ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 6, No. 5, 185-202 (2021)

www.astesj.com

Special Issue on Innovation in Computing, Engineering Science & Technology

ASTESJ

ISSN: 2415-6698

iDRP Framework: An Intelligent Malware Exploration Framework for Big Data and Internet of Things (IoT) Ecosystem

Osaretin Eboya*, Julia Binti Juremi

Asia Pacific University (APU), Faculty of Computing, Engineering, and Technology (FCET), Kuala Lumpur 57000, Malaysia

ARTICLE INFO

Article history:
Received: 24 June, 2021
Accepted: 20 September, 2021
Online: 30 September, 2021

Keywords:
Internet of Things (IoT) Security
iDRP framework Security
Integrated Security framework
Intelligent Network Security
Intelligent Malware Detection
Intrusion Detection System
Big Data Security
IoT iDRP framework
IoT Malware Security
IoT Botnet Security
Anomalies Detection Techniques
Multilayer Perceptron (MLP)
Deep Neural Network (DNN)
Deep Learning (DL)
Machine Learning (ML)
Artificial Neural Network (ANN)

ABSTRACT

The Internet of Things (IoT) is at a face paced growth in the advanced Industrial Revolution (IR) 4.0 in the modern digital world. Considering the current network security challenges and sophistication of attacks in the heavily computerized and interconnected systems, such as an IoT ecosystem, the need for an innovative, robust, intelligent and adaptive malware attacks and threats security solution is becoming predominant in the current cyberspace. An integrated and scalable IoT malware detection framework called iDRP framework with deep learning method was proposed as a solution to current IoT malware attacks that are largely obfuscated. The novel framework utilized systematic pre-processing and post-processing techniques and methods on the BoTNetIoT malware datasets that contains both benign and malicious IoT traffic data infected by modern day IoT attacks such as Mirai and Gafgyt etc. IoT malware variants in an IoT ecosystem. The raw IoT malware binaries were converted to image files (Gray-scaled) and computed statistically with synthesised sparsed and differential evolutionary hidden feature structures techniques, which were cyclically trained, tested, and cross-validated to establish empirical anomalies with precision in the detection, recognizing, and prediction of malware anomalies in a modern IoT ecosystem. Preliminary experiments were conducted with standardized image binary files such as the MNIST (2-D), and NORB (3-D) datasets as sound scientific exploratory experiments with profound results. The comparative results of the performance of our integrated techniques and methods on the BoTNetIoT IoT malware datasets achieved a 99.98% accuracy, 99.99% ROC/AUC, 99.95% precision, and 99.93 recall rate etc. utilizing the integrated iDRP framework mechanisms for effectively detecting IoT malware in an IoT ecosystem.

1. Introduction

This paper is an extension of the work originally presented in *IEEE 8th R10 Humanitarian Technology Conference (R10-HTC) 2020* [1]. The Internet of Things (IoT) has in recent times emerged as ubiquitous technology to everyday lives especially with the advent of the Industrial Revolution (IR) 4.0 in the digital world. The IoT technologies comprises of smart devices and objects interconnected in a heavily computerized network environment that constitutes the backbone of modern innovative critical infrastructures that supports fast-paced technological driven world. The IoT technologies has been disruptive in many industries such as: (1) IoT in Healthcare, (2) IoT in Manufacturing, (3) IoT in Transportation and Mobility, (4) IoT in Buildings, (5) IoT in Cities, (6) IoT in Agriculture, (7) IoT in Energy, (8) IoT in Retail and Marketing, (9) IoT in Logistics and Supply Chain, and (10) IoT in Industries across various sectors of the economy. Similarly, IoT technologies has brought diverse approaches in solving mundane tasks in these sectors by leveraging and amalgamating innovative and intelligent automation systems. Additionally, the IoT technologies at the present time has been able to help connect multiple devices and objects in an expansive interconnected network area while collecting high treasure trove of data – *big data*. The big data collected in an IoT ecosystem has become paramount to making business decisions, analytics, and gaining valuable insights in multidimensional industries in the modern era. Furthermore, this big data that are continuously generated in an a heavily interconnected environment such as the IoT ecosystem has inadvertently set off more attractions and incentives to the cyber squatters and cyber criminals in a digital world – *Cyber hacking*. The security of IoT ecosystem is ever more crucial and concerning to safeguarding critical infrastructures in the smart environments against prolific attacks and state-of-the-art attacks – *Cyber*

*Corresponding Author: Osaretin Eboya, Email: osaretin@ieee.org

https://dx.doi.org/10.25046/aj060521

intrusions. For example, in recent time there have been a number of cyberattacks that caused outages and losses such as the (https://www.msn.com/en-my/news/world/dc-police-suffer-massive-info-leak-after-ransomware-attack/ar-BB1gHTQl) attack and (https://www.msn.com/en-my/news/world/european-hackers-given-us-5-million-for-key-to-reopen-us-pipeline/ar-BB1gIq7K) outage coupled with the public health (https://www.msn.com/en-my/news/world/ireland-tests-cyber-attack-data-fix/ar-AAKe3Qd) compromise disruptions on critical infrastructures that serves an entire community in the modern society. This is one of the most significant attacks in recent time with massive consequences. The cyberattacks on critical infrastructures evidently indicates how vulnerable and compromising the present-day heavily computerized network systems can be, and consequently disruptive and detrimental to everyday lives in a digital world. Moreover, this clearly indicates that most *modern* highly interconnected critical infrastructures serving every day processes in the most developed world can be highly susceptible and vulnerable to being hacked with a myriad of modern malware attacks such as Ransomware attacks and '*Zero Day*' attacks. Theoretically, in the modern digital world, any device or object that can connect to a network system or grid can be hacked.

Considering the general consensus in the cybersecurity space that humans are usually the weakest link in the chain of command in the cybersecurity and network security effort, it is effectively safe to deduce that the current static, dynamic, and automated malware defense approaches against cyberattacks and cyber threats in an IoT ecosystem in a digital world is essentially a futile effort. Particularly in the bountiful cyberattacks and cyber threats warfare in the modern cyber space clearly indicates the fragility and exposure of current interconnected critical infrastructures and its related network systems. This has essentially led to the theory that *detection* is a better approach to combating cyberattacks and cyber threats in a smart ecosystem of massively interconnected computer network systems – *malware detection* [1]. Malwares are typically spread over an interconnected computer network system otherwise known as the internet, which is the core backbone of an IoT ecosystem. The lack of global unified principles and security of IoT protocols present major security and counter-intelligence conundrum on a daily basis in the IoT cyberworld. This inadvertently exposes various valuable resources and assets in an organization to the cybercriminals. The IoT ecosystem can be attacked, infected, and breached by different types of malicious software commonly known as malwares with categorized malware families such as: (a) Ransomwares, (b) Spywares, (c) Scareware, (d) Adware, (e) Viruses, (f) Worms, (g) Rootkits, (h) Botnets, (i) Trojan Horses that all threatens the *integrity*, *privacy*, and *security* of big data in a heavily computerized computer network system like an IoT ecosystem – *tampering of valuable assets; big dataset.* One of the major problems [1] with these malware families and their nefarious activities combined with innovatory technologies is that they have become even harder to detect with traditional and automated malware detection tools and techniques in a heavily computerized network system – *polymorphic malwares.* If and when potent malwares go undetected in a network system such as an IoT ecosystem, this can cause massive damages and disruptions to critical computer network infrastructures [1], loss of personal information, and potentially loss of livelihood and lives in a modern technological-reliant society – *obfuscation and evasion of malware detection.*

We proposed a novel IoT Security framework known as the *intelligent*, *detection*, *recognition*, and *prediction* (iDRP) framework [1] to address these computer network security challenges and problems in the modern digital world. The proposed iDRP framework is an innovative, intelligent, robust and adaptive framework with ultramodern approach to solving malware anomalies in an IoT ecosystem. In the unique approach proposed, a synergy of the subsets of Artificial Intelligence (Ai); Machine Learning (ML) and Deep Learning (DL) will be synthesized with modularity and scalability implementation for a lifelong training and learning capabilities. Eventually, the goal of the research work is to effectively detect, recognize, and predict anomalies in an IoT ecosystem innovatively using a subset of Artificial Neural Network (ANN) with focus on Multilayer Perceptron (MLP); *hierarchical* DL techniques i.e., Deep Neural Network (DNN) to solving the wide range of polymorphic malware anomalies problems in an IoT ecosystem.

2. Related Work

The drawback of heavily depending on the storage of big data set in one or more interconnected storage medium is that adversaries now have the perceived knowledge and understanding of where to target in their quest in wreaking havoc on present-day interconnected network systems. In the event that proper anomaly analysis mechanism for countering the attacks on the treasure trove of big data is not put in place, then, it means that the assailants will in most cases get away with their attacks either undetected or worst-case scenario, reside on the host system while plunging the gigantic and diverse data in the system [1]. The lack of highly-developed, efficient, robust security apparatus with well-established intelligent processes that can accurately measure and predict future occurrences of such attacks could be disastrous to the specific individual, organization, or government alike. The general IoT Security challenges range from Authentication, Access Control, Privacy, Confidentiality, Integrity, Policy Enforcement, Trust, Secure Middleware, Mobile Security [2],[3] [4], and Network Security. The complexity of the interactivity between the gigantic number of smart devices and objects together with smart network systems give rise to a major security gap in the IoT ecosystem. This poses big security risks due to the incessant and sophisticated cyber-attacks in the modern internet age – *IR 4.0*. A common denominator amongst all the aforementioned IoT Security challenges is the Distributed Denial of Service (DDoS) attack. The DDoS attacks occur on major global establishments on a regular basis [5]-[7]. Several peculiar IoT Security constraints such as integrity, availability, authentication, authorization, and privacy have hampered the efforts to address the growing IoT Security challenges posed by malicious actors.

The malicious attacks on large corporations such as Fortune 500 enterprises have clearly shown that the security of internet-connected devices and objects is paramount considering the fact that the particular DDoS Malware attack called the "Mirai Botnet" crippled even the network servers of these largest technology corporations. Some of these large corporations are situated in the United States and major European countries [8], (https://www.theguardian.com/technology/2016/oct/26/ddos-

attack-dyn-mirai-botnet), and (https://www.wired.com/story/reaper-iot-botnet-infected-million-networks/). This type of nefarious malware attacks contributes to the urgent needs for a viable solution to the lingering IoT Security challenges [6], [9], [10] with the ever-growing IoT inter-connected network environment. According to [8], [11], [12]. One of the security challenges of smart devices and objects today is the inability to *detect* when there is an intrusion in the IoT network system. This is largely due to the fact that most smart devices lack the capability to log and report when such malicious attack occurs in the IoT ecosystem. IoT Security needs to be improved and revolutionized to prevent, identify, and neutralize the malicious network traffic threats on the Billions of IoT connected servers. The exponential ramifications of the risks and costs that the malicious attacks on the IoT infrastructures pose [13] to businesses, governments, and individuals who rely on IoT services such as Healthcare, electricity, industrial production, social amenities, communications, and logistics is still unknown. Nevertheless, the researchers discovered that, the two major challenges that an IoT ecosystem currently face are; Low-end Embedded Devices [6], [8], [14] with insecure Operating System (OS), and Mirai-Styled Malware Attacks [10] otherwise known as Mirai Botnet, which is a modern and sophisticated variation of a Distributed Denial-of-Service (DDoS) attack on the current precarious IoT environments and its smart devices and objects.

2.1. IoT Attacks

IoT applications are prone to attacks from different hostile actors. The multidiscipline industries that adopt IoT as a technology have their own variation of attacks on their IoT applications and infrastructures. The concept of sensors connecting to each other and transmitting big data in a two-way traffic in an IoT ecosystem typically creates vulnerabilities [13], [15]-[17] in the IoT network system. In the Smart City ecosystem in Ukraine that utilizes Smart energy grid system to serve the city, 30 of such Smart energy were attacked [8], [16], and (https://www.thenational.ae/uae/smart-cities-open-door-to-cyber-attacks-say-security-experts-1.672214), and 80,000 residents were without power supply for several hours due to the adversarial malicious attack on the Smart Grid system. In the United States, 156 emergency sirens designed to alert residents of the city of Dallas [8], [18], and (https://www.nytimes.com/2017/04/08/us/dallas-emergency-sirens-hacking.html) in the event of critical emergencies such as earthquakes, floods, and nuclear attacks were set off because of an attack [2] on their Smart City system. The impact of such false alarm set off in such a malicious manner can be consequential in the end. There is a high likelihood of the residents of the city to ignore a true alarm warning in the event of an actual emergency, which could potentially lead to loss of lives and livelihood [2]. Similarly, 2,200 residents were without water supply (https://www.wired.com/2011/11/hackers-destroy-water-pump/) when hackers attacked and destroyed the Smart Water Pump Supply system in the municipality of Springfield, Illinois, United States.

