Advances in Science, Technology and Engineering Systems Journal Vol. 5, No. 3, 518-528 (2020)

www.astesj.com

ASTESJ

ISSN: 2415-6698

A Survey and an IoT Cybersecurity Recommendation for Public and Private Hospitals in Ecuador

Maximo Giovani Tanzado Espinoza*, Joseline Roxana Neira Melendrez, Luis Antonio Neira Clemente

Department of Computer Science, Universidad Politécnica Salesiana (UPS), Guayaquil, 010102, Ecuador

ARTICLE INFO

Article history:
Received: 12 April, 2020
Accepted: 06 June, 2020
Online: 25 June, 2020

Keywords:
IoT Cybersecurity
Health
Public Hospital and Private
IoT Architecture
Information Assets

ABSTRACT

It was analyzed the reference information on Cybersecurity architectures, models, standards, evaluations, mechanisms, and procedures applied to IoT domains, and public and private health area. The problem is the lack of proposals for IoT Cybersecurity in public and private hospitals to minimize random failures, ensure the privacy of personal data of patients, avoid the paralysis of the IoT medical network and minimize attacks on information assets. The objective is to perform a survey and an IoT Cybersecurity recommendation for public and private hospitals in Ecuador. The exploratory research was used to review references and specific analytical reasoning to end in a known scoop with a trusted solution. A survey of cybersecurity vs. competitiveness of hospitals in Ecuador resulted, a Model conceptual prototype of IoT Cybersecurity for a public or private hospital, an Architecture prototype of IoT Cybersecurity for a public or private hospital, and an Algorithm prototype of cybersecurity for IoT architecture. It was concluded that the cybersecurity standards applied to the design of IoT for a public or private hospital generates trust on information assets, preserves the confidentiality, integrity and availability of the information at the operational, tactical and strategic levels; the architecture prototype is between 59.38% and 99.71% of acceptable workload. This proposal is scalable and applicable to a public or private hospital regardless of the dimensions of areas, devices, floors, workers or other characteristics; the architecture only considers the hospital's own IoT devices and information; the devices of doctors or patients are not considered.

1. Introduction

Internet of Things (IoT) has significant popularity and growth in many areas and organizations, it is estimated that by 2030 there will be 125 billion connected devices [1].

On IoT network devices generate, deliver, monitor and process data; this data is sent and stored on private or public clouds; IoT is used in various areas such as sports, education, commerce, infrastructure, transportation and health [2]; other areas are factory, buildings, city, electrical networks, infrastructure and home [3]

In the health area, the integrity and availability of information for the care of patients have priority [2], while confidentiality guarantees the protection of information [4]; data encryption from device data delivery is required in this area..

Other research advises adopting standards, frameworks and best procedures to increase information security [5]; according to [6] to apply cybersecurity the following standards are used: International Organization for Standardization (ISO) 27001, National Institute of Standards and Technology (NIST), International Organization for Standardization 27032, International Information System Security Certification Consortium (ISC), Control Objectives for Information and Related Technologies (COBIT), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA), Health Information Trust Alliance (HITRUST), North American Electric Reliability Corporation (NERC); this standards made it easier to apply an audit.

Cyberscurity includes the security of cyberspace and applies Confidentiality, Integrity and Availability to information assets, in addition to guaranteeing the privacy of the participants [4];; it is to protect the information assets to minimize the threats of the information processed, collected and transported by interconnected applications; is an element in information security [6]; cybersecurity is established on convergence of computing, engineering, information systems, networks, human and political elements [7].

* Maximo Giovani Tandazo Espinoza, Email: mtandazo@ups.edu.ec

IoT Cybersecurity is a strategic mechanism for improvement and changes in IoT and increases the environment security; it also ensures that an infrastructure has connected devices in a safe environment and with appropriate use by users [8].

eHealth is an area coming from the intersection between medical informatics, public health and companies, here health and information services are collected, processed, delivered and improved through the Internet [4]; with the use of ICT, medical care is improved at the local, regional and global level [9].

Basic characteristics of IoT are: comprehensive information collection, reliable transmission of information, information processing and data transformation of medical system [8].

According to [10] medical knowledge doubles every 73 days, this makes health data valuable; in addition, there are more efforts to ensure the integrity and access to patient records; among the main attacks on IoT infrastructure are: Denial of Services (DoS), remote brute force attacks, man-in-the-middle, password tracking, trojans and data manipulation.

The problem is the lack of proposals for IoT Cybersecurity in public and private hospitals to minimize random failures, ensure the privacy of personal data of patients, avoid the paralysis of the IoT medical network and minimize attacks on information assets.

The health sector must maintain the historical information of the data generators; this data must be stored, processed and visualized through the infrastructure with efficiency and security for the hospital and service providers.

Why is an IoT cybersecurity analysis and recommendation necessary for public and private hospitals in Ecuador?

To determine the appropriate models or standards that provide security to an IoT environment, it is necessary to understand the security requirements in the design of IoT on health area.

The objective is to perform a survey and an IoT Cybersecurity recommendation for public and private hospitals in Ecuador.

References about IoT cybersecurity, IoT domains and health are: Anomaly detection of IoT cyberattacks [1], Cybersecurity of healthcare IoT-based systems [2], IoT Security Mechanisms for e-Health [3], Cybersecurity education and training in hospitals [4], A Novel Model for Cybersecurity Economics and Analysis [5], A comprehensive cybersecurity audit model [6], Identifying Core Concepts of Cybersecurity [7], IoT cybersecurity research [8], Evaluating EHR and health care in Jordan [9], Blockchain Secured Electronic Health Records [10], Campus IoT collaboration and governance [11], CyberSecurity: A Review of IoT [12], IoT solutions for health monitoring [13], Security and Privacy-Preserving Challenges of e-Health Solutions [14], Self-Service Cybersecurity Monitoring [15], Standardising a moving target [16], Cybersecurity Vulnerabilities, Attacks and Solutions in the Medical Domain [17], The governance of safety and security risks in connected healthcare [18], Framework for improving critical infrastructure cybersecurity [19].

The exploratory research is used for reference review and specific analytical reasoning to end in a known scoop with trusted solution.

The results are: Cybersecurity and competitiveness survey of hospitals in Ecuador, Model conceptual prototype of IoT Cybersecurity for a public or private hospital, Architecture prototype of IoT Cybersecurity for a public or private hospital, and Algorithm prototype of cybersecurity for IoT architecture.

It is concluded that the cybersecurity standards applied to the design of IoT for a public or private hospital generates trust on information assets, preserves the confidentiality, integrity and availability of the information at the operational, tactical and strategic levels; the architecture prototype is between 59.38% and 99.71% of acceptable workload.

