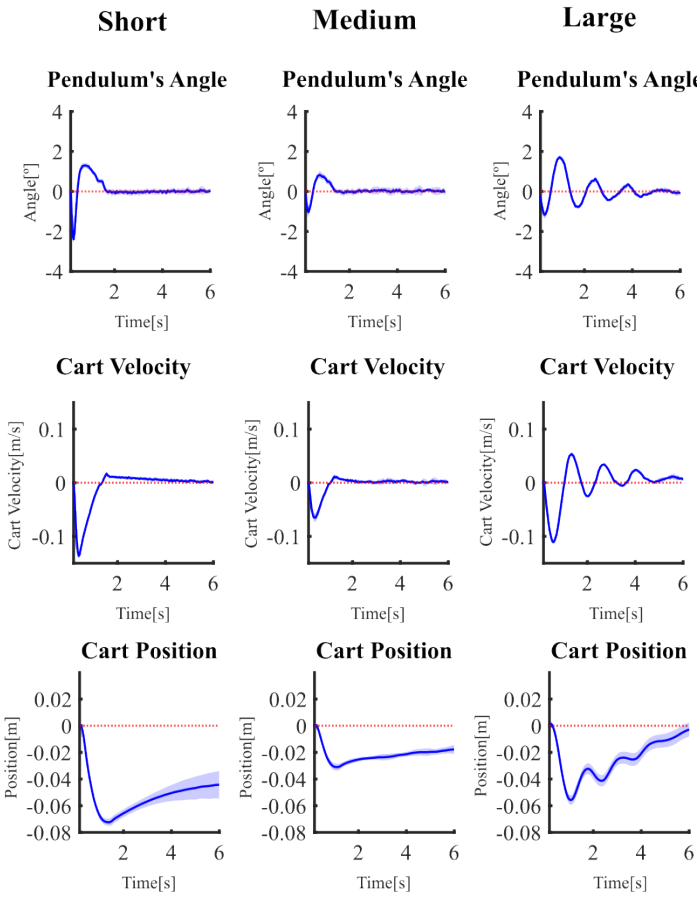


Figure 30: Responses of real, physically velocity-controlled inverted pendulums to impulsive disturbances delivered by the tapping mechanism. Results are for all three pendulum lengths in their low damping configurations. The solid blue line represents the mean response averaged across eight aligned recordings, and the light blue shading indicates the corresponding standard deviation.

16. Discussion

16.1. Summary

In this study, we demonstrated the design, implementation, analysis, simulation, and testing of an inverted pendulum. The mechanical system was built utilizing V-slot rail components and custom 3D printed parts.

Novel features of this work included:

1. The construction of a physical pendulum in which the pole length, viscosity, and resistive friction could be easily modified.
2. The construction of a testing rig, designed to apply consistent taps to the pendulum pole, to evaluate its reaction to impulsive disturbances.
3. Use of system identification to investigate and quantify the pendulum's uncontrolled dynamics as the physical characteristics of the pendulum system were changed.
4. The design of two linear controllers, based on observer-based full state feedback control modes, supporting either velocity or position control of the pendulum cart while balancing the pendulum pole.
5. Performance testing to investigate the pendulum's controlled dynamics as its physical characteristics were changed.

16.2. Uncontrolled pendulum oscillations

We first investigated the behavior of the pendulum in its stable downward inverted configurations. This was done for all three test pendulum pole lengths, as well as under conditions of both high and low static friction and high and low viscous damping. We examined the pendulum's free oscillations following an initial large angle displacement of approximately 90°, and also after initial small angle displacements of about 5°, caused by taps from the tapping mechanism. As expected, increasing the pole length reduced the oscillatory frequency of the pendulum.

Increasing viscosity using the paddle mechanism significantly reduced the decay time of oscillations in the large angle case. In this scenario, the added viscous resistance dominated the pendulum's oscillatory decay, resulting in an exponential reduction in amplitude over time. However, in the small angle condition, where static sliding friction was a significant source of decay, the paddle had minimal effect. This was evidenced by a more linear decay of oscillatory amplitude.

When we increased static friction equally in both the large and small angle cases, the effects differed. In the large angle case, this increase led to a noticeable, albeit modestly more linear, decay of oscillations. Conversely, in the small angle condition, the same level of friction had a dramatic effect, rapidly decelerating oscillations and bringing them to a standstill within just a few cycles.

These observations indicate that the viscous resistance from the paddle is better represented by the square of the movement velocity than by the linear model commonly used in mathematical modeling. This is particularly true since the paddle's effect is significant only during faster movements. Furthermore, at small amplitudes, where the effect of gravity acting on the pole produces minimal torque, any substantial static frictional resistance can dominate the damping behavior.

16.3. System identification

To estimate the pendulums' parameters, we applied a system identification procedure to the small angle dataset. This data best represents the small angle condition occurring during the balancing of the inverted pendulum. We used optimization to fit the predicted pendulum damped oscillatory decay waveform with data recorded from the pendulum in different configurations. We noted that including a friction term in the mathematical model of the non-inverted pendulum was necessary in this process. This addition accounts for the linear aspect of decay and achieves a good fit. The fitting procedure enabled the estimation of the viscous and static friction terms, as well as an updated estimate of the effective pendulum pole length, mass, and moment of inertia.

16.4. Controlled pendulum results

We undertook a sequence of system tests, starting with the standard pendulum pole length for which the controllers were developed. We then investigated how the stabilized pendulum pole responded to light taps from the tapper mechanism, creating impulses. This testing was carried out in both velocity and position control modes. In velocity mode, the cart could be driven with a feedforward velocity command to move left or right while maintaining balance. In position control mode, which operates with integral action on the cart's position, the control system maintains the pendulum's cart at a specified location. We observed distinct behavioral differences between the two control modes.

Unsurprisingly, velocity control, unconcerned with cart position, responded to disturbances to the pendulum pole with balancing movements of the cart, typically causing a positional shift. In position control mode, a disturbance similarly resulted in balancing movement, but the cart gradually returned to its initial position.

Since the cart's movement velocity is limited, any disturbance requiring faster movement would naturally result in a loss of balance. This limitation also affects the balancing robustness in velocity control mode. If the cart is already moving in one direction, its capacity for additional corrective velocity in that direction is restricted.

16.5. Transfer of controller operation to other pole lengths

To assess controller performance, we conducted balancing system tests using both shorter and longer pendulum pole lengths, comparing them to the standard length for which the controllers were developed. We found that the controllers operated well with the shorter length pendulum pole. However, with the longer pendulum pole, we observed some oscillatory behavior of the cart, particularly in position control mode. Despite this, the inverted pendulum balance was still maintained.

We note that the gains for both controller modes, derived from the Linear Quadratic Regulator (LQR) design process, were based solely on experimentation with the standard pendulum. Naturally, there remains a strong likelihood that more optimal controllers for both modes could exist, particularly if they were specifically designed for these varying pendulum lengths.

16.6. Future work

In the current study, we examined the effects of a relatively low-intensity, fixed impulsive disturbance on pendulums using a tapper mechanism. We utilized this setup to assess how the pendulums responded as their characteristics were altered and to observe the behaviors of velocity and position control. These tests did not result in a loss of balance; rather, they only evaluated the reactions necessary to maintain equilibrium. It would be enlightening to apply a wider range of impulse intensities and compare the behaviors related to loss of balance across the various conditions and controllers examined in this study. The existing

tapper mechanism could not be easily adjusted to provide a range of impulse intensities. For future research, constructing a tapper device that employs a motor to drive the tapper rod would be a valuable exercise, allowing for precise control over the impulse intensity.

Currently, we have examined the behavior of two different state feedback controller architectures for balancing a pendulum. Many other control approaches exist, and a comparison with methods such as PID (Proportional-Integral-Derivative) [16,17], and reinforcement learning [22–24], would be informative.

The inverted pendulum has been valuable in understanding human balance while standing [44–52]. Future studies within the framework of our pendulum system could further explore and model human behavior in such tasks. These studies could investigate factors that constrain human performance, including sensory feedback latency, noise in the control and sensory systems, as well as the force, stiffness, and speed of movement characteristics of muscles [68]. Such issues could be readily incorporated into the MATLAB simulations as well as real-time control of the physical pendulum system.

Conflict of Interest

The authors declare no conflict of interest.

Acknowledgment

Support for LAH was provided by the Engineering and Physical Sciences Research Council and The University of Plymouth. ISH was supported by The University of Plymouth. We also thank Jonathan Marsden and Gunnar Schmidtmann in the School of Health Professions at the University of Plymouth, for insightful discussions on this work.

References

[1] L. Alvarez-Hidalgo, I.S. Howard, “Gain scheduling for state space control of a dual-mode inverted pendulum,” in 2022 International Conference on System Science and Engineering (ICSSE), IEEE: 39–46, 2022, doi:10.1109/ICSSE55923.2022.9947361.

[2] P. Horáček, “Laboratory experiments for control theory courses: A survey,” Annual Reviews in Control, **24**, 151–162, 2000, doi:https://doi.org/10.1016/S1367-5788(00)90029-4.

[3] K.H. Lundberg, T.W. Barton, “History of inverted-pendulum systems,” IFAC Proceedings Volumes, **42**(24), 131–135, 2010, doi:https://doi.org/10.3182/20091021-3-JP-2009.00025.

[4] H. Wang, H. Dong, L. He, Y. Shi, Y. Zhang, “Design and simulation of LQR controller with the linear inverted pendulum,” in 2010 international conference on electrical and control engineering, IEEE: 699–702, 2010, doi: 10.1109/iCECE.2010.178.

[5] I. Kafetzis, L. Moysis, “Inverted Pendulum: A system with innumerable applications,” School of Mathematical Sciences, 2017.

[6] O. Boubaker, “The inverted pendulum benchmark in nonlinear control theory: a survey,” International Journal of Advanced Robotic Systems, **10**(5), 233, 2013, doi:https://doi.org/10.5772/55058.

[7] N. Muskinja, B. Tovornik, “Swinging up and stabilization of a real inverted pendulum,” IEEE Transactions on Industrial Electronics, **53**(2), 631–639, 2006, doi:10.1109/TIE.2006.870667.

[8] M. Turner, T.R. Cooley, “A Low-cost and Flexible Open-source Inverted Pendulum for Feedback Control Laboratory Courses,” in 2015 ASEE Annual Conference & Exposition, 26.63. 1-26.63. 13, 2015, doi:DOI:10.18260/p.23404.

[9] K. Kaheman, U. Fasel, J.J. Bramburger, B. Strom, J.N. Kutz, S.L. Brunton, “The experimental multi-arm pendulum on a cart: A benchmark system for chaos, learning, and control,” ArXiv Preprint ArXiv:2205.06231, 2022, doi:https://doi.org/10.48550/arXiv.2205.06231.

