SURVEY ARTICLE

Survey and testing of the IoT Cybersecurity Framework Using Intrusion Detection Systems

Carmen Beatriz Espinosa Garrido
Department of Engineering, Universidad Popular Autonoma del Estado de Puebla, Puebla, Mexico
carmenbeatriz.espinosa@upaep.edu.mx

Sandra Sendra Compte
Universitat Politècnica de València, València, Spain
sansenco@upv.es

Luis Rosales Roldan
Department of Engineering, Universidad Popular Autonoma del Estado de Puebla, Puebla, Mexico
luis.rosales@upaep.mx

Alejandra Aldrette Malacara
Department of Engineering, Universidad Popular Autonoma del Estado de Puebla, Puebla, Mexico
alejandra.aldrette@upaep.mx

Received: 16 August 2022 / Revised: 18 October2022 / Accepted: 20 October 2022 / Published: 30 October 2022

Abstract – The Internet of Things is a new paradigm that facilitates collecting business or personal data through smart devices with Internet connections. IoT devices are heterogeneous and have a limited computational capacity which represents a challenge for protecting data against cyber-attacks. This article surveys communication protocols, cybersecurity attacks and intrusion detection systems (IDSs). This study identifies the IoT protocols used for data transmission, and cybersecurity challenges and then presents a comparative analysis of IDSs. Next, the IoT cybersecurity framework, IoTCyFra, is surveyed by cybersecurity specialists. IoTCyFra is a validated IoT cybersecurity framework with an organizational structure that safeguards data and detects cybersecurity threats in an IoT infrastructure. It also explores how an IDS protects against cyberattacks through an IoT-controlled environment. Finally, the results and conclusions are reported.

Index Terms – Internet of Things, Cybersecurity, Intrusion Detection System, Framework, Cyberattacks, Communication Protocols.

1. INTRODUCTION

The Internet of Things (IoT) facilitates connectivity and data processing through electronic devices. It enables data collection through Internet-connected sensors for the medical, security, and other sectors [1]. IoT technology allows connections between intelligent devices and humans anytime, anywhere, facilitating decision-making in complex systems [2]. IoT devices are heterogeneous and limited in computing and energy resources, making them susceptible to security threats and attacks. These security vulnerabilities can lead to the unavailability of or unauthorized access to IoT systems, and there have therefore been several investigations focused on such security issues [3]. The largely unplanned, exponential implementation of IoT devices and applications has led to security breaches [4]. Symantec detected three billion daily cyberattacks on the IoT in 2017, and these are becoming ever more sophisticated and harder to identify [5].

1.1. Internet of Things and Cybersecurity

The IoT infrastructure comprises Internet-enabled sensors [6] that publish services and transfer content [7]. In this paradigm, everyday items, such as bulbs, locks, cameras, and thermostats, become smart devices [11] that collect data without human intervention and transfer them to the Internet cloud anywhere and anytime [9]. Before connecting to the Internet, IoT devices uniquely identify themselves in a distributed and decentralized infrastructure [10] using radio frequency, fast response codes, and wireless technology [11]. The data generated by IoT devices can be analyzed to inform decision-making in business applications [12], and for these data to retain their value, they must be reviewed [11].

Thus, the use of IoT devices and services has increased in the transportation, health, energy, business, social, and personal sectors [3], as well as in smart cities [13], science, industry, engineering, human assistance, and daily activities [14]. It connects millions of devices using varied technologies [15] and improves people's quality of life through energy industrialization [16]. The IoT requires a scalable, mobile, and wireless connection for specialized devices [7]. A basic IoT architecture consists of sensors, middleware, and application layers [17]. The communication protocols used are radio-frequency identification (RFID), Bluetooth, Wi-Fi networks, and ZigBee [18].

If IoT cybersecurity is compromised, there can be damaging disruption and disastrous effects on critical services [9]. Cybersecurity is one of the most important factors [14] protecting against cyberattacks by controlling access, customer privacy, secure communication, and secure storage [5]. There are, however, challenges in IoT security, such as access control and identity management for intelligent devices [5]. Other security issues are related to network traffic analysis tools [15] and communication protocols not designed for the IoT [10].

IoT devices are susceptible to cybersecurity threats because they have limited processing and storage capacity and intermittent connectivity capabilities to save energy and bandwidth. To implement cybersecurity measures, user trustworthiness and information transactions must be ensured [14]. For this purpose, systems such as firewalls, network access controls (NACs), and intrusion detection systems (IDSs) have been proposed. An IDS examines the activity between connected devices by network monitoring and issuing alerts[13].

An IoT architecture consists of perceptual, network, and application layers. The perceptual layer comprises IoT sensor nodes, which belong to the environment, motion, electrical, biosensor, identification, positioning, presence, machine vision, interaction, acoustic, force/load, hydraulic, chemical, and object information [19]. The network layer comprises network access and transmission and uses communication protocols such as 3G, WiMax, Wireless xDSL, and wired networks. The application layer includes information processing and sensor health monitoring [20].

In the IoT infrastructure, devices have sensors, actuators, programming logic, and communication interfaces. Within the network layer, media such as Ethernet, Wi-Fi, hybrid fiber-coaxial (HFC), and digital subscriber line (DSL) are used for data transmission. For data processing, protocols such as IEEE 802.15.4, Bluetooth low energy (BLE), WIFI HART, Z-Wave, LoRaWAN, 6LoWPAN, RPL, CoAP, and MQTT are used [13].

Ghori et al., 2020 mention that BLE makes an efficient energy use of IoT devices. Most BLE applications use a star topology network, but when mesh topology is used, the security vulnerabilities for BLE increase. A survey on BLE communication protocols detects security findings related to confidentiality and integrity [21].

Moreno-Cruz et al., 2020 design a new Wireless Communication Protocol (WCP) called de treNch for energy harvesting with standardisation and expansion for IoT wireless sensor networks with ultra-low energy level demand. It operates with asynchronous, synchronous transmissions, with small packet sizes and lightweight architecture that gives control to the nodes. They describe a security scheme with standard mechanisms without increasing processing time or energy consumption. They evaluate the performance of wireless networks with sensors using Zigbee and Z-Wave [22].

Ferrari et al., 2007 discuss communication protocol scenarios with direct transmission between remote nodes and network coordinators and where the data is transmitted through routers. They also show the Received Signal Strength Indication (RSSI) measure and the behavior of two communication protocols, Zigbee and Z-Wave. They analyze the network throughput, performance, delay, and connectivity through a simulation. The results are similar regarding network connection; in both cases, the connection is bimodal, i.e. complete or non-existent [23].

The IoT has adopted the IEEE 802.15.4 standard, and network devices use it with low power, low data rate operations and low processing capabilities. It is used in battery-powered wireless devices. It is a standard that supports IP-based applications with flexible latency, efficient performance, and quality of service (QoS) requirements. It is used in the agriculture and smart city industries for its low data rate and low energy communication. The topology contains coordinator and end devices [24].

Communication protocols such as ZigBee, SigFox, Lora WAN, BLE, Z-Wave and IEEE 802.15.4 allow data transfer in the network layer. A comparative analysis of these protocols is presented below, indicating their description, function, advantages, and disadvantages (see Table 1).

1.2. Intrusion Detection System

The limitation in the storage and computational capacity of the IoT devices makes it difficult to install security measures in the IoT nodes. An IDS can be used as a compensatory measure, which monitors the communication between devices and issues alerts to possible cyberattacks [13].

IDSs can detect attacks using signatures or pattern analysis. Signature-based detection has higher accuracy and a lower false alarm rate. Still, it does not detect unknown or zero-day attacks, whereas pattern-based detection can identify zero-day attacks with high false alarm rates [29]. IDS architecture consists of captured network packets, filtering, and examined packets and attack patterns. IDS performance evaluation considers metrics, such as the accuracy of specific attack categories, the accuracy of test classification; the number of false positives and false negatives; the detection rate; and the false positive rate [30]. IDS implementation can be analyzed equally by considering the true positive rate, false positive rate, false negative rate, classification rate, and receiver operating characteristics [5]. IDSs can misidentify traffic and therefore fail to react to real threats. One option to detect the traffic efficiently is implementing a hybrid IDS structure that relies on machine learning [31].

For IDS network packet analysis, datasets are used, which comprise a collection of network traffic containing user behavior, attacker behavior, and system configuration. Some of the datasets are DARPA/KDD Cup99, CAIDA, NSL-KDD, ISCX 2012, ADFA-LD/ADFA-WD, and CICIDS 2017 [5]. Others, such as MAWILab, SimpleWeb, IMPACT, UMass, Kyoto, IRSC, UNSW-NB15, UGR16, and HIKARI-2021 have also been generated [29]. The diversity of attacks, anonymity, available protocols, type of traffic capture, network configuration definitions, data labelling, heterogeneity, encryption, and metadata are considered to evaluate these datasets. Some disadvantages of these datasets are a lack of updates, the associated processing time, and the generated large files [30].

Several taxonomies have been proposed for IDSs. One consists of classification according to placement, analysis strategy, type of IoT intruder, and attack detection technique. Firstly, the position can be centralized, distributed, or hybrid. Next, the analysis strategy can be anomaly-based, signature-based, or specification-based. Then, the type of intruder can be physical, network, software, or encrypted. Finally, the attack detection technique can be machine learning or deep learning (see Table 2) [13].

Table 1 Comparative analysis of the communication protocols used in the network layer. ZigBee, SigFox, Lora WAN, Bluetooh Low Energy and Z-wave.

Protocol	Description	Function	Advantages	Disadvantages
ZigBee [25]	Used to automate homes and buildings [25]. Composed of a coordinator, router, and terminal equipment [26].	Trustworthiness provided by authentication key [25].	Low cost and energy consumption. Robustness and flexibility [25].	Used for short distance communication [25].
SigFox [27]	Used in 60 countries within Europe. Based on the IEEE 802.15.4 standard.	Unlicensed bands of 915 MHz (USA) and 868 MHz (Europe).	Low cost. Uses free licenses.	Only for short distances. Half-duplex.
LoRa WAN [28]	It operates via a centralized model and in star mode.	Composed of end devices, gateway, and remote servers.	Low energy consumption. Long-range technology.	Unidirectional communication between end devices and gateway.
BLE [21].	Considers IoT device’s battery.	It operates with start and mesh topology.	Efficient energy consumption.	Vulnerabilities at mesh topology, related to integrity and confidentiality.
Z-wave [23].	For commercials and home applications. It sends short control messages from one node to many.	Bands of 908 MHz (USA) and 868 MHz (Europe). Layer composition: MAC, transfer, routing, and applications.	Low cost. The home control network has battery-powered, DC-powered, fixed, and mobile nodes.	Low bandwidth. Half-duplex. Only for short distances, 70 – 100. meters.
IEEE 802.15.4 [24].	WiFi network devices use it with low power, low data rate and low processing capabilities.	The topology contains coordinator and end devices.	Supports IP-based applications with flexible latency, performance, and QoS	It does not support varying network conditions.

Table 2 Taxonomy of IDSs for the IoT [13]

Placement Strategy	Analysis Strategy	Intrusions	Attack Detection Techniques
Centralized	Anomaly-based	Physical intrusions	Machine learning techniques
Distributed	Signature-based	Network intrusions	Deep learning techniques
Hybrid	Specification-based	Software intrusions	
		Encryption intrusions	

Another IDS taxonomy involves either signature-based or anomaly-based categorizations. Those based on signatures use pattern-matching techniques to detect attacks and issue alerts. Those based on anomalies use statistical, knowledge, or machine learning techniques. Any difference between the behavior and the model is seen as an anomaly [5]. A further IDS classification is based on being in misuse mode or anomaly detection mode. In the first, data are evaluated and compared with a signature base. In anomaly detection, abnormal traffic is identified by acquiring, processing, and classifying the patterns [32].

1.3. IoT Infrastructure Cyberattacks

The security challenges in any network involve prevention, detection, and mitigation strategies [33]. Cyber threats to the IoT infrastructure can be white box, where the attacker has complete knowledge of the target system; black box, where the attacker has no information but could learn it; and grey box, where the adversary has limited knowledge of the system to attack [34]. It is shown at Table 3 some cyberattacks on IoT infrastructure.

1.3.1. Adversarial IDS Machine Learning Attacks

Traditional methods and techniques against cyber threats are not appropriate for IoT vulnerabilities, so there is a need for improved security solutions. Machine learning techniques have been applied to detect IoT security threats, in which neural networks classify attacks in the IDS.

However, machine learning in IDSs is impacted by adversarial attacks. One option to improve the performance of IDS-based deep learning for the IoT is tocuse a variant of the feed-forward neural network (FNN), known as a self-normalizing neural network (SNN), and the BoT-IoT dataset. FNN is significantly degraded by adversarial threats, from a 95% prediction rate to 24%. However, SNN is more resilient to these malicious attacks, with a 9% improvement in performance [33].