2. Materials and Methods

2.1. Materials

The researchers designed a system to detect and alert unusual attacks or activities on IoT network or distributed network over smart city by using two types of intrusion; the first one is installed on software to detect abnormal activities or behavior, the second one is installed on network to detect attacks, through monitoring it reduces the probability of assaults on the network [1]. The researchers proposed a 4-layer IoT architecture for the health area; the layers are sensors, network, services and, applications; they analyzed international standards and applied them to each layer according to the function, responsibility and scope of the architecture [2]. The researchers highlighted the security requirements in confidentiality, integrity and availability, for this they recommended using an ISO standard; they named open IoT architectures, here they focused on a 7-layer architecture, each called: things, acquisition, network, aggregation, centralization, warehouse and application; among its advantages it has authorizations, encryption and identification [3]. For minimize human errors, avoid data breaches and reduce vulnerabilities on health services; the researchers proposed a governance framework to adopt cybersecurity on health, the areas it covers are platforms, storage, software, data and people; cybersecurity approach in a hospital is based on laws, availability of services, recovery and adaptation for staff [4]. The authors made guidelines to obtain the cost and benefits of processes applied in cybersecurity; this model reviews the practices, standards and quantitative risk analysis, presents the impact on hardware and software assets [5]. To guarantee cybersecurity in organizations, the authors proposed an audit model; it serves to verify the strategy adopted to minimize risks, it also evaluates the security policy [6]. The interviewed experts affirmed that Confidentiality, Integrity and Availability are important and transversal concepts on cybersecurity [7]. It was reviewed 3, 4 and 5 layer IoT architectures; the most used layers are sensors or perception, network, services or middleware, application or business; they described the applications on health, transportation and smart domains; they also described the standards that are used on IoT cybersecurity [8]. The authors' recommendations were to update the health system, educate staff, connect the public health sector with the private, attach importance to the security and privacy of health data [9]. The benefits of hybrid blockchain were used on health data proposal, under the standard of protection and regulations with notification rights, access to information, transparency and data portability for patients [10]. The University of Texas produced a list of requirements to apply cybersecurity on IoT network; they applied it on a farm and in the parking area of the university campus; they affirm the need for time to identify connected devices, work on a governance model,

the development of a standard architecture for the organization, the use of NIST as a framework for cybersecurity [11]. IoT Cybersecurity in IoT domain was proposed; for this they used a 3-layer IoT architecture; the first perception layer captures the sensors, Gateway, guest computers; the second network layer includes Wireless Fidelity (WiFi), Global System for Mobile Communications (GSM), 2G, 3G and, other access connections; the third application layer comprises smart environments [12].

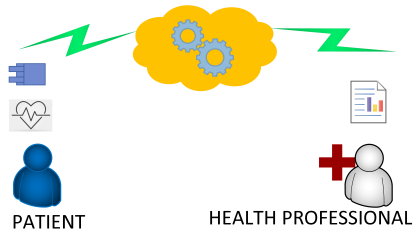


Figure 1: Architecture IoT for a patient

The researchers created an electrocardiography device for the service and monitoring of the patient's health in the IoT environment (Figure 1); the data is stored in the cloud of a provider, in addition the provider applies HIPAA for health data security [13].

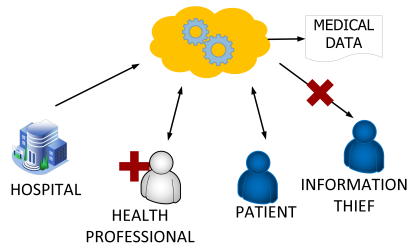


Figure 2: Architecture IoT for hospital

The researchers reviewed the privacy and security of various works, described various recording models for health data; the study presented a health architecture that has hospitals, patients and doctors, and also deposits its data in a cloud (Figure 2); they stated the challenges in the cloud are interoperability standards, expensive models, performance, privacy and, security [14]. In a process of construction, execution and monitoring on IoT domain, cybersecurity was applied to supervise and generate early alarms; the objective was to anticipate problems or attacks in the implementation through metrics [15]. The researchers analyzed cybersecurity standards applied to IoT, the standards are ISO 27000 series, GSM Association, Open Web Application Security Project (OWASP), Publicly Available Specification (PAS), machine to machine (M2M); several organizations applied IoT Cybersecurity based on law, consulting, technology companies, research centers, commercial organizations [16]. The researchers proposed a medical IoT architecture to safeguard information with characteristics such as: scalable, confidentiality keeping, general and efficient transmission; these characteristics are in areas such as: health files, medical systems, imaging systems, sensors, and information systems, and several medical systems have been tabulated [17]. The author analyzed the security correlation of medical devices that are used and interconnected in medical centers; she disclosed incidents, threats and vulnerabilities in medical devices, and analyzed the ISO, International Electrotechnical Commission (IEC), Medical Device Regulation (MDR), NIST standards [18].

Table 1: Measurement of proposals on cybersecurity

Ref.	Proposal	Process	Model metrics
[1]	Detection method in IoT	Detect cyberattacks on Smart city nodes through learning algorithms to detect attack behavior	Performance 98%
[2]	Health system in IoT	Protects information with international NIST, ISO, PHI and HIPAA standards, uses 4-layer architecture	There are no metrics
[3]	Health system in IoT	It is used 7-layer architecture, security mechanisms and big data for data analysis	There are no metrics
[4]	Governance framework	Cybersecurity approach in a hospital is based on laws, availability of services, recovery and adaptation for staff	There are no metrics
[5]	Socio economic model	Measure the cost and benefit of cybersecurity, quantitative analysis, audits and standards.	There are no metrics
[6]	Audit model	Contains 18 domains, ranking formats	There are no metrics
[8]	Layered IoT models	Descriptions and types of attacks at each layer, types of cybersecurity standards by layer	There are no metrics
[10]	Hybrid blockchain	Data string with permissions to update information, use HIPAA	There are no metrics
[11]	Security framework on IoT domains	Uses NIST for governance and control of wireless and mobile communications	There are no metrics
[12]	Analysis of IoT 3-Layer Architecture	Cybersecurity application to protect authentication, information privacy	There are no metrics
[13]	Health IoT device	Generate and send data to the cloud, use data sending protocols and HIPAA	There are no metrics
[15]	Monitoring code	Processes for instantiating a cybersecurity infrastructure	There are no metrics
[17]	Architectures	Analysis of cybersecurity architectures in health domains	There are no metrics

The references with their models, processes and measurement are summarized for better understanding (Table 1), only one proposal presents the performance of the model, they carried out tests and others only present the models, other proposals use HIPAA and NIST to secure the information.

2.2. Methods

2.2.1. Scope of proposal

Applying the NIST Framework Core are cybersecurity activities, results, standards and best practices that are frequent in critical sections of the infrastructure; these activities pay off across the organization from the operational, middle and executive levels; the framework has five simultaneous functions: Identify, Protect,

Detect, Respond and Recover; these activities facilitate a high-level strategic approach to managing cybersecurity risks in an organization [19].