[10] F. Grasser, A. D’arrigo, S. Colombi, A.C. Rufer, “JOE: a mobile, inverted pendulum,” IEEE Transactions on Industrial Electronics, **49**(1), 107–114, 2002, doi:10.1109/41.982254.

[11] H. Vasudevan, A.M. Dollar, J.B. Morrell, “Design for control of wheeled inverted pendulum platforms,” Journal of Mechanisms and Robotics, **7**(4), 41005, 2015, doi:https://doi.org/10.1115/1.4029401.

[12] M. Hehn, R. D’Andrea, “A flying inverted pendulum,” in 2011 IEEE International Conference on Robotics and Automation, IEEE: 763–770, 2011, doi:10.1109/ICRA.2011.5980244.

[13] S. Awtar, N. King, T. Allen, I. Bang, M. Hagan, D. Skidmore, K. Craig, “Inverted pendulum systems: rotary and arm-driven-a mechatronic system design case study,” Mechatronics, **12**(2), 357–370, 2002, doi:https://doi.org/10.1016/S0957-4158(01)00075-7.

[14] B. Tomar, N. Kumar, M. Sreejeth, “Optimal Control of Rotary Inverted Pendulum Using Continuous Linear Quadratic Gaussian (LQG) Controller,” in 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), IEEE: 1–6, 2023, doi:10.1109/ICCCNT56998.2023.10306449.

[15] P. Strakoš, J. Tůma, “Mathematical modelling and controller design of inverted pendulum,” in 2017 18th International Carpathian Control Conference (ICCC), IEEE: 388–393, 2017, doi:10.1109/CarpathianCC.2017.7970431.

[16] K. Sultan, A. Mirza, “Inverted Pendulum, Analysis, Design and Implementation,” Visionaries Document, 2003.

[17] K. Razzaghi, A.A. Jalali, “A new approach on stabilization control of an inverted pendulum, using PID controller,” Advanced Materials Research, **403**, 4674–4680, 2012, doi:https://doi.org/10.4028/www.scientific.net/AMR.403-408.4674.

[18] I.S. Howard, “A modular 3D-printed inverted pendulum,” in Towards Autonomous Robotic Systems: 20th Annual Conference, TAROS 2019, London, UK, July 3–5, 2019, Proceedings, Part I 20, Springer: 413–424, 2019, doi:https://doi.org/10.1007/978-3-030-23807-0_34.

[19] C.A. Ibanez, O.G. Frias, M.S. Castanon, “Lyapunov-based controller for the inverted pendulum cart system,” Nonlinear Dynamics, **40**, 367–374, 2005, doi:https://doi.org/10.1007/s11071-005-7290-y.

[20] Y. Yang, P. Wang, T. Zhang, “Modelling and controller design of planar inverted pendulum system,” in 2014 International Conference on Mechatronics, Electronic, Industrial and Control Engineering (MEIC-14), Atlantis Press: 57–61, 2014, doi:10.2991/meic-14.2014.14.

[21] H. Lipson, Robots on the run, 2019, doi:doi: https://doi.org/10.1038/d41586-019-00999-w.

[22] M. Safeea, P. Neto, “A Q-learning approach to the continuous control problem of robot inverted pendulum balancing,” Intelligent Systems with Applications, 200313, 2023, doi:https://doi.org/10.1016/j.iswa.2023.200313.

[23] Y. Ma, D. Xu, J. Huang, Y. Li, “Robust Control of An Inverted Pendulum System Based on Policy Iteration in Reinforcement Learning,” Applied Sciences, **13**(24), 13181, 2023, doi:https://doi.org/10.3390/app132413181.

[24] S. Israilov, L. Fu, J. Sánchez-Rodríguez, F. Fusco, G. Allibert, C. Raufaste, M. Argentina, “Reinforcement learning approach to control an inverted pendulum: A general framework for educational purposes,” PLoS One, **18**(2), e0280071, 2023, doi:https://doi.org/10.1371/journal.pone.0280071.

[25] M. Deisenroth, C.E. Rasmussen, “PILCO: A model-based and data-efficient approach to policy search,” in Proceedings of the 28th International Conference on machine learning (ICML-11), 465–472, 2011.

[26] C.W. Anderson, “Learning to control an inverted pendulum using neural networks,” IEEE Control Systems Magazine, **9**(3), 31–37, 1989, doi:10.1109/37.24809.

[27] V. Mladenov, G. Tsenov, L. Ekonomou, N. Harkiolakis, P. Karampelas, “Neural network control of an inverted pendulum on a cart,” in WSEAS International Conference. Proceedings. Mathematics and Computers in Science and Engineering, World Scientific and Engineering Academy and Society, 2009.

[28] A. Suresh, M.P.F. Queen, V.A.T.P. Symon, A. Linsely, “Control and stabilization of inverted pendulum using GA based controller,” International Journal of Mechanical Engineering and Technology, **8**(8), 748–756, 2017.

[29] S. Omatu, S. Deris, “Stabilization of inverted pendulum by the genetic algorithm,” in Proceedings of IEEE international conference on evolutionary computation, IEEE: 700–705, 1996, doi:10.1109/ICEC.1996.542687.

[30] E.S. Sazonov, P. Klinkhachorn, R.L. Klein, "Hybrid LQG-neural controller for inverted pendulum system," in Proceedings of the 35th Southeastern Symposium on System Theory, 2003., IEEE: 206–210, 2003, doi:10.1109/SSST.2003.1194559.

[31] P. Kumar, K. Chakraborty, R.R. Mukherjee, S. Mukherjee, "Modelling and controller design of inverted pendulum," International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), **2**(1), 2013.

[32] W. Zhong, H. Rock, "Energy and passivity based control of the double inverted pendulum on a cart," in Proceedings of the 2001 IEEE International Conference on Control Applications (CCA'01)(Cat. No. 01CH37204), IEEE: 896–901, 2001, doi:10.1109/CCA.2001.973983.

[33] J. Baek, C. Lee, Y.S. Lee, S. Jeon, S. Han, "Reinforcement learning to achieve real-time control of triple inverted pendulum," Engineering Applications of Artificial Intelligence, **128**, 107518, 2024, doi:https://doi.org/10.1016/j.engappai.2023.107518.

[34] W. An, Y. Li, "Simulation and control of a two-wheeled self-balancing robot," in 2013 IEEE International Conference on Robotics and Biomimetics (ROBIO), IEEE: 456–461, 2013, doi:DOI: 10.1109/ROBIO.2013.6739501.

[35] M. Hasan, C. Saha, M.M. Rahman, M.R.I. Sarker, S.K. Aditya, "Balancing of an inverted pendulum using PD controller," Dhaka University Journal of Science, **60**(1), 115–120, 2012, doi:DOI: 10.3329/dujs.v60i1.10348.

[36] H.-S. Juang, K.-Y. Lum, "Design and control of a two-wheel self-balancing robot using the arduino microcontroller board," in 2013 10th IEEE International Conference on Control and Automation (ICCA), IEEE: 634–639, 2013, doi:DOI: 10.1109/ICCA.2013.6565146.

[37] S. Wang, L. Cui, J. Zhang, J. Lai, D. Zhang, K. Chen, Y. Zheng, Z. Zhang, Z.-P. Jiang, "Balance control of a novel wheel-legged robot: Design and experiments," in 2021 IEEE International Conference on Robotics and Automation (ICRA), IEEE: 6782–6788, 2021, doi:10.1109/ICRA48506.2021.9561579.

[38] K. Darvish, L. Penco, J. Ramos, R. Cisneros, J. Pratt, E. Yoshida, S. Ivaldi, D. Pucci, "Teleoperation of humanoid robots: A survey," IEEE Transactions on Robotics, 2023, doi:10.1109/TRO.2023.3236952.

[39] A. Bratta, M. Focchi, N. Rathod, C. Semini, "Optimization-Based Reference Generator for Nonlinear Model Predictive Control of Legged Robots," Robotics, **12**(1), 6, 2023, doi:https://doi.org/10.3390/robotics12010006.

[40] J.A. Castano, J. Humphreys, E. Mingo Hoffman, N. Fernández Talavera, M.C. Rodriguez Sanchez, C. Zhou, "Benchmarking Dynamic Balancing Controllers for Humanoid Robots," Robotics, **11**(5), 114, 2022, doi:https://doi.org/10.3390/robotics11050114.

[41] S. Kajita, M. Morisawa, K. Miura, S. Nakaoka, K. Harada, K. Kaneko, F. Kanehiro, K. Yokoi, "Biped walking stabilization based on linear inverted pendulum tracking," in 2010 IEEE/RSJ International Conference on Intelligent Robots and Systems, IEEE: 4489–4496, 2010, doi:10.1109/IROS.2010.5651082.

[42] D.A. Winter, "Human balance and posture control during standing and walking," Gait & Posture, **3**(4), 193–214, 1995, doi:https://doi.org/10.1016/0966-6362(96)82849-9.

[43] F. Quijoux, A. Nicolaï, I. Chairi, I. Bargiotas, D. Ricard, A. Yelnik, L. Oudre, F. Bertin-Hugault, P. Vidal, N. Vayatis, "A review of center of pressure (COP) variables to quantify standing balance in elderly people: Algorithms and open-access code," Physiological Reports, **9**(22), e15067, 2021, doi:https://doi.org/10.14814/phy2.15067.

[44] P. Gawthrop, I. Loram, M. Lakie, H. Gollee, "Intermittent control: a computational theory of human control," Biological Cybernetics, **104**, 31–51, 2011, doi:https://doi.org/10.1007/s00422-010-0416-4.

[45] I.D. Loram, H. Gollee, C. van de Kamp, P.J. Gawthrop, "Is Intermittent Control the Source of the Non-Linear Oscillatory Component (0.2–2Hz) in Human Balance Control?," IEEE Transactions on Biomedical Engineering, **69**(12), 3623–3634, 2022, doi:10.1109/TBME.2022.3174927.

[46] J.G. Milton, "Time delays and the control of biological systems: An overview," IFAC-PapersOnLine, **48**(12), 87–92, 2015.

[47] J. Milton, J.L. Cabrera, T. Ohira, S. Tajima, Y. Tonosaki, C.W. Eurich, S.A. Campbell, "The time-delayed inverted pendulum: implications for human balance control," Chaos: An Interdisciplinary Journal of Nonlinear Science, **19**(2), 2009, doi:https://doi.org/10.1063/1.3141429.

[48] A. Kot, A. Nawrocka, "Modeling of human balance as an inverted pendulum," in Proceedings of the 2014 15th International Carpathian Control Conference (ICCC), IEEE: 254–257, 2014, doi:10.1109/CarpathianCC.2014.6843607.