The malicious attacks on IoT applications are not limited to Smart Cities and critical infrastructures alone, but also Smart Automobile compute system where attackers targeted a popular Smart Car maker and hijacked its core automation compute system that powers their connected cars for their financial gains. The financial gains, also known as "*Cryptojacking*" [13], [18], [19] where hackers use illegally acquired computational resources to mine the cryptocurrency shows that hackers will launch attacks on IoT applications for monetary reasons. In Smart Healthcare system [13], attackers have successfully hacked [6], [8] a heart monitoring electronics health (e-health) infrastructure that intelligently monitors and analyses patient's heart rate and helps prevent cardiac arrest and heart attacks [20]. Furthermore, the security of a Smart Home system that helps parents monitor their infants was compromised when attackers [6], [8] were able to obtain the login credentials of the Smart Home system and about 700 Webcam feeds of babies were posted on the internet [13], [20] in a malicious attempt by the hackers. The security breaches ultimately led to privacy [20] on the victims of the IoT attacks. All these incessant IoT attacks [6], [13] indicate that IoT devices and objects are more vulnerable and susceptible [19], [21] to various hostile adversaries who are constantly looking for weaknesses [16], [18] in the IoT infrastructures and IoT software applications

2.2. IoT Malwares

Malicious software and worms are very devastating to the IoT applications' ecosystem. Malware such as worms pose greater threats to the security of IoT applications. Some of the known malware worms are Mirai Botnets [22], Ransomware [20], [23], Over The Air (OTA) Worm [21],[24], and Struxnex Worm. According to the case study and analysis conducted by [18], discovered that Mirai Botnet can be directed towards the disruption of the availability of the targeted IoT application and the IoT compute resources in the IoT environment. In addition, [8],[23] classified the Ransomware as primarily Crypto Ransomware, and Locker Ransomware, which encrypts and locks critical files, respectively in an IoT ecosystem have increased by a staggering 670% and 350% between 2015 and 2017 respectively and continue to grow exponentially nowadays. The implications of such malicious software are severe and could disrupt and harm crucial IoT infrastructure and potentially cripple an entire IoT ecosystem as evident [13],[19] in the coordinated attacks by hackers on the key connected internal applications in the city of Atlanta, United States.

The OTA Worm exploits vulnerabilities in the IoT smart devices and objects and spreads in the IoT environment by compromising the integrity, privacy, and security of the interconnected devices and objects therein. The OTA Worm embeds itself into the IoT ecosystem thereby causing a breakdown of the IoT ecosystem referred to as an "epileptic seizure" [6], [16], [24] of the specific IoT smart devices and objects at a close range of 350 meters to the building with the help of a drone or Unmanned Arial Vehicle (UAV) equipped with the malicious worm. Moreover, the mode of launching the OTA Worm attack is also carried out with mobility such as physically getting close or driving cars to a close proximity of the IoT subject. Even though the OTA Drone Worm [6], [16], [24] was successfully launched on a major Smart home appliances manufacturer's Smart bulb product line, it was, however, performed in a controlled environment and the concerned manufacturer of the defected IoT Smart Light Bulb was notified, and the appropriate fix was implemented, which now reduces the possible attack range to 1 meter [6], [16], [24]. However, the risk of exploitation by enemies is present. This shows that malicious adversaries are becoming more sophisticated

in their approach towards unleashing malicious worm attacks with technological advancement. Furthermore, the Struxnex Worm, which is a variant and obfuscation of malicious worm was directed at Smart Industry such as the Uranium plant [6] connected to an IoT infrastructure to intelligently monitor and analyse the increment and decrement of the acceleration of the centrifuge and enrich the Uranium plant as the need arise autonomously. The main goal of the Struxnex worm is to infect and break down the smart devices and objects in a Smart Industrial ecosystem [18] such as a Uranium plant.

2.3. IoT Existing Security Challenges and Gaps

The core existing gap in the IoT Security paradigm is IoT security, IoT privacy [3], [4], [17], [19]. However, this research has gone further with the IoT security and IoT integrity dimension. The importance of anomaly detection in an IoT ecosystem cannot be overemphasized in various IoT industries such as Smart Healthcare, Smart Education, Smart Agriculture, and Smart manufacturing, and Smart Buildings and Smart Cities [13], [25]-[28]. In the IoT Security dimension, we explored and discovered that research has been done on the Classification and Visualization of IoT security [20], [21], [29] in which the researchers performed experiments to visualize and compare different classes of malware in a similarity matrix table based on the images and features of some malware samples such as Worms and Trojans Horses. Their research work can be improved further to increase the accuracy of the detected similarities of the various malware samples and increase the performance of the workload on big data. Moreover, the experiment was conducted using 'mechanical' compute method, which means that their method could possibly detect existing malware at a significant slow pace, coupled with the fact that, their classification and visualization method cannot intelligently predict future occurrences [13], [19], [20] of such IoT malware anomalies autonomously.

3. Methodology

We present the schematic illustration process of the work proposed iDRP framework, including the realization of the universal approximations of Multilayer Perceptron (MLP) with multiple hidden layers by exploiting the capabilities of H-ELM and other related techniques [30]-[33], which have the preeminent underexplored potentials for accelerated speed, rapid feature learning, and improved classification performance [30], [31], [34], [35].

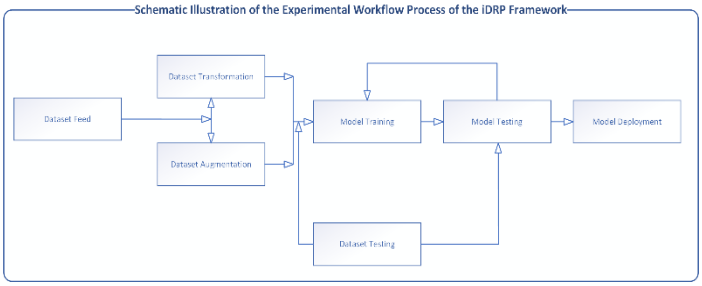

Figure 1: Schematic Illustration of the Experimental Workflow Process of the iDRP Framework

Figure 1 Shows the schematic illustration of the setup of the experimental workflow process of the iDRP framework. The big dataset will be fed into the system, when then gets transformed by various MLP techniques such as augmentation, normalization and classification techniques, and subsequently prepared for the algorithm. Feature extractions will be carried out by augmenting and fine-tuning the big dataset for the generalization and capability of the proposed iDRP framework.

The experimental implementation is to demonstrate the proof-of-concept of the proposed iDRP framework using the generalized MLP techniques for demonstrating how a non-traditional malware detection mechanism [32], [33] can be applied to systematically, dynamically, adaptively, and intelligently detect, recognize, and predict malware anomalies in the generated big data of an IoT ecosystem through converted image file, such as a log file, and binary dataset to create synthesized Machine Learning (ML) and Deep Learning (DL) models. Based upon the premise that attackers are getting more sophisticated with the advancement of technology every day, and considering that attackers have been developing malwares that can dynamically modify their signatures while in the network environment, which approximately makes it more difficult to detect. This fundamentally relegates the notion of applying the traditional and automated Signature-Based Analysis method to solving a potential attacks and threats in an IoT ecosystem. Furthermore, the Heuristic-Based Analysis method, which is otherwise known as Behavioural-Based Analysis technique applied by several Anti-Virus and Anti-Malware vendors on computer network systems has not been sufficient either. Hence, there are various gaps [19],[20],[36] in the field of study to develop a novel approach to solving the inherent and existential security threats in computer network systems, especially in the fast-growing IoT ecosystems that has now become ubiquitous to everyday life. The hypothesis is that nowadays, contaminated and malicious programs in an IoT ecosystem can easily masquerade themselves as benign software applications once in the network space. Therefore, a dynamic, robust, and intelligent Pattern-based model approach to discerning and distinguishing the genuine and malicious program in a system as counter-intelligence is paramount as the building block to proactively combating an unwanted and illegitimate program from executing and consequently causing some irreversible damages and potentially loss of lives in an IoT ecosystem with its critical infrastructures.

To explore the binary classification and analysis techniques, we will be using the standardized Modified National Institute of Standards and Technology (MNIST) dataset (http://yann.lecun.com/exdb/mnist/), which has been demonstrated to have the capability to be embedded with malicious codes (virus-MNIST) (https://arxiv.org/abs/2103.00602) adaptively, NORB (https://cs.nyu.edu/~yann/research/norb/) to perform the experiment by encoding the dataset, which will serve as a standard benchmark for comparative training, testing, evaluation, and analysis of the experiment.

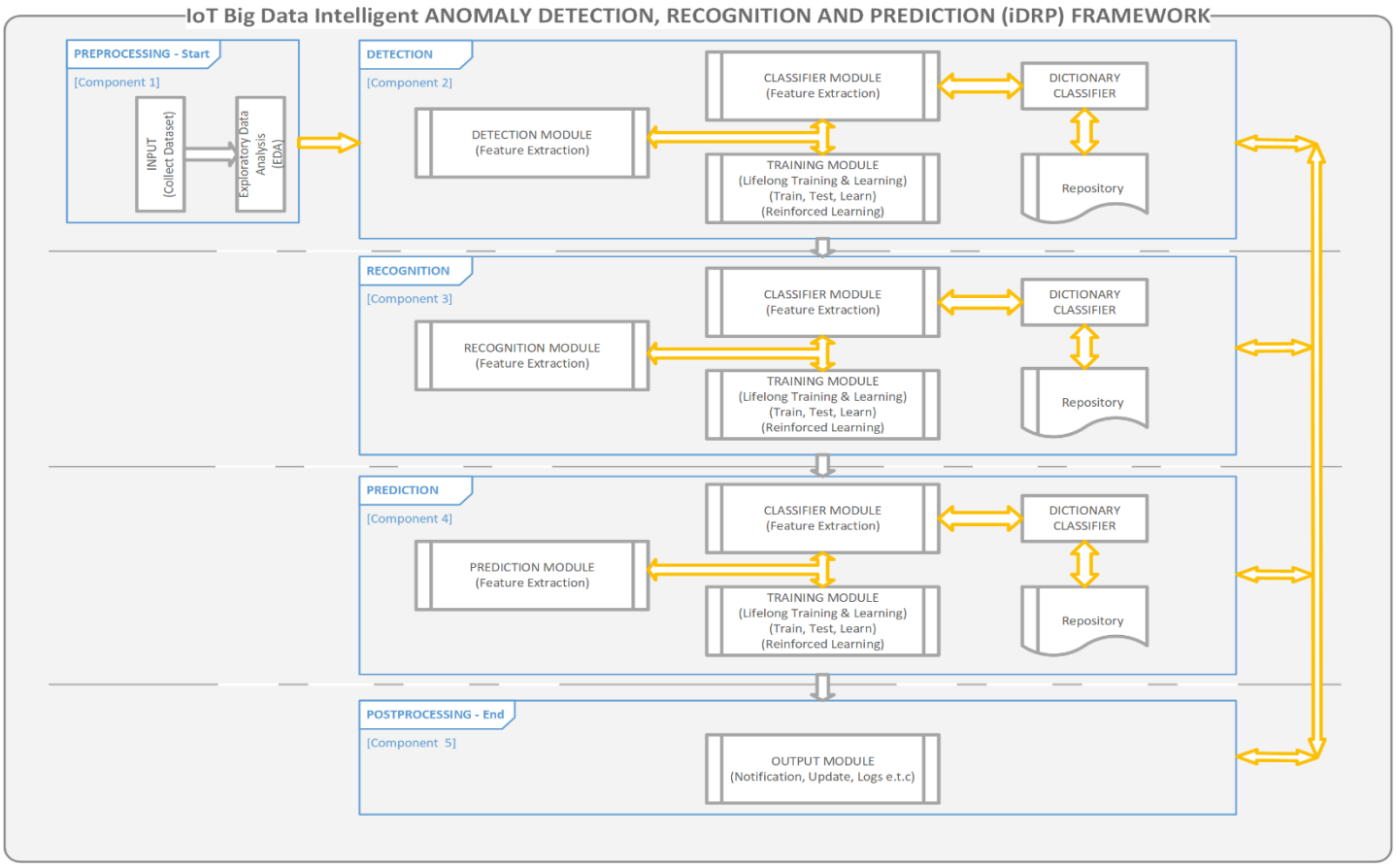

Figure 2: Proposed iDRP framework for Anomaly (Malware) Identification in IoT ecosystem – Overview [1]

4. The Proposed iDRP Framework Architecture

This section provides the analysis of the proposed Intelligent anomalies detection, recognition, and prediction (DRP) also known as iDRP-framework as shown in Figure 2. The conceptualization of the proposed iDRP-framework is based on the relationship between feature extraction, feature classification, precision in the identification of anomalies, and predictions of anomalies in the generated dataset of IoT ecosystem. Table 1 and 2 displays the synthesis of the list of the development techniques comparatively in tandem with the corresponding frameworks' techniques to be synthesized and applied for the development and validation of the proposed intelligent framework. The information gathered in the literatures of this research study has clearly shown that there still exist gaps in effectively tackling the myriad of anomaly detections, identifications, and recognition in complex data sets generated in an IoT ecosystem.

The limitation in the forecasting of anomalies (malwares) in the IoT ecosystem forms the spine of this research study and consequently the creation of an Intelligent framework called iDRP-framework to address the issues of anomalies (malwares) identification in an IoT ecosystem. In particular, the ability to accurately Detect, Recognize, and Predict (DRP) anomalies (malwares) from logging big datasets generated in an IoT ecosystem cannot be overemphasized.