- Adopt NIST Cybersecurity Framework applied in [2] and [11];
- Adopt HIPAA used in [2] and the framework described in [19];
- The architecture oriented to strong Confidentiality, Integrity and Availability properties through ISO / IEC 27001 applied in [12];
- Adopt cybersecurity standards for layers [8];
- Establish a 6-layer architecture;
- The generated data is saved, processed and retrieved on cloud;
- Establish three user profiles: patients, medical professionals and hospital administration;
- Only hospital medical devices are considered.

2.2.2. *Cybersecurity attacks*

The types of security attacks were summarized from references (Table 2):

Table 2: Cybersecurity attacks

Ref.	Information collection attacks	Database attacks	Website attacks, Middleware or Application	Operation device attacks, sensing or network
[8]	Information damage level	Malicious scripts, un-authorized	Malicious insider, under infrastructure, virtualization threat, phishing, virus, trojan	Replay attacks, timing attacks, node capture, routing information,
[12]	Not considered	Not considered	Physical attacks, Malicious code injection, Spear-Phishing attack, Sniffing Attack.	Routing attacks, DoS, Data transit attacks
[17]	Operating System vulnerability , Open SHH vulnerability	Password intrusion, Vulnerability intrusion, SQL Injection	Cross-site scripting, cross-site request forgery, Cross-heterogeneous network attacks	Dropbear SSH Server, DoS
[18]	Un-authorized access	Uncontrolled distribution of passwords	Malware on systems	Malware on devices, DoS, software update

Attacks are independent of an organization, they are internal or external, they occur on devices, network, user access, software, any hardware, protocols, physical, logical; Attacks can deny or interrupt service.

2.2.3. *Cybersecurity IoT elements*

There is a relationship between health, IoT and cybersecurity; between IoT and Health the relationship is the application of security standards for devices and communication; between health and cybersecurity the relationship is the laws for the protection of patient information; between cybersecurity and IoT the relationship is the application of data protection standards.

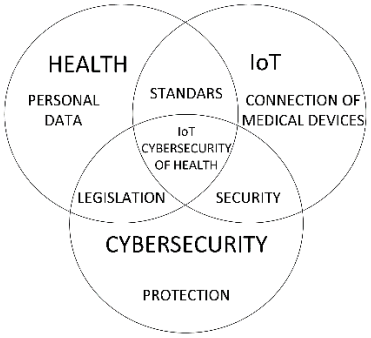


Figure 3: Elements to adapt IoT cybersecurity to health

As show in Figure 3 the connection between health, IoT and cybersecurity; in health we have the personal data of the patients; IoT includes medical devices that capture data over a network, in cybersecurity are the data protection standards.

2.2.4. *Ecuador data*

According to National Institute of Statistics and Censuses of Ecuador [20]: There were 175 public hospitals and 490 private hospitals in 2016; in 2017 there were 179 public hospitals and 466 private hospitals; in 2018 there were 183 public hospitals and 451 private hospitals.

In public hospitals: Attention to people in 2016, 2017 and 2018 was 752000, 780208 and 807245 respectively; in availability of spaces or beds in the years 2016, 2017 and 2018 was 12300, 13400 and 14144 respectively.

In private hospitals: Attention to people in 2016, 2017 and 2018 was 376000, 364000 and 357000 respectively; in availability of spaces or beds in the years 2016, 2017 and 2018 was 10600, 10100 and 9700 respectively.

In 2018, the provision of spaces or beds in the Ministry of Public Health is 40.47%; Ministry of National Defense is 2.30%; Social Security is 15.86%, other public is 1.97%, private non-profit is 10.6% and private for-profit is 29.03%; at the country level, the main areas of care in descending statistical order are: general services, medicine, gynecology, surgery, pediatrics, neonatology, traumatology, psychiatry, cardiology, urology, infectology, gastroenterology, otorhinolaryngology, ophthalmology and other services.

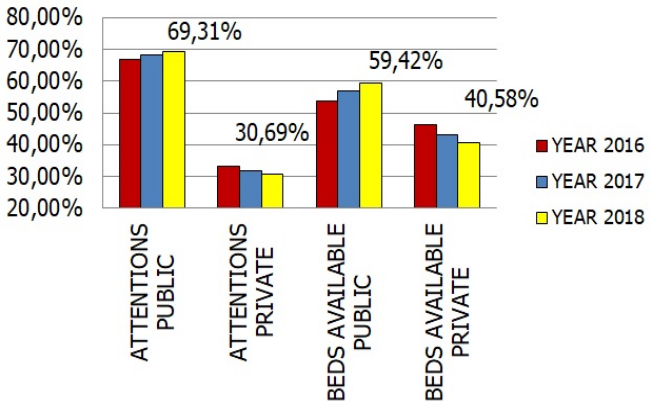


Figure 4: Attentions and public / private availability

In 2018 (Figure 4), public hospitals attended 69.31% of cases and a capacity of available beds of 59.42%; private hospitals attended 30.69% of cases and a capacity of available beds of 40.58%; the public sector each year has the greatest burden on medical care and spaces.

3. Results

The following results were obtained:

- Cybersecurity and competitiveness survey of hospitals in Ecuador
- Model conceptual prototype of IoT Cybersecurity for a public or private hospital
- Architecture prototype of IoT Cybersecurity for a public or private hospital
- Algorithm prototype of cybersecurity for IoT architecture

3.1. Cybersecurity and competitiveness survey of hospitals in Ecuador

The Latin American cybersecurity indices for 2017 [21], the cybersecurity indices for 2018 [22] and the competitiveness indices for 2017-2018 [23] were tabulated; to understand the impact and connection between these indices (Figure 5).

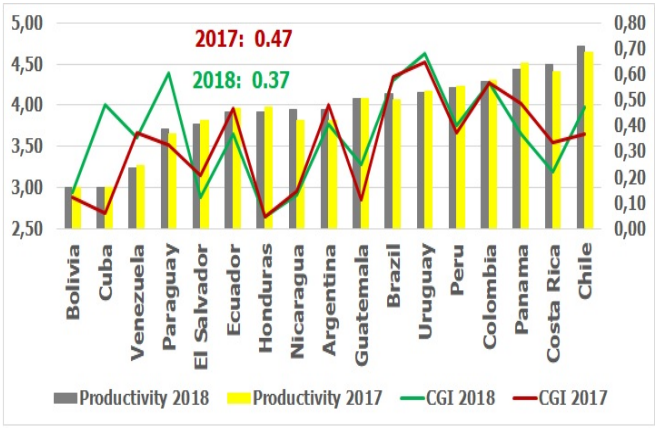


Figure 5: Cybersecurity Index vs. Competitiveness

2017 and 2018 of the Global Cybersecurity Index (CGI) and Global Competitiveness Report were considered; the first are the indicators of responsibility of the countries in the matter of cybersecurity, it was issued by the United Nations; the second is the set of institutions, policies and factors that establish the level of productivity, it was issued by the Economic Forum.