[49] I.D. Loram, M. Lakie, "Human balancing of an inverted pendulum: position control by small, ballistic-like, throw and catch movements," The Journal of Physiology, **540**(3), 1111–1124, 2002, doi:https://doi.org/10.1113/jphysiol.2001.013077.

[50] J.-L. Sung, C.-Y. Hong, C.-H. Liu, P. Lee, L.-Y. Guo, N.-H. Lin, C.-W. Yen, L.-J. Liaw, "Characterizing the validity of the inverted pendulum model for quiet standing," Journal of Healthcare Engineering, **2021**, 1–6, 2021, doi:https://doi.org/10.1155/2021/8884614.

[51] I.D. Loram, H. Gollee, M. Lakie, P.J. Gawthrop, "Human control of an inverted pendulum: is continuous control necessary? Is intermittent control effective? Is intermittent control physiological?," The Journal of Physiology, **589**(2), 307–324, 2011, doi:https://doi.org/10.1113/jphysiol.2010.194712.

[52] P. Morasso, A. Cherif, J. Zenzeri, "Quiet standing: The single inverted pendulum model is not so bad after all," PLoS One, **14**(3), e0213870, 2019, doi:https://doi.org/10.1371/journal.pone.0213870.

[53] S. Franklin, J. Česonis, D.W. Franklin, "Influence of visual feedback on the sensorimotor control of an inverted pendulum," in 2018 40th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), IEEE: 5170–5173, 2018, doi:10.1109/EMBC.2018.8513461.

[54] J. Česonis, S. Franklin, D.W. Franklin, "A simulated inverted pendulum to investigate human sensorimotor control," in 2018 40th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), IEEE: 5166–5169, 2018, doi:10.1109/EMBC.2018.8513434.

[55] R. Leib, J. Česonis, S. Franklin, D.W. Franklin, "LQG framework explains performance of balancing inverted pendulum with incongruent visual feedback," in 2019 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), IEEE: 1940–1943, 2019.

[56] S. Franklin, J. Česonis, R. Leib, D.W. Franklin, "Feedback delay changes the control of an inverted pendulum," in 2019 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), IEEE: 1517–1520, 2019, doi:10.1109/EMBC.2019.8856897.

[57] F. Ghorbani, M.A. Shooredeli, M. Teshnehlab, "Fault tolerant improvement with chaos synchronization using Fuzzy-PID control," in 2013 13th Iranian Conference on Fuzzy Systems (IFSC), IEEE: 1–5, 2013, doi:10.1109/IFSC.2013.6675645.

[58] M.F. Hamza, H.J. Yap, I.A. Choudhury, A.I. Isa, A.Y. Zimit, T. Kumbasar, "Current development on using Rotary Inverted Pendulum as a benchmark for testing linear and nonlinear control algorithms," Mechanical Systems and Signal Processing, **116**, 347–369, 2019, doi:https://doi.org/10.1016/j.ymssp.2018.06.054.

[59] M.H. Raibert, H.B. Brown Jr, "Experiments in balance with a 2D one-legged hopping machine," 1984, doi:https://doi.org/10.1115/1.3149668.

[60] H.-S. Juang, K.-Y. Lum, "Design and control of a two-wheel self-balancing robot using the arduino microcontroller board," in 2013 10th IEEE International Conference on Control and Automation (ICCA), IEEE: 634–639, 2013.

[61] S. Monteleone, F. Negrello, G. Grioli, M.G. Catalano, A. Bicchi, M. Garabini, "A method to benchmark the balance resilience of robots," Frontiers in Robotics and AI, **9**, 2022, doi:https://doi.org/10.3389/frobt.2022.817870.

[62] J.C. Simbach, J. Priest, "Another look at a damped physical pendulum," American Journal of Physics, **73**(11), 1079–1080, 2005, doi:http://dx.doi.org/10.1119/1.1858488.

[63] L.F. da C. Zonetti, A.S.S. Camargo, J. Sartori, D.F. De Sousa, L.A. de O. Nunes, "A demonstration of dry and viscous damping of an oscillating pendulum," European Journal of Physics, **20**(2), 85, 1999, doi:DOI: 10.1088/0143-0807/20/2/004.

[64] I.R. Lapidus, "Motion of a harmonic oscillator with sliding friction," Am. J. Phys, **38**(11), 1360–1361, 1970, doi: http://dx.doi.org/10.1119/1.1976111.

[65] M.I. Molina, "Exponential versus linear amplitude decay in damped oscillators," The Physics Teacher, **42**(8), 485–487, 2004, doi:http://dx.doi.org/10.1119/1.1814324.

[66] K.J. Åström, R.M. Murray, Feedback systems: an introduction for scientists and engineers, Princeton university press, 2021.

[67] C.B. Moler, Numerical computing with MATLAB, SIAM, 2004.

[68] D.W. Franklin, D.M. Wolpert, "Computational mechanisms of sensorimotor control," Neuron, **72**(3), 425–442, 2011, doi:10.1016/j.neuron.2011.10.006.

ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 8, No. 6, 144-154 (2023)

www.astesj.com

Special Issue on Innovation in Computing, Engineering Science & Technology

ASTESJ

ISSN: 2415-6698

Optimizing the Performance of Network Anomaly Detection Using Bidirectional Long Short-Term Memory (Bi-LSTM) and Over-sampling for Imbalance Network Traffic Data

Toya Acharya*, Annamalai Annamalai, Mohamed F Chouikha

Electrical and Computer Engineering, Prairie View A & M University, Prairie View, Texas,77446, USA

ARTICLE INFO

Article history:
Received: 07 November, 2023
Accepted: 22 December, 2023
Online: 30 December, 2023

Keywords:
Network Anomaly Detection
Sampling
Machine Learning
Deep learning
Bidirectional-LSTM
NSL-KDD
Random Under Sampling (RUS)
Random Over Sampling (ROS)
SMOTE
Data Imbalance

ABSTRACT

Cybercriminal exploits integrity, confidentiality, and availability of information resources. Cyberattacks are typically invisible to the naked eye, even though they target a wide range of our digital assets, such as internet-connected smart devices, computers, and networking devices. Implementing network anomaly detection proves to be an effective method for identifying these malicious activities. The traditional anomaly detection model cannot detect zero-day attacks. Hence, the implementation of the artificial intelligence method overcomes those problems. A specialized model, known as a recurrent neural network (RNN), is specifically crafted to identify and utilize sequential data patterns to forecast upcoming scenarios. The random selection of hyperparameters does not provide an efficient result for the selected dataset. We examined seven distinct optimizers: Nadam, Adam, RMSprop, Adamax, SGD, Adagrad, and Ftrl, with variations in values of batch size, epochs, and the data split ratio. Our goal is to optimize the performance of the bidirectional long short-term memory (Bi-LSTM) anomaly detection model. This optimization resulted in an exceptional network anomaly detection accuracy of 98.52% on the binary NSL-KDD dataset. Sampling techniques deal with the data imbalance problem. Random under-sampling, which involved removing data from the majority classes to create a smaller dataset, was less efficient for deep learning models. In contrast, the Synthetic Minority Oversampling Technique (SMOTE) successfully generated random data related to the minority class, resulting in a balanced NSL-KDD multiclass dataset with 99.83% Bi-LSTM model detection accuracy. Our analysis discovered that our Bidirectional LSTM anomaly detection model outperformed existing anomaly detection models compared to the performance metrics, including precision, f1-score, and accuracy.

1. Introduction

This paper is an extension of "Efficacy of Bidirectional LSTM Model for Network-Based Anomaly Detection" [1] presented at the conference IEEE 13th Symposium on Computer Applications & Industrial Electronics (ISCAIE) in 2023.

Information technology has revolutionized how essential data is conveyed, utilizing bits to transfer a wide range of information from one point to another. This transmitted data can encompass diverse forms, such as voice, images, or data, including sensitive details like banking information, personal records, and network traffic. Numerous tools and techniques are available to identify and thwart unauthorized access.

Anomaly is an unusual pattern present in the dataset. Some techniques or methods are required to detect those anomalies from the dataset. The anomaly is also called the outliers during the study of anomaly detection. Anomaly detection is used in large fields to sense abnormal patterns, such as in business, network attack detection, monitoring health conditions, detecting fraud credit card transactions, and detecting malicious activities in mission-critical systems. Detecting anomalies is critical in cyber security for achieving solid safeguards against cyber criminals. Figure 1. provides brief information about the taxonomy of anomaly detection methods [2].

The security of information resources is ensured when the three fundamental principles of computer security—confidentiality, integrity, and availability (CIA)—are appropriately obeyed [3]. An intrusion detection system is a mechanism used to monitor and scrutinize computer or network- related activities to identify potential threats by assessing the frequency at which computer security guidelines are violated based on confidentiality, integrity, and availability. Intrusion is any unwelcome and illegal activity within an organization's internet-connected end terminal or

*Corresponding Author: Toya Acharya, tacharya@pvamu.edu

https://dx.doi.org/10.25046/aj080614

network-connected devices. These illegal activities aim to gain entry to a business computer or network device. An alternative term for intrusion is a malicious activity that disrupts the fundamental principles of information resource protection known as the CIA triad. An intrusion detection system examines computer network and host activities, pinpointing dubious traffic and abnormalities. Intrusion detection and prevention systems scrutinize traffic from both internal and external sources to identify potentially malicious actions.

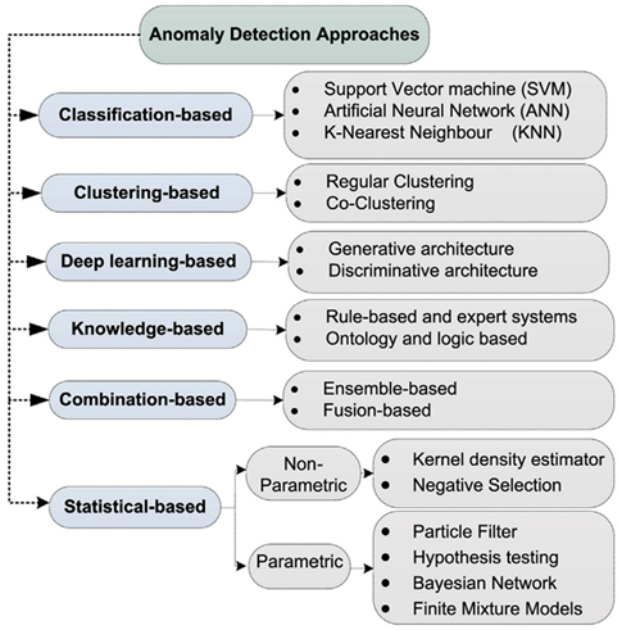


Figure 1: Taxonomy of Anomaly Detection [2]

Detection of misuse and/or intrusion involves identifying potentially suspicious activities within a network or on hosts. Misuse detection focuses on recognizing deviations from established rules by individuals with valid system access rather than actual intrusions. For instance, when an employee uses the Internet for personal purposes in violation of company policy, it constitutes a misuse intrusion. In contrast, intrusion detection is designed to identify unauthorized individuals, such as external hackers or government spies, who lack authorized system access. The intrusion detection system primarily focuses on spotting ongoing intrusions within the system or network but does not proactively prevent malicious activities.