Adversarial attacks involve the application of unidentified perturbations in the machine learning process, incorrectly detecting malicious events. In these threats, the attacker may have control of the trained data, the detection model, the sample feature set, Oracle, or deep manipulation. The attacks can consist of:

- Poisoning, which is the manipulation of the dataset to influence detection;
- Time interference, which is the obfuscation of detection, changing its sensitivity;
- Evasion attack is the incorrect classification of malicious data [35].

Attackers use local search, combinatorial optimization, or convex programming to identify the adversarial perturbation that compromises machine learning operation. Concerns have been generated for deep machine learning using the Fast Gradient Sign Method (FGSM) and Jacobian-Based Saliency Map Attack (JSMA). Generative Adversarial Network (GAN)-based adversarial machine learning attacks have also been created and validated that can evade an IDS with black-box parameters, preserving network performance. An IDS can defend against adversarial attacks by opting for adversarial training in machine learning models and thus learning from possible adversarial perturbations. However, it will only enact improvement against the trained adversarial examples [36].

IDS is exposed by an adversarial GAN attack, called attackGAN, which is a black box and evades IDS, ensuring network functionality. AttackGAN is based on Wasserstein GAN and has a higher success rate in black-box attacks against IDS compared to the Fast Gradient Sign Method (FGSM), Project Gradient Descent (PGD), CW attack and GAN-based algorithms. This is experimentally validated using the NSL-KDD dataset. To develop network security systems, adversarial attacks and game defense are recommended [37].

Machine learning has also been used for wireless network security and has enabled device monitoring and anomaly detection. However, it has been vulnerable to adversarial machine learning attacks, causing a loss of wireless communication radio performance. These attacks occur in wireless networks as follows:

- Jamming attack: the transmitter monitors the channel status (busy) and transmits when the channel is idle.

- Spectrum poisoning attack: the attacker changes the characteristics of the channel state so that the transmitter wrongly decides to transmit.
- Priority violation attack: the attacker forces the transmitter to make incorrect decisions, such as an evasion attack.
- As a defense mechanism, it is proposed that the IoT transmitter selectively performs incorrect actions so that the exploratory attack does not happen [38].

1.3.2. Botnets Attacks

Kolias et al. explain that IoT devices are vulnerable to botnet attacks due to weak protection, low maintenance, poor monitoring, misconfiguration, and a lack of operating system updates. One botnet identified in 2016 is Mirai—a DDoS attack that sends 1.1 Tbps traffic to a target system. An unauthorised login can infect webcams, DVRs, routers, and other IoT devices. This botnet scans IoT systems through ports 23 or 2323, although it can be detected by its signature data, scanning ports, the reports generated, or the exchanged messages. It already has variants such as Persira, which uses port 81; Lua, which uses command and control encrypted; and BrickerBot, which uses the SSH port. As a form of botnet mitigation, it is recommended to follow best practices and security standards for IoT [39].

1.3.3. BLE Attacks

BLE technology has specific network attacks, such as Key Negotiation of Bluetooth (KNOB), BLE injection-free attacks, bluejacking, bluebugging, bluesnarfing and DoS attacks. Therefore, an IDS is recommended to detect security threats, protect against zero-day vulnerabilities, and avoid applications unavailability [21].

1.3.4. Industrial IoT Attacks

The Industrial IoT (IIoT) infrastructure is susceptible to cyberattacks; these attacks could be classified as attacks on physical components, software components and network components. To avoid these threats, their architecture should consider security requirements, such as security, privacy, reliability, safety, and resilience [40].

1.3.5. Denial-of-Service

The Denial-of-service (DoS) attack disturbs the availability of services by receiving massive traffic over the network. It is the most common attack on the IoT network and could affect all the network layers, from physical to applications. This threat is originated from remote sites, and it could be dispersed, named distributed DoS (DDoS). This attack could cause the unavailability of services or authentication threats. The prevention and detection of this attack could be done through an IDS [41].

Table 3 IoT Cyberattacks

Cyberattacks	Description	Type of attacks	Mitigation
Adversarial attacks	Unidentified perturbations in the machine learning process, erroneously detecting malicious events [35].	Poisoning, time interference, evasion attack [35]. Jamming attack, spectrum poisoning attack, priority violation attack	Use a SNN and the BoT-IoT dataset. Machine learning process for learning from possible adversarial perturbations. IoT transmitter selectively performs incorrect actions.
Botnet attacks [39].	DDoS attack that sends 1.1 massive traffic to a target system through compromised IoT devices.	Port scanning, command and control encrypted [38].	Follow best practices and security standards for IoT.
BLE attacks [21].	Attacks focused at BLE technology.	KNOB, BLE injection free attack, bluejacking, Bluebugging, Bluesnarfing, DoS.	IDS to detect security threats.

IIoT attacks [40]	Attacks on physical components, on software components, on network components.	Unauthorized access, trojans, worms, DoS, DDoS, WiFi unauthorized access, cloud infrastructure unauthorized access.	Cybersecurity solution with privacy, reliability, safety, and resilience.
DoS attack [41]	Disruption of the availability of services when receiving massive traffic through the network.	DoS, DDoS.	Prevention and detection through an IDS.

1.4. Paper Organization

The first section of this paper describes the IoT, IoT cybersecurity, IDSs and IoT cyberattacks. Then, the second section presents research related to IoT cybersecurity. The third section covers the methodology. In the fourth section, the results are set out, which comprise a comparative analysis of IDSs for IoT infrastructure; validation of the IoTCyFra cybersecurity framework via an IT specialist survey; the IoTCyFra operation mode, and testing of the IoTCyFra cybersecurity framework in the categories of policies and procedures, protect operation and identify threats. Finally, the results and conclusions are presented in section four. This work aimed to validate and test a cybersecurity framework for the IoT named IoTCyFra. It was concluded that it efficiently detected cyberattacks on IoT infrastructure and could be easily implemented.

2. LITERATURE REVIEW

Some methods assessing IT infrastructure risks are COBIT, Austrian IT Security Manual, EBIOS, ISO/IEC 27007, MARION, MEHARI, and OCTAVE Allegro. At Langlangbuana University, operational vulnerabilities and risk analysis are assessed with OCTAVE Allegro. After implementing ISO/IEC 27002 security controls, a risk reduction per the OCTAVE Allegro assessment is obtained [42]. The ISO 27001 standard has a noticeable influence on information security to maintain the triad of information security. Implementing the security domains of ISO 27001 improves confidentiality, integrity, and availability [43]. On the other hand, NIST CSF is used to assess the cybersecurity of a government organization. The information for the assessment is obtained through a NIST CSF tool, which identifies the organization's ongoing situation. Performing a self-assessment and implementing security policies can be complex. There is a lack of flexible and accessible mechanisms that reflect the current cybersecurity context of an organization and simplify the process of implementing a cybersecurity standard [44].

Kafle et al. present the standardization of IoT in the International Telecommunication Union (ITU). The ITU has standardized IoT with industry and academia, defining requirements, capabilities, frameworks, use cases, and applications. ITU standards related to IoT have technical characteristics, conditions, frameworks, terminology, and collection of use cases, although technical specifications such as architecture and protocols are still missing. The ITU-T Y.2060 reference model shows the functions and capabilities of IoT architecture. The ITU-T M2M Focus Group identifies M2M service requirements. ITU-T Study Group 20 standardizes IoT technologies, services, and applications. IoT requirements are listed in ITU-T Y.2066. ITU-T Y.3031 is an IoT identification framework, while ITU-T Y.3034 specifies mechanisms for heterogeneous networks through an ID in the IoT infrastructure [45].

There is a significant amount of current research related to IoT cybersecurity. International companies are incrementally utilizing IoT devices, and their value partially depends on data, applications, and cybersecurity services [11]. IoT technology tends to improve people's quality of life through automation, which saves time and money [17], but security issues remain. Several investigations have addressed IoT cybersecurity, defining the state of IoT security, its principles, and the challenges focused on authentication, privacy, confidentiality, access control, trust management, standard policies, and countermeasures [3]. There have been investigations concerning confidentiality, privacy, and other aspects of IoT cybersecurity [46].

In addition, IoT security standards and frameworks have been created, highlighting the architecture, applications, and functions [8]. Additionally, models, diagrams, and implementations of IoT technology and devices have been presented. However, there remain areas for improvement concerning security and data privacy [14]. Some security framework proposals involve mitigating IoT security threats using IoT secure sensors in the computational cloud [47]. Additionally, software/hardware design methodologies have been integrated to prevent, detect, diagnose, isolate, and apply countermeasures based on security findings [48]. Alternatively, a formal framework for IoT security analysis has been presented, considering IoT data, devices, policies, network dependencies, and threats [15].

Furthermore, a security model for the IoT has been proposed with crucial points in its taxonomy [48]. Similarly, a taxonomy with quality attributes, security mechanisms, and policies has been presented to identify attacks and reduce vulnerabilities in IoT systems [6]. Another taxonomy for network security attacks on the IoT was designed to identify flaws and risks while developing programs or applications [9].

Complementarily, Ammar et al., 2018 conducted a security survey of the leading IoT frameworks. Each identifies the architecture, application development, hardware, and security features. The reviewed platforms are AWS IoT, ARM Bed OS, Azure IoT suite, Google's Brillo/Weave, Ericson's Calvin, Apple's Homekit, and Samsung's Smart-things. They are robust and immune to attacks; however, design flaws still expose users to significant security risks, so the authors recommend physical protection on IoT devices to ensure data privacy [8].

Similarly, Kandasamy et al., 2020 investigate IoT security vulnerabilities and introduce a unique risk classification and quantification method for IoT. They analyze the reference frameworks NIST CSF, OCTAVE, TARA, ISO/IEC 27001, ISO/IEC 30141, and ISO/IEC 27030. Their findings are as follows: NIST does not focus on IoT; OCTAVE manages information assets, threats, and risks; TARA improves the quality of risk and control assessments, and ISO/IEC cybersecurity standards manage risks and guide security and privacy.

In another approach, Vijayakumaran et al., 2020 present Next-Generation Cyber Security Architecture (NGCS) for Industrial Internet of Things (IIoT) applications that protects real-time data transmission from devices to cloud storage. It provides an automaton defense system for a real-time Wi-Fi environment. They conclude that a focus on preventing cybersecurity threats is primarily needed.

Table 4 Related Works

Researches	Years	Advantages	Disadvantages
Jufri et al. [42]	2017	Implementation of ISO 27002 to reduce security risks. Risk assessment is done with OCTAVE Allegro.	The cybersecurity risks increase with the lack of written cybersecurity regulations.
Kolias et al. [39]	2017	The risk of cyber-attacks can be reduced by following IoT security best practices.	The security of IoT devices is weak, with poor maintenance and misconfiguration.
Diro & Chilamkurti. [54]	2018	Improve the accuracy in cyber-attack detection and downgrade false alarm rate with deep learning at IDS.	Deep learning for diverse datasets and machine learning methods has yet to be integrated into IDS.
Hernandez Ramos et al. [55]	2018	Create a technical framework based on a fuzzy technic on the MQTT protocol. Discover and report security flaws and vulnerabilities.	It is only available for MQTT protocol protection. It needs to automate the error detection.
Matheu-Garcia et al. [56]	2019	Propose a security certification methodology for automated IoT assets, considering device lifecycle and ETSI functionalities.	Challenges for this framework include heterogeneity of equipment, current schemes, and the absence of a database of IoT vulnerabilities.
Wazoel Lubua & Pretorius. [57]	2019	Develop a security framework for business continuity.	Lack of a procedure for security policies creation. It depends on key people for formalizing the guidelines and reviewing policies.
Zarca et al. [51]	2020	Mitigation of cyber-attacks using a network model with SDN, NVF and honeypots in IoT.	Honeypots do not yet work for 5G networks in IoT.

Sulay et al. [43]	2020	Implement ISO to enforce data confidentiality, integrity, and availability.	The achievement of the strategic objective depends on the organizational assets.
Adi et al. [49]	2020	Propose a framework for IoT applications to learn how they work.	It does not consider how IoT devices can adaptively learn in environments with limited computational resources.
Ghori et al. [21]	2020	Identify that BLE with mesh topology is energy efficient.	Self-configuration mechanisms are also needed to support the start-up of BLE mesh networks.
Kwon et al. [58]	2020	Recognize with the Cyber Threat Dictionary what type of cyber-attack is affecting the system	More defense-attack mapping tools should be developed to help cybersecurity personnel.
Vijayakumaran et al. [40]	2020	Present Next Generation Cyber Security Architecture (NCSA) automates the process of data transmission and detects cybersecurity attacks efficiently for IIoT.	Need to focus more on preventing cybersecurity attacks.
Xiong et al. [59]	2021	They propose a threat modelling language for enterprise security based on the ATT&CK Mitre Matrix.	This model still needs to be tested with other sources of attacks, such as CVE and CWE and to measure security probabilistically.
Georgiadou et al. [60]	2021	Identify, classify, and analyze security gaps in infrastructure. Create policy, procedures and strategies based on ATT&CK.	They recommend exploring the cultural framework of cybersecurity to assess the current state of an organization.
Frayssinet Delgado et al. [61]	2021	Propose the use of the methodology based on the NIST CSF for governmental organizations.	It is recommended to have incidence statistics and to have trained personnel.