Evidently, the extraction of miniscule features of the big datasets to assist in the '*fine-grained classification*' of features of complex datasets has been demonstrated by other researchers [30],[36] to help in the precision of anomaly identification in an IoT ecosystem.

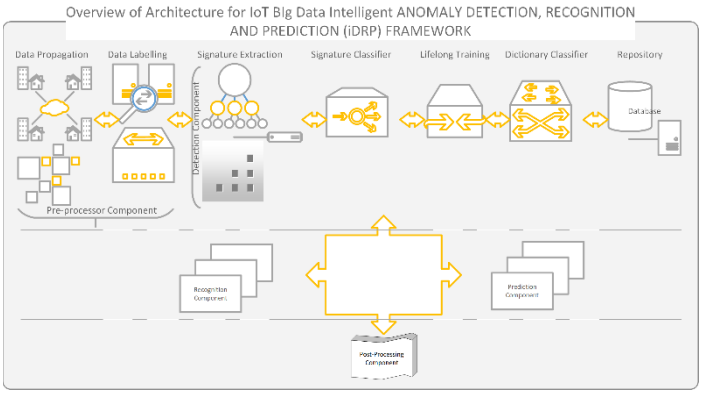

Figure 3: Proposed iDRP framework for Anomaly (Malware) Identification in IoT ecosystem – Architecture Breakdown

Figure 3 illustrates the overview of the proposed iDRP framework architecture with the "*Data Augmentation*" segment consisting of data propagation, data labelling, feature extraction, and feature representation etc. The proposed iDRP framework architecture is flexible, robust, and adaptive in its design to intelligently and effectively extract mapped minuscule information in the stacked layers of the proposed iDRP framework for detecting, recognizing, and predicting malware binaries in an IoT ecosystem.

Table 1: Synthesized Components of Development and Validation of the Proposed iDRP Framework I [1]

No	Comparative Features of Synthesised Frameworks I							
	Features	H-ELM	SAPIM	Smart Weather	Flight Monitoring	eTRIKS	Data Lifecycle	DRIPROM
1	Pre-processor	✓	×	✓	✓	✓	✓	✓
2	Detection	✓	✓	✓	✓	✓	✓	✓
3	Recognition	✓	×	×	×	×	✓	✓
4	Prediction	×	✓	×	×	×	×	×
5	Post-processor	×	×	×	×	×	×	×
6	Lifelong Learning	×	×	×	×	×	×	×
7	Lifelong Training	×	×	×	×	×	✓	×
8	Cyclic Feed	×	×	×	×	×	✓	×

Key: H-ELM (Tang, Deng and Huang, 2016), SAPIM (Wang et al., 2018), Smart Weather (Onal et al., 2017), Flight Monitoring (Li, Ming and Li, 2017), eTRIKS (Oehmichen et al., 2017), Data Lifecycle (Arass, Tikito and Souissi, 2018), DRIPROM (Cuzzocrea and Damiani, 2018).

Table 2: Synthesized Components of Development and Validation of the Proposed iDRP Framework II

No	Comparative Features of Synthesised Frameworks II						
	Features	IoT-HarPSecA Framework	3-Way IoT Framework	IoT-Flock Framework	FIFAC Framework	BiDeL Framework	Combat Intelligence Framework
1	Pre-processor	✓	×	×	×	✓	✓
2	Detection	✓	✓	✓	✓	✓	✓
3	Recognition	✓	×	×	×	×	✓
4	Prediction	×	✓	×	×		
5	Post-processor	×	×	×	×	×	×
6	Lifelong Learning	×	×	×	×	✓	×
7	Lifelong Training	×	×	×	×	×	✓
8	Cyclic Feed	×	×	✓	✓	×	✓

Key: IoT-HarPSecA Framework (Samaila et al., 2020), 3-Way IoT Security Framework (Zeeshan, Reed and Siddiqui, 2019), IoT-Flock Framework (Ghazanfar et al., 2020), FIFAC Framework (Awadelkarim Mohamed and Abdallah M. Hamad, 2020), BiDeL Framework (Otoo-Arthur and van Zyl, 2020), Combat Intelligence Information Monitoring Framework (Jin, Xing and Wang, 2020).

Table 1 and Table 2 lists the synthesis of the development techniques comparatively in tandem with the corresponding frameworks' techniques to be applied for the development and validation of the proposed iDRP framework.

4.1. Overview of Proposed iDRP Framework

Notably, Figure 1 shows the diagram of the proposed iDRP framework with extraction mechanism as a pre-processor and cyclical post-processor apparatus of logged complex dataset in an IoT ecosystem. These form the backbone of the novelty in the proposed iDRP framework. Significantly, from what has been learnt from the literatures of the existing knowledge domain that was conducted through the in-depth investigations, the aforementioned gaps in the anomalies (malwares) identification in an IoT ecosystem will be effectively tackled with the proposed technique for the novel iDRP framework.

4.2. Components of Proposed iDRP Framework

- *Preprocessing* – The pre-processing component, which is one of the major contributing steps in the framework to effectively address the aforementioned identified problems in the anomaly identification in IoT ecosystem. This component 1 involves the incorporation of Pre-Processor of a complex dataset by using ML technique like the enhanced traditional Data Augmentation techniques – blend of Enhanced Data Augmentation techniques and Propagations.
- *Detection* - The signatures extracted in component 1 will be fed forward to the component 2, the detection component for effective classification of signatures and labels i.e., '*fine-grained classification*' mechanism for feature learning to precisely detect Malware anomalies in an IoT ecosystem. Likewise, the Learning and Training of anomalies signatures experiments will be conducted extensively combined with Dictionary Classifiers and the Database of both the new and historical malwares in the detection component.
- *Recognition* - A similar procedure will be performed in the component 3, the recognition component, with the primary aim of precisely recognizing each specific Malware in the logged complex data of IoT ecosystem.
- *Prediction* - Correspondingly, in the component 4, Prediction component, the forecast of anomalies will be rationalized and realized by synthesizing the components 2, 3 and 4 for accurate predictions of the occurrence of anomalies in an IoT ecosystem.
- *Postprocessing* - In component 5, Post-Processing, the assessed anomalies will be fed back into the entire system in a cyclic manner. This '*feed-forward*' and '*feed-backward*' propagation methods that were applied and implemented in the model of the framework will essentially ensure that the framework is well-adjusted, robust, intelligent, and adaptable adequately to address the growing threats and risks in the IoT security paradigm.

4.3. Preliminary Experiment for Proposed iDRP Framework

The preliminarily experiments were conducted using MNIST dataset, a standardized dataset, which is comprised of small 28x28 pixels of randomized hand written number images with corresponding annotated numbers as labels. The MNIST dataset presents a better experimental starting point for developing the MLP for the recognition of patterns in the converted log file image with minimal pre-processing and formatting overhead cost for the ML and DL models. The standardized MNIST dataset used in this experiment contains 34,300 training set samples and 14,700 test images of 28x28 = 784 pixels for each image, which is a subset of original 60,000 training set samples of the standard benchmark MNIST dataset.

4.4. Conceptual Implementation of Proposed Framework

The Data Augmentation techniques and propagation techniques [30],[31],[37], which helped with the '*fine-grained extraction and classification*' of signatures of complex datasets were applied to the model implementation of the proposed novel iDRP framework. The applied research approach for the development of the iDRP framework is implemented using Python Programming language (https://www.python.org/), which is an open-source language with rich and extensive libraries that is easily accessible to the general masses. Keras (https://keras.io/), a high-level library that is built upon a low-level library such as TensorFlow (https://www.tensorflow.org/) is used for implementing the required Neural Network (NN) with simplistic interface that is built on the Python platform as a native Python library. TensorFlow serves as the tensor manipulation library to Keras, as a bridge low-level Application Programming Interface (API) for the robustness of implementing minimalistic and concise NN models. Significantly, Keras has several extensible modules that are suitable and adaptable to advanced scientific research work, which has formed the basis for the informed decision to choose the combination in implementing the complex NN models

especially for the stacking of the various layers; hierarchical models for this experiment.

4.5. Neural Network (NN) of Framework

The NN has been able to provide access and manipulation to the fed benchmarked dataset dynamically while exploring the binary features of the converted logged image files with different categories in the pre-processing of the dataset, while the necessary adjustments were made accordingly. Importantly, different layered NN combinations have been explored while calling upon the Functional model, '*tf.keras*' to provide the building blocks and backend support for the configurable NNs [29] for the training, testing, and prediction in the application. The novelty of the approach in the development of the proposed iDRP framework is to use dynamic Pattern-Based model approach to intelligently and accurately detect, recognize, and predict anomaly in an IoT ecosystem.

4.6. H-ELM Derivative Formula

A formular for the H-ELM was derived from [30],[31] as a result of the amalgamation of the Radial Bias Function (RBF) nodes with the defined Activation function [30] for mapping indiscriminate features of the converted logged datasets of an IoT ecosystem. The primary aim is to precisely approximate the continuous targets with mobility at the evolving RBF nodes adaptively [30],[31],[37]. This ensures the irregular initialization of the hidden nodes H in a given set of big data in an IoT ecosystem. This is expected to significantly reduce the training errors while increasing the precision in the accuracy of the output with better performance and speed.

$$H = \begin{bmatrix} h(x_1) \\ \vdots \\ h(x_N) \end{bmatrix} = \begin{bmatrix} h_1(x_1) & \dots & h_L(x_1) \\ \vdots & \vdots & \vdots \\ h_1(x_N) & \vdots & h_L(x_N) \end{bmatrix} \quad (1)$$

where H is the randomized hidden layer output matrix, which denotes the hidden nodes and output weights of the Neural Network, while $x_1 \dots x_N$ is the number of training dataset.

$$\boldsymbol{T} = \begin{bmatrix} \boldsymbol{t_1^T} \\ \vdots \\ \boldsymbol{t_N^T} \end{bmatrix} = \begin{bmatrix} \boldsymbol{t_{11}} & \dots & \boldsymbol{t_{1m}} \\ \vdots & \vdots & \vdots \\ \boldsymbol{t_{N1}} & \dots & \boldsymbol{t_{Nm}} \end{bmatrix} \quad (2)$$

where T represents the training dataset of the target matrix.

In order to optimize the performance of the ELM feature mapping, the following formula is applied:

$$\beta = \mathrm{H}^{\mathrm{T}} \left(\frac{1}{\lambda} + HH^T\right)^{-1} T \quad (3)$$

The resultant output of the ELM feature mapping will be

$$f(x) = h(x)\beta = h(x)\, \mathrm{H}^{\mathrm{T}} \left(\frac{1}{\lambda} + HH^T\right)^{-1} T \quad (4)$$

Alternatively, the equation is condensed to

$$\beta = \left(\frac{1}{\lambda} + HH^T\right)^{-1} H^T T \quad (5)$$

The derived output function of the ELM feature mapping is

$$f(x) = h(x)\beta = h(x) \left(\frac{1}{\lambda} + HH^T\right)^{-1} H^T T \quad (6)$$

In the hidden nodes H of the training dataset, hidden information can now be exploited and extracted from the hidden layers h to transform T the output weights β. This will ensure minimal fine-tuning of the parameters or weights of the hidden layers with stable minimal overhead cost to achieve maximum output. This randomized approximation and differential evolution technique has been proven [30]-[32] to be effective, which ultimately secures the increment in both the feature learning and classification.

5. The Need to Convert IoT Malware Binaries to Images

The technological advancements in present-day cyberattacks has made the activities of advanced attackers more complex to detect as a result of emerging obfuscation techniques [27], [38], [39] and interactions [40] with stealth variations carried out on IoT ecosystems.

In modern times, the emerging polymorphic malware attacks in the IoT ecosystems have been a major concern [1] due to complex obfuscation code structures that are mostly time based [41], [42]. These IoT malware signatures attacks that are predominantly multivariate [39], [40], [42]-[44] are updated sequentially on a minute-by-minute or hour-by-hour basis by the attackers, thereby inundating and *silencing* any potential alert system, which may cause massive vulnerabilities for exploitations in an IoT ecosystem. The current widespread detection and mitigation mechanisms for these emerging polymorphic IoT malware attacks that are largely obfuscated intricately can be problematic and resource intensive to both the traditional and automated malware detection solutions such as the signature based (e.g., large database), and automated based techniques (insufficient information) etc., adopted by major cybersecurity vendors, practitioners, and researchers in the cross-discipline cybersecurity industries. The domain experts and analysts may write different rules manually or automatedly to detect complex obfuscated malware scripts in an IoT ecosystem as a possible approach to solving the problem, the caveat to such an approach in determining the benignity or maliciousness of such malware binaries in an IoT ecosystem is that it would be near impossible to efficiently and accurately determine either a clean or infected malware script in the IoT ecosystem – *subtle obfuscated IoT malware classification problem.* It certainly would be time and resource intensive to adequately write thousands and/or millions of rules for virtually all current and new malware obfuscation variants in the contemporary IoT ecosystem.