There are two main types of methods for detecting intrusions: signature-based systems, known as SIDS, and anomaly-based systems, referred to as AIDS. Anomaly detection systems are further categorized into network-related and host-related intrusion detection systems. The identification of normal or anomalous data in anomaly detection techniques is achieved through the utilization of labels.

A SIDS identifies suspicious activities through pattern matching with known external attack patterns, which fall into two categories: misuse detection and knowledge-based detection. This anomaly detection model compares the recent signature with a previously stored signature in its database. When a match occurs between these signatures, the IDS signals the presence of malicious activities within the network. Regular updates to the signature database are crucial to effectively detect malicious activities in a network. However, it's important to note that this type of detection system cannot identify zero-day attacks, as these novel attack types may not yet be contained in the signature archive. This anomaly detection model delivers optimal detection outcomes for recognized signatures associated with malicious activities. This type of anomaly detection model is known for its straightforward configuration and comprehensibility. Widely adopted intrusion detection systems include Snort and NetSTAT. In the traditional setup, the SIDS examines network packets and matches them against stored signatures. However, newly introduced attacks not yet included in the signature database can reduce intrusion detection accuracy. To address these limitations, the anomaly-based anomaly detection model offers enhancements and boosts the overall anomaly detection rate. The anomaly-based intrusion detection approach is designed to identify malicious and unreliable network exploitation activities within the corporation.

AIDS effectively addresses the limitations included in SIDS approaches. Likewise, the anomaly-based intrusion model leverages statistical-based, machine learning, and knowledge-based techniques to model the typical behaviors of network traffic. An "anomaly" refers to any behavior that deviates from these established norms, and such traffic anomalies can harm computers and network devices. Anomaly-based detection can occasionally yield false results due to shifts in user behavior. AIDS can generate errors even when legitimate users alter their usual habits. This approach comprises two key stages: the testing and the training stages. In the training stage, the model is trained using normal traffic data to establish a baseline or "normal profile." In the testing stage, previously unseen data is employed to evaluate the model's performance. The primary benefit of this methodology is its ability to detect zero-day attacks.

Three distinct anomaly detection methods include unsupervised, semi-supervised, and supervised anomaly detection methods based on the target class. AIDS addresses the limitations of SIDS by employing knowledge-based methods, machine learning, and statistical-based to model normal behaviors. Figure 1 outlines the various approaches to anomaly detection [2].

Deep learning has the capability to generate improved representations, enhancing the development of effective anomaly detection models. In contrast, conventional machine learning algorithms for network-related abnormality detection are more appropriate for smaller datasets and often rely on performance influenced by the implementation of feature engineering. The model benchmark indicators of conventional anomaly detection models are significantly influenced by the split ratio. While these conventional ML methods are uncomplicated and require minimal resources, they face limitations when dealing with extensive datasets and large feature sets, making them unsuitable for tasks such as machine vision, image translation, natural language processing, and similar applications.

The convolutional neural network is primarily employed for computer vision using image datasets, with the lower layers' neurons responsible for feature reduction. These lower layers typically recognize image corners, boundaries, and intensity called small-scale features. As the information progresses to higher

layers, the network integrates these lower-level features to create forms, basic shapes, and partial objects. The final layer of the network amalgamates these lower-level features to generate the output. LSTM operates distinctively from a CNN as it is commonly applied for processing and predicting outcomes based on sequential data. Unlike CNNs, Recurrent Neural Networks (RNNs), including LSTMs, were specifically designed to preserve long-range information within a sequence, preventing the loss of important details in lengthy sequences. The Bidirectional LSTM (BiLSTM) enhances this by introducing an additional LSTM layer that reverses the flow of information, effectively addressing issues such as vanishing gradients.

The deep learning methodology tackles challenges inherent in conventional machine learning, specifically its ability to handle extensive datasets and numerous features. The efficacy of anomaly detection algorithms based on deep learning depends on various factors, including the choice of hidden layers, determination of activation function, neurons, batch size, and epochs during both model training and testing. Strategic decisions regarding these hyperparameters, along with considerations for the ratio of the train to test data and the design of deep neural networks, are essential for improving the precision of network anomaly detection systems.

In addition to fine-tuning hyperparameters, handling imbalanced data is vital, and creating a balanced dataset using various sampling methods contributes to improved anomaly detection. Under-sampling reduces data size, posing challenges for deep learning models. At the same time, over-sampling methods generate duplicate random data, proving more effective for deep learning models to improve the anomaly detection performance in network-based anomaly detection models.

2. Literature Review

The continuous generation of data generates big data and poses challenges for traditional machine learning algorithms, requiring extensive feature engineering efforts to perform adequately. Deep learning significantly enhances detection performance in such scenarios. However, the effectiveness of network anomaly detection varies on numerous factors, with the nature of the dataset (whether balanced or unbalanced), the hyperparameter of the neural network, the amount of model train and test data, and the architecture of the neural network in the deep learning model. These elements collectively play a crucial role in successfully identifying anomalies in the network.

In their study, the researchers utilized the Bidirectional LSTM to alleviate the considerable requirements for feature reduction inherent in conventional machine learning-based anomaly detection approaches [4]. Additionally, they implemented data augmentation in data preprocessing of minor attacks user to root (U2R) and root to local (R2L) to create a well-adjusted NSL-KDD. This methodology resulted in higher anomaly detection accuracy of 90.73% and f1-scores of 89.65%.

In their study, presented an algorithm for network intrusion detection that integrated a deep hierarchical network with hybrid sampling, incorporating SMOTE to create a balanced dataset [5]. They utilized a hybrid approach that combined CNN and Bi-LSTM for anomaly detection accuracy of 83.58% on NSL-KDD and 77.16% on UNSW-NB15.

In their study, presented a method utilizing bidirectional generative adversarial networks (Bi-GAN) on the CIC-DDoS2019 and NSL-KDD datasets [6]. The Bi-GAN model exhibited strong performance, particularly on the imbalanced NSL-KDD, achieving an f1-score of 92.68% and an accuracy of 91.12%. The Bi-GAN approach was employed to enhance the performance of the NSL-KDD imbalance dataset.

In their study, implemented a new method involving auxiliary classifier generative adversarial network (ACGAN) and ACGAN with SVM to tackle data unevenness concerns by leveraging GAN to produce synthetic attack network traffic for intrusion detection systems [7]. These artificially generated attacks were merged with the existing data, resulting in an extended dataset. Research carried out on the RAWDATA, CICIDS2017, UNSW-NB15, and NSL-KDD showed that among the support vector machine, decision tree, and random forest models, the decision tree achieved a superior f1-score of 92% on the balanced NSL-KDD dataset.

In [8], researchers utilized an assorted ensemble-aided approach to binary and multi-class network anomaly detection models to tackle the challenge of uneven traffic data in network traffic-related datasets, including NSL-KDD, UNSW-NB15, and KDD99 datasets. This approach achieved a true positive rate and area under the ROC curve of 94.5% and 96.2% on the NSL-KDD, respectively.

According to their finding, the authors [9] concluded that the efficiency of the anomaly detection algorithm is improved when the number of output labels is reduced. This observation was explored across different conventional machine learning algorithms, including Naïve Bayes, J48, random forest, bayesinNet, bagging, and bayesinNet. The evaluation used three network datasets: KDD99, CICIDS2017_Thrusday, and UNSW-NB15.

In [10], the researchers observed the effectiveness of a recurrent neural network-based intrusion detection system (RNN-IDS) in multi-class and binary-class scenarios. Performance on the NSL-KDD was observed, which is affected by the number of neurons and different learning rates. Experimental outcomes illustrated that RNN-IDS is adept at constructing a classification approach with high accuracy, outperforming traditional machine learning classification methods, including random forest, artificial neural network, J48, and support vector machine in both multiclass and binary network intrusion-related datasets. In their publication [11], presented a network anomaly detection technique utilizing a convolutional autoencoder and attained a model accuracy of 96.87% on the NSL-KDD. The convolutional autoencoder methodology was utilized to simplify and determine the most significant features of the network anomaly dataset.

In [12], the authors investigated the usefulness of several autoencoders in detecting network anomalies. They compared four different types of autoencoders, including sparse autoencoders, undercomplete deep autoencoders, and denoising autoencoders, using the NSL-KDD. Sparse deep denoising autoencoder yielded a model accuracy of 89.34% compared with other models.

In [13], the authors presented a model centered around a 5-layer autoencoder (AE) tailored for network abnormality detection. The fine-tuned model designs demonstrated proficiency in attribute learning and the dimension of data reduction, resulting in improved performance metrics, including model accuracy and f1-score. The model produces the highest accuracy and f1-score of 90.61% and 92.26% on the NSL-KDD, respectively. The researchers employed the reconstruction error to determine whether the network traffic is regular or attacked.

In [14], [15], the researchers proposed a network anomaly detection approach with a combination of convolutional neural networks and bidirectional LSTM applied to the KDD99. They explored the influence of the number of nodes, the number of hidden layers and memory elements on it, and the number of epochs to improve their anomaly detection model accuracy. The performance metrics of different models, such as J48, k-nearest neighbors, NB, deep forest, RF, and convolutional neural network combined with bidirectional LSTM, were evaluated. The convolutional neural network bidirectional LSTM exhibited the ultimate model detection accuracy of 95.40%.

In [16], the researchers assessed both single-layer and four-layer LSTM models for weather forecasting, utilizing a weather-related dataset from Hang Nadim Indonesia Airport. The top model validation accuracy of 80.60%. The four hidden layers comprise 50, 90, 100, and 200 memory elements. The split ratio for testing and training dataset was used at 0.30, and the models underwent training for 500 epochs.

The researchers in [17] adopted a deep learning approach utilizing bidirectional LSTM, implemented on the UNSW-NB15 and KDDCUP99, and achieved notable outcomes with a 99% accuracy rate for both datasets. Numerous current models encounter difficulties in effectively detecting uncommon attack traffic types, notably user-to-root and remote-to-local traffic, which often demonstrate lower detection accuracy than other types of attacks. The researchers in [18] deployed an intrusion detection system based on bidirectional LSTM to address the mentioned encounters on the NSL-KDD. This anomaly detection approach, utilizing Bi-LSTM, achieved a model detection accuracy of 94.26 % for binary NSL-KDD data.