Adi et al. propose a framework for IoT applications that shows the current situation, installation of machine learning, and discovery techniques for IoT devices. This framework is implemented with ontology, builds knowledge autonomously in various IoT domains, and has ontology databases, parameters, and hypotheses. But it does not consider adaptive learning on IoT devices with limited computational resources [49]. On the technical side, a service interface for IoT platform security has been developed, which solves the problem of device heterogeneity and reduces device resource consumption [50]. In contrast, a multilevel trust method based on an intelligence system has been proposed for IoT attack reduction and energy consumption optimization [16]. Fuzzy logic has also been used to detect IoT security attacks [10]. Similarly, software-defined networking (SDN) technology has also been used within IoT networks to mitigate cyberattacks [11].

Zarca et al. propose using Software Defined Networking (SDN) and Network Function Virtualization (NVF) to install honeypots in IoT. Technologies such as NFV and SDN in honeypots establish data security in IoT through authentication, authorization, and quality of service. Honeypots are virtual services with resource consumption that pretend to be real within IoT, so attackers are distracted from their real targets and allow specialists to execute countermeasures. Honeypots serve as decoys for attackers, through routing, ThingPot and HIoTPOT. With honeypots in IoT, it is possible to mitigate attacks such as DoS, bots or unknown vulnerabilities with full connectivity and on demand [51].

Alhowaide et al. recommend managing data size in IDS to detect threats faster and improve machine learning performance. They consider IoT network data as 5V (volume, velocity, variety, veracity, and value) database, to which dimension reduction can be done. They experiment with NSL, NB15, BoTNetIoT and BOTIoT datasets. It turns out that Principal Component Analysis (PCA) is the best method to reduce the database and Random-Forest (RF) is the best to distinguish the least amount of information. Dimension reduction is efficient because it reduces noise, data redundancy and improves data classification [52].

Alsaedi et al. comment that the KDDDCPU99, NSL-KDD, UNSW-NB15, ISCX, LWS-NDR, AWID, UNSW-IoT and UNSW-IoT datasets have shortcomings, because they do not include IoT/IIoT features, do not have sensor data, telemetry data or do not contain IoT attack scenarios. They propose a new IoT/IIoT dataset, called TON_IoT, which includes easy labeling, traffic classification, telemetry, operating systems and network traffic, collected from IoT devices. This dataset is simulated in an IIoT infrastructure, with machine learning and deep learning, implemented with tools such as SDN, NFV and NSX-VMWware [53]. The related IoT cybersecurity researches are presented in Table 4.

3. IOT CYBERSECURITY FRAMEWORK USING IDS

3.1. Methodology

The methodology used in this study was quantitative and correlational. It began with a literature review on IoT, cybersecurity, cyberattacks and IDS, identifying the current issues. A comparative analysis of IDS technology was then carried out. Next, an IoT cybersecurity framework was selected and surveyed by information technology (IT) security specialists. Additionally, a controlled IoT environment was set for cyberattack simulation. Finally, the results and conclusions were reported (see Figure 1).

From the literature review, cybersecurity standards and frameworks were identified, such as NIST CSF, ISO/IEC 27002, OCTAVE Allegro, [62], ISA/IEC 62443, the Lubua reference framework [57] and IoT Cybersecurity Framework (IoTCyFra) using IDSs [63]. As IoTCyFra, shown in Figure 2, is generated from a comparative analysis of the previous frameworks, it is selected for an IT security specialist survey.

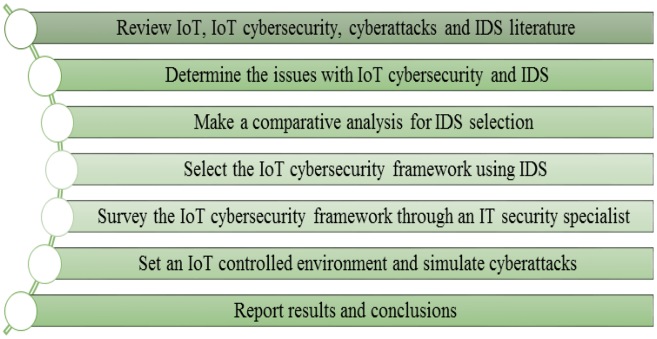

Review IoT, IoT cybersecurity, cyberattacks and IDS literature
Determine the issues with IoT cybersecurity and IDS
Make a comparative analysis for IDS selection
Select the IoT cybersecurity framework using IDS
Survey the IoT cybersecurity framework through an IT security specialist
Set an IoT controlled environment and simulate cyberattacks
Report results and conclusions

Figure 1 Investigation Methodology

3.2. Comparative Analysis of IDSs

This sub-section presents the comparative analysis of the IDSs, as shown in Table 5 and in the Figure 2. Based on the literature, a hybrid IDS model using the Aegean Wi-Fi dataset (AWID) has been proposed to improve IDS technology, which identifies intruders and zero-day attacks with a low false alarm rate through experimentation. This hybrid structure relies on machine learning clustering procedures. We concluded that it improved the effectiveness of IDS deployment in Wi-Fi, resulting in higher accuracy (94.9%), better proficiency, and limited disadvantages [31].

An IDS has also been created to protect critical infrastructure based on machine learning, composed of federated learning (FL) and active learning (AL) using local datasets. FL was shown to be collaborative and allow data privacy, whereas AL increased reliability by 7.07% in 10 queries [64].

Additionally, an IDS for SDN's control and data planes was examined. In the control plane, a flow-based IDS is installed, which inspects the incoming flow to the controller, and in the data plane, a signature-based IDS is implemented to check traffic from open flow switches. A machine-learning-based classifier is used for the flow IDS, whereas Snort is used for the signature IDS. It was identified that using the essential features and multiple classifiers improved the processing time and accuracy with a low incidence of false alerts [65].

Similarly, a new binary and multiclass convolutional neural network (CNN) classification model was investigated to identify anomalies in the NSLKDD dataset. This model achieved good accuracy, detection rates, and training. An accuracy of 98% was obtained [66]. However, the CNN technique lacks the precision to detect repeated or new attacks.

Another model used was artificial intelligence (AI) for IDSs, with an optimal convolutional neural network and long short-time memory network (LSTM). It distinguishes attacks with unidentified and coded patterns and uses the CSIC-2010 and CICIDS2017 datasets with accuracy values of 91–93%, the precision of 86–98%, and F-note within the range of 80–82%. AI-IDS has the benefits of continuous training and optimization [67].

An IDS for detecting abnormal behavior in systems was proposed for the MQTT protocol. A simulation was performed in an IoT environment using the MQTT protocol, in which the IDS prototype performed analysis to identify abnormal traffic or threats. This model is based on machine learning and deep learning using NSL-KDD and USNW-NB15 datasets in real-time. As a result, the detection metrics were improved with a maximum throughput of 1.5 sec each time the cyber-attack was launched [68].

A data security strategy with machine learning involves knowing the adversary, being proactive, and protecting oneself. Machine learning and reconnaissance techniques are not the ultimate answer to threats and to preventing the risk of unknown attacks; a proactive model can be adopted, which consists of anticipating the attacker by first identifying relevant threats against the system, designing and simulating attacks, designing necessary countermeasures, and finally repeating the process to development. For adversarial threat mitigation, machine learning algorithms must also detect unknown unknowns using robust methods for anomaly and novelty detection and even human intervention [34].

When using machine learning in IDSs, it is essential to maintain control of the trained data, detection model, feature set, Oracle, and in-depth manipulation. This can be achieved with measures to control access to IDS systems and event logs, manage high administration privileges for IDS systems, separate the installation of the detection model and NIDS machines, safeguard the traffic analysis process, install detection mechanisms complementary to the IDS to prevent reverse engineering, separately store the IDS event log, and differentiate between possible attacks [35].

On the other hand, Diro and Chilamkurti design and implement distributed deep learning with the NSL-KDD dataset to detect cyber-attacks on IoT elements in a smart city. Distributed deep learning requires processing and communication to be as close to the data source as possible. The evaluation shows improvements in accuracy, detection rate, false alarm rate, and metrics performance, making the distributed detection mechanism with deep learning more effective than centralized detection mechanisms [54].

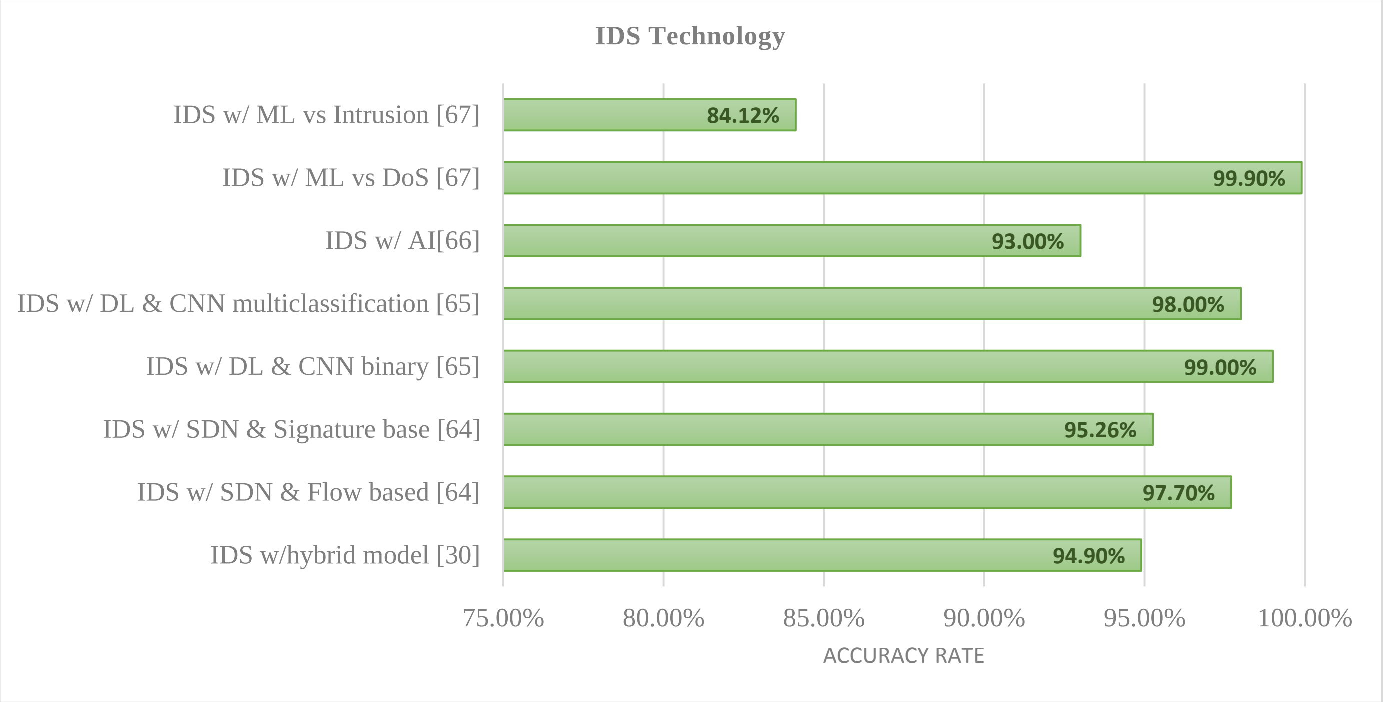


Figure 1 IoT Comparative Analysis of IDS Technology. Accuracy Rate

Alternatively, [69] reviews 20 types of research from 2009 to 2017 for IDS in IoT. They use the taxonomy of location strategy, detection method, and security threat. The literature reviews locate IDSs in IoT as centralized, hybrid, distributed, or undefined. The threats identified are routing attacks, DoS, man-in-the-middle, botnet, 6LoWPAN sensor threats, black holes, worms, and ID cloning. The IDS detection methods are anomaly-based, specification-based, signature-based, or hybrid (with signatures and anomaly detection). Other threat detection methods are related to nodes monitoring infrastructure neighbors or self-monitoring their health status and the packets they transfer. In addition, an artificial immune system mechanism, computational intelligence algorithms, complex event processing, free OS antivirus, or clusters in the network are used to detect threats. These works still do not cover all IoT technologies, nor all the variety of attacks, and no similar point is seen in the features of IDS for IoT, so the use of IDS in IoT still needs development.