Evidently, the aforementioned complex IoT malware detection approaches are no longer suitable for current growing subtle and complex obfuscated cybersecurity paradigm for five (5) major reasons: (1) the distinct fragments (sections) of converted IoT malware image file can be visualized [27], [38]; (2) the distinct textural patterns of the converted IoT malware image files can be classified (and reclassified), and analyzed using image processing [27], [45] classification techniques commonly applied in computer vision [30], [31]; (3) the advanced attackers typically modify or reuse codes to generate new variants of complex obfuscated IoT malware scripts [38]-[40]; (4) the vector structures of converted IoT malwares image files of the same family are similar [27], which means vectorized representation (i.e., faster speed) of the IoT malware image files will be sufficient to be fed directly as

input into the similar ML-DL algorithms [30], [31] built for image and pattern recognitions [27], [45]-[47]; (5) the captured IoT malware dataset once converted to image files will be immutable (nondestructive and tamper proof), so there is no workaround its state by the attackers. Therefore, an amalgamation and syntheses of the modern ML-DL techniques and methods designed utilizing converted immutable IoT malware binaries to image files is both a logical and pragmatic solution to the current rapidly growing complex IoT malware problems that would scale adaptively.

5.1. The Benefits of Converting IoT Malware Binaries to Images

One of the biggest advantages of converting IoT malware binaries to Gray-scale image files is the fact [27] that the IoT image maintains the structures and patterns with rich information – *structural integrity*. The immutability of the IoT image files guarantees that converted complex IoT malware scripts will always be reliable to work with (ensuring a total control of the collected IoT malware dataset in the environment without the risk of compromise externally) by leveraging the ever-growing advancement of modern technologies such as Artificial Intelligence. Moreover, the structural integrity of the stately converted IoT malware image files facilitate the high-level precision and accuracy of detection of minuscule byte codes of the clean or infected codes with corresponding Cross-Validation techniques of modern ML-DL algorithms – *efficient detection, recognition, and prediction of anomalies in an IoT ecosystem.* Another advantage of converting IoT malware binaries to image file is the speed (time) of processing and computing the thousands and millions of both the benign and malicious IoT malware image file vectors using ML-DL techniques – *computational time*.

5.2. Visualization of IoT Malware Image for Exploitations

The textural and structural anatomy of IoT malware image files reveals the intricacies and patterns of the minuscule information that are sufficient for synthesized spatial and differential exploitations and analysis [27], [30], [31] of the tiniest byte codes (exploiting hidden structural and textural information by utilizing advanced ML-DL techniques and methods i.e., '*fine-grained*' layer-by-layer mapping and representations) of the features of converted complex IoT malware image files with high-level precision and accuracy in an IoT ecosystem – effectively distinguishing the benignity and maliciousness within a few bytes of codes as shown in Figures 4 and 5.

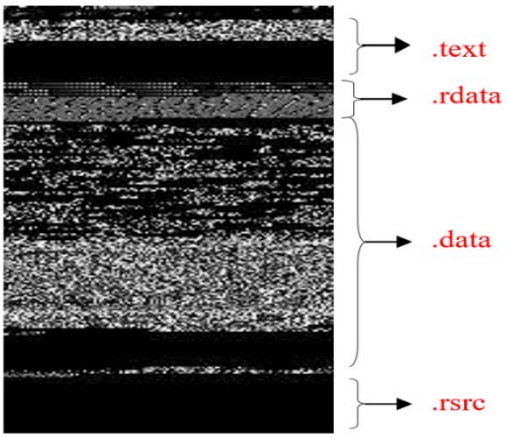

Figure 4: Visual structure of IoT Malware image file

The Figure 4 above shows the visual representation of the sections of a converted IoT malware image file with different segment textures (https://code.google.com/p/pefile/). The above section representations (*.text* = '*fine grained*' section with unique validity of data on the Operating System (OS) level e.g., Windows, Linux, *.rdata* and *.data* = the uninitialized and initialized scripts are the header and section table of the file that distinctively separates the unlaunched and launched codes respectively, *.rsrc* = the resource section that contains mostly padded zeros. These structures and patterns are important because the slightest of modifications (changes) in the variations of IoT malware binary codes can be easily detected stately – often within a few bytes.

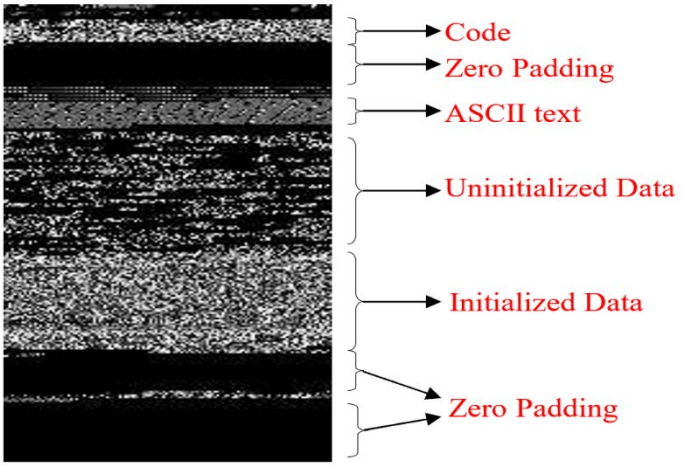

Figure 5: Visual structure of IoT Malware image file (Rich Information)

The Figure 5 above shows the rich visual representation of the section of an IoT malware image file with extensive details for exploitations and analysis. The segmented textures and patterns are essential for the pattern recognition of both benign and malicious IoT malware binaries converted to image files in an IoT ecosystem. The various segments of the IoT malware binary file structure are easily isolated for the synthesis of spatial and evolutionary feature mapping (i.e., spatial and evolutionary data matrix), extractions, representations, classifications, and Cross-Validation of the hidden minuscule features (i.e., the IoT malware signatures in the *header*, *sections 1*, *2*, and *section+n*) of the converted IoT malware image files by utilizing ML-DL techniques and methods with high-level precision and speed of detection of complex obfuscated anomalies in an IoT ecosystem.

5.3. Overview of Converting IoT Malware Binaries to Images

The conversion of typical binary files is based on standardized OS binary file format structures, which is analogous to debugging and homologous to reverse engineering of malware binary programs structurally. This can be simply performed using various *python* libraries such as *pefile* (https://code.google.com/p/pefile/) for fundamental exploration, understanding, and analysis of the layout features of a binary program. However, for a more in-depth exploration, exploitation, and analysis of rich hidden features, a systematic approach has to be applied to gain valuable insight into the various layers and architectures of the IoT malware binary file to image file. These procedures for converting IoT malware binaries to image files consists of the following five (5) fundamental steps: (1) Sort Dataset (i.e., variants, variant name,

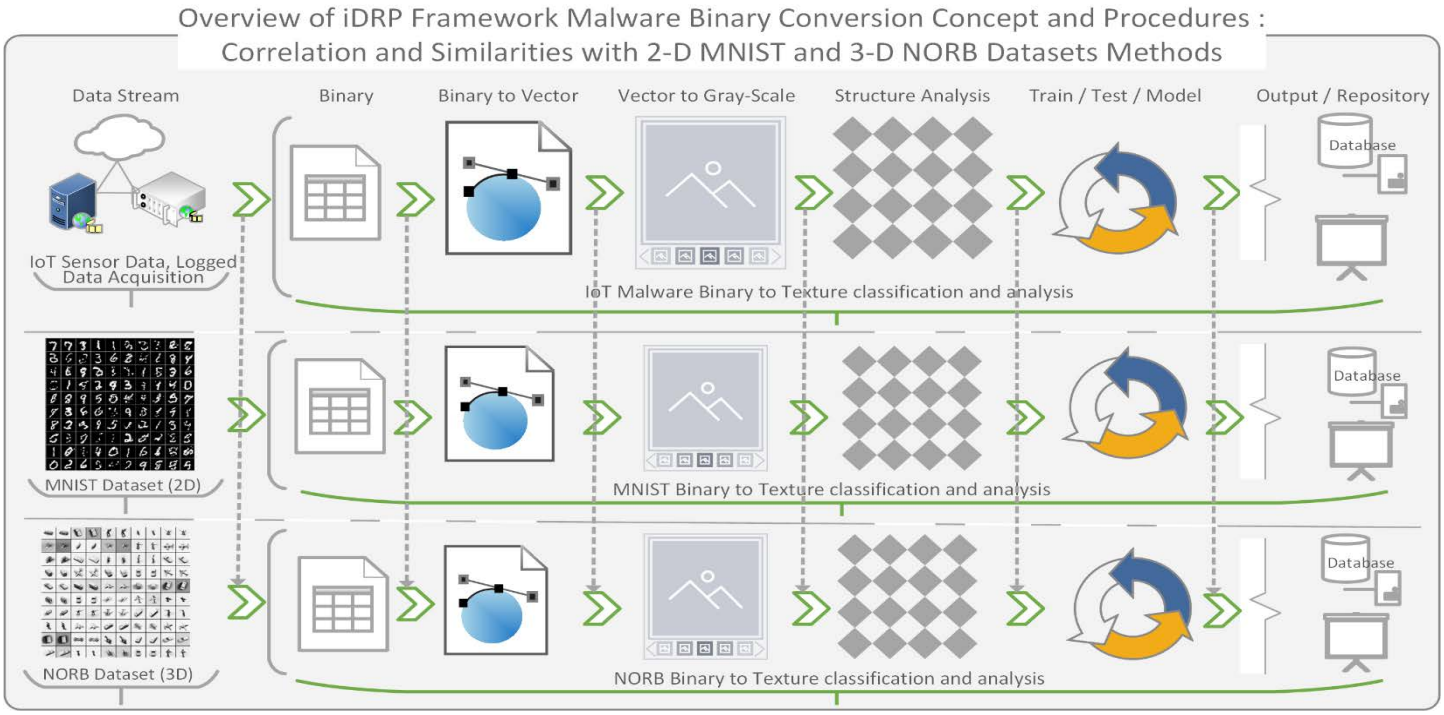

Figure 6: Comparison of similarities between the classification and analysis procedures for IoT malware images and MNIST and NORB datasets

no. of occurrence) retrieved by attributes; (2), Import Libraries (e.g., os, *numpy*, *scipy*, and *array*) to access and extrapolate the IoT malware binaries; (3) Augment IoT Dataset (i.e., *reshape*, *resize*, and *scale* et al) the dataset; (4) Standardize the IoT dataset; (5) Save the converted IoT malware images in a repository. Thereafter, feature selections techniques for consistent feature vectors (i.e., color range, intensity, pattern structure) can be performed on the converted IoT malware image files and processed as input feature classifications – *supervised learning*.

6. Experimental Implementation of iDRP Framework

The approach for the experiment of the proposed novel iDRP framework [1] involves the cleaning, manipulation, and extraction of IoT malware binaries to be preprocessed, and visualized as IoT malware image file for the evolutionary exploitation of hidden minuscule segment features for both supervised and unsupervised structural features representations and classifications with high-level precision to detect, recognize, and predict anomalies in a heavily computerized network system such an IoT ecosystem.

This experimental implementation of the proposed novel iDRP Framework is a proof-of-concept for the research study. The experiments were conducted with several distinct structural different datasets (BoTNet-IoT [43], MNIST, virus-MNIST, and NORB datasets etc.), yet similar conceptual procedures and methods (e.g., Figure 6) in the multiclassification and analysis to extrapolate meaningful hidden information for sound scientific evaluations and validation quantitatively. The Figures 7, 8, 9, 10 represent and demonstrate the correlations between the textual standardization methods of the IoT malware images, MNIST images, and NORB images datasets. This is to enable the systematic implementation and evaluation of the performance of the proposed novel iDRP framework techniques and methods (e.g., Figures 11, 12, 13, 14) for optimal malware binaries' classification and analysis in the present-day IoT ecosystem. The datasets used to perform the experiments were converted to 8-bit gray-scale 2-D array with a channel range between 0 to 255 for consistencies in the datasets. Essentially, this process generates a vectorized 8-bit binaries, which are then converted to the gray-scale 2-D image files for structural texture uniformity for extracting and detecting padded hidden information in a logged IoT malware file.

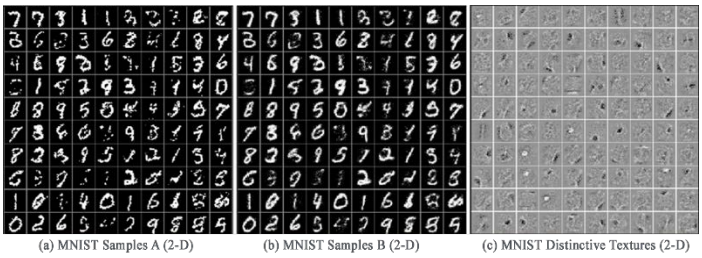

Figure 7: MNIST (2-D) images to Gray-scale images (0 to 255) standard channel

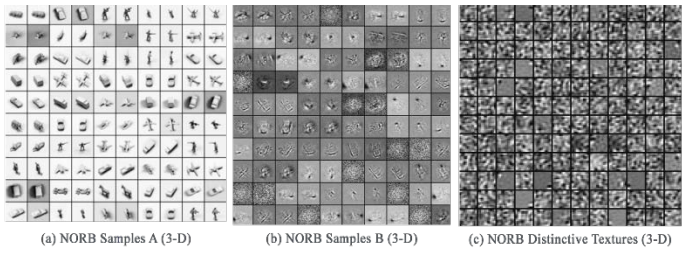

Figure 8: NORB (3-D) images to Gray-scale images (0 to 255) standard channel

The 3-D NORB image files, which has uneven generic object representations such as animals, vehicles, and nature etc. provide similar abundant natural environment and characteristics for representing, visualizing, and detecting certain distinct patterns of structurally complex textures of IoT malware variants that conceals hidden features that modern polymorphic and new malware engines in an IoT environment exhibits. This hypothesis was helpful for the scientific empirical and statistical observations

for the classification and analysis for the detection of IoT malware anomalies with high level precision and performance in the experiment for uniquely solving contemporary IoT malware obfuscation problems by attackers [1].