The study in [19] delved into the influence of batch size and learning rates on the performance of CNN, focusing on image classification, particularly in the context of medical images. The results indicate that a larger batch size does not necessarily lead to higher accuracy. Moreover, the choice of learning rate and optimizer significantly affects performance. The authors found that reducing the learning rate and batch size, particularly during fine-tuning, enhances the network's training effectiveness.

Diverse strategies were implemented to address the challenge of data imbalance, encompassing techniques such as data augmentation discussed in [4], application of SMOTE detailed in [5], the use of GAN technology explored in [6], [7], the assistance of Heterogeneous ensemble methods investigated in [8], and the reduction of the target class by combining smaller classes into a new category as discussed in [9]. A considerable number of research endeavors in the realm of deep learning for network anomaly detection have been scrutinized, incorporating methodologies like RNNIDS outlined in [10], CAE featured in [11], Autoencoder examined in [12], multilayer AE explored in [13], convolutional neural network combined with bidirectional LSTM hybrid methods presented in [14] and Bi-LSTM discussed in [17]-[18].

The researchers in [17] and [18] did not provide details on data pre-processing, the train-test split ratio, or adopting bidirectional LSTM hyper-parameters in their model study. Similarly, the researchers in [16] conducted weather forecasting using Bi-LSTM without specifying the hyperparameter values. In [10], there was no analysis information on epochs and the train test split ratio for the KDDTrain+ dataset. Most of the literature reviewed emphasizes enhancing model accuracy in conventional or deep learning algorithms. However, there is a notable lack of focus on deciding on hyper-parameters in deep learning approaches, determining the train test split ratio, and defining the architecture of neural networks. Some researchers do not clarify how these values are applied in their work. Consequently, our research aims to address these limitations in the network anomaly detection approaches by conducting experiments on NSL-KDD.

3. Contributions

The literature review examines a gap in the existing network intrusion detection systems during anomaly detection. The primary contribution of this research is to bridge this gap by proposing network anomaly detection models specifically tailored for imbalanced multiclass datasets.

Arbitrarily selection of hyperparameters does not yield efficient anomaly detection performance on the given dataset. This research investigates the impact of epochs, batch size, and optimizers on the efficacy of a bidirectional LSTM anomaly detection model using the multiclass NSL-KDD.

The choice of the amount of training data and testing data also influences the model's performance. A larger training dataset requires a longer training time, whereas a smaller dataset leads to quicker model training. The model's efficacy is contingent on the data size utilized for both training and testing, a factor we explored by adjusting the test train split ratio to enhance the performance of network traffic anomaly detection on the NSL-KDD.

More layers add complexity to the neural network-based model. The program execution time (program training and testing time) is large compared to small numbers of neural network layers and memory elements. The memory elements and layers in the neural network architecture influence the network anomaly detection performance. Investing layers and memory elements of neural networks improves the bidirectional LSTM on the NSL-KDD.

The careful choice of machine learning and/or deep learning algorithms significantly impacts the effectiveness of network anomaly detection. This study introduces the creation and deployment of a network traffic anomaly detection system utilizing a bidirectional LSTM-based recurrent neural network model. The developed model demonstrates a remarkable anomaly detection accuracy of 98.52 % in the network, particularly for the binary NSL-KDD.

The primary challenge when dealing with real datasets is the presence of imbalanced data. Various approaches can be employed

to address this issue. In the NIDS multiclass dataset, both under-sampling and over-sampling methods are applied to tackle data imbalance. Notably, oversampling methods proved to be more effective, achieving the highest detection accuracy of 99.83% for the multiclass NSL-KDD datasets.

4. Model Description

The proposed model consists of different steps, which are listed:

1. Data collection and modelling
2. Data cleaning and pre-processing
3. Bidirectional LSTM model preparation
4. Model training and testing
5. Evaluation model
6. Compare the model for decision

Figure 3 illustrates the schematic for the model based on Bidirectional LSTM. More elaborate explanations of the methods outlined above for the proposed model will be provided in the following sections.

4.1. Data Collection and Modelling

During this study, we employed the KDDTrain+ dataset, one of the subset data from the NSL-KDD.

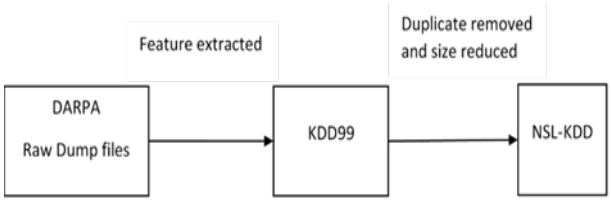


Figure 2: DARPA, KDD99, and NSL-KDD Datasets

The NSL-KDD data is derived from the DARPA KDD99 data, as depicted in Figure 2, after the removal of noise and unwanted data. This includes the complete training data from the NSL-KDD set, including features named attack_type and difficulty. It encompasses 41 attributes and covers five separate attack categories: denial of service, normal, remote_to_local, probe, and user_to_root. NSL-KDD [20] represents an enhanced version of the KDD99 network traffic anomaly data, eliminating duplicate entries in the training data and ensuring the absence of repeated records in the test data. The KDDTrain+ dataset comprises 125,973 records and includes 41 attributes. Notably, this is balanced, with 53.46% of total traffic being normal and 46.54% of total traffic entry being abnormal. We picked this data because it is balanced data between normal and abnormal traffic records within the subset, making it suitable for binary network anomaly detection data. Those numbers of attack class information from the NSL-KDD data were utilized to create the multiclass dataset for the experiment, detailed in the data pre-processing section.

4.2. Data Cleaning and pre-processing

The KDDCup99 data is widely employed in experiments related to anomaly detection in computer network traffic. It consists of network-related traffic that transfers from the virtual network environment utilized for the third knowledge discovery and data mining tools competition. The KDD99 network traffic data is a revision of the 1998 DARPA. The KDDCup99 dataset comprises three components: the "Whole" dataset, the "10% KDD," and the "Corrected KDD." The "Whole" dataset encompasses various attack traffic and one normal network traffic connection. This data involves two training data subsets: a full training data subset and a 10% training data subset. The "Whole" dataset consists of 4,898,431 individual records containing 41 attributes labeled as normal or an attack.

As indicated in reference [20], the KDD99 dataset encompasses 22 distinct attack traffic categorized into four classes: Denial of Service, Unauthorized Access to Local Privileges (U2R), Unauthorized Remote Machine Access (R2L), and Scan Network (Probe). The NSL-KDD data contains four sub-datasets, including KDDTest-21, KDDTest+, KDDTrain+_20Percent, and KDDTrain+. Notably, the KDDTrain+_20Percent and KDDTest-21 portions are sub-datasets derived from the KDDTest+ and KDDTrain+, respectively.

The KDDTrain+ dataset is designated as the training dataset, while the KDDTest+ dataset serves as the testing dataset for the machine learning model. KDDTest-21 is a subset of the test dataset that excludes the most challenging traffic records (with a score of 21), and KDDTrain+_20Percent is a subset of the training dataset, encompassing 20% of the entire training dataset. It's important to note that the traffic records found in KDDTest-21 and KDDTrain+_20Percent are already included in the test and train datasets, respectively. The NSL-KDD dataset addresses the limitations found in the KDD'99 dataset. Unlike KDD'99, NSL-KDD ensures the absence of redundant values in both the train and test datasets.

Notably, NSL-KDD is advantageous due to its smaller test and train sets, eliminating the need for random selection of a small data subset, thus making experiments more cost-effective. Each record in the NSL-KDD dataset comprises 42 features, with 41 of them corresponding to the traffic input and the final label denoted as either "normal" or "abnormal." In the KDDTrain+ contains 125,973 total network traffic records and 41 generated attributes, the data cleaning and pre-processing assigns a target label of ‘1’ for normal traffic and ‘0’ for attack traffic records, transforming the multiclass network traffic data into a binary class.

achine learning and deep learning algorithms work only for numeric values, so ‘'protocol_type,' 'service,' and 'flag' are categorical attributes transformed into numeric values, either ‘0’ or ‘1’ using one hot encoding method called dummy one hot encoding. The dataset is then normalized using the standard scalar method. Correlation-based feature reduction is also implemented where those features with a correlation factor exceeding 0.5 are preserved to reduce the features. Binary class data is employed in experiments A to E. In experiment F, the multiclass (class 5) version of the NSL-KDD dataset is utilized. Prior to training and testing the BI-LSTM model, a sampling method is applied to balance the unbalanced multiclass data. Further details on data preprocessing and model information can be found in the experimental section in the subsequent chapter.

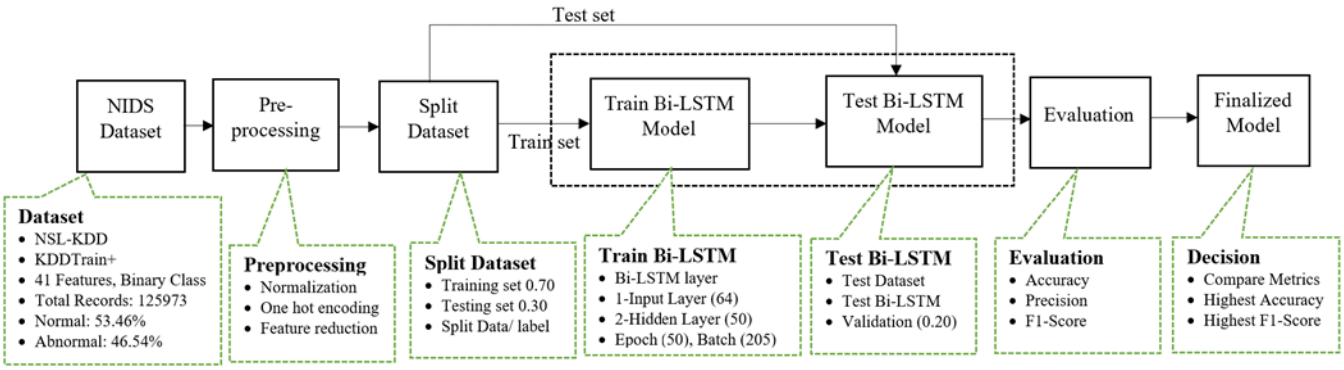


Figure 3: Bidirectional LSTM model block diagram

4.3. Train and test data preparation

The train data and test data splitting method separate the data randomly into two different subsets of the dataset. These two subsets of data contain the designed amount of data based on our selection. Since our pre-processed dataset represents just one portion of the data, we employ two separate datasets for implementing the machine learning algorithms. Researchers typically have flexibility in determining the train-test split ratio, with common choices of 80% to 20%, 60% to 40%, 70% to 30%, and 75% to 25%. We conducted experiments to determine our model's most optimal splitting ratio and found that a 70% training and 30% testing dataset ratio yielded the best performance.