3.3. Survey of the IoTCyFra

In this section, we describe the survey of the IoYCyFra shown at Figure 3. A self-administered and anonymous survey was used to validate the IoTCyFra. The budget for its construction and application was low, whereas the depth of the data obtained was high. It was also easy to answer, analyze, and perform comparisons.

The questionnaire was administered to 15 specialists with between 1 and over 16 years of experience in IT and IT security. The specialists worked in an IT and network solutions SME company established more than ten years ago, and in an international IT company established more than 25 years ago in Puebla, Mexico. The specialists in the survey have data security experience with national and international customers and hold the following cyber security certifications: Cyber Security Foundation/CertiProf, CCNP Security/Cisco, ISO 27001:2013 Lead Auditor ISMS, Capability Maturity Model Integration v1.2, and others.

From the SME, three specialists from a group of 5 were interviewed. From the global IT company, 12 out of a group of 25 security specialists were interviewed. The survey was self-administered with four general questions and 17 questions related to the IoT cybersecurity framework using a Likert scale. Five points were defined in the Likert scale to measure the attitude towards the IoT cybersecurity framework using IDS technology. The values used were as follows: Extremely unimportant (1), Very unimportant (2), Neutral (3), Very important (4), and Extremely important (5) (see Table 6).

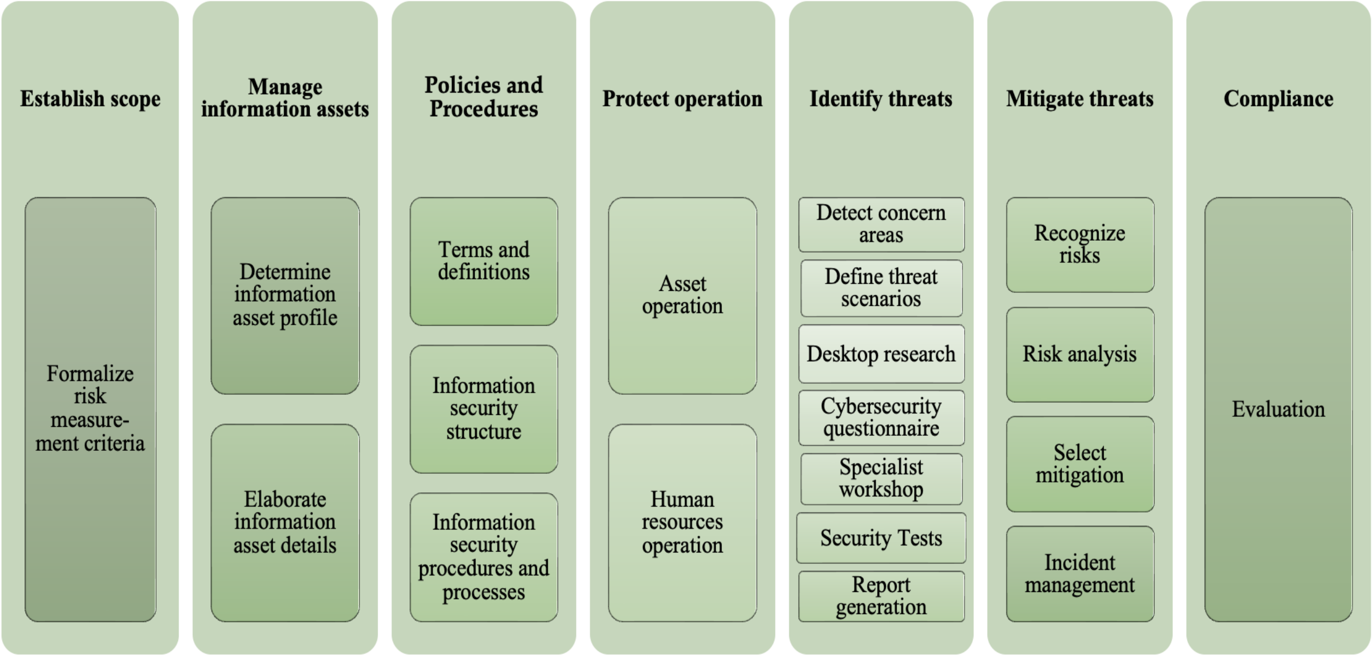


Figure 3 IoT Cybersecurity Framework, IoTCyFra, using IDSs [63]

For an IoT cybersecurity framework, how important is it… (1) Extremely unimportant, (2) Very unimportant, (3) Neutral, (4) Very important, and (5) Extremely important	(1)	(2)	(3)	(4)	(5)
to have a responsible authority?					
to be aligned with the business strategy?					
to have information asset management?					
to have a glossary of information security terms and definitions?					
to establish and formalize data security policies and procedures?					
to communicate information security policies?					
to have an informal guide, apart from the main policy?					
to have an established procedure in emergent cases?					
to implement security controls in the IoT operation, such as authentication, access control, data encryption, among others?					

to have continuous training for IoT specialists?					
to identify threats via a questionnaire to specialists?					
to identify threats via open collaboration with end users?					
to identify information security risks?					
to mitigate or accept the detected information risks?					
to implement an intrusion detection system in the IoT infrastructure?					
to have information security incident management?					
to formalize a communication plan in a security incident?					

3.3.1. Reliability of the Measuring Instrument

Cronbach's alpha was used to measure the reliability of the validation instrument. Minitab was used to calculate this coefficient and the result was 0.9283, showing that it was a reliable instrument. The values of the correlation matrix also remained positive.

3.3.2. Analysis of the IoTCyFra Validation Data

The 15 specialists who answered the questionnaires had the following profiles: 7 IT specialists/architects, 7 IT security specialists/architects, 3 IoT specialists/architects, and one unified communications specialist. There were ten specialists (66.7%) with more than seven years of IT and cybersecurity experience. The most known security framework, by 13 (86.7%) specialists, was ISO 27001:2013, followed by COBIT, which was known by eight specialists (53.3%), and in third place was NIST, which 7 (46.7%) specialists knew. The main problems with an IoT infrastructure framework were the understanding of deliverables (10 specialists, 66.7%) and the complexity of implementation (7 specialists, 46.7%). The main elements of the IoT security framework were considered to be the procedures (9 specialists, 69%), followed by the structure (7 specialists, 53.8%).

The attitudes of IT and cybersecurity specialists towards the elements of the IoT security framework were measured. It was found that 8 (53.3%) considered it "very important" to have a responsible authority, and 12 (80.0%) stated that it was "very important" for it to be aligned with the business strategy. Information asset management was indicated as "very important" by 10 (66.7%) specialists. The glossary of terms and definitions was "very important" for 10 (66.7%) specialists, and 9 (60.0%) specialists indicated that it was "extremely important" to establish and formalize policies and procedures. It was "extremely important" to communicate security policies, according to 7 (46.7%) specialists.

Nine specialists considered an informal guideline, in addition to the central policy, "very important" (60.0%). Eight (53.3%) specialists also said it was "extremely important" to have a procedure in an emergency. Another "extremely important" element for 9 (60.0%) specialists was the implementation of security controls in operation, such as authentication, access control, and data encryption, among others. Identifying threats through desktop research was considered to be "very important" by 8 (53.3%) specialists. Identifying threats through a questionnaire to specialists was considered "neutral" by 7 (50%) specialists. Another way to identify threats is via open collaboration with end users, which was considered "very important" by 10 (66.7%) specialists.

Identifying information security risks was "very important," according to 8 specialists (53.3%). Nine (60.0%) specialists said it was "extremely important" to mitigate or accept the information risks detected. It was also "very important" to select an information risk mitigation method, according to 9 (60.0%) specialists. Eight (53.4%) specialists said that it was "extremely important" to implement an intrusion detection system. The management of information security incidents was considered "very important" by 8 (53.3%) specialists, and 11 (73.3%) of the specialists said that it was "very important" to formalize and communicate a communication plan for security incidents.

3.4. IoTCyFra Operation

This section describes the IoTCyFra mode of operation (see Figure 4). This starts with establishing the scope to formalize security risk criteria. Then, the policies and procedures section is defined, in which the IoT and cybersecurity terms and definitions are listed, the information security structure is created, and the information security procedures and processes are generated. The information security procedures and processes guide the other categories to define objectives, steps, responsibilities, and deliverables. The related categories are asset operation, human resources operation, detecting concern areas, determining threat scenarios, desktop research, IoT cybersecurity questionnaire, workshop with specialists, security testing, recognizing risks, mitigation selection, risk analysis, and incident management.

Once the procedures have been defined, the next step is to determine the information asset profile, in which the information asset profile is created, and information asset details are identified. This is followed by the protect operation category, consisting of asset and human resources operations.

After asset operation, the next category is identifying threats, consisting of detecting concern areas, defining threat scenarios, desktop research, IoT cybersecurity questionnaire, workshop with specialists, and security tests, which will generate a report to be delivered to and evaluated by the cybersecurity manager.

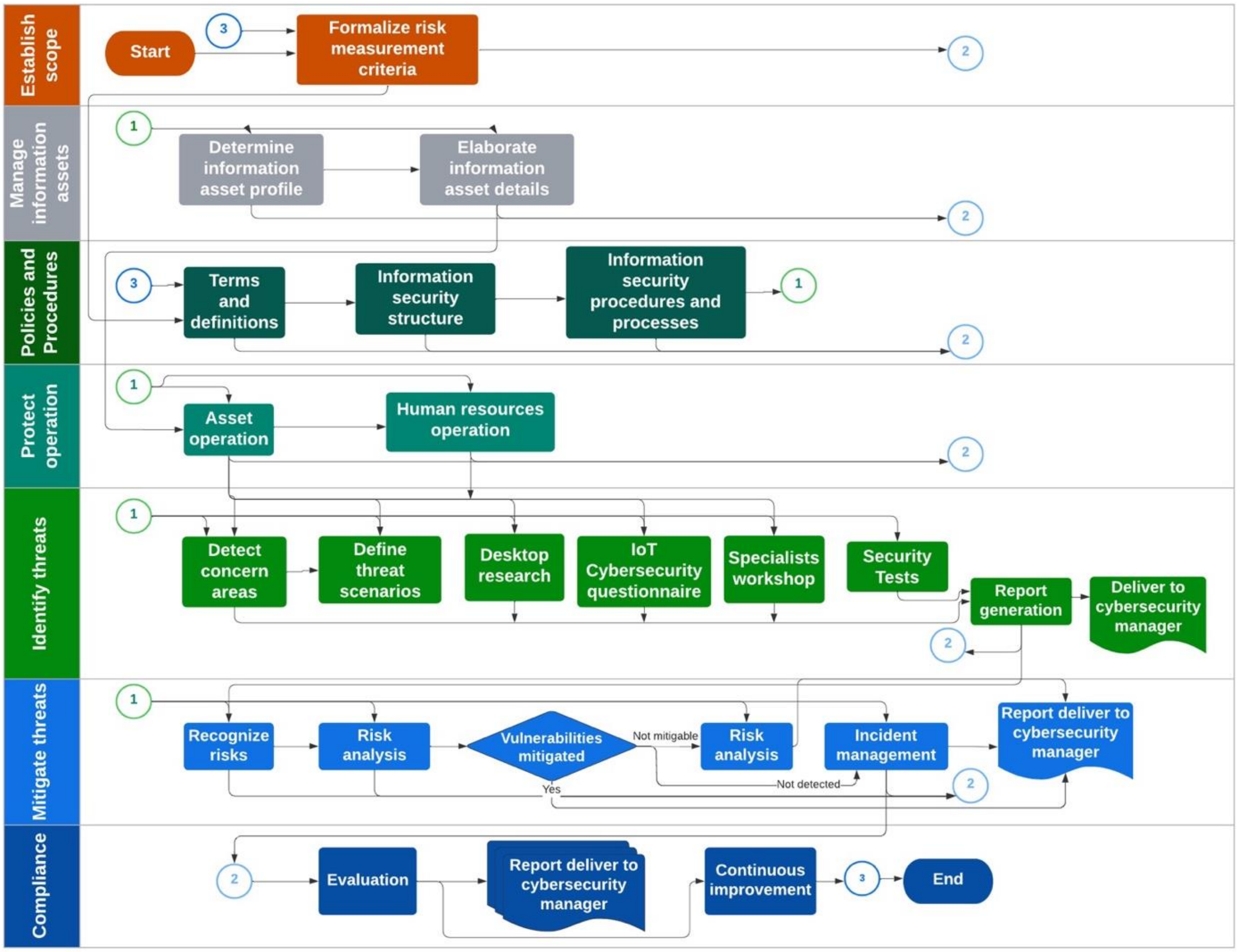

Establish scope
Start
3
Formalize risk measurement criteria
2
Manage information assets
1
Determine information asset profile
Elaborate information asset details
2
Policies and Procedures
3
Terms and definitions
Information security structure
Information security procedures and processes
1
2
Protect operation
1
Asset operation
Human resources operation
2
Identify threats
1
Detect concern areas
Define threat scenarios
Desktop research
IoT Cybersecurity questionnaire
Specialists workshop
Security Tests
Report generation
Deliver to cybersecurity manager
2
Mitigate threats
1
Recognize risks
Risk analysis
Vulnerabilities mitigated
Not mitigable
Risk analysis
Incident management
Report deliver to cybersecurity manager
Not detected
Yes
2
Compliance
2
Evaluation
Report deliver to cybersecurity manager
Continuous improvement
3
End

Figure 4 IoTCyFra Mode of Operation

Once the threats have been identified, the next step is to mitigate threats by identifying risks and selecting mitigation measures. If the vulnerabilities can be mitigated, then the evaluation proceeds, but a risk analysis is performed if the threats cannot be mitigated. This will be addressed under the incident management category if any vulnerability is exploited. The results are documented in the identify threats subcategories, and a report is submitted to the cybersecurity manager. Each subcategory is evaluated, and the result is a report delivered to the IoT cybersecurity manager. Based on these results, improvements can be made in the categories of formalizing security risk measurement criteria, terms and definitions, information security structure, and information security procedures and processes.