We performed the experiments on the premise and fact [48] that malware of the same family has similar characteristics and textures, while being distinct from other malware families in nature. Comparatively [48], for visual analysis of IoT malware binaries, the binary fragments of polymorphic and new malware variants are visually similar and consistently fragmented alike by the same token in terms of their image dissections and layouts as with their primitive nature irrespective of the malware variants or obfuscations and their specialized binary complex code structures.

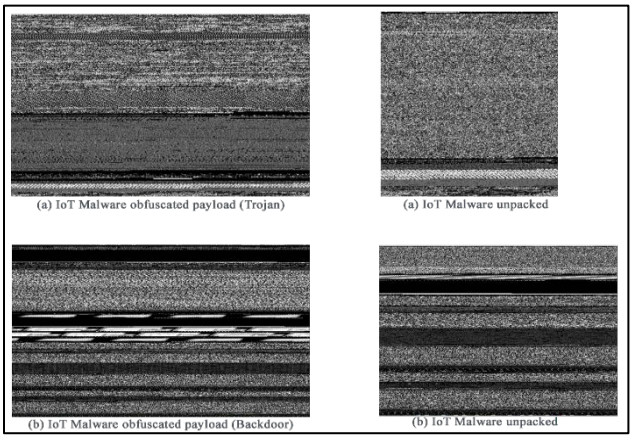

Figure 9: Captured IoT malware images with binaries I

Therefore, we approached the problem by proposing an iDRP framework techniques and methods that leverages both the H-ELM [30] and E-HELN [31] techniques and methods for universal approximation using differential evolution for optimized generation of complex image features to precisely extrapolate hidden features of IoT malware binary images files for expedient training and learning in the DNN. The advantage of these synthesized techniques and methods is that they both provide an optimized classification and characteristics learning and training coupled with minuscule and hidden feature representation modules for accurately *detecting*, *recognizing*, and *predicting* IoT malware binaries speedily.

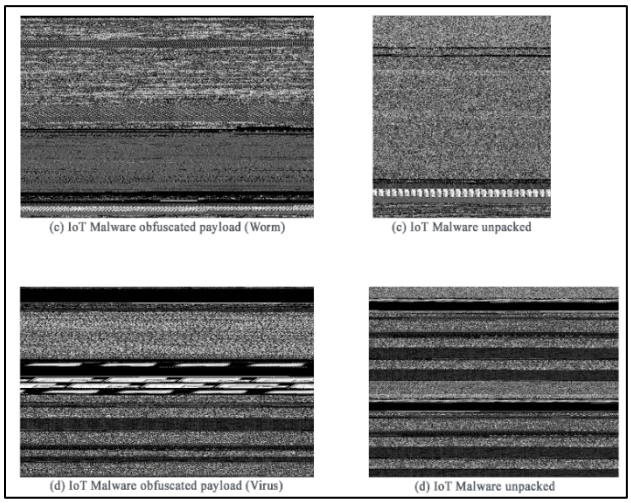

Figure 10: Captured IoT malware images with binaries II

The generative model techniques and methods that were applied cyclically in the iDRP framework to provide better discriminative capabilities for analyzing and evaluating the captured IoT malware binary information and statistics with high level precision and performance.

Overall, we explored and computed (gray-scaled etc.,) the binaries of the engineered BoTNetIoT malware dataset [43] exploits (Botnet attacks e.g., Mirai, Gafygt and their variants, and benign traffic etc. on IoT objects, devices, and environs), split them into 70% (training) and 30% (testing) ratio processed systematically and Cross-validated with a combination of both authentic benign and infected IoT malware traffic dataset with different strains [43], similar techniques and methods as with the statistical exploratory MNIST and NORB datasets experiments performed. The converted IoT malware gray-scaled images were normalized (min-max normalization, anti-aliasing techniques etc.), flattened, reshaped into 1-D and 2-D pixel and arrays for consistency and standardization. These were performed with the structured techniques and methods by applying the evolutionary adversarial training and testing techniques and methods for classification and Cross-validation to accurately estimate the comparative capabilities and skills (e.g., accuracy, precision, recall, and F1-score etc.) of the implemented techniques and methods in the proposed and implemented experiments. These were conducted for effective classification estimation and validation – *pre-processing of data*. These matched aggregated distribution of the train-test split techniques and methods together with the resampling methods, which are both semi-supervised and unsupervised classification clustered enabled the optimized resampling of the utilized datasets quantitatively. Specifically, with the categorical distributions mapped against data distributions of the IoT malware binaries and structures, empirical and statistical analysis of the results were scientifically established.

Evidently, captured IoT malware binary classification and analysis using the proposed integrated novel iDRP framework techniques and methods contributed provides treasure trove of hidden information exploited with both 2-D and 3-D images synthesized based on their distinct structural compositions and textures unpacked in comparison to static, dynamic, and automated analysis techniques and methods that are prone to present-day complex and unpacked code obfuscation and time consuming.

6.1. Pre-Processing Component Technique Overview

The data Pre-processing component in the proposed iDRP framework involved the augmentation, transformation, and classification of the raw dataset that are fed and parsed into the network. Feature extraction and mapping of the sparse data feed for layer representation of random features were performed to fully exploit the minuscule information [1] in the converted logged image files for universal approximation (i.e., MD5 Hashes and malware binaries) of the mapped datasets in the IoT ecosystem.

Figure 11 shows the pre-processing component of the proposed iDRP framework and its integration into the overall architecture. The pre-processor 'feed-forward' the systematically processed dataset (i.e., 'fine-grained' gray-scaled converted logged file) directly into the detection component of the proposed iDRP framework to ensure the universal approximation and classification of the precision and accuracy of detection of

anomaly is optimized for high-performance with detailed description for exploits – preparation of dataset for standardization.

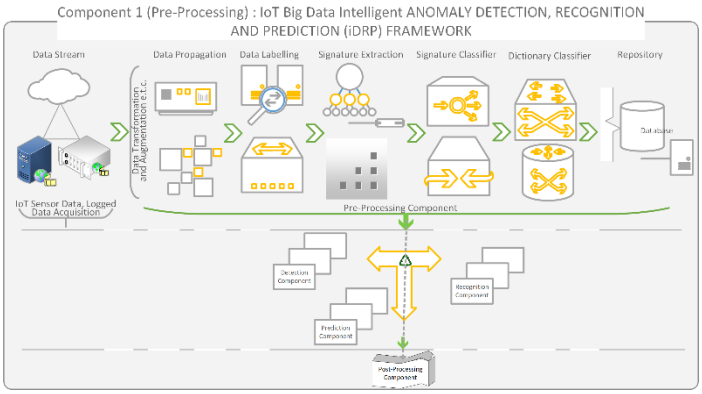

Figure 11: Pre-processing Component of iDRP Framework Overview

The systematic data manipulation techniques such as the systematic extrapolation of feature representations to form the vectorized structures applied in the experiment substantially helped in the distinction of the effective assignment of randomized and differentiated hidden layer weightages synthesized. The feature immutability techniques to stately capture complex code implemented in effect ensures that the feature extractions and data augmentations performed are compact and dynamic to materially eliminate unnecessary redundancies in the generated data. These scalable techniques intrinsically set the approximation numbers of the hidden nodes in the converted logged file of the original input dataset to achieve compact features for exploitations. Uniquely, these innovative and intelligent techniques implemented radically extrapolates rich hidden features for universal approximation competence on both the raw datasets and converted logged file to ensure that the delay in the binary classification analysis is effectively mitigated for optimal outputs in the proposed iDRP framework. Expediently, the compact features extracted and delivered to the next 'following' components iteratively, which is the detection components in the proposed iDRP framework.

6.2. Detection Component Technique Overview

The detection component involves the identification, determination, and classification of converted logged file dataset, whether such dataset is benign or infected. Considering this is a binary classification problem, several techniques [1] were deployed to achieve the expected results by conducting several systematic experimentations to discover the best suitable techniques. In particular, the systematic cross-validation splits, and weightage allocation techniques were beneficial for the classification precision and accuracy in the experiment of the detection component of the proposed iDRP framework.

Figure 12 shows the detection component of the proposed iDRP framework that is strategically the responsible component for determining whether the pre-processed data feed in the network is benign or infected with optimized classification precision and accuracy with maintained high-performance in an IoT ecosystem. Mainly, the mapped converted logged files are systematically rescaled and gray-scaled before they are dynamically fed 'feed forward' into the DNN of the IoT ecosystem.

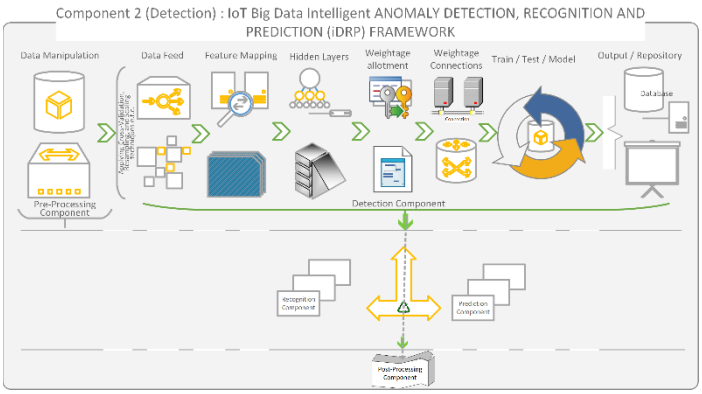

Figure 12: Detection Component of iDRP Framework Overview

The primary focus of the detection component is to intelligently identify the presence of polymorphic malware anomalies [1] with high level of accuracy in the converted logged dataset, which creates the unique separation of concern in its architecture – design principle. The detection component is robustly and innovatively designed in its structure to encapsulate the interaction between the dynamic and static states of the dataset in the converted logged file of an IoT ecosystem. By and large, the detection components feed and receives immutable mapped hidden information dynamically to exploit with other modular components in the proposed iDRP framework. The 'Loose Coupling' and yet cohesion of the detection component [1] essentially promotes the dynamic and robust interaction of the various components directly or indirectly connected to it in the proposed iDRP framework while explicitly performing the primary function of detecting anomalies (randomly and differential mapping hidden features) in the network system.

6.3. Recognition Component Technique Overview

The recognition component is inherently responsible for identifying what class of anomaly the detected malware family is associated with or lack thereof [1]. The recognition component explicitly curates the type of anomalies present if found in the network by precisely defining the exact variants or obfuscation of the IoT malware anomalies for launching attacks such as zero-day attacks. This unique technique involves the heuristic classification of variants of IoT malware anomalies in the network system [1], which are universally approximated in the random and differential feature mapped converted logged file that are rescaled and represented as gray-scale images in an IoT ecosystem.

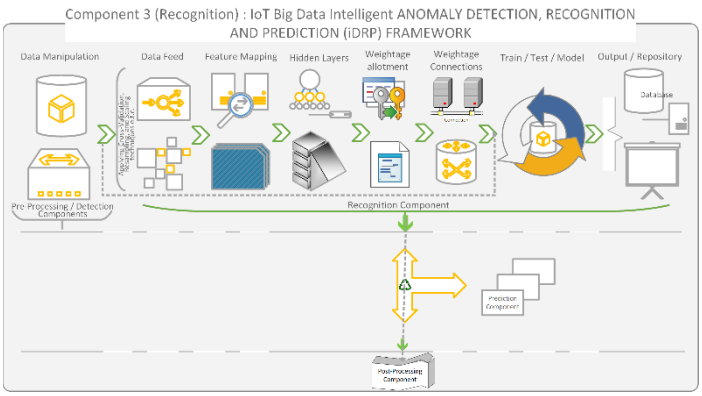

Figure 13: Recognition Component of iDRP Framework Overview

Figure 13 shows the recognition component of the proposed iDRP framework. The recognition component in the architecture of the proposed iDRP framework facilitates the structural distinction of the universally approximated mapped converted logged file in the DNN of the IoT ecosystem. Thereby determining and identifying the particular class of malware anomalies that each existential or inherent malware family belongs to while intelligently discovering new variants or obfuscation of such IoT malware anomalies in the process from the repository that could potentially result in a zero-day attack in an IoT ecosystem. This unique technique provides the capability for the proposed iDRP framework to be able to adaptively and robustly perform the required intelligent classification precision and accuracy [1] of recognizing specific types of anomalies in IoT ecosystem with high performance. The systematic integration of data from both the Pre-Processor and detection components ensures that there is both shared characteristics and cohesion amongst the interconnected components of the proposed iDRP framework. Constructively, the arbitrary boundaries established between the multi-directional connections that are 'Loosely coupled' essentially eliminates constraints in the shared information such as hidden layer features to and from 'fro' the recognition components to the preceding and forwarding components virtually in the proposed iDRP framework – architecture intelligence.