Cybersecurity values are between 0.01 and 0.99 on the secondary Y axis; the CGI of Ecuador in 2017 was 0.47 and in 2018 the CGI was 0.37; Ecuador is below 0.50; the CGI of Uruguay in 2017 was 0.65 and in 2018 the CGI was 0.68; Uruguay is highly committed to implementing cybersecurity.

Competitiveness values are between 0 and 5 on the main Y axis; Ecuador's competitiveness in 2017 was 3.96 and in 2018 it was 3.91; Chile's competitiveness in 2017 was 4.64 and in 2018 it was 4.71; Chile, Costa Rica and Panama are the first countries with the best productivity in 2018; Uruguay, Paraguay and Brazil are the first countries with the best cybersecurity application in 2018.

It is evident that the levels of competitiveness are not directly linked to the levels of cybersecurity.

Data from the World Health Organization (WHO) observatory were tabulated in the category of health information systems, among Latin American countries from 2008 to 2016; from each country (Figure 6) were obtained the score for the application of international health guidelines (HR), the average percentages of: reliability of the information systems in the Civil Registry for cause of death (CRCD), Civil Registry for births (CRBI) and data integrity due to death (INCD).

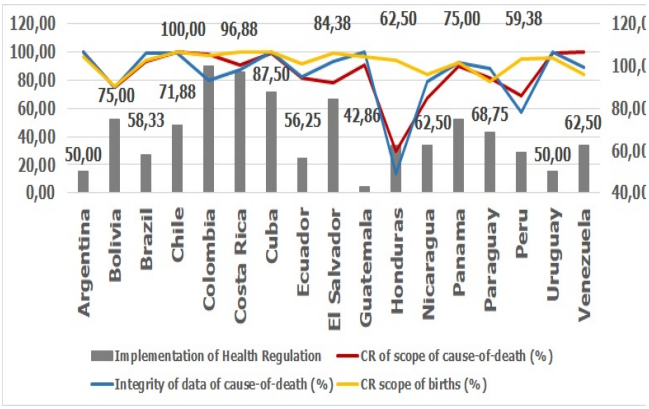


Figure 6: Health Regulations vs. Computer Registry

Colombia has 100 points in HR, in CRCD it has 98.06%, in INCD it has 80% and in CRBI it has 96.97, it follows that this country applies ICTs at an excellent level; Costa Rica has 96.88 points in HR, in CRCD it has 90.87%, in INCD it has 87% and in CRBI it has 99.66%, it follows that this country applies ICTs at an excellent level; Ecuador has 56.25 points in HR, in CRCD it has 81.77%, in INCD it has 82% and in CRBI it has 91.59%, it follows that this country applies ICTs at a good level.

In descending order by CRCD, Ecuador is in eleventh place; in descending order by INCD, Ecuador is in twelfth place; in descending order by CRBI, Ecuador is in thirteenth place; in descending order by HR, Colombia and Costa Rica are the first countries to apply health guidelines, Ecuador is in fourteenth place.

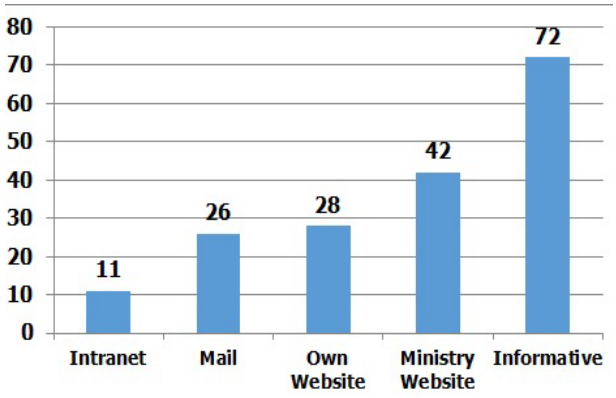


Figure 7: ICT in public hospitals of Ecuador

Review of infrastructure and hospital deficiencies in Ecuador

The web pages of 129 public hospitals were reviewed (Figure 7); it was found that 22 hospitals have a newsletter in pdf format on the website of the Ministry of Public Health of Ecuador (MSP), in addition it was considered that 50 hospitals have the same newsletter, 11 hospitals have their own intranet with institutional mail and their own website; 26 hospitals have institutional mail; 28 hospitals have their own website; 42 hospitals have their information attached to the MSP website; it follows that in 11 hospitals it is possible to implement a Cybersecurity IoT in the short term due to their existing intranet infrastructure.

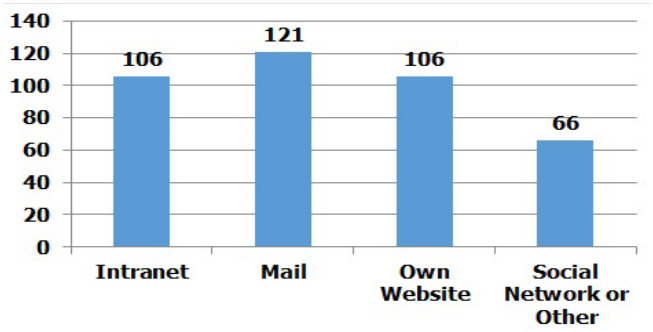


Figure 8: ICT in private hospitals of Ecuador

The web pages of 186 private hospitals were reviewed (Figure 8); here 106 hospitals have their own intranet; 121 hospitals use institutional mail; 106 hospitals have their own web page and 66 use social networks or third party pages for their communications; here it is possible to implement an IoT Cybersecurity to the 106 hospitals in the short term.

In the public sector only 8% of hospitals can apply IoT Cybersecurity to existing networks; 57% of hospitals can apply IoT Cybersecurity in the private sector; in the other hospitals, they must start from the design of the IoT infrastructure for the hospital; each IoT infrastructure depends on the physical infrastructure of the hospital; therefore we do not propose standard IoT network design; in Ecuador, the time and cost of applying IoT cybersecurity to hospitals depends on political, economic, cultural or social factors.

Critical review of existing IoT and cybersecurity measures

The MSP controls and regulates the implementation of the Ecuador National Health System of public and private entities; the public sector is made up of ministry hospitals, hospital of the armed forces, police hospital, social security, municipal care centers; the private sector is made up of a cancer society and private medicine; at the country level, hospitals are classified into 3 levels of hospitals; among the users are: the population without the ability to pay, the population with the ability to pay, members of the armed forces, members of the police, workers affiliated with social security and the population without social insurance [24].