3.5. IoTCyFra Security Model Tests

This section presents the testing of the IoTCyFra. The categories used were policies and procedures, protect operations, and identifying threats.

3.5.1. Policies and Procedures

In the policies and procedures category, an IoT architecture was defined within the subcategory of information security procedures and processes, with the perception, network, and application layers (see Figure 5).

In the perception layer, IoT sensors are implemented, which send data to the IoT public cloud. In the network layer, the data are forwarded to the Internet via a router and a Wi-Fi access point (AP), and the data are inspected through a firewall and a virtual IDS. Finally, in the application layer, the data and the monitoring status are displayed in the IoT portal.

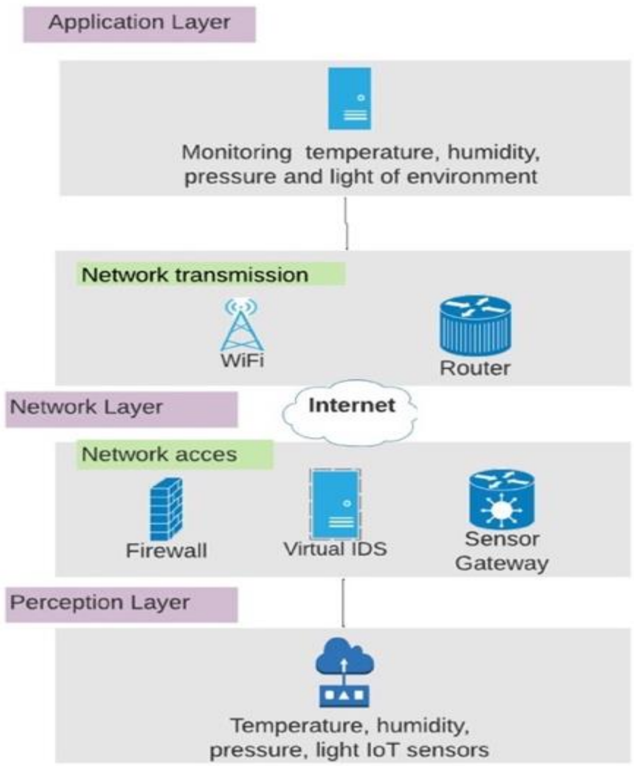


Figure 5 IoT Cybersecurity Architecture for Testing

3.5.2. Protect Operation

The protect operation category was considered with the subcategory of asset operation. A simulated IoT architecture was implemented with an application, network, and perception layer (see Figure 6). The Arduino Oplà device was installed in the perception layer, with dynamic sensors for temperature, atmospheric pressure, humidity, and light. A TP-Link R605 virtual firewall/switch/router, a virtual Suricata 6.0.5 IDS, and a gateway M4 WiLink 3 were installed at the network layer. A residential Internet connection with a bandwidth of 100 Mbps was used. The application layer contains the IoT public cloud that receives and displays the data from the Arduino temperature, humidity, pressure, and light sensors. The IoT architecture flowchart is shown below. Initially the user switches on the temperature, humidity, pressure, and light sensors, and the notification process. Then, the sensors send the data to the Arduino IoT Cloud via the Internet. The data transmitted are inspected using Suricata IDS. If any abnormal traffic is detected, an alarm will be sent; if not, the traffic will be forwarded to the Internet. Additionally, the communicated data are captured via a mirror port at the switch, and this traffic is analyzed firstly with the Wireshark tool, then via the CVE ® database and the MITRE ATT&CK ICS matrix. Finally, the information is displayed on a portal in the Arduino IoT cloud (see Figure 7).

3.5.3. Identify Threats

In the identify threats category, subcategory security testing, an IoT-controlled environment was installed and cybersecurity attacks on the Arduino sensors were simulated. The cybersecurity attacks were performed from a laptop with the Kali Linux platform within the internal network. The first simulated attack was a password search of the Arduino sensors, and the technique used was brute force using the Hydra tool. This attempted to attack the SSH network port. The result was that the Arduino device rejected the connection, and the password could not be obtained. The next cybersecurity attack was scanning the network ports on the Arduino sensors, using the nmap and SSL scan tools. With Nmap, the following TCP opened ports were detected: 801, 1117, 1248, 1334, 2119, 4224, 9000, 10024, 10626, 18040, 30951, 34573, and 49152. In the second scan, the status of all the ports was "ignored". With SSL scan, the SSH network port was shown as closed. Then, a DoS attack was executed on the Arduino sensors through ports 80 and 8443, using the Metasploit tool. When the DoS attack was performed through port 80, the Arduino sensor continued to send information to the IoT public cloud; however, when it was directed through port 8443, the sensors could no longer communicate with the IoT public cloud, as this port was used for data transmission.

3.5.3.1. Traffic Analysis Using Wireshark

A mirror mode port was set up on the switch to detect the traffic transferred from the Arduino sensors to the IoT public cloud. The traffic was analyzed using the Wireshark tool. The IP addresses of the wireless AP, Arduino sensors, switch, router, firewall, IDS, simulated attacker laptop, and the IoT public cloud were detected. When analyzing the normal traffic capture from the Arduino sensors, it was observed that the protocols used were TLS v.2 in the transport layer and MQTT as the data application protocol. The TLS protocol traffic represented 33.6% of all the traffic. The traffic capture was also analyzed using the Suricata 6.0.3 tool, through which the pcap file was processed with the default rules. The configuration consisted of 27,463 inspection signatures, 1236 IP rules, 4199 payload inspection rules, 21,786 application layer inspection rules, and 107 decoding events. It was found that there were no packets with invalid checksums, and 42 alerts were detected. The alerts referred to packets with invalid time tags forwarded between the router and an Internet site with the IP 142.250.81.10. The default rules for the MQTT protocol in Suricata will alert when MQTT protocol packets do not have a connected, published, subscribed, unsubscribed, double connection, message, invalid QoS level, id message, or unassigned type message event.

Next, the traffic generated during the attack simulation was analyzed using the Wireshark tool. An increase in packets transmitted at 2000 packets/second (see Figure 8) was detected during scanning the network ports, i.e., transmission of 7.56 Mbs in 6.51 minutes.

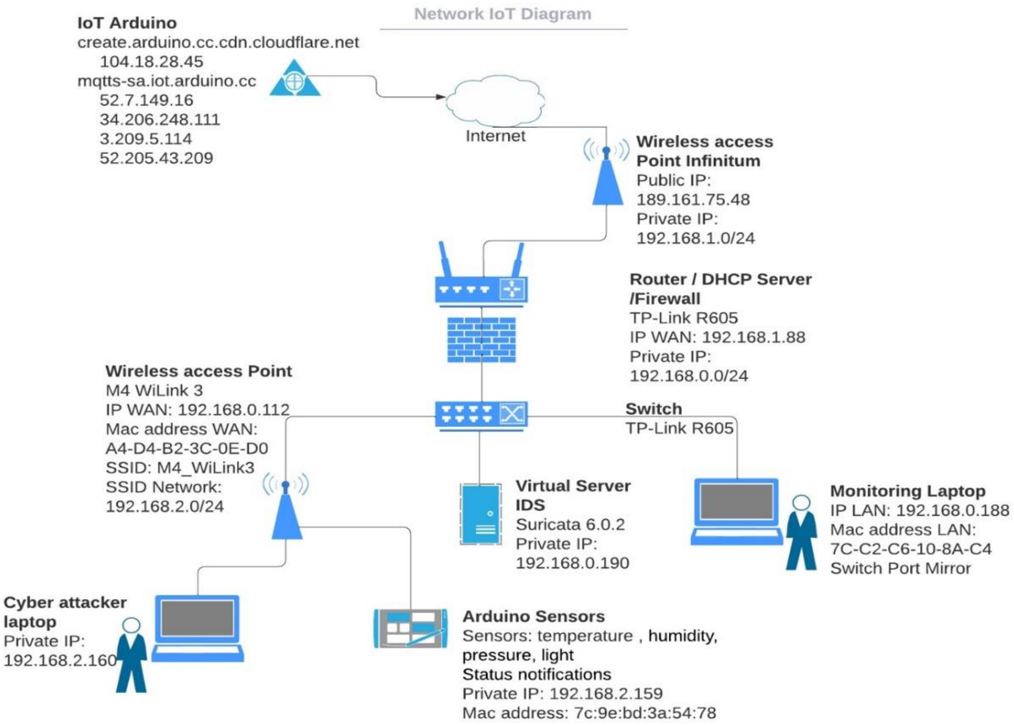


Figure 6 Network Diagram of the IoT Cybersecurity Model

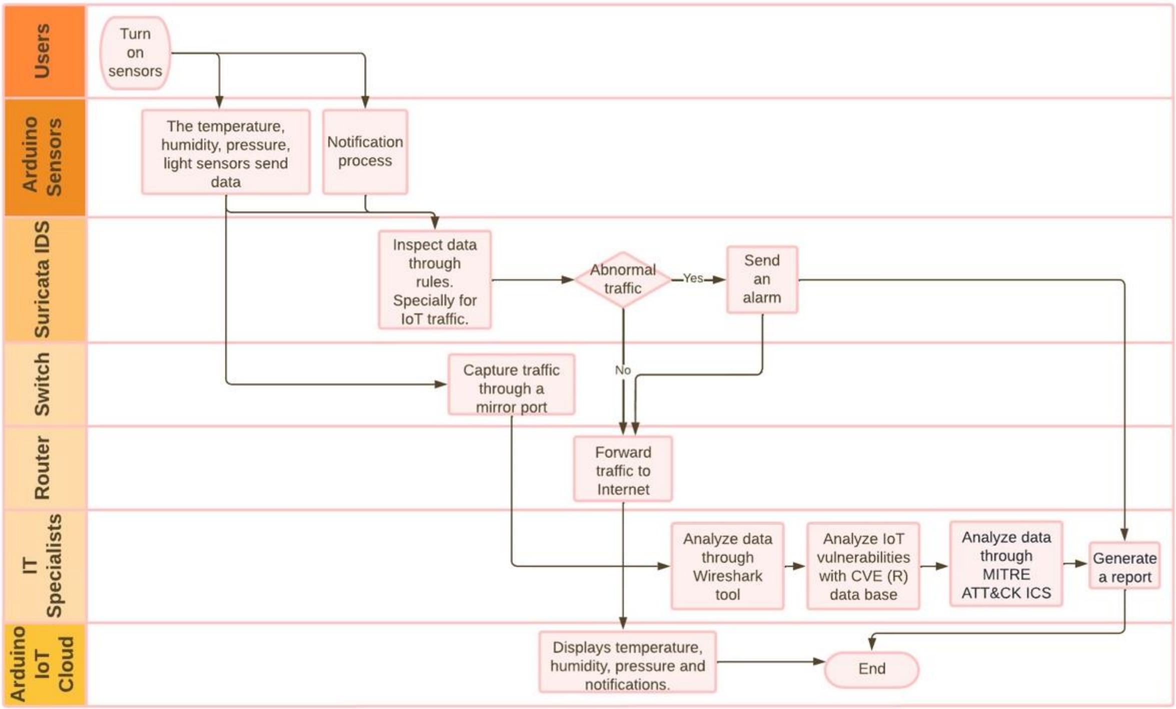

Users
Arduino Sensors
Suricata IDS
Switch
Router
IT Specialists
Arduino IoT Cloud
Turn on sensors
The temperature, humidity, pressure, light sensors send data
Notification process
Inspect data through rules. Specially for IoT traffic.
Abnormal traffic
Yes
No
Send an alarm
Capture traffic through a mirror port
Forward traffic to Internet
Analyze data through Wireshark tool
Analyze IoT vulnerabilities with CVE (R) data base
Analyze data through MITRE ATT&CK ICS
Generate a report
Displays temperature, humidity, pressure and notifications.
End