6.4. Prediction Component Technique Overview

The prediction component is practically responsible for predominantly predicting the occurrence of captured malware anomalies in the IoT ecosystem. The systematic elimination of unnecessary '*checkpointing*', '*overlearning*', and '*overfitting*' etc. techniques applied in the implementation of the prediction component effectively helped in the classification precision and accuracy of the predicted malware binaries innovatively in the experimental implementation of the proposed iDRP framework.

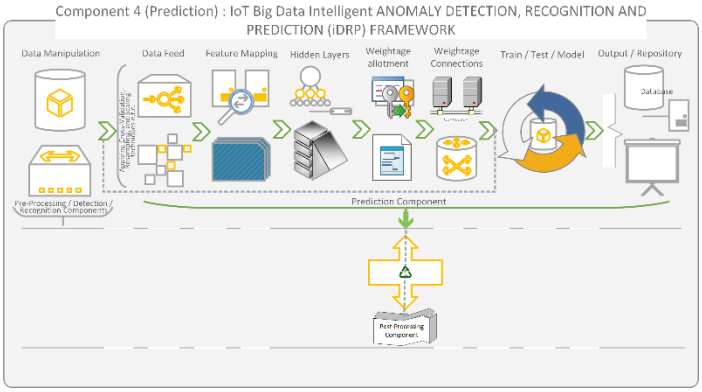

Figure 14: Prediction Component of iDRP Framework Overview

Figure 14 shows the prediction component of the proposed iDRP framework. One of the main features of the prediction components is that it can be configured to predict specialized family of malware binaries that are captured in the IoT ecosystem. Likewise, the systematic assignment of numerical score in the prediction component implementation ensures that the '*learning curve*' of the prediction classification precision and accuracy is properly monitored and dynamically optimized for high-performance. Crucially, the loss or error in the prediction component is systematically calibrated to ensure that the network is neither '*under-fitting*' nor '*under-learning*' to achieve maximum probabilistic outcomes in detection, recognition and prediction of malware binaries in an IoT ecosystem.

The prediction component employs the network weights to accurately predict the occurrence of malware binaries in the network system. The cyclical and infinite interconnection of the prediction component [1] to other components with accessibility to the repositories in the network ensures that the continuous learning of rapidly evolving malware families is adaptively and intelligently tackled in the growing threats and attacks on the technologically driven IoT ecosystem. In the prediction component, rigorous systematic estimate of the capability of the DNN model were performed exclusively. The prediction component of the proposed iDRP framework is highly effective predominantly due to the capability to systematically stabilize the universal approximation of the mapped hidden features that are fully exploited in the network – intelligent classification prediction technique.

6.5. Post-Processing Component Technique Overview

The Post-Processing component ensures the cyclical and infinite enhancement of the information distributed in the entire proposed iDRP framework [1]. The optimization techniques implemented guarantees that the loss i.e., 'validation loss' in the network model will always be minimized while fostering the continuous and lifelong learning in the network. The substantially reintroduction of the refined information dynamically and innovatively into the network forms the unsupervised building block technique in the overall implementation of the proposed iDRP framework. Broadly, the 'autoencoder' combined with the 'weightage reloading' concepts [1] are integral aspects of the unique features of the Post-Processing component in effectively maximizing the classification precision and accuracy support for the other interconnected components in the proposed iDRP framework.

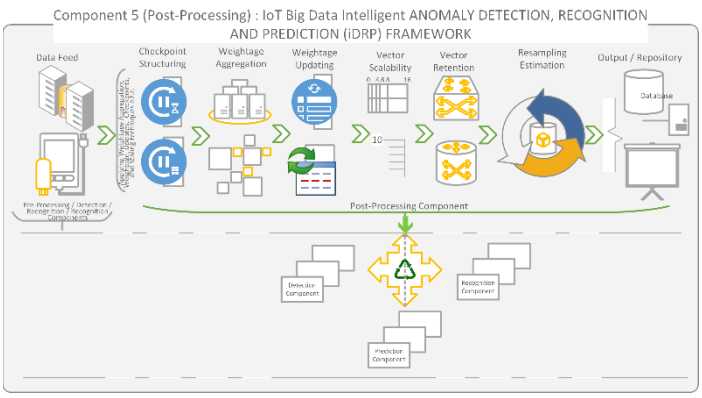

Figure 15: Post-Processing Component of iDRP Framework Overview

Figure 15 shows the Post-Processing component of the proposed iDRP framework. The systematic implementation techniques implemented in the Post-Processing component provide the comparable performance for the convergence of both the training and testing models for stochastic consistencies in the network while storing the models for exploration capabilities in the IoT ecosystem [1]. The Post-Processing component adequately helped stabilize the performance behaviour in the operations of the

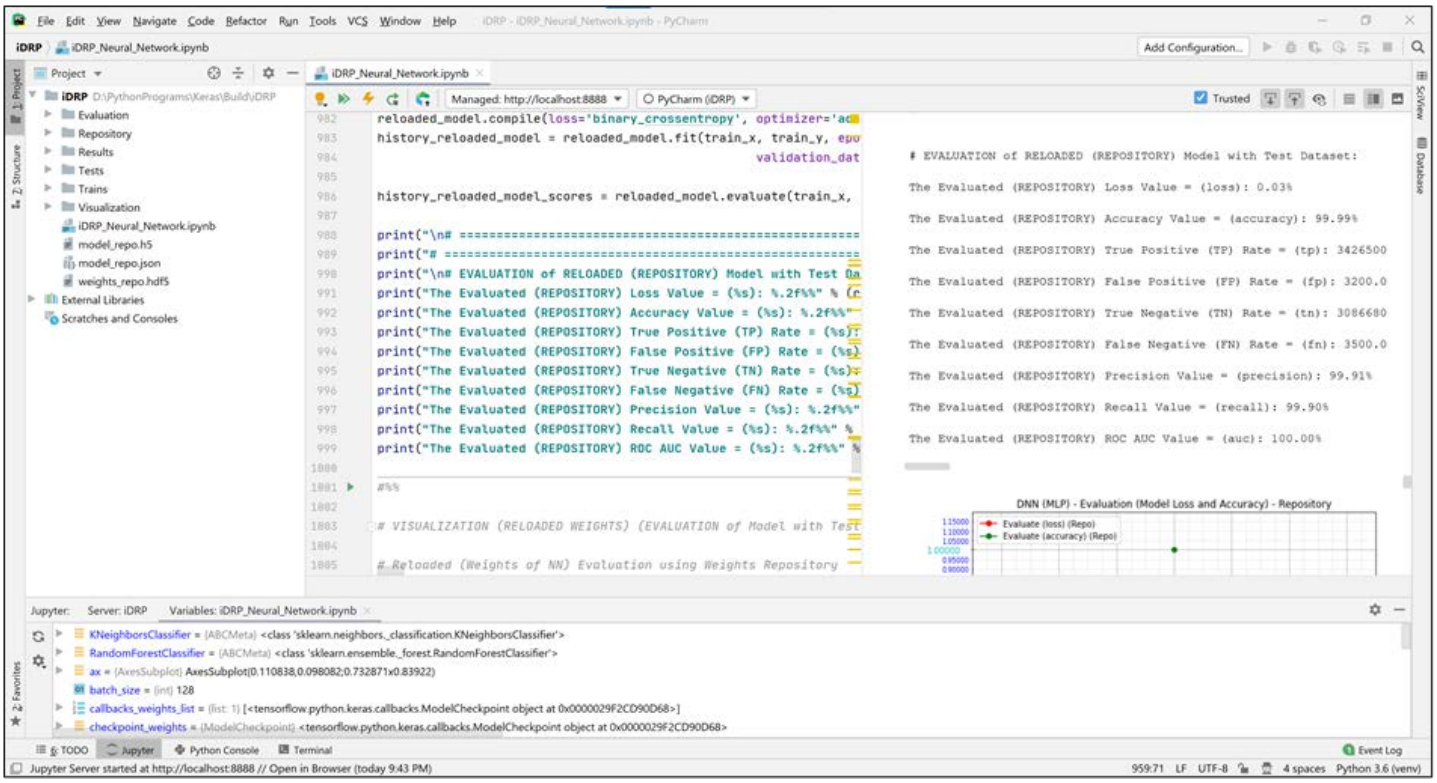

Figure 16: Results of implemented experiment of iDRP Framework with the corresponding snippet of metrics for evaluation

overall proposed iDRP framework via the *checkpoint structuring*, *weightage aggregation*, *weightage updating*, and *vector scaling and retention* techniques etc. With minimal 'hyper-parameterization', 'regularization', and 'resampling' techniques etc., the robust and innovative Separation of Concerns technique effectively helped to reduce redundancies in the implementation of the network for optimal competence and high-performance in detecting, recognizing, and predicting malware binaries and anomalies in a massively computerized network system such as an IoT ecosystem.

Specifically, the Post-Processing component is pivotal in the construction of the defined weights of the hidden features exploited for the lifelong learning of the overall proposed iDRP framework. With the Post-Processing component in the architecture of the proposed iDRP framework, minimal 'fine-tuning' is required while the other interconnected components can fully explore compact features in the universally approximated hidden features in the network [1]. Essentially, these specialized innovative and dynamic techniques implemented in the experiment further help to minimize the training, testing and learning time and overhead cost for both the existing and new datasets in the network [1]. The historical information aggregation technique in the network of the proposed iDRP framework are used to systematically discover and generate visualization and analysis of the classification precision and accuracy together with its overall high competency and performance.

6.6. Summary of Components Techniques

The generalized Artificial Neural Network (ANN) applied in the experimental implementation of this proposed iDRP framework is systematic and innovative Multilayer Perceptron (MLP) with Deep Neural Network (DNN) with integrated modular components to expedite the cross-validation methods for universal approximation and classification towards the effective learning, training, and testing capabilities for optimal outcome. The amalgamations of the unique innovative and intelligent random and differential feature extraction, augmentation, transformation, scaling, universal approximation, compactness, mapping, auto encoding, weightage saving, and weightage reloading, vector scaling and retention, cross-validation, resampling etc., techniques were successfully designed and implemented in the interconnected components of proposed iDRP framework to achieve core optimal results. The specialized immutable randomized and differentiated projections techniques implemented in the experiment formed the core of the feature representations of the complex malware binaries for classification precision, accuracy and analysis in the implementation of the proposed iDRP framework – *binary classification problem with complex structure system*.

The '*checkpoints*' of the network structures were set up to save model weights architecture intelligently and automatically whenever there is any improvement attained in the model classification system. The best part of some of the amalgamated specialized techniques implemented is that if there is no improvement in the weight classification of the model, then, the last highest improved weights will be applied in the model. Thereby maximizing the capability to accurately detect, recognize, and predict captured and generated malware binaries anomalies in an IoT ecosystem. The singularity of each of the components in the proposed iDRP framework ensured an easy to manage and maintain network. This generalized Separation of Concern technique ensures that each component in the proposed iDRP framework remains consistent and true to its primary function in the architecture.

The dynamic and innovative abstraction and segregation of the different components the implemented proposed iDRP framework makes it adaptable to the growing threats and attacks in the heavily computerized systems and smart technologies such as an IoT ecosystem. This fundamentally delineates specialized responsibilities amongst the various components in the network with flexible boundaries. Essentially, malware binaries data are analyzed and shared in the interconnected components while at its core separated in execution to perform specified operations in the proposed iDRP framework. The strategy deployed in the experimental implementation of the proposed iDRP framework has demonstrated the intelligent capabilities to determine the slightest of improvements in the network model weightage's structure and only save the best weights and architecture model together for future usage. This simply means that the overall system has been designed to continually learn, adapt, improve and perform better with time in combating the ever-growing malware threats such as the prevalent polymorphic IoT malware threats and attacks in the IoT ecosystem.

The overall procedures involve (a). pre-processing of dataset, (b). loading of dataset, (c). augmentation of dataset (d). creating of model architecture (e). compiling of model (f). fitting of model (g). evaluation of model (h). saving of model weights (i). loading of saved model weights (j). evaluation of saved model (k). post-processing of outcome. These approaches were conducted in multiple hidden layers Neural Network 'feed-forward' propagation and cyclic method using Deep Learning (DL) models to precisely, efficiently and optimally and intelligently detect, recognize, and predict (iDRP) anomalies in an IoT ecosystem. Cumulatively, several ANN techniques were leveraged innovatively and intelligently to significantly improve the classification precision, accuracy, and performance in the implementation of the proposed iDRP framework. Notably, the dynamic and innovative extensibility and maintainability of the proposed iDRP framework has made it highly adaptable and adoptable in effectively safeguarding and protecting critical infrastructures in multi-industries that depends on heavily computerized interconnected network systems and smart technologies such as an IoT ecosystem in the digital space.

7. Results, Observations and Discussions

A 100% accuracy rate, 100% ROC/AUC rate together with a precision rate of 99.94%, and recall rate of 99.90%, and merely a loss rate of 0.02% were achieved in the preliminary implementation of the iDRP framework experiment. Please see Figure 16 screenshot for the output of results and metrics. These results were attained based on the syntheses of the various techniques and procedures applied and discussed in the previous sections.