4.4. Bidirectional LSTM model preparation

A recurrent neural network comprises feedback paths that analyze data sequences and patterns to make predictions. These loops enable data sharing among nodes, facilitating predictions based on accumulated information referred to as memory. RNNs have been effectively applied to address machine learning challenges, including tasks such as language preprocessing models, human voice/ speech recognition, and image processing.

The LSTM-based model resolves the challenge of vanishing gradients encountered in RNNs. The LSTM architecture comprises a memory block and three units: input gates, output gates, and forget gates. These gates function similarly to read, write, and reset functions for the cells. Due to the presence of those three gates, LSTM memory cells can effectively store and retrieve data over prolonged times, mitigating the issue of vanishing gradients.

Conventional RNNs are limited in their capacity only to consider past context information. In contrast, Bidirectional RNNs overcome this constraint by analyzing data in forward (left to right) direction and backward (right to left) directions. This involves integrating two hidden layers, with the outcomes subsequently forwarded to a shared output layer. In a conventional LSTM neural network, the output signal/data is generated directly. In contrast, a bidirectional LSTM neural network incorporates both directions (forward and backward) layers at each stage, contributing the signal to the neural network activation layer. This configuration captures data from both preceding and succeeding data, allowing the bidirectional LSTM neural network model to predict the target sequence of each element by considering finite sequences in the circumstances of both past and future elements. This is achieved by employing two consecutive LSTMs—one processing data from both directions. Traditional RNNs are constrained by their dependence solely on the previous perspective. Bidirectional LSTM defeats this limitation by examining data feed from both directions through two hidden neural network layers and then forwarding the results to a similar recurrent neural network output layer.

In a standard LSTM-based model, the model prediction is usually obtained directly via the given dataset. Conversely, the outputs from the forward layers and backward layers from each stage are combined and input into the activation layer in the bidirectional LSTM model. This resulting output encapsulates data from past and future data from the memory blocks in LSTM. The bidirectional LSTM predicts the labels or sequence from each element by leveraging finite sequences within the circumstances of preceding and following items. This process is accomplished through the sequential processing of two LSTMs—one data sequence from right to left direction and the same data sequence from left to right.

The selection of neural network architecture components, including input layers, hidden layers, output layers, layer sizes, activation functions, and dropout rates, is a critical step following data preprocessing. Hyperparameter tuning is an integral part of this research. Initially, hyperparameters are chosen randomly for experimentation, as discussed in more detail in the subsequent experimental sections. The data sampling approaches are implemented to deal with the data unevenness problem. Random oversampling and random under-sampling methods created the balanced multiclass dataset.

To initiate the random selection of the Bidirectional LSTM architecture, the neural network comprises a single input layer with 64 neurons and a dropout rate of 20%. It features two hidden layers with 50 neurons each, both employing a 20% dropout rate. The output layers consist of a single dense layer, and the choice of activation function depends on the nature of the target class size, whether binary or multi-class. Once this model is defined, it is compiled using the appropriate loss function and optimizer in preparation for training.

4.5. Evaluation Bi-LSTM model

Multiple experiments have been conducted to analyze the efficacy of the bidirectional LSTM model, revealing inconsistencies in the effectiveness of both machine learning and deep learning models. Consequently, a comprehensive analysis of the model's hyperparameters becomes imperative for performance

improvement. The selection of the optimizer, batch size, epochs, and train test splitting ratio is guided by a comparison of anomaly detection accuracy and f1-score metrics for the bidirectional LSTM model. Ultimately, the bidirectional LSTM's performance metrics are juxtaposed with previous research findings to assess its efficacy. Additionally, two distinct sampling methods, namely random under-sampling and random oversampling, were experimented with on the NSL-KDD and compared using the bidirectional LSTM model.

4.6. Compare performance for decision-making.

After conducting model testing and evaluation, the decision-making process involves selecting the most suitable model pipeline from various alternatives. During this research, multiple sets of experiments are conducted to optimize the hyperparameters for the Bi-LSTM model, aiming to enhance its performance. These hyperparameters encompass factors such as optimizers, epoch count, batch size, neural network architecture, class size selection, and methods for preprocessing raw data. This optimization process is driven by comparing performance metrics obtained from these diverse sets of experiments. Additionally, the performance metrics of the bidirectional LSTM anomaly detection models for NSL-KDD data are compared with published literature results.

5. Experiments and Results

Sets of experiments were conducted on a Windows 10 laptop with a 64-bit architecture, equipped with 16GB of random-access memory and an i7-1.99GHz processing unit. Python3.7.13, Keras2.6.0, and TensorFlow2.9.1 were utilized in this research. The investigation into train and test data split ratio, numbers of epochs, optimizers, and batch size for the bidirectional LSTM model was carried out across various experiments, as elaborated below. The intrusion detection system leverages machine and deep learning techniques for anomaly detection. Python is utilized to code network intrusion detection models, using packages such as NumPy, Pandas, Keras, imblearn, and Sci-kit-learn for developing machine learning models. Additionally, tools like WEKA, Java, C#, Visual C++, and MATLAB are commonly employed in intrusion detection.

To ensure reproducibility, seed values are configured to obtain consistent results across multiple runs on the Jupyter Notebook platform. Subsequently, the experimental results are presented in the form of plots or tables, using the Microsoft Office suite for analysis.

5.1. Experiment: Optimizers Vs. Bi-LSTM performance

During this experimentation, the bidirectional LSTM was applied to the NSL-KDD, the details of which are outlined in the preceding sections. An appropriate optimizer is essential for enhancing the network traffic anomaly detection model's training time and the overall efficacy of the model. The choice of optimizer holds significant importance as it expedites results for the ML/DL model. The choice of the optimization algorithm made by a deep learning practitioner directly impacts both the training speed and the ultimate predictive performance of their model. TensorFlow is an open-source machine-learning library containing nine optimizers: Adam, Ftrl, Adagrad, Adamax, Adadelta, SGD, RMSProp, gradient descent, and Nadam. Among them, seven optimizers were experimented with to achieve the highest performance of the model.

Table 1: Optimizer Vs. Accuracy

training data= 70%, Epochs = 50, batch size= 512				
SN	Optimizer	Accuracy %	Precision %	f1-score %
1	**Nadam**	**98.26**	**97.76**	**98.37**
2	Adam	98.24	97.66	98.35
3	RMSprop	98.19	97.56	98.31
4	Adamax	97.95	97.40	98.08
5	SGD	91.19	88.67	92.02
6	Adagrad	61.86	58.22	73.59
7	Ftrl	53.14	53.14	69.40

In this experimental task, the hyperparameter values were picked randomly, and the performance metrics and optimizers are outlined in Table 1. The structure of the bidirectional LSTM model contained 64 units, featuring two B-LSTM hidden layers having 50 units in each, along with the dense output layer. Each layer within the BLSTM model utilized an activation function called relu and 20% drop-out rate of 20%.

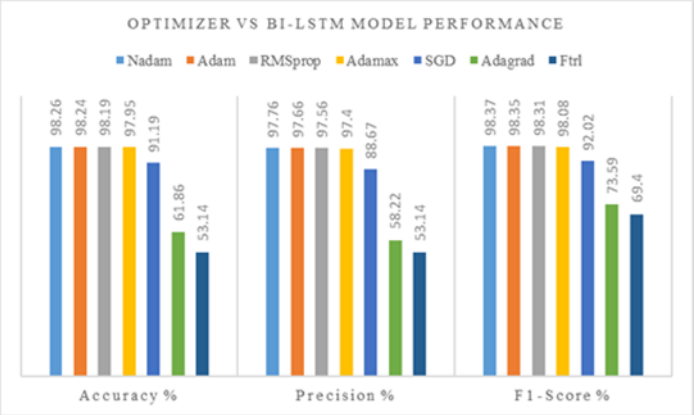


Figure 4: Optimizer Vs. Bi-LSTM performance

Observing the above results (Table 1 and Figure 4), it is determined that the Nadam optimizer is the victorious optimizer, with the winning performance metrics having an accuracy of 98.26%, precision of 97.76%, and f1-score of 98.37%. Nadam enhances the Adam algorithm by integrating Nesterov momentum, resulting in an improved performance of the Adam optimizer.

5.2. Experiment: Train test split ratio Vs. performance

In this experiment, we investigated the impact of both the train test split ratio and model performances. The process of data splitting is crucial in data science, particularly when preparing machine learning models using the available data.

The train test split methodology is utilized to calculate the efficiency of machine learning algorithms in predicting results from data that were unseen during the model training phase. Once the model gets trained, the test dataset is applied, and no fixed percentage split ratio to divide into training and test sets from the given dataset. The splitting ratio is explored to enhance the model performance by utilizing the Nadam optimizer on binary NSL-KDD data.

Table 2: Train test split ratio Vs. performance

optimizer = Nadam, Epochs = 50, Batch_size = 512			
Testing data %	accuracy %	precision %	f1-score %
10	98.15	97.55	98.29
20	98.21	97.57	98.33
30	**98.24**	**97.66**	**98.36**
40	98.18	97.52	98.30
50	98.13	97.50	98.26
60	98.10	97.52	98.24
70	98.12	97.65	98.25
80	97.82	97.39	97.97
90	97.92	97.31	98.07

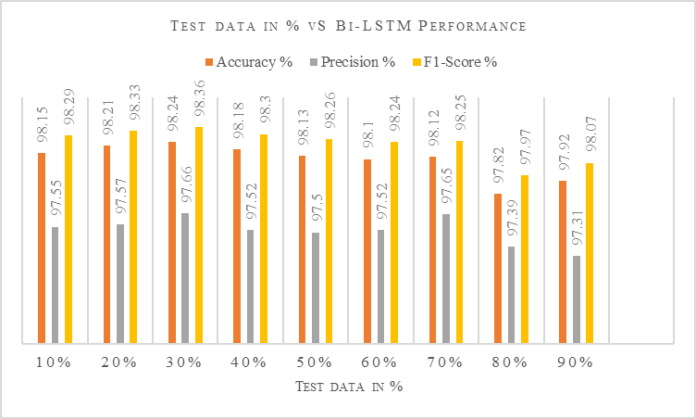


Figure 5: Test data size in % Vs. Bi-LSTM model performance

This experimental work presents the train test split ratio that achieves the optimal performance for our network traffic anomaly detection model on the NSL-KDD. The performances are tabulated in Table 2. and the plot is shown in Figure 5, where a 30% test split percentage results in the model's highest accuracy of 98.48% and f1-score of 98.57%.