Figure 7 IoT Architecture Flowchart

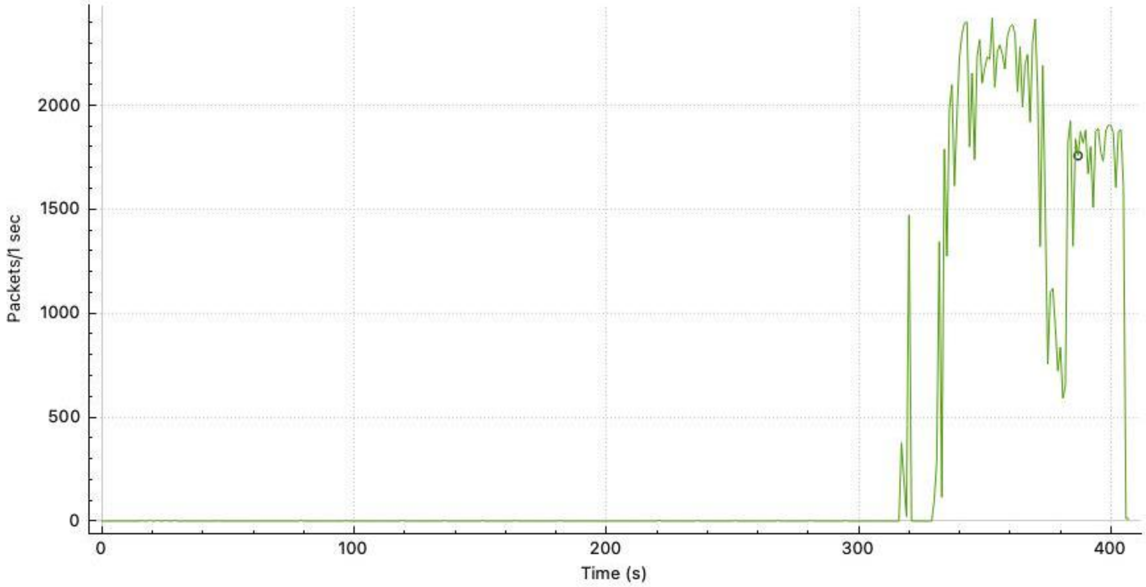


Figure 8 Scanning of Network Ports to Arduino Sensors. Packets/Second. Filtered Packets from IoT Networks

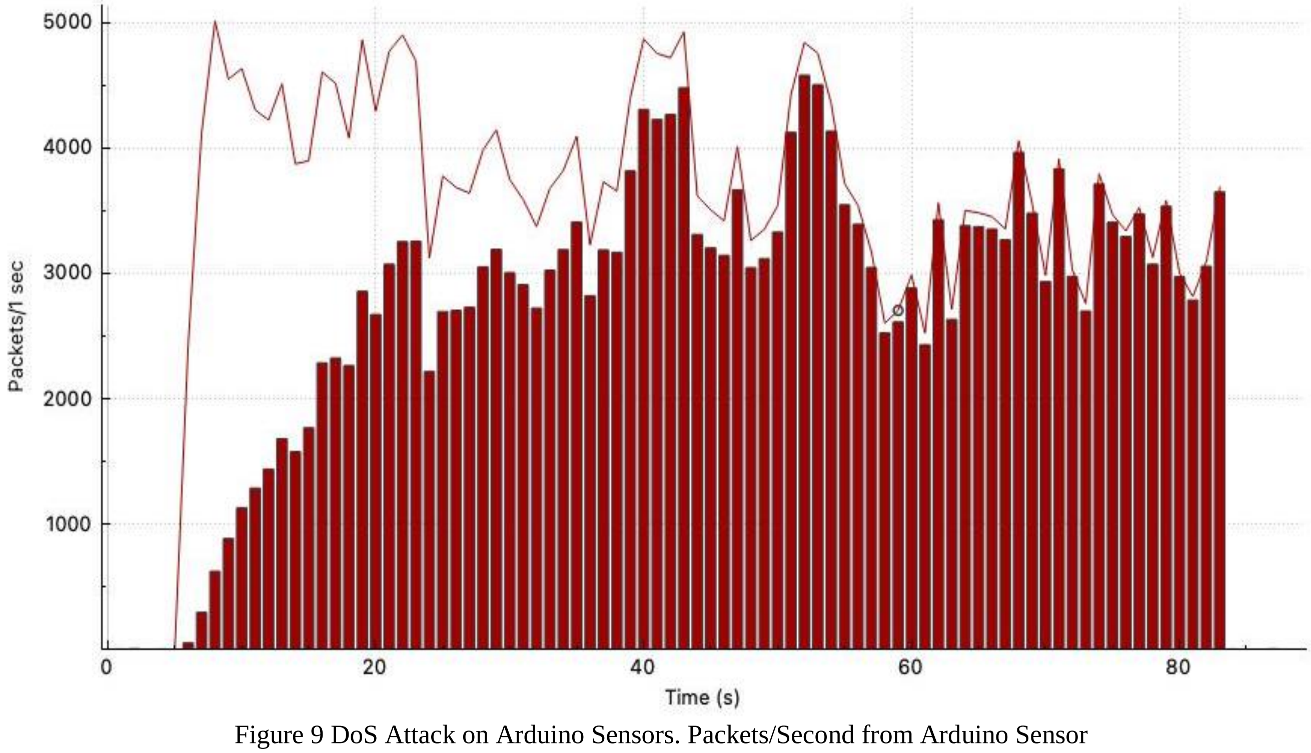


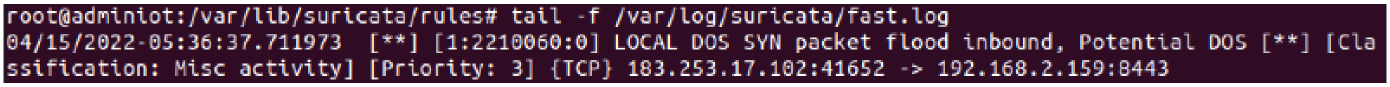
Figure 9 DoS Attack on Arduino Sensors. Packets/Second from Arduino Sensor

The DoS attack was performed from a public IP to the Arduino sensors over port 8443. During the DoS attack simulation, the packet transmission increased, and 80-second peaks of 5000 packets/second were detected (see Figure 9); the detail of the packet indicates the time, source and destination IP, and protocol. Transmission of 15 Mbs in 77.48 seconds was observed. The bulk packets transmitted had SYN status, with the note that a new TCP session started with the same ports as an earlier session, through port TCP 8443.

3.5.3.2. Analysis of Traffic Using IDS Suricata

During the Suricata IDS inspection, it was observed that the default rules did not detect DoS attacks. Therefore, the rules were configured to send alerts regarding DoS events [70]. The

DoS events were then sent again, and the alerts “potential DoS” were received by Suricata (see Figure 10).



```
root@adminiot:/var/lib/suricata/rules# tail -f /var/log/suricata/fast.log
04/15/2022-05:36:37.711973  [**] [1:2210060:0] LOCAL DOS SYN packet flood inbound, Potential DOS [**] [Cla
ssification: Misc activity] [Priority: 3] {TCP} 183.253.17.102:41652 -> 192.168.2.159:8443
```

Figure 10 Alert of Potential DoS Attack in IDS Suricata

3.5.3.3. Review of CVE Vulnerabilities

The MQTT protocol was detected in the normal traffic capture; therefore, the related vulnerabilities in the CVE® database published on 6 May 2022 [71] were reviewed. In total, there were 76 CVE ® vulnerabilities associated with IoT tools; the most frequently stated were Cesanta Mongoose, Totolink, Eclipse Mosquitto, Sealevel Systems, Zephyr MQTT, Contiki, AWS, RIOT, Qualcomm Technologies, BigIP, Apache ActiveMQ, and IBM MessageSlight, among others (see Table 7).

Table 7 Number of CVE® MQTT Vulnerabilities in IoT Tools

IoT Tools	# Vulnerabilities
Cesanta Mongoose	9
Totolink	8
Eclipse Mosquitto	8
Sealevel Systems	6
MQTT	5

A review of vulnerabilities was performed taking into consideration the principles of the security triad: integrity, confidentiality, and data availability. Twenty-five threats were detected, relating to data integrity through unauthorized remote code execution, unauthorized data transfer and request, impersonation of MQTT servers, and arbitrary file overwriting (see Table 8).

Table 8 CVE® MQTT Vulnerabilities Affecting IoT Data Integrity

Security findings	# Vulnerabilities
Unauthorized remote code execution	20
Unauthorized data transfer and requests	1
Impersonate an MQTT server	3
Arbitrary file overwriting	1

There were 16 vulnerabilities associated with data confidentiality through unauthorized disclosure of information, no reference to initial pointers, and unauthorized access (see Table 9).

Table 9 Number of CVE® MQTT Vulnerabilities Affecting IoT Data Confidentiality

Security findings	# Vulnerabilities
Unauthorized disclosure of information	6
No reference to the initial pointer	1
Unauthorized access	9

There were 40 vulnerabilities that impacted data availability through DDoS attacks, scripture out of boundaries, MQTT system failures, memory failures, buffer overflows, and unauthorized traffic blocking (see Table 10).

Table 10 Number of CVE® MQTT Vulnerabilities Affecting Data Availability in the IoT

Security findings	# Vulnerabilities
DDoS	15
Scripture out of boundaries	2
MQTT system failure	9
Memory failure	7
Buffer overflow	5

3.5.3.4. MITRE ATT&CK ICS Matrix Vulnerability Review

The MITRE ATT&CK framework of Tactics, Techniques, and Common Adversary Knowledge was also used for the vulnerability review. It addresses the why, how, and who of cyberattacks on a digital infrastructure [60]. The ATT&CK ICS matrix for the Industrial Control System (ICS) describes the behavior of adversaries in an industrial network, consisting of 11 tactics, 81 techniques, and 50 mitigations [60]. The MQTT protocol vulnerabilities detected in CVE ® are identified in the MITRE ATT&CK ICS matrix [56] (see Table 11). Selected techniques related to MQTT and documented in CVE ® are indicated in gray below.

Table 5 Comparative Analysis of IDS Technology. Own Elaboration

IDS	Description	Methodology	Detection technique	Dataset	Outstanding rate	Advantages	Disadvantages
IDS with hybrid model [31]	It identifies intruders and zero-day attacks with a low false alarm rate.	Experimentation	1. Classification by machine learning. 2. Clustering process.	1. KDDCUP99 and UNSW-NB15 2. Wi-Fi Aegean (AWID).	True positive rate, 94.40 %. False positive rate, 5.10 %. Accuracy rate: 94.9%.	• Effective in Wi-Fi. • Decreases false positive rate and false negative rate. • Increases discovery rate. • Zero-day attack identification.	• Possible vulnerability to adversarial attacks.
IDS for industrial applications [64]	It protects critical infrastructure.	Literature review.	1. Federated learning. 2. Active learning. 3. Deep neural network.	Local dataset.	Accuracy rate: + 1.51 - 6.06%. Active learning increases accuracy by 7.07% in 10 queries.	• Collaborative and personalized training. • Correctly classifies data testing.	• Possible vulnerability to adversarial attacks.
IDS for SDN [65]	Located in the control and in the data plane.	Training of a multilayer classifier.	1. Flow-based using machine learning in control plane. 2. Signature-based ID, localized in data plane. Using Snort.	NSL-KDD	Accuracy rate: Flow based, 97.7%. Signature based, 95.26%.	• Reduced processing time. • Better classification accuracy. • Lower false alarm rate. • High level of security in the SND.	• Early detection of insider attackers is still lacking. • Possible vulnerability to adversarial attacks.
IDS based on deep learning [66]	It uses convolutional neural network architecture with multiclass and binary classification.	Evaluation of IDS investigations.	1.New binary classification model. 2. Convolutional neural network (CNN) multiclass.	NSLKDD	Accuracy rate: CNN binary classification, 99%. CNN multiclassification, 98%.	• CNN reduces the shortage of IDS classification function cost, high precision, and high detection rate.	• No precision because of detection of repeated or new attacks.
IDS with artificial intelligence [67]	Real-time unencrypted traffic inspection.	HTTP real-time data selection experiment.	1. CNN-LSTM model. 2. LSTM-CNN model.	CSIC-2010 CICIDS2017	Accuracy rate: 91–93%. Precision: 86–98%. F-note range: 80–82%.	• Improves analysis of large numbers of unidentified events.	• Revalidation for suspicious events because of false positive alarms.
IDS for IoT [68]	Detect abnormal behavior for the MQTT protocol.	Literature review.	Machine learning with decision trees.	NSL-KDD USNW-NB15	Accuracy rate: DoS, 99.9%, Intrusion, 84.12%	• Improves detection metrics to 1.5 sec once the cyberattack is launched.	• Possible vulnerability to adversarial attacks.