Since 2014, the Public Administration has among its actions the implementation of a technological architecture and information security framework [25], according to references, there is no application of Cybersecurity to IoT in public or private hospitals.

The proposal [26] presented an IT Governance Model between Cobit and ISO 27002 to provide Information Security in Public Hospitals; aligns with IT and Hospital objectives in health data security; Ecuador's investment in Health is $ 11 billion based on health law; It should be emphasized that Ecuador does not have a standard to safeguard the confidentiality, integrity and availability of health data.

3.2. Model conceptual prototype of IoT Cybersecurity for a public or private hospital

The NIST Framework is applied in organizations of any size and helps to understand cybersecurity risks, risk management and protect information assets; this framework has good practices for managing resources on cybersecurity protection issues.

The ISO 27001 standard has the information security guidelines to maintain the reliability, integrity and availability of the information, allowing the hospital to assess and mitigate risks; it also allows improving the competitiveness and image of the hospital.

HIPAA is used to protect the patient's private medical information and data, which is legislation that provides privacy and security provisions; this law is widely accepted due to the increase in violations of health information.

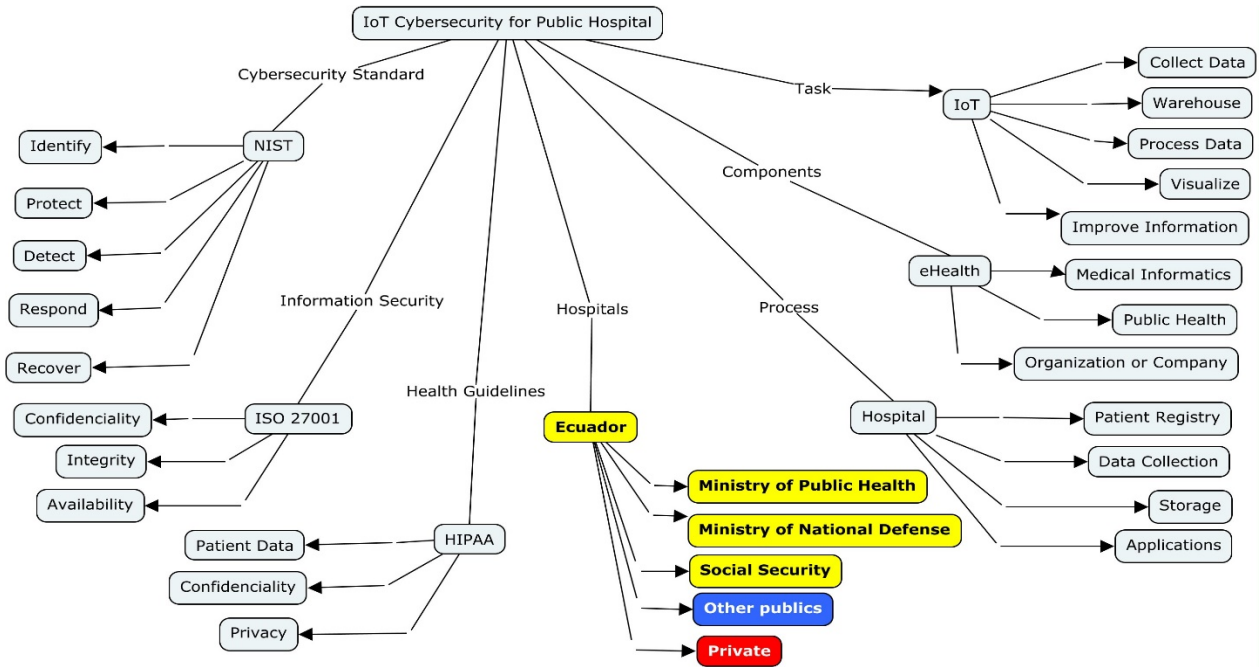
An IoT performs activities such as: Collecting patient data is done through the medical devices that generate the data and have access to the hospital's IoT; the collection is wired or wireless; storing patient data in a repository that has their access validated, may be their own space or a provider's space; process the data that was collected by the devices, the medical result is useful information for the health professional; improving information through correct management supports the health professional in the quality of the service; visualize the information through the applications and personalized systems on health area, indicators and reports are generally presented.

eHealth has components and medical software to manage the knowledge towards health professionals, the objective is to maintain the health care of the population; this care is carried out in a hospital that the government provides care to citizens.

The general information processes in a hospital occur from the patient arrival when taking and saving their personal and medical data; data collection is through the devices connected to IoT; storage guarantees the integrity of information and is presented in personal and medical applications or information systems.

As show in Figure 9 the cybersecurity components that apply to IoT of a public or private hospital, among its components are NIST, ISO 27001 and HIPAA standards; the other IoT, eHealth and hospital components manage the data and convert it into information and valid knowledge for health professionals.

The model assists in the management of medical results such as: diagnosis, prevention, follow-up, prediction, prognosis, treatment or relief of the disease, relief of an injury or disability, updating of physiological or pathological data, results of sample examinations, organ or blood donations.



3.3. Architecture prototype of IoT Cybersecurity for a public or private hospital

Cybersecurity was proposed at the time of designing an IoT for a public or private hospital, that is, not applying late security; each layer with its elements and functions to apply security management from the beginning and continuously; the hardware and software of the hospital and providers must operate and integrate in a reliable way. The architecture adopts standards to apply IoT hardware, software, sensors, control, storage, services and users; reduces implementation costs, reduces delivery times, and increases security levels. A NIST framework is used because it is a common language for dealing with security risks and ISO standard good practices are used.

The following layers were proposed:

3.3.1. First Layer: Medical Devices

This level gathers all the data from the devices through medical equipment, sensors and other equipment, captures the physical world and uploads it to the digital world; at this layer DoS attacks are very likely; according to [18] there are four groups of devices in the health area:

- Implantable medical devices, such as pacemakers, skin sensors and other implantable cardiac devices.
- Portable medical devices, such as portable insulin pumps.
- Mobile devices, such as glucose measuring devices or insulin pumps.
- Stationary medical devices, such as tomography scanners

Security requirements: raise the level of data confidentiality transferred between devices, for integrity devices must use encryption and device authentication to prevent the entry of strangers.

3.3.2. Second Layer: Network

The routing and exchange of data between devices must be in a reliable transmission from the first layer, to transmit data wireless, wired and communication protocols are used; this layer has wireless sensors, access points, and a gateway to transfer data to storage with high reliability; here the data is added, filtered and transmitted between the sensors. Security requirements: Sensors and nodes must be authenticated to avoid strange nodes, confidentiality and integrity are significant in the data.

3.3.3. Third Layer: Services

In this layer the confidentiality, integrity and authenticity of the transferred data are managed through the IoT architecture, the services are called from devices, sensors, servers and systems; it could be vulnerable to internal or underlying attacks; developed services must keep the application safe and transparent of the IoT network.