5.3. Experiment: Batch size Vs. performance

This experimental work presents the train test split ratio that achieves the optimal performance for our network traffic anomaly detection model on the NSL-KDD. The performances are tabulated in Table 2. and the plot is shown in Figure 5, where a 30% test split percentage results in the model's highest accuracy of 98.48% and f1-score of 98.57%.

Table 3: Batch size Vs. model performance

Optimizer = Nadam, epochs = 105, testing data split= 0.30			
batch size	**f1-score %**	**accuracy %**	**prgm exe time (sec)**
50	**98.58**	**98.48**	2127.235
500	98.47	98.36	514.770
350	98.51	98.4	527.153
450	98.51	98.41	454.989
250	98.46	98.35	616.466
150	98.52	98.42	858.070
300	98.55	98.45	553.444
200	98.55	98.45	796.898
400	98.48	98.38	460.884
15	98.56	98.45	5671.738
100	98.56	98.46	1228.779

A smaller batch size entails the introduction of limited data samples into the Bi-LSTM anomaly detection model, necessitating a lengthier training period than a larger batch. The performance metrics and batch size are presented in Table 3. The experimented results indicate that when applying this model to the NSL-KDD, a batch of 50 produces optimal accuracy and s1-score. A larger batch of data through the model takes less training time but exhibits lower accuracy, highlighting a significant trade-off for this Bi-LSTM network traffic anomaly detection model.

5.4. Experiment: Epochs Vs. performance

In machine learning, an epoch represents one complete pass through all the training data during a model's training. During each epoch, the model is exposed to the entire dataset, and the model's parameters (weights and biases) are adjusted based on the error or loss calculated from the model's predictions compared to the actual target values.

Table 4: Epochs Vs. model performance

optimizer = Nadam, batch= 50, test data= 30% , train data = 70%			
epoch	accuracy	f1-Score	prgm exe time (sec)
175	98.48	98.58	3965.207
100	98.48	98.58	1878.803
125	98.48	98.58	2470.620
5	97.9	98.03	127.058
35	98.35	98.46	761.278
205	**98.52**	**98.62**	4103.767
50	98.38	98.48	942.129
45	98.37	98.47	1002.092
75	98.46	98.56	1465.514
150	98.48	98.58	2934.249
25	98.3	98.41	527.524
15	98.13	98.25	322.529
Accuracy and f1-score in %, prgm exe time:: program train and testing time			

In practice, the epoch is a hyperparameter set before the training begins. The choice of the epoch size depends on factors such as the model's complexity, the data size, and the model's convergence behavior during training. Selection of a small epoch may result in model underfitting, where the machine learning model hasn't learned the underlying patterns in the data. However, a large size epoch may lead the model to overfit, where the model starts memorizing the training data instead of generalizing well to unseen data. The epoch selection can be any integer value that lies between 1 to infinity. By tradition, the ML/ DL researcher selects large values of epochs.

This experiment aims to identify the optimal number of epochs that yield the highest accuracy for the Bi-LSTM model. Similar to the previous experiment, the Bi-LSTM hyperparameters were randomly selected. Longer epochs result in extended training times for the model. The random numbers of epoch values were chosen between 5 to 205, and the accuracy and f1-score were found to be highest at 205 epochs. However, it's important to note that a larger epoch value increases the training time for our model. In this experiment, a batch of 205 sizes enhances the accuracy of the Bi-LSTM network traffic anomaly detection model, achieving a detection rate of network anomalies at 98.5%.

5.5. Experiment: Model layers parameters Vs. accuracy

In our prior experiments, 5.1 to 5.4, we investigated the impact of various hyperparameters, including the optimizer, number of epochs, batch size, and the train test data split ratio. Our results

reveal that the combination of the Nadam optimizer, 205 epochs, a batch size of 50, and a train test split ratio of 70%: 30% delivers optimal performance after evaluating the model performance metrics.

Table 5: Bi-LSTM architecture Vs. accuracy

optimizer = Nadam, batch_size = 50, test data= 30%, train data=70%						
Input layer		Hidden layer 1		Hidden layer 2		acc. %
neuron	act. fn	neuron	act. fn	neuron	act. fn	
8	relu	8	relu	8	relu	97.48
4	sigmoid	4	sigmoid	4	sigmoid	97.05
16	relu	16	relu	16	relu	97.93
16	selu	16	selu	16	selu	97.97
64	**sigmoid**	**50**	**sigmoid**	**50**	**sigmoid**	**98.52**
49	sigmoid	128	sigmoid	128	sigmoid	98.18
80	relu	64	relu	64	relu	98.48
4	relu	4	relu	4	relu	97.55
act.fn::activation function, acc:: model accuracy						

This study investigated different configurations of neurons and activation functions for the neural network of the Bi-LSTM model. The dense output layer is structured to provide probabilities for distinguishing between normal and abnormal classes, rendering the softmax activation function the most appropriate selection for the binary class dataset.

This experiment evaluated diverse configurations of Bi-LSTM neurons and activation functions for input and hidden layers. Several results from the conducted experiment are outlined in Table 4. Based on the tabulated results, 64 neurons in the input layer and 50 neurons in each hidden layer of our model produce the ultimate accuracy of 98.52 % in the domain of network anomaly detection.

5.6. Experiment: Sampling Vs. performance metrics for multiclass NSL-KDD dataset

Since these data represent a refined version of the KDD99 dataset, minimal data preprocessing is required. The downloaded train data (KDDTrain+) with the target class was initially separated from the training dataset to establish the class label. Among the remaining numerical features, three categorical attributes, 'protocol_type,' 'service,' and 'flag,' are extracted. Dummy one-hot encoding methods convert categorical into numerical values, while the numerical features are normalized using standard scaling methods. Subsequently, both feature sets are merged into a unified data frame, resulting in the final data set.

The attack types on both KDD99 and NSL-KDD are presented in Table 6. The network attack traffic in these datasets is classified into 'Denial of Service,' 'Probe,' 'Remote to Local,' and 'User to Root' [21]. A denial-of-service attack prevents legitimate users from accessing resources via the network, causing a disruption in the availability of those resources. On the other hand, a probe is a scanning attack aimed at identifying vulnerabilities in a system connected to the network. This probing attack targets weaknesses and facilitates potential compromise of the system.

Table 6: Attack types and traffic information in NSL-KDD

Class	Attack Types	Data
Probe	Satan, MScan, Upsweep, Saint, Nmap, Portsweep	11656
U2R	Ps, Perl, Buffer_overflow, Sqlattack, Rootkit, Loadmodule, Xterm	52
Normal		67343
R2L	Spy, Ftp_write, Guess_Password, Imap, Phf, Multihop, Warezmaster, Xlock, Warezclient, Xsnoop, Snmpguess, Snmpgetattack, Named, Httptunnel, Sendmail	995
DoS	Back, Worm, Apache2 Neptune, Smurf, Pod, Teardrop, Udpstorm, Processtable, Land	45927
Total traffic data		12593

Likewise, the remote-to-local attack involves illegal access to a remote terminal. The user-to-root attack entails gaining privilege as a root user, with the root password obtained through various techniques such as password sniffing, brute-forcing, or social engineering.

Under-sampling is a straightforward approach and a method for addressing the class imbalance in datasets. This technique involves preserving all data within the minority class while reducing the volume of data in the majority class. It represents one of several tools available to data scientists for enhancing the accuracy of insights extracted from initially imbalanced datasets. In under-sampling, data samples from the majority class are randomly chosen and removed until a balanced distribution is achieved. This reduction in data volume can alleviate storage constraints and enhance processing efficiency. However, it's significant to note that this reduction may result in the loss of valuable information.

Conversely, oversampling is employed when the available data is insufficient in quantity. Its objective is to rectify dataset imbalance by augmenting the number of rare samples. Instead of discarding abundant samples, oversampling techniques generate new rare samples through replication, bootstrapping, or SMOTE (Synthetic Minority Over-Sampling Technique). SMOTE, which stands for synthetic minority over-sampling technique, is a specific form of oversampling that involves the synthetic generation of data points for the minority class. In this process, a random selection of k nearest neighbors is chosen to determine the appropriate oversampling level.

After preprocessing, the NSL-KDD KDDTrain+ multiclass data initially exhibits imbalanced class distributions. Various techniques can be employed to rectify this imbalance, including under-sampling, over-sampling, and hybrid sampling. Our experiment utilized an automated sampling approach combining random under-sampling and SMOTE to restructure the data for all classes based on our implemented sampling method. Random oversampling consists of randomly choosing instances from the minority class, replacing them, and incorporating them into the training dataset. On the other hand, random under-sampling entails randomly selecting instances from the majority class and removing them from the dataset.

Table 7: Bi-LSTM with random under-sampling and performance

BI-LSTM Model with Random Under-Sampling and Performance				
Epochs= 50, Batch_size= 512, Data = NSL-KDD Multiclass (5 class) _RUS				
SN	**Class**	**Precision %**	**Recall %**	**F1-Score %**
1	DoS	100	100	100
2	Probe	100	79.17	88.37
3	R2L	88.89	80	84.21
4	U2R	73.68	93.33	82.35

5	Normal	86.67	100	92.86
Average		**91.29**	**89.74**	**89.81**
Accuracy = **89.74** %				
Program exe time = 17.72 sec				

The number of new datasets generated depends on each target class's original data size. Random under-sampling reduced the NSL-KDD data to 52 instances in each of the five classes by randomly eliminating data points. Conversely, SMOTE, an oversampling technique, augmented the dataset by introducing additional data points. During this experiment, substantial data augmentation created well-balanced datasets, with each target class containing 67,343 instances.

The balanced NSL-KDD data has been partitioned into training and testing subsets to facilitate the training and evaluation of the Bidirectional LSTM model. As determined in previous experiments, the train test data split ratio of 70%:30%.

The architecture of the Bi-LSTM neural network mirrors that used in prior experiments, with the input layer containing 64 elements and both hidden layer1 and hidden layer2 comprising 50 elements. A trade-off analysis was conducted to determine the optimal combination of epochs and batch size while considering the Bi-LSTM model's performance.