Table 11 MITRE ATT&CK® Matrix for ICS [56]

Initial Access	Execution	Persistence	Privilege Escalation	Evasion	Discovery	Lateral Movement	Collection	Command and Control	Inhibit Response Function	Impair Process Control	Impact
Drive-by Compromise	Change Operating Mode	Modify Program	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Automated Collection	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Command-Line Interface	Module Firmware	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Data from Information Repositories	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Execution through API	Project File Infection		Indicator Removal on Host	Remote System Discovery	Lateral Tool Transfer	Detect Operating Mode	Standard APP Layer Protocol	Block Command Message	Module Firmware	Denial of View
External Remote Services	Graphical User Interface	System Firmware		Masquerading	Remote System Information Discovery	Program Download	I/O Image		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet Accessible Device	Hooking	Valid Accounts		Rootkit	Wireless Sniffing	Remote Services	Man in the Middle		Block Serial COM	Unauthorized Command Message	Loss of Control
Remote Services	Modify Controller Tasking			Spoof Reporting Message		Valid Accounts	Monitor Process State		Data Destruction		Loss of Productivity and Revenue
Replication Through Removable Media	Native API						Point & Tag Identification		Denial of Service		Loss of Protection
Rogue Master	Scripting						Program Upload		Device Restart/Shutdown		Loss of Safety
Spearphishing Attachment	User Execution						Screen Capture		Manipulate I/O Image		Loss of View
Supply Chain Compromise							Wireless Sniffing		Modify Alarm Settings		Manipulation of Control
Transient Cyber Asset									Rootkit		Manipulation of View

4. CONCLUSION

IoT technology is emerging and growing significantly because it facilitates decision-making, automation, and mobility, and improves the quality of life by saving money and time through automatized processes, among other things. However, data security deficiencies remain because the IoT nodes or sensors are heterogeneous and have limited computational and energy resources. Cybersecurity standards are complex and not exclusively focused on the IoT. In this investigation, the literature was reviewed, IoT cybersecurity problems and cyberattacks were defined, and a comparative analysis of IDSs was performed. Then the IoTCyFra framework was surveyed by IT security specialists, and a cyberattack simulation was done in a controlled IoT environment.

Furthermore, the cyberattack simulation was done using the IoTCyFra framework; in the category "Policies and procedures" and the subcategory "Information security procedures and processes", the IoT architecture was defined. In the category "Protect operation" within the subcategory "Asset operation", a controlled environment was installed. The network traffic was inspected using Suricata IDS and captured using a mirror port at the switch. In the category "Identify threats" and the subcategory "Security testing", cybersecurity attacks were simulated. Consequently, the Suricata IDS sent alarms when it detected DoS events. Then, the captured traffic was analyzed using the Wireshark network tool, and the IoT vulnerabilities were analyzed using the CVE database and the MITRE ATT&CK ICS matrix.

Therefore, it is concluded that the IoTCyFra framework is a validated cybersecurity framework for the IoT that takes into consideration organizational scope, asset management, policies and procedures, operation protection, threat identification and mitigation, risk management, and process compliance to protect data and identify cyber threats within an IoT infrastructure. The IoTCyFra considers business strategy, human resources, and continuous improvement. It also simplifies implementation by not requiring the input of specialist expertise.

This survey focuses on the recent IoT research trends investigating cybersecurity and cyberattacks. The literature exposes that surveys are presented for IoT security solutions as standards, taxonomies, frameworks, and technical models intended to protect IoT data. The contribution of this article is that it compares the IDS solutions for IoT and surveys and tests the IoTCyFra. This survey's emphasis is to describe the current issues of IoT cybersecurity and recognises a cybersecurity framework that facilitates the application of security controls for IoT data protection. This survey could assist the security specialist in the implementation of the proper security requirements and avoid cybersecurity threats in an IoT infrastructure.

In future research, the validation process will be carried out across most of the states in the central region of Mexico. Then, a use case will be developed using the IoTCyFra framework in a productive IoT services company, involving a variety of sensors and simulating other cyberattacks.

REFERENCES

[1] A. Khan, S. Siddiqui, M. Irshad, S. Ali, M. Saleem, and S. Iqbal, “Analytical Method to Improve the Security of Internet of Things with Limited Resources,” EAI Endorsed Transactions on Internet of Things, vol. 5, no. 18, p. 163502, 2019, doi: 10.4108/eai.13-7-2018.163502.

[2] E. A. Shammar and A. T. Zahary, “The Internet of Things (IoT): a survey of techniques, operating systems, and trends,” Library Hi Tech, vol. 38, no. 1. Emerald Group Holdings Ltd., pp. 5–66, Apr. 06, 2020. doi: 10.1108/LHT-12-2018-0200.

[3] R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, “Internet of Things (IoT) Security : Current Status , Challenges and Prospective Measures,” The 10th International Conference for Internet Technology and Secured Transactions (ICITST-2015) Internet, pp. 336–341, 2015.

[4] M. A. Obaidat, S. Obeidat, J. Holst, A. Al Hayajneh, and J. Brown, “A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures,” Computers, vol. 9, no. 2, pp. 2–43, 2020, doi: 10.3390/computers9020044.

[5] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, “Survey of intrusion detection systems: techniques, datasets and challenges,” Cybersecurity, vol. 2, no. 20, 2019.

[6] I. Alqassem and D. Svetinovic, “A taxonomy of security and privacy requirements for the Internet of Things (IoT),” in IEEE International Conference on Industrial Engineering and Engineering Management, 2014, vol. 2015-Janua, pp. 1244–1248. doi: 10.1109/IEEM.2014.7058837.

[7] S. Babar, P. Mahalle, A. Stango, N. Prasad, and R. Prasad, “Proposed security model and threat taxonomy for the Internet of Things (IoT),” Communications in Computer and Information Science, vol. 89 CCIS, pp. 420–429, 2010, doi: 10.1007/978-3-642-14478-3_42.

[8] M. Ammar, G. Russello, and B. Crispo, “Internet of Things: A survey on the security of IoT frameworks,” Journal of Information Security and Applications, vol. 38, pp. 8–27, 2018, doi: 10.1016/j.jisa.2017.11.002.

[9] M. Nawir, A. Amir, N. Yaakob, O. B. Lynn, and C. Engineering, “Internet of Things (IoT): Taxonomy of Security Attacks,” 2016 3rd International Conference on Electronic Design (ICED), August 11-12, 2016, Phuket, Thailand, pp. 321–326, 2016.

[10] M. D. Alshehri and F. K. Hussain, “A fuzzy security protocol for trust management in the internet of things (Fuzzy-IoT),” Computing, 2018, doi: 10.1007/s00607-018-0685-7.

[11] S. Singh and N. Singh, “Internet of Things (IoT): Security challenges, business opportunities & reference architecture for E-commerce,” in Proceedings of the 2015 International Conference on Green Computing and Internet of Things, ICGCIoT 2015, 2016, pp. 1577–1581. doi: 10.1109/ICGCIoT.2015.7380718.

[12] A. A. Hayajneh, M. Z. A. Bhuiyan, and I. McAndrew, “Improving internet of things (IoT) security with software-defined networking (SDN),” Computers, vol. 9, no. 1, 2020, doi: 10.3390/computers9010008.

[13] A. Thakkar and R. Lohiya, “A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT: Recent Updates, Security Issues, and Challenges,” Archives of Computational Methods in Engineering, vol. 28, no. 4, pp. 3211–3243, Jun. 2021, doi: 10.1007/s11831-020-09496-0.

[14] N. Sklavos and I. D. Zaharakis, "Cryptography and security in internet of things (IoTs): Models, schemes, and implementations," in 2016 8th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2016, 2016. doi: 10.1109/NTMS.2016.7792443.

[15] M. Mohsin, Z. Anwar, G. Husari, E. Al-shaer, and M. A. Rahman, "IoTSAT : A Formal Framework for Security Analysis of the Internet of Things (IoT)," 2016 IEEE Conference on Communications and Network Security (CNS) IoTSAT:, 2016.

[16] K. Mabodi, M. Yusefi, S. Zandiyan, L. Irankhah, and R. Fotohi, "Multi-level trust-based intelligence schema for securing of internet of things (IoT) against security threats using cryptographic authentication," Journal of Supercomputing, 2020, doi: 10.1007/s11227-019-03137-5.

[17] A. Tewari and B. B. Gupta, "Security , Privacy and Trust of different Layers in Internet-of-things (IoTs) Framework," Future Generation Computer Systems, 2018, doi: 10.1016/j.future.2018.04.027.

[18] M. Grabovica, D. Pezer, S. Popić, and V. Knežević, "Provided security measures of enabling technologies in Internet of Things (IoT): A survey," in 2016 Zooming Innovation in Consumer Electronics International Conference, ZINC 2016, 2016, pp. 28–31. doi: 10.1109/ZINC.2016.7513647.

[19] C. M. de Morais, D. Sadok, and J. Kelner, "An IoT sensor and scenario survey for data researchers," Journal of the Brazilian Computer Society, vol. 25, no. 1, Dec. 2019, doi: 10.1186/s13173-019-0085-7.

[20] J. de Huang and H. C. Hsieh, "Design of gateway for monitoring system in IoT networks," in Proceedings - 2013 IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing, GreenCom-iThings-CPSCom 2013, 2013, pp. 1876–1880. doi: 10.1109/GreenCom-iThings-CPSCom.2013.348.

[21] M. R. Ghori, T. C. Wan, and G. C. Sodhy, "Bluetooth low energy mesh networks: Survey of communication and security protocols," Sensors (Switzerland), vol. 20, no. 12. MDPI AG, pp. 1–35, Jun. 01, 2020. doi: 10.3390/s20123590.

[22] F. Moreno-Cruz, V. Toral-López, A. Escobar-Molero, V. U. Ruíz, A. Rivadeneyra, and D. P. Morales, "Trench: Ultra-low power wireless communication protocol for iot and energy harvesting," Sensors (Switzerland), vol. 20, no. 21, pp. 1–21, Nov. 2020, doi: 10.3390/s20216156.

[23] G. Ferrari, P. Medagliani, S. di Piazza, and M. Martalò, "Wireless sensor networks: Performance analysis in indoor scenarios," EURASIP J Wirel Commun Netw, vol. 2007, 2007, doi: 10.1155/2007/81864.

[24] X. Wang, C. Gu, F. Wei, and S. Lu, "Security and Privacy for Edge-Assisted Internet of Things Security Proof for the SKKE Protocol," Security and Communication Networks, vol. 2021, 2021, doi: 10.1155/2021/9029664.

[25] S. Ding, J. Liu, and M. Yue, "The Use of ZigBee Wireless Communication Technology in Industrial Automation Control," Wirel Commun Mob Comput, vol. 2021, 2021, doi: 10.1155/2021/8317862.

[26] M. Magdin, M. Valovič, Š. Koprda, and Z. Balogh, "Design and realization of interconnection of multifunctional weighing device with sigfox data network," Agris On-line Papers in Economics and Informatics, vol. 12, no. 2, pp. 99–110, Jun. 2020, doi: 10.7160/aol.2020.120209.

[27] R. Berto, P. Napoletano, and M. Savi, "A lora-based mesh network for peer-to-peer long-range communication," Sensors, vol. 21, no. 13, Jul. 2021, doi: 10.3390/s21134314.

[28] A. Ferriyan, A. H. Thamrin, K. Takeda, and J. Murai, "Generating network intrusion detection dataset based on real and encrypted synthetic attack traffic," Applied Sciences (Switzerland), vol. 11, no. 17, Sep. 2021, doi: 10.3390/app11177868.

[29] A. Thakkar and R. Lohiya, "A Review of the Advancement in Intrusion Detection Datasets," in Procedia Computer Science, 2020, vol. 167, pp. 636–645. doi: 10.1016/j.procs.2020.03.330.

[30] Nivaashini M., Thangaraj P., Sountharrajan S., Suganya E., and Soundariya R.S, "Effective Feature Selection for Hybrid Wireless IoT Network Intrusion Detection Systems Using Machine Learning Techniques," Ad Hoc & Sensor Wireless Networks, vol. 49, pp. 175–206, 2021.