3.3.4. Fourth Layer: Interface

This layer presents custom applications according to the hospital and patients; it applies protocols and standards with functional systems for users; doctors, patients, administrators and providers access information through interfaces or indicators. Security requirements: User authentication for access, protection of user privacy, defining profiles, data processing and checking software vulnerabilities.

3.3.5. Fifth Layer: Cloud

Cloud Computing provides capabilities to create, store and retrieve patient information, here the hospital, medical care points, doctors and laboratories view / update patient data. The cloud provider provides analytics, access management, data protection, and service integration. It is recommended to use AWS to process, store and transmit health information; this cloud

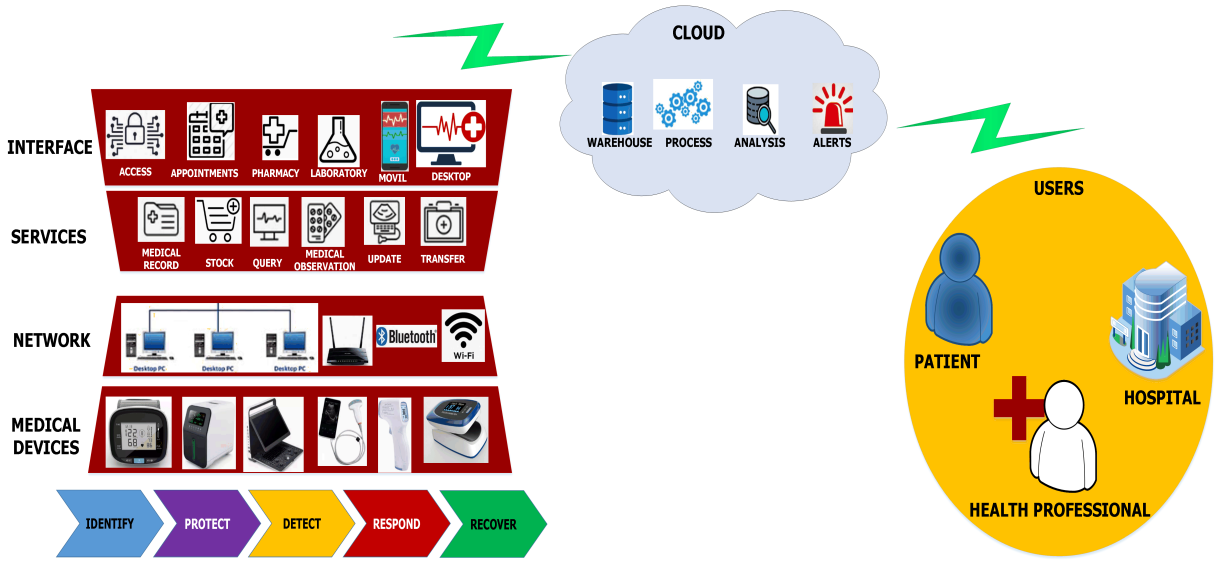


Figure 10: Architecture prototype of IoT Cybersecurity for a public or private hospital

allows HIPAA to be applied in a secure environment; the main characteristics of this cloud are: assignment of individual policies, roles and profiles; encrypted web content, registration and backup data; security groups to limit access to services; management of systems or web applications; encrypted MySQL database, registration, monitoring and alerts.

3.3.6. Sixth Layer: Users

Only three participants were considered in this layer: the patients that generated the data through medical devices, health professionals and the hospital; patients leave control of their health information on cloud servers, this is perceived by the patient as a threat to their privacy; as a requirement of this layer is the data integrity it stored; access to users can be by web, mobile or desktop application because the service layer allows delivery of information to any type of application.

As show in Figure 10 the importance of maintaining the confidentiality, integrity, availability, reliability and authenticity of user data on a public or private or hybrid environment; in addition, there may be people or groups interested in the health information such as laboratories, health providers and others.

Another component of the architecture is NIST Framework Core with its activities in infrastructure design; these activities are detailed below:

Identify: For identification, inventories of physical devices, systems and platforms are taken; data flow, business communication, external information systems also enter in the inventory, all organization resources are given a priority value, in addition third-party roles and responsibilities are identified; in addition to the organization, the mission, vision and objectives are identified, that is, the role of the organization in the health sector, the functions and critical services; in the evaluation, vulnerabilities are identified, information threats are reviewed, internal and external threats are identified.

Protect: The authentication and access category manages the credentials of devices, users and processes; in the training category, hospital staff, providers, and patients receive cybersecurity education, roles, and responsibilities according to policies; in the data security category, it is managed to protect the confidentiality, integrity and availability of the information; the information assets in any state or transaction are protected; in the protection of information management, security policies are implemented to defend information systems and assets.

Detect: In the anomalies category, the data flow for users and systems is managed, determine impacts and collect data on the attack, in addition to establishing alert guidelines; in the monitoring category, the physical network, people activities, unauthorized codes, providers activities, and unauthorized devices are reviewed to minimize activities against cybersecurity.

Respond: Response procedures are planned for possible cybersecurity incidents; in the communication category, the staff knows the response activities to an event, incident information, passing information according to the plans; others activities are: investigation of the notifications, the impact of the incident, forensic analysis, classification of incidents and vulnerability management are carried out, mitigating incidents, lessons learned.

Recover: Recovery procedures are defined and executed to ensure the replacement of information assets in the event of an incident; these procedures should be improved with the lessons learned; in the communication category, the hospital's relationships and reputation are managed, and recovery activities are also communicated.

The ISO 27001 standard maintains the confidentiality, integrity and availability of information on phases of NIST framework.

Architecture features:

- Interoperability to avoid interruption of operations,
- Scalability to connect with smart devices,
- Storage to support data delivered by devices,
- Communication overload to support communication between nodes,

- Processing overhead to perform algorithms on data and deliver it as information,
- Resistance to failures affecting the network,
- An IoT network solves the limits of growth, access, space, data transfer and data transformation; with the features the health system / environment improves the category of information and services.

IoT cybersegurity applied to the health area supports services such as: medical information, individualization, hospital emergency, monitoring, delivery and supervision of medicines, medical equipment, medical waste tracking, blood management, infection review and others.

Formula to measure the architecture workload

A formula was proposed to evaluate the architecture based on the layers, quantities were established according to the components for each layer, the Equation (1) is:

$$Occ = ABS\left(\sin\left(\sqrt{\frac{(Qd * Qn) + (Qs * Qi)}{Qp * Qu}}\right)\right) \quad (1)$$

Here:

Occ = Occupation or workload of architecture; *Qd* = Quantity of medical devices; *Qn* = Quantity of receiving nodes; *Qs* = Quantity of services available; *Qi* = Quantity of interfaces; *Qp* = Quantity of processes in the cloud; *Qu* = Quantity of final users.