In like manner, a 99.98% accuracy rate, 99.99% ROC/AUC ROC/AUC rate together with a precision rate of 99.95%, and recall rate of 99.93 %, and a mere loss rate of 0.03% were achieved in the actual implementation of the integrated iDRP framework experiment using real IoT malware dataset – BoTNetIoT dataset.

The metrics used in evaluating the experimental implementation of the proposed iDRP framework are: Accuracy rate, Precision rate, Recall rate, Receiver Operator Characteristic (ROC) and Area Under the Curve (AUC) rate, Loss rate, True Positive (TP) rate, False Positive (FP) rate, True Negative (TN) rate, False Negative (FN), and F1-Score respectively.

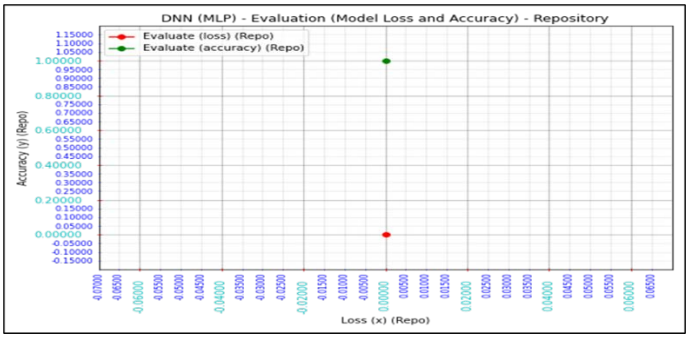

Figure 17: Graph of Accuracy and Loss Results of implemented experiment of proposed iDRP Framework

Figure 17 shows the result of the evaluated models of the experimental implementation together with the corresponding rates and scores. The 100% accuracy value, 100% ROC/AUC value with a precision value of 99.90%, and crucially with a much lower False Positive (FP) rate. that were attained in the experimental implementation of the proposed iDRP framework shows that there is a correlation in the accuracy, ROC/AUC, and precision rate in the Deep Learning (DL) classifiers in tandem with the hypothesis of the research study. It further proves that the experimental implementation of the proposed iDRP framework in this research study is highly innovative, applicable, useful, relevant and efficient; accurate, precise, robust, dynamic, adaptable, and scalable in detecting, recognizing, and predicting anomalies in the form of polymorphic malwares in an IoT ecosystem.

The visualization of the results of the models evaluated were represented in plotted Deep Neural Network graphs and charts to gain better insights and understanding of the complex binary classification matrix problems and solutions in the experimental implementation of the proposed iDRP framework. Figure 10 displays the optimal efficiency and accuracy correspondingly with insignificant loss rates in relations to the performance of the evaluated model for detecting, recognizing, and predicting the anomalies in an IoT ecosystem. Minimal training was required.

Logically, it is understandably that 50 epochs would likely fare better than a 5 epochs of model training and testing of datasets. At the same time, with a direct comparison of the regular 50 epochs with the 50 epochs' '*Checkpointing*' Deep Neural Network model technique of intelligently and systematically saving and reloading the best performance weightage in the repository of the overall system, a 100% accuracy rate and a 100% ROC/AUC rate together with a 99.94% precision rate and 99.90% recall rate of detection, recognition, and prediction of the anomalies in an IoT ecosystem was achieved in the experiment.

7.1. Cross-Validation and Evaluation Performance of Predictor Model Results

The results of the various output attained in the experiment on the proposed iDRP framework network has been reported in Table 3. The output of the different techniques towards the innovative synthesis, augmentations permutations, adjustments, and tuning of parameters in the Neural Networks together with various optimization techniques in the experiment has been extensively

investigated and compared to show the selected outcome in the project.

Table 3: Comparison of the Experimental Results

Cross-Validation Classification Parameter Tuning Metrics of iDRP (MLP) Model using *Keras* Library with Tensorflow Backend

Dataset (MNIST)	NN Layers	Epoch (Iterations)	Optimizer	Learning Rate	TPR	FPR	Precision	Recall	MAE	F-Score	Accuracy (%)	Training Time (s)
✓	5	5	ADAM	0.02	0.924	0.924	0.924	0.924	0.200	0.947	92.43	1.00
✓	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
✓	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
✓	50	50	ADAM	0.02	0.996	0.996	0.996	0.996	0.159	0.979	99.60	10.00
✓	50	50	ADAM	0.01	0.999	0.998	0.999	0.998	0.010	0.998	100.00	0.03

Legend: MLP=**Multilayer Perceptron,** NN=**Neural Network,** Learning Rate=**Dropout Rate,** TPR=**True Positive Rate,** FPR=**False Positive Rate,** MAE=**Mean Absolute Error,** F-Score=**Measure of Test Accuracy**

Table 3 displays the comparison in the various parameter tuning and optimizations performed in the experiments together with their corresponding metrics and results. It is evident that the continuous tuning process has significant impact on the overall output, especially with the classification precision and accuracy of the predictors. Likewise, the optimization parameter ADAM plays a vital role in minimizing loss function while increasing the speed of the convergence of the Neurons in the system. The dynamic and cyclic hyperparameter tuning approach in the Neural Network construct of this experiment will ultimately facilitate an incremental and better outcome.

7.2. Comparison of Generalized Artificial Neural Network (ANN) Results

The selection of the appropriate NN model for the implementation of the proposed iDRP framework involved the systematic experimentations of various streamlined and focused ANNs such as Recurrent Neural Network (RNN), Convolutional Neural Network (CNN), Multilayer Perceptron (MLP), and Hybrid Network (synergy of RNN and CNN) to effectively determine the best possible NN model for the binary classification problem of this nature.

Table 4: Comparison of Artificial Neural Network (ANN) - RNN, CNN, MLP, and Hybrid Models Results

No.	Metric \ ANN	RNN	CNN	MLP	Hybrid (RNN + CNN)
1	Detection	98.53%	99.71%	**100.00%**	99.83%
2	Recognition	98.24%	99.64%	**100.00%**	99.84%
3	Prediction	97.32%	99.52%	**100.00%**	98.91%

Table 4 shows the comparison between the various NNs in determining the chosen NN for the implementation of the proposed iDRP framework. Evidently, MLP performed best for the binary classification of precision and accuracy in the experiment – binary classification problem.

The MLP NN mainly performed better with model flexibility in terms of training, testing, and development. The optimal capability for an MLP NN to be abstracted in its architecture design and robustly extract fine-grained features with universal approximation made it a perfect candidate for the implementation NN model of the proposed iDRP framework. Chiefly, the MLP NN allows the Separation of Concerns in its architecture by creating boundaries (methods, and objects) for the several interconnected components in the proposed iDRP framework while providing the layers and tiers the independent capability for each component to maintain their core operations dynamically.

7.3. Comparison of Classification Techniques on Standardized Datasets Results – Preliminary Experiment

The amalgamations of innovative MLP techniques applied in the implementation of the proposed iDRP framework network demonstrated to be advantageous in the specialized classification precision and accuracy on accurately detecting, recognizing, and predicting malware binaries in the standardized dataset in an IoT ecosystem.

Table 5 shows the comparison of the different classification results of experiments on standardized datasets. The synthesized innovative techniques in the proposed iDRP framework network technique that have been successfully implemented have proven to be more efficient and competent in tackling polymorphic IoT malware attacks and their variants or obfuscation that are typically responsible for zero-day attacks in a heavily computerized network system and smart technologies such as the IoT ecosystem. The learning capabilities and accuracy of a specific predictor problem of this nature was significantly amplified through the innovative classification precision and accuracy techniques that were proposed and implemented in the systematic experiments iDRP framework network.

Table 5: Comparison of Classification Experimentations Techniques with Standardized Datasets and Results – Preliminary Experiment

No.	Technique \ Dataset	MNIST	NORB
		Accuracy (%)	Accuracy (%)
1	SAE	98.60	86.28
2	SDA	98.72	87.62
3	DBN	98.87	88.47
4	DBM	99.05	89.65
5	MLP-BP	97.39	84.20
6	ML-ELM	99.04	88.91
7	H-ELM	99.13	91.28
8	iDRP	**100.00**	**100.00**

Key: SAE (Stacked Auto Encoders), SDA (Stacked Autoencoders), DBN (Deep Belief Networks), DBM (Deep Boltzmann Machines), MLP-BP (Multilayer Perceptron Back Propagation), ML-ELM (Machine Learning Extreme Learning Machine, H-ELM (Hierarchical Extreme Learning Machine), iDRP (Intelligent Detection Recognition Prediction)

7.4. Comparison of Classification Techniques on Standardized Datasets (BoTNetIoT) Results

The standardized IoT malware generic traffic metric and evaluation were used as parameters to compare the effectiveness of the learning and training techniques in correlations with the validation of the techniques applied to detecting benign and malicious network traffic in an IoT ecosystem. Table 6 shows the attained results.

Table 6 indicates that the proposed novel iDRP framework techniques and methods perform better with other notable techniques for IoT malware detections. Significantly, the optimal results were achieved with the synthesis of both the discriminative features and differential evolution techniques for the universal approximation of the extrapolated hidden information together with connected structures in the integrated iDRP framework.

Table 6: Comparison of Classification Techniques on Standardized IoT Malware Datasets (BoTNetIoT) Results

No.	Techniques	Accuracy	Precision	Recall	F-score
1	Resnet34 [41]	92.39%	93.57%	64.55%	76.40%
2	Resnet50 [41]	94.50%	95.78%	94.02%	94.90%
3	MobileNet [41]	91.32%	91.67%	91.03%	91.35%
4	SOINN [41]	91.75%	89.68%	95.52%	92.50%
5	iDRP	**99.98%**	**99.95%**	**99.93%**	**99.97%**

Evidently, the innovative iDRP framework network techniques performed better with even the state-of-the-art MLP NN techniques and methods etc. The flexibility, extensibility, stability, and maintainability in the architecture design of the innovative iDRP framework network that were developed have demonstrated to be optimal in helping achieve the overall outcome. Through the leveraged innovative and systematic techniques implemented in the experiments of the proposed iDRP framework network, it is safe to mention that the optimal security and protection of heavily computerized network systems and smart technologies such as an IoT ecosystem against evolving attacks and threats can be better managed with improved innovation and intelligence in the digital ecosystem.

8. Conclusion

The novelty of this work are the systematic integrations, techniques and methods of the adaptive and scalable *pre-processing* and *post-processing* components designed and developed for multi-class classifications and capturing the immutable vector state structures from categorical distributions to mapped data distributions in order to estimate and exploit hidden textural features of converted polymorphic and new IoT malware binary images in correlations with their aggregated distributions in a network. Together with, the modular *detection*, *recognition*, and *prediction* components DL approach provided new concepts through the syntheses of the three (3) key components with the *multi-class classification*, *data augmentation*, *vector scaling and retention*, *clustering*, *cross-validation*, and *resampling* techniques and methods etc., synthesized and interconnected evolutionarily by the *post-processing* techniques in the proposed novel iDRP framework, which can be multidisciplinary. In particular, considering the textural and structural changes in polymorphic and new malware variants or obfuscation, the applied techniques and methods that were designed and developed ensured the improved and accurate *detection*, *recognition*, and *prediction* of the complex code malwares that specifically changes their binary structures on execution in an IoT ecosystem. A higher level of feature extraction and classification estimation of the modular hidden layer information were achieved to intelligently and efficiently detect the present-day obfuscation of malware attacks and infections in an IoT ecosystem. Overall, the derived intelligent immutability of the stately vectorized mapped data estimation techniques and methods implemented ensured optimal results in the experiments.

We conducted and tested the proposed implemented experiments with sound scientific procedures and processes to provide the proof-of-concept by conceptualizing and applying conventional scientific processes such as conducted in the engineering, medical, animal science fields etc., to establish empirical and statistical analysis in the performed experiments i.e., structurally complex, yet similar vector images; MNIST (2-D) and NORB (3-D) datasets prior to the comparative real IoT malware (BoTNetIoT) dataset converted image files as benchmark, which is analogous to animal to human experiments in the pure science and engineering fields systematically. The premise of the research experiments is to discover conclusive scientific approaches, techniques, and methods to solving polymorphic and new malware anomalies problems in an IoT ecosystem. These were achieved by applying the aforementioned procedures and techniques to solving the IoT malware problems with new ideas in this work. Extensive analysis was conducted by synthesizing the various techniques on the big datasets utilized in the proposed experiments. The syntheses of the integrated procedures and techniques in the proposed novel iDRP framework, which consists of five (5) components; *pre-processor*, *detection*, *recognition*, *prediction*, and *post-processor* components provided the seamless evolutionary information distributions for a high-level accuracy result in the experiment. Standardized metrics such as *accuracy* rate, *ROC/AUC* rate, *precision* rate, *True Positive* (TP) rate, *False Positive* (FP) rate, *True Negative* (TN) rate, *False Negative* (FN) rate, *recall* rate, and *F1-Score* were calculated and recorded to effectively determine the performance of the finalized generative DNN models in the proposed and implemented systematic experiments of the iDRP framework research.

In the end, the resultant output of the proposed experiments was tested and evaluated to achieve the best performance and consistency, accuracy, and precision etc., of the comparative aggregated model results achieved. As a result, a 100% accuracy rate, 100% ROC/AUC rate, 99.94% precision rate, and 99.90% recall rate were successfully achieved with the preliminary experiment, while with a real IoT malware data, BoTNetIoT, a 99.98% accuracy rate, 99.99% ROC/AUC rate, 99.95% precision rate, and 99.93 recall rate were successfully attained as solution with the synthesized techniques and methods to the regression and binary classification problems for intelligent malware anomalies detection in an IoT ecosystem.