Table 8: Bi-LSTM with SMOTE technique and performance

BI-LSTM Model with SMOTE and Performance				
Epochs= 50, Batch size= 512, Data = NSL-KDD Multiclass (5 class) RUS				
SN	**Class**	**Precision %**	**Recall %**	**F1-Score %**
1	DoS	99.99	99.98	99.98
2	Probe	99.99	99.98	99.98
3	R2L	99.99	99.18	99.59
4	U2R	99.18	1	99.59
5	Normal	1	99.99	1
Average		**99.83**	**99.83**	**99.83**
Accuracy = **99.83** %				
Program exe time = 770.52 sec				

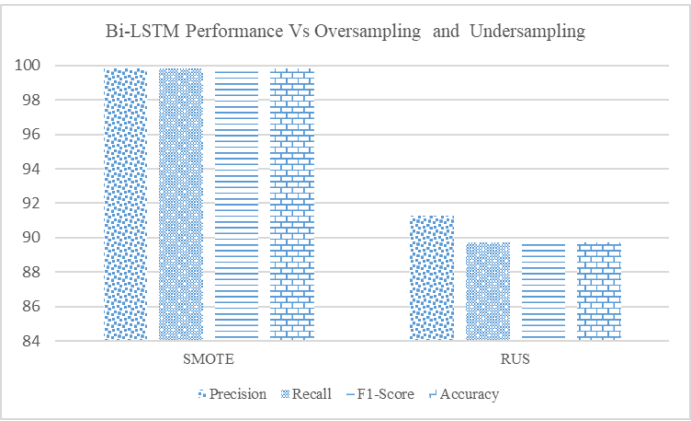


Figure 6: Bi-LSTM performance Vs. oversampling and under-sampling

In our hyperparameter tuning, we aimed to balance program execution time and model performance, as previously demonstrated. As a result, the model was trained for 50 epochs using a batch size of 512 and the Nadam optimizer with a learning rate of 0.041, as detailed in the accompanying table.

The random under-sampling methods produce the NIDS multiclass accuracy of 89.74%, average precision of 91.29 %, recall of 89.74%, and 89.91% f1-score referenced from Table 7. The program execution time is short as compared with oversampling.

Table 8. Shows the performance of the Bi-LSTM with over-sampling methods called SMOTE where the default value of K, i.e., 5, is taken during this experiment. The nearest neighbors value K defines the neighborhood of samples to generate the synthetic samples. We listed the individual class performance as well as average class performance. Figure 6 shows the visualization plot to compare the under-sampling and over-sampling performance on the NSL-KDD multiclass dataset using the Bi-LSTM model. The over-sampling (SMOTE) for the NSL-KDD multiclass dataset provides the 99.83% average precision, recall, and F1 score.

6. Conclusion

The Highest performance is achieved during network traffic anomaly detection using the bidirectional LSTM model. The combination of tunned different hyperparameters (from the above experiments) values, including epoch, optimizer, and batch size, outperformed the anomaly detection model. Determination of hyperparameters' values for the Bi-LSTM anomaly detection model on the NSL-KDD dataset highly contributes to the domain of anomaly detection using machine learning and deep learning. Similarly, we can use no fixed split ratio values for the efficient anomaly detection model. This research work determines the split ratio to produce the highest performance on anomaly detection using the Bi-LSTM model on the NSL-KDD dataset. The combination of neural network architecture memory elements plays an important role in training and testing the model during network anomaly detection. Data imbalance is another main problem to deal with during network anomaly detection. The sampling techniques either delete the data entry randomly or generate the data entry randomly. The sampling technique balances the data in the multiclass dataset. During this research work, the implementation of the random up-sampling methods outperformed the model and produced the highest performance.

We compare our results with existing research [17] to prove that our model is outperformed on the KDD-NSL multiclass dataset. The previously completed research compared their model performance in paper at 99.70% with the other previously researched model's performance, such as Artificial Neural Network (ANN) model at 95%, Decision Tree and Random Forest with 92.60%, Linear Regression, and Random Forest with 94%, Random Forest, and Bayesian Network with 93.4 %, Deep Neural Network with 97% [17]. Our proposed model pipeline for the Bi-LSTM-based network anomaly detection model delivers a higher accuracy of 99.83% is greater than the obtained model performance in research work [17]. The values of bidirectional LSTM model hyperparameters, including epochs values, optimizer, batch size, train test slit ratio, and SMOTE sampling technique for the multilayer bidirectional LSTM neuron architecture (layers, activation function, and memory units) are examined to achieve the highest anomaly detection model performance. The results from these experiments consistently demonstrate that the bidirectional LSTM model, configured with the explored parameters, significantly enhances detection accuracy and f1-score. This model can be experimented with using different network intrusion datasets. Creating a new network intrusion

dataset with the latest network attacks will be the extension of this task in the future.

Conflict of Interest

The authors declare no conflict of interest.

Acknowledgment

The National Science Foundation (NSF) and Scholarship for Service CyberCorps (SFS CyberCorps) programs support this research study. The award information of NSF and CyberCorps are #1910868 and #2219611, respectively. This cannot be completed without the continuous support of advisors and the Electrical and Computer Engineering Departments of Prairie View A&M University

References

[1] T. Acharya, A. Annamalai, M.F. Chouikha, "Efficacy of Bidirectional LSTM Model for Network-Based Anomaly Detection," in 13th IEEE Symposium on Computer Applications and Industrial Electronics, ISCAIE 2023, Institute of Electrical and Electronics Engineers Inc.: 336–341, 2023, doi:10.1109/ISCAIE57739.2023.10165336.

[2] N. Moustafa, J. Hu, J. Slay, "A holistic review of Network Anomaly Detection Systems: A comprehensive survey," Journal of Network and Computer Applications, **128**, 33–55, 2019, doi:10.1016/j.jnca.2018.12.006.

[3] S. Samonas, D. Coss, THE CIA STRIKES BACK: REDEFINING CONFIDENTIALITY, INTEGRITY AND AVAILABILITY IN SECURITY.

[4] Y. Fu, Y. Du, Z. Cao, Q. Li, W. Xiang, "A Deep Learning Model for Network Intrusion Detection with Imbalanced Data," Electronics (Switzerland), **11**(6), 2022, doi:10.3390/electronics11060898.

[5] K. Jiang, W. Wang, A. Wang, H. Wu, "Network Intrusion Detection Combined Hybrid Sampling with Deep Hierarchical Network," IEEE Access, **8**, 32464–32476, 2020, doi:10.1109/ACCESS.2020.2973730.

[6] W. Xu, J. Jang-Jaccard, T. Liu, F. Sabrina, J. Kwak, "Improved Bidirectional GAN-Based Approach for Network Intrusion Detection Using One-Class Classifier," Computers, **11**(6), 2022, doi:10.3390/computers11060085.

[7] L. Vu, Q.U. Nguyen, "Handling Imbalanced Data in Intrusion Detection Systems using Generative Adversarial Networks," Journal of Research and Development on Information and Communication Technology, **2020**(1), 1–13, 2020, doi:10.32913/mic-ict-research.v2020.n1.894.

[8] T. Acharya, I. Khatri, A. Annamalai, M.F. Chouikha, "Efficacy of Heterogeneous Ensemble Assisted Machine Learning Model for Binary and Multi-Class Network Intrusion Detection," in 2021 IEEE International Conference on Automatic Control and Intelligent Systems, I2CACIS 2021 - Proceedings, Institute of Electrical and Electronics Engineers Inc.: 408–413, 2021, doi:10.1109/I2CACIS52118.2021.9495864.

[9] T. Acharya, I. Khatri, A. Annamalai, M.F. Chouikha, "Efficacy of Machine Learning-Based Classifiers for Binary and Multi-Class Network Intrusion Detection," in 2021 IEEE International Conference on Automatic Control and Intelligent Systems, I2CACIS 2021 - Proceedings, Institute of Electrical and Electronics Engineers Inc.: 402–407, 2021, doi:10.1109/I2CACIS52118.2021.9495877.

[10] C. Yin, Y. Zhu, J. Fei, X. He, "A Deep Learning Approach for Intrusion Detection Using Recurrent Neural Networks," IEEE Access, **5**, 21954–21961, 2017, doi:10.1109/ACCESS.2017.2762418.

[11] Z. Chen, C.K. Yeo, B.S. Lee, C.T. Lau, "Autoencoder-based network anomaly detection," in Wireless Telecommunications Symposium, IEEE Computer Society: 1–5, 2018, doi:10.1109/WTS.2018.8363930.

[12] M. Ganesh, A. Kumar, V. Pattabiraman, "Autoencoder based network anomaly detection," in Proceedings of 2020 IEEE International Conference on Technology, Engineering, Management for Societal Impact Using Marketing, Entrepreneurship and Talent, TEMSMET 2020, Institute of Electrical and Electronics Engineers Inc., 2020, doi:10.1109/TEMSMET51618.2020.9557464.

[13] W. Xu, J. Jang-Jaccard, A. Singh, Y. Wei, F. Sabrina, "Improving Performance of Autoencoder-Based Network Anomaly Detection on NSL-KDD Dataset," IEEE Access, **9**, 140136–140146, 2021, doi:10.1109/ACCESS.2021.3116612.

[14] J. Gao, "Network Intrusion Detection Method Combining CNN and BiLSTM in Cloud Computing Environment," Computational Intelligence and Neuroscience, **2022**, 2022, doi:10.1155/2022/7272479.

[15] T. Acharya, A. Annamalai, M.F. Chouikha, "Efficacy of CNN-Bidirectional LSTM Hybrid Model for Network-Based Anomaly Detection," in 13th IEEE Symposium on Computer Applications and Industrial Electronics, ISCAIE 2023, Institute of Electrical and Electronics Engineers Inc.: 348–353, 2023, doi:10.1109/ISCAIE57739.2023.10165088.

[16] A.G. Salman, Y. Heryadi, E. Abdurahman, W. Suparta, "Single Layer & Multi-layer Long Short-Term Memory (LSTM) Model with Intermediate Variables for Weather Forecasting," in Procedia Computer Science, Elsevier B.V.: 89–98, 2018, doi:10.1016/j.procs.2018.08.153.

[17] P. TS, P. Shrinivasacharya, "Evaluating neural networks using Bi-Directional LSTM for network IDS (intrusion detection systems) in cyber security," Global Transitions Proceedings, **2**(2), 448–454, 2021, doi:10.1016/j.gltp.2021.08.017.

[18] Y. Imrana, Y. Xiang, L. Ali, Z. Abdul-Rauf, "A bidirectional LSTM deep learning approach for intrusion detection," Expert Systems with Applications, **185**, 2021, doi:10.1016/j.eswa.2021.115524.

[19] I. Kandel, M. Castelli, "The effect of batch size on the generalizability of the convolutional neural networks on a histopathology dataset," ICT Express, **6**(4), 312–315, 2020, doi:10.1016/j.icte.2020.04.010.

[20] M. Tavallaee, E. Bagheri, W. Lu, A.A. Ghorbani, "A detailed analysis of the KDD CUP 99 data set," in IEEE Symposium on Computational Intelligence for Security and Defense Applications, CISDA 2009, 2009, doi:10.1109/CISDA.2009.5356528.

[21] L. Dhanabal, S.P. Shantharajah, "A Study on NSL-KDD Dataset for Intrusion Detection System Based on Classification Algorithms," International Journal of Advanced Research in Computer and Communication Engineering, **4**, 2015, doi:10.17148/IJARCCE.2015.4696.