Ten scenarios were simulated with the six parameters of the formula (Figure 11).

These were grouped in pairs as follows: medical devices with receiving nodes at Hardware Level, available services with interfaces at Software Level and cloud processes with final users at Process Level; in the first scenario the hardware level is 80, the software level is 108, the process level is 36 and the workload is 59.38%; in the fifth scenario the hardware level is 135, software level is 128, process level is 9 and the efficiency is 76.78%; in the tenth scenario the hardware level is 80, software level is 110, process level is 195 and the efficiency is 83.44%.

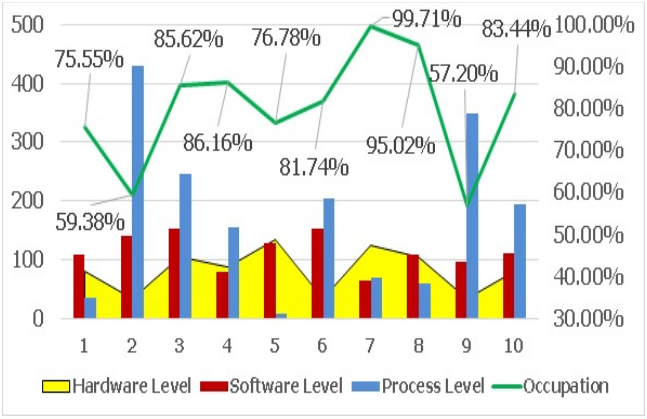


Figure 11: Workload of architecture prototype IoT Cybersecurity

As shown in Figure 11 the cross-line the workload of IoT cybersecurity in ten scenarios, in this simulation the minimum value was 59.38% and the maximum value was 99.71%; the average workload of this simulation was 80.06%.

We can deduce that the increase in the number of medical devices and data receiving nodes together with the low number of processes influence of the architecture.

An algorithm that applies cybersecurity on design of IoT architecture for a public or private hospital was proposed.

Flowchart techniques (Figure 12) were used to express and apply cybersecurity in the IoT architecture, it consists of two phases called Determine and Apply; the first phase Determine begins with taking inventories at the hospital such as mission, mission, needs, information assets, devices, and network parameters; having the complete record of inventories and parameters, the second phase Apply can be executed; here, the security standards specified in each layer are adopted and applied; otherwise, the inventory and parameters of the hospital must be reviewed again and the algorithm must be run again.

It is necessary to clarify that in case of massive patient assistance to the hospital, the IoT architecture is scalable in terms of the number of devices and storage, in addition this proposal considers the hospital's own devices; regardless of pandemic times or infections such as HIV, Ebola, H1N1, swine flu or COVID-19.

4. Discussion

Principles of Results: The architecture consists of continuous improvement by the functions of the NIST Framework Core in IoT design and adoption of standards.

Relationships of results: the conceptual model has elements that are used on architecture; the architecture has the layers and standards that the algorithm implements through activities.

Exceptions: the architecture only considers smart hospital devices, they are not considered patient-specific devices, BYOD does not apply; it does not consider the carbon footprint produced by the use of devices in the hospital, nor the costs of devices, nor the number of devices in the network, nor the payment values for the cloud.

The results of this research agree with: applying cybersecurity [4], [7], [8]; use HIPAA for health standard [2], [10], [13] and [14]; use NIST for cybersecurity standard [2] and [11]; the benefits of cloud computing are high considering the low cost, storage, access, processing, updating of information and supports the growth of data [14] and [15]; apply IoT cybersecurity to protect information assets [2], [3], [12], [15] and [16]; it use ISO / IEC 27000 series standard [2], [12], and [16].

Theoretical consequence of the research: The modular design of the IoT cybersecurity architecture allows the interconnection of devices, network, services, applications, cloud and users to support growth and adjustment of critical areas of the hospital; the architecture is adapted to the hospital that safeguards the information assets through layers and adopted standards in phases determined by the algorithm.

Possible practical applications: In 2018 Ecuador had 183 public hospitals and 451 private hospitals; the design and

implementation of IoT Cybersecurity in a hospital can be replicated regardless of the dimensions of areas, devices, floors, workers and other characteristics.

IoT recommendations with security measures

We present standard IoT security measures for any public or private health hospital in Ecuador; we emphasize that this proposal is for architecture in hospitals, here IoT devices and hospital information are secured; devices belonging to doctors or patients are not included or considered; the recommendations are in 3 blocks:

In design phase:

- Select upgradeable devices with standard protocols
- Apply network segmentation for connected IoT devices
- Identification and authentication of devices against the IoT network
- Perform device installation and configuration procedures
- Analysis planning and efficiency verification on devices In implementation phase:
- Device management not accessible from the internet
- Configure connection ports only for access to hospital devices
- Verify privacy and confidentiality of data on devices
- Physical and logical evaluation of the devices before their integration into the IoT network
- Restrict or secure access to the cloud interface In Operation phase:
- Continuous change of default credentials of IoT devices
- Continuous app updates on IoT devices
- Disable inactive connectivities
- Network connectivity and device integration
- Use Big Data to monitor the behavior of devices
- Delete of data from unused devices

5. Future work and Conclusions

As future work we proposed an cybersecurity analysis of internet medical things for care centers in Ecuador.

It was concluded that the cybersecurity standards applied to the design of IoT for a public or private hospital generates trust on information assets, preserves the confidentiality, integrity and availability of the information at the operational, tactical and strategic levels; the architecture prototype is between 59.38% and 99.71% of acceptable workload. With the continued growth of health data, there is a market for clinical data validated and verified by health professionals.

Security is adopted from the design of the infrastructure through standards, framework and good practices to minimize risks, ensure each layer and connectivity; the architecture simplifies the distribution and the relationship between the components.

Critical analysis:

Proper understanding of security requirements are important to this IoT cybersecurity recommendation for public and private hospitals in Ecuador; because health information is sensitive, indispensable for the early evaluation and diagnosis of human beings; that referring to the term cybersecurity, the following concepts converge: protection, security and legislation; here the first two terms (protection and security) are covered by Ecuador as evidence by Figure 6; but the legislative dimension is not very well implemented, so the proposed model covers this deficiency.

Conflict of Interest

The authors declare no conflict of interest.

Acknowledgment

The authors thank to Universidad Politécnica Salesiana del Ecuador.

References

[1] I. Alrashdi, A. Alqazzaz, E. Aloufi, R. Alharthi, M. Zohdy, and H. Ming, "AD-IoT: Anomaly detection of IoT cyberattacks in smart city using machine learning," *2019 IEEE 9th Annu. Comput. Commun. Work. Conf. CCWC 2019*, pp. 305–310, 2019, DOI 10.1109/CCWC.2019.8666450.