[31] A. Amin Aburomman and M. bin Ibne Reaz, "Review of IDS Develepment Methods in Machine Learning," International Journal of Electrical and Computer Engineering (IJECE), vol. 6, no. 5, pp. 2432–2436, 2016, [Online]. Available: http://iaesjournal.com/online/index.php/IJECE

[32] O. Ibitoye, O. Shafiq, and A. Matrawy, "Analyzing Adversarial Attacks Against Deep Learning for Intrusion Detection in IoT Networks," Dec. 2019.

[33] B. Biggio and F. Roli, "Wild patterns: Ten years after the rise of adversarial machine learning," Pattern Recognit, vol. 84, pp. 317–331, Dec. 2018, doi: 10.1016/j.patcog.2018.07.023.

[34] G. Apruzzese, M. Andreolini, L. Ferretti, M. Marchetti, and M. Colajanni, "Modeling Realistic Adversarial Attacks against Network Intrusion Detection Systems," Digital Threats: Research and Practice, Jun. 2021, doi: 10.1145/3469659.

[35] M. Usama, M. Asim, S. Latif, H. Qadir, and Ala-Al-Fuqaha, "Generative Adversarial Networks for launching and thwarting Adversial Attacks on Network Intrusion Detection Systems," 2019.

[36] S. Zhao, J. Li, J. Wang, Z. Zhang, L. Zhu, and Y. Zhang, "AttackGAN: Adversarial Attack against Black-box IDS using Generative Adversarial Networks," in Procedia Computer Science, 2021, vol. 187, pp. 128–133. doi: 10.1016/j.procs.2021.04.118.

[37] Y. Sagduyu, Y. Shi, and T. Erpek, "IoT Network Security from the Perspective of Adversarial Deep Learning," Cornell University, May 2019, Accessed: Jun. 12, 2022. [Online]. Available: https://arxiv.org/abs/1906.00076

[38] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," Computer (Long Beach Calif), 2017.

[39] C. Vijayakumaran, B. Muthusenthil, and B. Manickavasagam, "A reliable next generation cyber security architecture for industrial internet of things environment," International Journal of Electrical and Computer Engineering, vol. 10, no. 1, pp. 387–395, 2020, doi: 10.11591/ijece.v10i1.pp387-395.

[40] A. Mehmood, M. Mukherjee, S. H. Ahmed, H. Song, and K. M. Malik, "NBC-MAIDS: Naïve Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks," Journal of Supercomputing, vol. 74, no. 10, pp. 5156–5170, Oct. 2018, doi: 10.1007/s11227-018-2413-7.

[41] M. T. Jufri, M. Hendayun, and T. Suharto, "Risk-Assessment Based Academic Information System Security Policy Using OCTAVE Allegro and ISO 27002," Nov. 2017.

[42] L. Sulay et al., "Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana Application of ISO 27001 and its influence on the information security of a Peruvian private company," Propósitos y Representaciones, vol. 8, no. 3, pp. 786–296, Sep. 2020, doi: 10.20511/pyr2020.v8n3.786.

[43] A. Ibrahim, C. Valli, I. McAteer, and J. Chaudhry, "A security review of local government using NIST CSF: a case study," Journal of Supercomputing, vol. 74, no. 10, pp. 5171–5186, Oct. 2018, doi: 10.1007/s11227-018-2479-2.

[44] V. P. Kafle, Y. Fukushima, and H. Harai, "Internet of Things standarization in ITU and prospective networking technologies," IEEE Communications Magazine, pp. 43–49, 2016.

[45] W. Park and S. Ahn, "Performance Comparison and Detection Analysis in Snort and Suricata Environment," Wireless Pers Commun, vol. 94, pp. 241–252, 2017, doi: 10.1007/s11277-016-3209-9.

[46] A. Rahman, M. Daud, and M. Mohamad, "Securing Sensor to Cloud Ecosystem using Internet of Things (IoT) Security Framework," ICC '16: Proceedings of the International Conference on Internet of things and Cloud Computing, vol. 2016, no. 79, pp. 1–5, 2016.

[47] S. Babar, A. Stango, P. Neeli, J. Sed, and R. Prasad, "Proposed Embedded Security Framework for Internet of Things (IoT)," IEEE, pp. 1–5, 2011.

[48] E. Adi, A. Anwar, Z. Baig, and S. Zeadally, "Machine learning and data analytics for the IoT," Neural Comput Appl, vol. 32, no. 20, pp. 16205–16233, Oct. 2020, doi: 10.1007/s00521-020-04874-y.

[49] M. Kim, N. Y. Lee, and J. H. Park, "A security generic service interface of internet of things (IoT) platforms," Symmetry (Basel), vol. 9, no. 9, 2017, doi: 10.3390/sym9090171.

[50] A. M. Zarca, J. B. Bernabe, A. Skarmeta, and J. M. Alcaraz Calero, "Virtual IoT HoneyNets to mitigate cyberattacks in SDN/NFV-Enabled IoT networks," IEEE Journal on Selected Areas in Communications, vol. 38, no. 6, pp. 1262–1277, Jun. 2020, doi: 10.1109/JSAC.2020.2986621.

[51] A. Alhowaide, I. Alsmadi, and J. Tang, "PCA, Random-forest and pearson correlation for dimensionality reduction in IoT IDS," Sep. 2020. doi: 10.1109/IEMTRONICS51293.2020.9216388.

[52] A. Alsaedi, N. Moustafa, Z. Tari, A. Mahmood, and Adna N Anwar, "TON-IoT telemetry dataset: A new generation dataset of IoT and IIoT for data-driven intrusion detection systems," IEEE Access, vol. 8, pp. 165130–165150, 2020, doi: 10.1109/ACCESS.2020.3022862.

[53] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for Internet of Things," Future Generation Computer Systems, vol. 82, pp. 761–768, May 2018, doi: 10.1016/j.future.2017.08.043.

[54] S. Hernández Ramos, M. T. Villalba, and R. Lacuesta, "MQTT Security: A Novel Fuzzing Approach," Wirel Commun Mob Comput, vol. 2018, 2018, doi: 10.1155/2018/8261746.

[55] S. N. Matheu-García, J. L. Hernández-Ramos, A. F. Skarmeta, and G. Baldini, "Risk-based automated assessment and testing for the cybersecurity certification and labelling of IoT devices," Comput Stand Interfaces, vol. 62, pp. 64–83, 2019, doi: 10.1016/j.csi.2018.08.003.

[56] E. Wazoel Lubua and P. D. Pretorius, "Cyber-security Policy Framework and Procedural Compliance in Public Organisations," in Proceedings of the International Conference on Industrial Engineering and Operations Management Pilsen, 2019, pp. 23–26. [Online]. Available: https://thelawdictionary.org/policy-framework/

[57] R. Kwon, T. Ashley, J. Castleberry, P. McKenzie, and S. N. Gupta Gourisetti, "Cyber threat dictionary using MITRE ATTCK matrix and NIST cybersecurity framework mapping," in 2020 Resilience Week, RWS 2020, Oct. 2020, pp. 106–112. doi: 10.1109/RWS50334.2020.9241271.

[58] W. Xiong, E. Legrand, O. Aberg, and Lagerström Robert, "Cyber security threat modeling based on the MITRE Enterprise ATT&CK Matrix," Softw Syst Model, pp. 1–21, 2021.

[59] A. Georgiadou, S. Mouzakitis, and D. Askounis, "Assesing MITRE ATT&CK Risk Using a Cyber-Security Culture Framework," Sensors, vol. 21, no. 3267, pp. 1–14, 2021.

[60] M. Frayssinet Delgado, D. Esenarro, F. F. Juárez Regalado, and M. Díaz Reátegui, "Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations," 3C TIC: Cuadernos de desarrollo aplicados a las TIC, vol. 10, no. 2, pp. 123–141, Jun. 2021, doi: 10.17993/3ctic.2021.102.123-141.

[61] D. Sulistyowati, F. Handayani, and Y. Suryanto, "Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS," International Journal on Informatics Visualization, vol. 4, no. 4, pp. 225–230, 2020.

[62] C. B. Espinosa Garrido and L. Rosales Roldan, "Marco de referencia de ciberseguridad para dispositivos de IoT usando la tecnología de IDS," in Décima Segunda Conferencia Iberoamericana de Complejidad, Informática y Cibernética, Mar. 2022, pp. 210–215.

[63] V. Kelli, V. Argyriou, T. Lagkas, G. Fragulis, E. Grigoriou, and P. Sarigiannidis, "Ids for industrial applications: A federated learning approach with active personalization," Sensors, vol. 21, no. 20, Oct. 2021, doi: 10.3390/s21206743.

[64] K. Muthamil Sudar and P. Deepalakshmi, "An intelligent flow-based and signature-based IDS for SDNs using ensemble feature selection and a multi-layer machine learning-based classifier," Journal of Intelligent and Fuzzy Systems, vol. 40, no. 3, pp. 4237–4256, 2021, doi: 10.3233/JIFS-200850.

[65] M. S. Akhtar and T. Feng, "Deep Learning-Based Framework for the Detection of Cyberattack Using Feature Engineering," Security and Communication Networks, vol. 2021, 2021, doi: 10.1155/2021/6129210.

[66] A. Kim, M. Park, and D. H. Lee, "AI-IDS: Application of Deep Learning to Real-Time Web Intrusion Detection," IEEE Access, vol. 8, pp. 70245–70261, 2020, doi: 10.1109/ACCESS.2020.2986882.

[67] J. Aveleira-Mata, Á. L. Muñoz-Castañeda, M. T. García-Ordás, C. Benavides-Cuellar, J. A. Benítez-Andrades, and H. Alaiz-Moretón, "IDS prototype for intrusion detection with machine learning models in IoT systems of the Industry 4.0," Dyna (Spain), vol. 93, no. 3, pp. 270–275, May 2021, doi: 10.6036/10011.

[68] L. Santos, C. Rabadão, and R. Gonçalves, "Intrusion Detection Systems in Internet of Things," Jun. 2018.

[69] "Suricata Detect Dos Attack," Open Source Libs, May 06, 2022. https://opensourcelibs.com/lib/suricata-detect-dos-attack (accessed May 04, 2022).

[70] "CVE - Search Results," The MITRE Corporation, May 06, 2022. https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=mqtt (accessed May 04, 2022).

[71] "Matrix | MITRE ATT&CK®," MITRE ATT&CK, Apr. 21, 2022. https://attack.mitre.org/matrices/ics/ (accessed May 03, 2022).

Authors

Carmen Beatriz Espinosa Garrido obtained a PhD in Strategic Planning and Technology Management at Universidad Popular Autonoma del Estado de Puebla. She graduated with a BSc degree in Computer Science at Universidad Popular Autonoma del Estado de Puebla and then with an MSc in Computer Science at Universidad de las Americas Puebla. She has expertise in security network services and has worked at an international Information Technology company for 12 years. Her research area of interest is the Internet of Things, cybersecurity, and networks.

Sandra Sendra Compte is a high-level researcher with an affiliation in the Escuela Politécnica Superior de Gandia at the Department of Communications. Currently, she is working as a professor at Universitat Politècnica de València. She has published 79 journal articles and has written eight book chapters. She is ranked as one of the first women researchers in telecommunications in Spain, according to the scientific quality index H estimated by Clarivate Analytics.

Luis Rosales Roldan is a researcher and professor at Universidad Popular Autonoma del Estado de Puebla. He obtained an MSc degree in Telecommunications Engineering at ESIME Zacatenco, Mexico and a PhD in Communications and Electronics at ESIME Culhuacan, Mexico. He also learned a post-doctoral program at Chuo University, Tokyo, Japan. He belongs to the National System of Researchers in Mexico. His research areas include Watermarks, Signal Processing, Information Security, and Embedded Systems.

SURVEY ARTICLE

Alejandra Aldrette Malacara is a researcher and professor at Universidad Popular Autonoma del Estado de Puebla. She learned BSc in Computer Systems Engineering with Magna Cum Laude, MSc in Business Administration with Cum Laude, and another MSc in Computer Systems Science at Universidad de las Americas Puebla. She obtained a PhD in Information Technology and Data Analysis Decisions with an Honorable Mention by Universidad Popular Autonoma del Estado de Puebla. She has worked as Coordinator and Director of the IT department at Universidad Popular Autonoma del Estado de Puebla. She is certificated at ITIL Foundation, ITIL intermediate level certifications (in Planning, Operation, Strategy, Transition, and Continuous Improvement), ISO/IEC 27001, and Cobit 5, among others.

How to cite this article:

Carmen Beatriz Espinosa Garrido, Sandra Sendra Compte, Luis Rosales Roldan, Alejandra Aldrette Malacara, "Survey and testing of the IoT Cybersecurity Framework Using Intrusion Detection Systems", International Journal of Computer Networks and Applications (IJCNA), 9(5), PP: 601-623, 2022, DOI: 10.22247/ijcna/2022/215920.