Future Work

The future work would be to evaluate the systematic '*checkpointing*' of various weightages and best performing weights measurement together with the corresponding network topography and architecture in IoT security models, which will be verified, validated and explored further for better security solution in expanding heavily computerized interconnected systems.

Conflict of Interest

The authors declare no conflict of interest.

Acknowledgment

The authors received no specific funding for this research work.

References

[1] O. Eboya, J. Juremi and M. Shahpasand, "An Intelligent Framework for Malware Detection in Internet of Things (IoT) Ecosystem," in 2020 IEEE 8th R10 Humanitarian Technology Conference (R10-HTC), 1 - 6, 2020, doi: 10.1109/r10-htc49770.2020.9356961.

[2] R. AL MOGBIL, M. AL ASQAH and S. EL KHEDIRI, "IoT: Security Challenges and Issues of Smart Homes/Cities," in 2020 International Conference on Computing and Information Technology (ICCIT-1441), 1 - 6, 2020, doi: 10.1109/iccit-144147971.2020.9213827.

[3] E. Tabane and T. Zuva, "Is there a room for security and privacy in IoT?," in 2016 International Conference on Advances in Computing and Communication Engineering (ICACCE), 1-6, 2016, doi: 10.1109/icacce.2016.8073758.

[4] C. Vorakulpipat, E. Rattanalerdnusorn, P. Thaenkaew and H. Dang Hai, "Recent challenges, trends, and concerns related to IoT security: An evolutionary study," in 2018 20th International Conference on Advanced Communication Technology (ICACT), 1 - 6, 2018, doi: 10.23919/icact.2018.8323773.

[5] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in 2017 IEEE International Congress on Big Data (BigData Congress), 1 - 6, 2017, doi: 10.1109/bigdatacongress.2017.85.

[6] N. Neshenko, E. Bou-Harb, J. Crichigno, G. Kaddoum and N. Ghani, "Demystifying IoT Security: An Exhaustive Survey on IoT Vulnerabilities and a First Empirical Look on Internet-Scale IoT Exploitations," in 2019 IEEE Communications Surveys & Tutorials, 2702-2733, 2019, doi: 10.1109/comst.2019.2910750.

[7] Y. Seralathan et al., "IoT security vulnerability: A case study of a Web camera," in 2018 20th International Conference on Advanced Communication Technology (ICACT), 1 - 6, 2018, doi: 10.23919/icact.2018.8323685.

[8] N. Karie, N. Sahri and P. Haskell-Dowland, "IoT Threat Detection Advances, Challenges and Future Directions," in 2020 Workshop on Emerging Technologies for Security in IoT (ETSecIoT), 1 - 6, 2020, doi: 10.1109/etseciot50046.2020.00009.

[9] O. Georgiana Dorobantu and S. Halunga, "Security threats in IoT," in 2020 International Symposium on Electronics and Telecommunications (ISETC), 1 - 6, 2020, doi: 10.1109/isetc50328.2020.9301127.

[10] M. Antonakakis et al., "Understanding the mirai botnet," 1st ed. Vancouver, BC, Canada: Proceedings of the 26th USENIX Security Symposium, USENIX Association, 2017.

[11] K. Sha, R. Errabelly, W. Wei, T. Yang and Z. Wang, "EdgeSec: Design of an Edge Layer Security Service to Enhance IoT Security," in 2017 IEEE 1st International Conference on Fog and Edge Computing (ICFEC), 1 - 6, 2017, doi: 10.1109/icfec.2017.7.

[12] I. Waz, M. Sobh and A. Bahaa-Eldin, "Internet of Things (IoT) security platforms," in 2017 12th International Conference on Computer Engineering and Systems (ICCES), 1 - 5, 2017, doi: 10.1109/icces.2017.8275359.

[13] W. Iqbal, H. Abbas, M. Daneshmand, B. Rauf and Y. Bangash, "An In-Depth Analysis of IoT Security Requirements, Challenges, and Their Countermeasures via Software-Defined Security," in IEEE Internet of Things Journal, 10250-10276, 2020, doi: 10.1109/jiot.2020.2997651.

[14] E. Baccelli et al., "RIOT: An Open Source Operating System for Low-End Embedded Devices in the IoT," in IEEE Internet of Things Journal, 4428-4440, 2018, doi: 10.1109/jiot.2018.2815038.

[15] R. Johari, N. Gaurav, S. Chaudhary and A. Pramanik, "START: Smart Stick based on TLC Algorithm in IoT Network for Visually Challenged Persons," in 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), 1 - 6, 2020, doi: 10.1109/i-smac49090.2020.9243517.

[16] A. Gupta and R. Johari, "IOT based Electrical Device Surveillance and Control System," in 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), 1 - 5, 2019, doi: 10.1109/iot-siu.2019.8777342.

[17] L. Tawalbeh, H. Tawalbeh, H. Song and Y. Jararweh, "Intrusion and attacks over mobile networks and cloud health systems," in 2017 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 1 - 6, 2017, doi: 10.1109/infcomw.2017.8116345.

[18] Y. Zheng, A. Pal, S. Abuadbba, S. Pokhrel, S. Nepal and H. Janicke, "Towards IoT Security Automation and Orchestration," in 2020 Second IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA), 1 - 6, 2020, doi: 10.1109/tps-isa50397.2020.00018.

[19] M. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, I. Ali and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," in IEEE Communications Surveys & Tutorials, 1646-1685, 2020, doi: 10.1109/comst.2020.2988293.

[20] F. Hussain, R. Hussain, S. Hassan and E. Hossain, "Machine Learning in IoT Security: Current Solutions and Future Challenges," in IEEE Communications Surveys & Tutorials, 1686-1721, 2020, doi: 10.1109/comst.2020.2986444.

[21] M. Bettayeb, O. Waraga, M. Talib, Q. Nasir and O. Einea, "IoT Testbed Security: Smart Socket and Smart Thermostat," in 2019 IEEE Conference on Application, Information and Network Security (AINS), 1 - 6, 2019, doi: 10.1109/ains47559.2019.8968694.

[22] J. Moos, "IoT, Malware and Security," in 2017 ITNOW, 28-29, 2017, doi: 10.1093/itnow/bwx013.

[23] A. Zahra and M. Shah, "IoT based ransomware growth rate evaluation and detection using command and control blacklisting," in 2017 23rd International Conference on Automation and Computing (ICAC), 1 - 5, 2017, doi: 10.23919/iconac.2017.8082013.

[24] E. Ronen, A. Shamir, A. Weingarten and C. O'Flynn, "IoT Goes Nuclear: Creating a Zigbee Chain Reaction," in 2018 IEEE Security & Privacy, 54-62, 2018, doi: 10.1109/msp.2018.1331033.

[25] S. Sonune, D. Kalbande, A. Yeole and S. Oak, "Issues in IoT healthcare platforms: A critical study and review," in 2017 International Conference on Intelligent Computing and Control (I2C2), 1 - 5, 2017, doi: 10.1109/i2c2.2017.8321898.

[26] M. Mekala and P. Viswanathan, "A Survey: Smart agriculture IoT with cloud computing," in 2017 International conference on Microelectronic Devices, Circuits and Systems (ICMDCS), 1 - 6, 2017, doi: 10.1109/icmdcs.2017.8211551.

[27] P. Rughoobur and L. Nagowah, "A lightweight replay attack detection framework for battery depended IoT devices designed for healthcare," in 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS), 1 - 7, 2017, doi: 10.1109/ictus.2017.8286118.

[28] A. Ukil, S. Bandyoapdhyay, C. Puri and A. Pal, "IoT Healthcare Analytics: The Importance of Anomaly Detection," in 2016 IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), 1 - 4, 2016, doi: 10.1109/aina.2016.158.

[29] S. Venkatraman and M. Alazab, "Classification of Malware Using Visualisation of Similarity Matrices," in 2017 Cybersecurity and Cyberforensics Conference (CCC), 1 - 5, 2017, doi: 10.1109/ccc.2017.11.

[30] J. Tang, C. Deng and G. Huang, "Extreme Learning Machine for Multilayer Perceptron," in 2016 IEEE Transactions on Neural Networks and Learning Systems, 809-821, 2016, doi: 10.1109/tnnls.2015.2424995.

[31] Y. Zeng, L. Qian and J. Ren, "Evolutionary Hierarchical Sparse Extreme Learning Autoencoder Network for Object Recognition," in 2018 Symmetry, 1 - 11, 2018, doi: 10.3390/sym10100474.

[32] M. Shahini, R. Farhanian and M. Ellis, "Machine Learning to Predict the Likelihood of a Personal Computer to Be Infected with Malware," in 2019 SMU Data Science Review, 1 - 24, 2019, doi: https://scholar.smu.edu/datasciencereview/vol2/iss2/9/.

[33] J. Villanueva, R. Juanatas and L. Lacatan, "Malware Predictor using Machine Learning Techniques," in 2020 Research Gate, 5665 - 5674, 2020, doi: https://www.researchgate.net/publication/339935591_Malware_Predictor_using_Machine_Learning_Techniques.

[34] A. Onal, O. Berat Sezer, M. Ozbayoglu and E. Dogdu, "Weather data analysis and sensor fault detection using an extended IoT framework with semantics, big data, and machine learning," in 2017 IEEE International Conference on Big Data (Big Data), 2037-2046, 2017, doi: 10.1109/bigdata.2017.8258150.

[35] J. Wang, C. Liu, M. Zhu, P. Guo and Y. Hu, "Sensor Data Based System-Level Anomaly Prediction for Smart Manufacturing," in 2018 IEEE International Congress on Big Data (BigData Congress), 158-165, 2018, doi: 10.1109/bigdatacongress.2018.00028.

[36] N. Zeeshan, M. Reed and Z. Siddiqui, "Three-way Security Framework for Cloud based IoT Network," in 2019 International Conference on Computing, Electronics & Communications Engineering (iCCECE), 183-186, 2019, doi: 10.1109/iccece46942.2019.8941877.

[37] B. Li, X. Ming and G. Li, "Big data analytics platform for flight safety monitoring," in 2017 IEEE 2nd International Conference on Big Data Analysis (ICBDA), 1 - 3, 2017, doi: 10.1109/icbda.2017.8078837.

[38] Y. Xing, H. Shu, H. Zhao, D. Li and L. Guo, "Survey on Botnet Detection Techniques: Classification, Methods, and Evaluation," in 2021 Mathematical Problems in Engineering, 1-24, 2021, doi: 10.1155/2021/6640499.

[39] Y. Song, S. Hyun and Y. Cheong, "Analysis of Autoencoders for Network Intrusion Detection," in 2021 Sensors, 4294, 2021, doi: 10.3390/s21134294.

[40] T. Palla and S. Tayeb, "Intelligent Mirai Malware Detection for IoT Nodes," in 2021 Electronics, 1241, 2021, doi: 10.3390/electronics10111241.

[41] G. Bendiab, S. Shiaeles, A. Alruban and N. Kolokotronis, "IoT Malware Network Traffic Classification using Visual Representation and Deep Learning," in 2020 6th IEEE Conference on Network Softwarization (NetSoft), 1 - 9, 2020, doi: 10.1109/netsoft48620.2020.9165381.

[42] R. Kozik, M. Pawlicki and M. Choraś, "A new method of hybrid time window embedding with transformer-based traffic data classification in IoT-networked environment," in 2021 Springer, 1 - 9, 2021, doi: 10.1007/s10044-021-00980-2.

[43] A. Alhowaide, I. Alsmadi and J. Tang, "Towards the design of real-time autonomous IoT NIDS," in 2021 Cluster Computing, 1 - 14, 2021, doi: 10.1007/s10586-021-03231-5.

[44] K. Sudheera, D. Divakaran, R. Singh and M. Gurusamy, "ADEPT: Detection and Identification of Correlated Attack Stages in IoT Networks," in 2021 IEEE Internet of Things Journal, 6591-6607, 2021, doi: 10.1109/jiot.2021.3055937.

[45] Q. Ngo, H. Nguyen, V. Le and D. Nguyen, "A survey of IoT malware and detection methods based on static features," in 2020 ICT Express, 280-286, 2020, doi: 10.1016/j.icte.2020.04.005.

[46] P. Sudhakaran, C. Malathy, T. Vardhan and T. Sainadh, "Detection of Malware from IOT Devices Using Deep Learning Techniques," in 2021 Journal of Physics: Conference Series, 1 - 7, 2021, doi: 10.1088/1742-6596/1818/1/012219.

[47] B. Khammas, "The Performance of IoT Malware Detection Technique Using Feature Selection and Feature Reduction in Fog Layer," in 2020 IOP Conference Series: Materials Science and Engineering, 1 - 11, 2020, doi: 10.1088/1757-899x/928/2/022047.

[48] K. Han, J. Lim, B. Kang and E. Im, "Malware analysis using visualized images and entropy graphs," in 2015 International Journal of Information Security, 1-14, 2015, doi: 10.1007/s10207-014-0242-0.