[2] A. Strielkina, O. Illiashenko, M. Zhydenko, and D. Uzun, "Cybersecurity of healthcare IoT-based systems: Regulation and case-oriented assessment," in *2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT)*, 2018, pp. 67–73, DOI 10.1109/DESSERT.2018.8409101.

[3] D. Minoli, K. Sohraby, and B. Occhiogrosso, "IoT Security (IoTSec) Mechanisms for e-Health and Ambient Assisted Living Applications," *Proc. - 2017 IEEE 2nd Int. Conf. Connect. Heal. Appl. Syst. Eng. Technol. CHASE 2017*, pp. 13–18, 2017, DOI 10.1109/CHASE.2017.53.

[4] J. Rajamaki, J. Nevmerzhitskaya, and C. Virag, "Cybersecurity education and training in hospitals: Proactive resilience educational framework (Prosilience EF)," *IEEE Glob. Eng. Educ. Conf. EDUCON*, vol. 2018-April, pp. 2042–2046, 2018, DOI 10.1109/EDUCON.2018.8363488.

[5] P. Rathod and T. Hamalainen, "A Novel Model for Cybersecurity Economics and Analysis," *IEEE CIT 2017 - 17th IEEE Int. Conf. Comput. Inf. Technol.*, pp. 274–279, 2017, DOI 10.1109/CIT.2017.65.

[6] R. Sabillon, J. Serra-Ruiz, V. Cavaller, and J. Cano, "A comprehensive cybersecurity audit model to improve cybersecurity assurance: The cybersecurity audit model (CSAM)," *Proc. - 2017 Int. Conf. Inf. Syst. Comput. Sci. INCISCOS 2017*, vol. 2017-Novem, pp. 253–259, 2018, DOI 10.1109/INCISCOS.2017.20.

[7] G. Parekh *et al.*, "Identifying Core Concepts of Cybersecurity: Results of Two Delphi Processes," *IEEE Trans. Educ.*, vol. 61, no. 1, pp. 11–20, Feb. 2018, DOI 10.1109/TE.2017.2715174.

[8] Y. Lu and L. Da Xu, "Internet of things (IoT) cybersecurity research: A review of current research topics," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2103–2115, 2019, DOI 10.1109/JIOT.2018.2869847.

[9] A. F. Klaib and M. S. Nuser, "Evaluating EHR and health care in Jordan according to the international health metrics network (HMN) framework and standards: A case study of hakeem," *IEEE Access*, vol. 7, pp. 51457–51465, 2019, DOI 10.1109/ACCESS.2019.2911684.

[10] D. Akarca, P. Xiu, D. Ebbitt, B. Mustafa, H. Al-Ramadhani, and A. Albeyatti, "Blockchain Secured Electronic Health Records: Patient Rights, Privacy and Cybersecurity," *Conf. Proc. 2019 10th Int. Conf. Dependable Syst. Serv. Technol. DESSERT 2019*, pp. 108–111, 2019, DOI 10.1109/DESSERT.2019.8770037.

[11] J. Webb and D. Hume, "Campus IoT collaboration and governance using the NIST cybersecurity framework," *IET Conf. Publ.*, vol. 2018, no. CP740, pp. 1–7, 2018, DOI 10.1049/cp.2018.0025.

[12] A. Abdullah, R. Hamad, M. Abdulrahman, H. Moala, and S. Elkhediri, "CyberSecurity: A Review of Internet of Things (IoT) Security Issues, Challenges and Techniques," *2nd Int. Conf. Comput. Appl. Inf. Secur. ICCAIS 2019*, pp. 1–6, 2019, DOI 10.1109/CAIS.2019.8769560.

[13] I. Medvediev, O. Illiashenko, D. Uzun, and A. Strielkina, "IoT solutions for health monitoring: Analysis and case study," *Proc. 2018 IEEE 9th Int. Conf. Dependable Syst. Serv. Technol. DESSERT 2018*, vol. 2015, pp. 163–168, 2018, DOI 10.1109/DESSERT.2018.8409120.

[14] S. Chenthara, K. Ahmed, H. Wang, and F. Whittaker, "Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing," *IEEE Access*, vol. 7, pp. 74361–74382, 2019, DOI 10.1109/ACCESS.2019.2919982.

[15] J. Diaz, J. E. Perez, M. A. Lopez-Pena, G. A. Mena, and A. Yague, "Self-Service Cybersecurity Monitoring as Enabler for DevSecOps," *IEEE Access*, vol. 7, pp. 100283–100295, 2019, DOI 10.1109/access.2019.2930000.

[16] I. Brass, L. Tanczer, M. Carr, M. Elsden, and J. Blackstock, "Standardising

a moving target: The development and evolution of IoT security standards," *IET Conf. Publ.*, vol. 2018, no. CP740, pp. 1–9, 2018, DOI 10.2139/ssrn.3437681.

[17] A. Razaque *et al.*, "Survey: Cybersecurity Vulnerabilities, Attacks and Solutions in the Medical Domain," *IEEE Access*, vol. 7, pp. 168774–168797, 2019, DOI 10.1109/ACCESS.2019.2950849.

[18] I. M. Skierka, "The governance of safety and security risks in connected healthcare," *IET Conf. Publ.*, vol. 2018, no. CP740, pp. 1–12, 2018, DOI 10.1049/cp.2018.0002.

[19] M. Barrett, "Framework for improving critical infrastructure cybersecurity," *Proc. Annu. ISA Anal. Div. Symp.*, vol. 535, pp. 9–25, 2018.

[20] INEC Instituto Nacional de Estadisticas y Censo, "Registro Estadístico de Camas y Egresos Hospitalarios-Ecuador," *Regist. estadístico y Egr. 2018*, 2018.

[21] U. T. International, *Global Cybersecurity Index (GCI) 2017*, no. November. 2017, DOI 10.1111/j.1745-4514.2008.00161.x.

[22] International Telecommunication Union, *Global Cybersecurity Index (GCI) 2018*. 2018, DOI 10.1111/j.1745-4514.2008.00161.x.

[23] K. Scwab, *The Global Competitiveness Index Report 2017-2018*, no. 31. 2018.

[24] R. Lucio, N. Villacrés, and R. Henríquez, "Sistema de salud de Ecuador," *Salud Publica Mex.*, vol. 53, no. SUPPL. 2, pp. 177–187, 2011.

[25] D. R. L. Pulles, D. M. C. Urquizo, and Ms. A. C. MBA, "The Present Situation of e-Health and mHealth in Ecuador," vol. 4, no. 3, pp. 261–267, 2017.

[26] D. Pillo-Guanoluisa and R. Enríquez-Reyes, "Gobierno de TI con énfasis en seguridad de la información para hospitales públicos," *Maskana*, vol. 8, no. 0, pp. 42–55, 2017.