ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

INTRUSION DETECTION SYSTEMS IN INTERNET OF THINGS: A RECENT STATE OF THE ART

RACHID HDIDOU[1], MOHAMED EL ALAMI[2]

[1,2]ERMIA Team, Department of Mathematics and Computer Science, National School of Applied Sciences

Tangier, Abdelmalek Essaadi University, Morocco

E-mail: [1]hdidou.rachid@etu.uae.ac.ma, [2]m.elalamihassoun@uae.ac.ma

ABSTRACT

Recently, the Internet of Things (IoT) has become a main technology in several areas such as smart networks, smart homes, smart cities, and others. By 2025, it is expected that more than 75 billion objects will be connected. This increase in internet-related objects implies the growth of cybercrimes against IoT networks. Since IoT is a set of heterogeneous objects, standard security techniques such as firewalls and antivirus are not sufficient to properly secure IoT infrastructures. This highlights the need to use flexible solutions such as Intrusion Detection Systems (IDS) which is the subject of our research. Our main objective is to determine the flaws and limitations of the existing solutions. To achieve this goal, we analyzed more than 60 articles on Intrusion Detection Systems in the Internet of Things. In this paper, we presented a taxonomy of Intrusion Detection Systems and a study on the architecture of the Internet of Things as well as attacks against the Internet of Things. Finally, we presented a detailed state of the art with the Problems, limitations of existing solutions, and open research issues for future research.

Keywords: *IDS, IoT, Intrusion Detection System, Internet of Things, IoT Security.*

1. INTRODUCTION

Internet of Things refers to all physical objects connected to the Internet, and that can communicate with each other without human intervention. IoT is becoming a leading technology in the technological revolution of the 21st century, and recently billions of objects are connected to the internet.

To use IoT technology in industrial fields, it is necessary to increase the performance of IoT applications such as energy consumption, resource consumption, availability of services, and security of IoT applications and networks. The security of IoT technology is among the important points that must be increased for the use of IoT applications, especially IoT applications in areas that contain private information of people or organizations.

IoT security is a domain that contains multiple paths to follow for example, cryptographic solutions, anti-malware solutions, and IDS solutions which are our objective. IDS is a security mechanism that is based on the collection, analysis, and detection of network traffic. Security researchers propose several IDS to develop solid solutions.

The exponential evolution of connected objects implies an evolution in the types of attacks against IoT applications and networks. This implies the need to present more effective and adaptable IDSs with new types of attacks.

Recently, the number of articles that deal with the use of IDSs to present security solutions for Internet of Things networks has increased, with several techniques, methodologies, and models. Due to this increase in the treatment of this subject, it is necessary to make a state-of-the-art and detailed analytical study that gives a very clear vision on the state of progress, the remaining problems, and the limitations of the existing solutions as well as the future avenues of research in this topic.

Our main objective of this scientific paper is to present a direct, global, and detailed vision on the subject "Intrusion Detection Systems in Internet of Things". To achieve this goal, we will try to present, firstly, a detailed study on intrusion detection systems, the architecture of the Internet of Things and the attacks impacting this technology, secondly, a state art on our subject of treatment, and finally an analytical study and comprehensive discussion of the collected, summarized and analyzed works.

This work will be one of the most important works in recent years in the research area covered. Seeing that our work will give a very clear vision of the current state of the use of IDSs to secure the Internet of Things, and all the necessary points for future research work in this direction such as the techniques, methods, models used, detection techniques, the most frequent attacks, existing problems, and future research directions.

As part of preparing this work, Firstly, we have collected more than 60 articles that were published between 2009 and 2023 and are collected from journals indexed in Databases known by their scientific confidentiality such as IEEE Xplore Digital Library, ACM Digital Library, Scopus, Web Of Science, ScienceDirect, Google Scholar, and B-On). Second, all collected articles are read, summarized, and analyzed with an extraction of all important information such as the detection method and the attacks detected. Finally, a statistical analysis is presented with a discussion of the analyzed research work and a vision of future research directions.

The rest of this work is organized as follows: Section II contains a background on the main terms in our work such as Internet of Things and Intrusion Detection System. Then, section III presents related works and section IV is the state of the art. Afterward, analysis and discussion will be presented in section V. Then the existing problem and the open research issues will be presented in the VI section and finally, section VII will give conclusions and the direction of our future work.

2. BACKGROUND

Before presenting the state of the art on our subject, in this section, we will first introduce the main terms such as Intrusion Detection System and Internet of Things.

2.1 Intrusion Detection System

Intrusion Detection System: It is a security system that monitors and analyzes network traffic for harmful activity or policy violations and alerts the information system administrator when suspicious activity is discovered [1] [2].

Several works that deal with IDSs present a taxonomy of them, and Figure 1, provides some important points for IDSs:

There are two types of intrusion detection systems, these two types are described below:

•Network Intrusion Detection System (NIDS): It is a specific computer or device installed in a specific location on the network to monitor and analyze the incoming and outgoing network traffic or a segment of the network for ongoing attacks to secure the system against network-level threats. NIDS can be installed in several locations such as a direct connection to a port covering a switch, a network connection, and an online connection [3].

•Host Intrusion Detection System (HIDS): It is a system that runs on a computer, server, or other computing device. The main purpose of HIDS is to monitor and analyze the entering and exiting traffic from a computing device in which it is installed to detect intrusions on that device if they exist. It can be considered as an agent that monitors and analyzes the machine.

It is possible to mix the two previous types in a single intrusion detector solution. This type of detection, Hybrid IDS, is based on NIDS and HIDS and benefits from the advantages. Of both types to increase the performance of the intrusion detection system, but this technique has its drawbacks such as being difficult to manage, expensive cost, and others. From a detection method point of view, IDS can be divided into two types, signature-based IDS, and anomaly-based IDS:

•Signature-Based: It is a type of IDS that uses patterns called signatures to detect attacks using specific criteria such as sequences of bytes in network traffic, known malicious instruction sequences used by malware, the number of 0 and 1 in network traffic, and others. Signature-based IDSs easily detect attacks whose patterns exist in the system, but they suffer against new attacks whose patterns are not known.

•Anomaly-Based: On the other hand, signature-based IDS, and anomaly-based IDS classify traffic or activities as normal or abnormal based on certain rules, rather than signatures. This detection technique is effective in detecting new attacks. Modern anomaly-based IDS uses dynamic learning techniques such as Machine Learning, Deep Learning, and Artificial Neural Networks to improve the performance of the detection system.

Based on the location of the installation of IDSs, we can divide them into 3 main categories:

•Centralized IDS: In a centralized IDS, analysis and intrusion detection operations are carried out by a single manager (network node). In this architecture, several monitoring modules can be

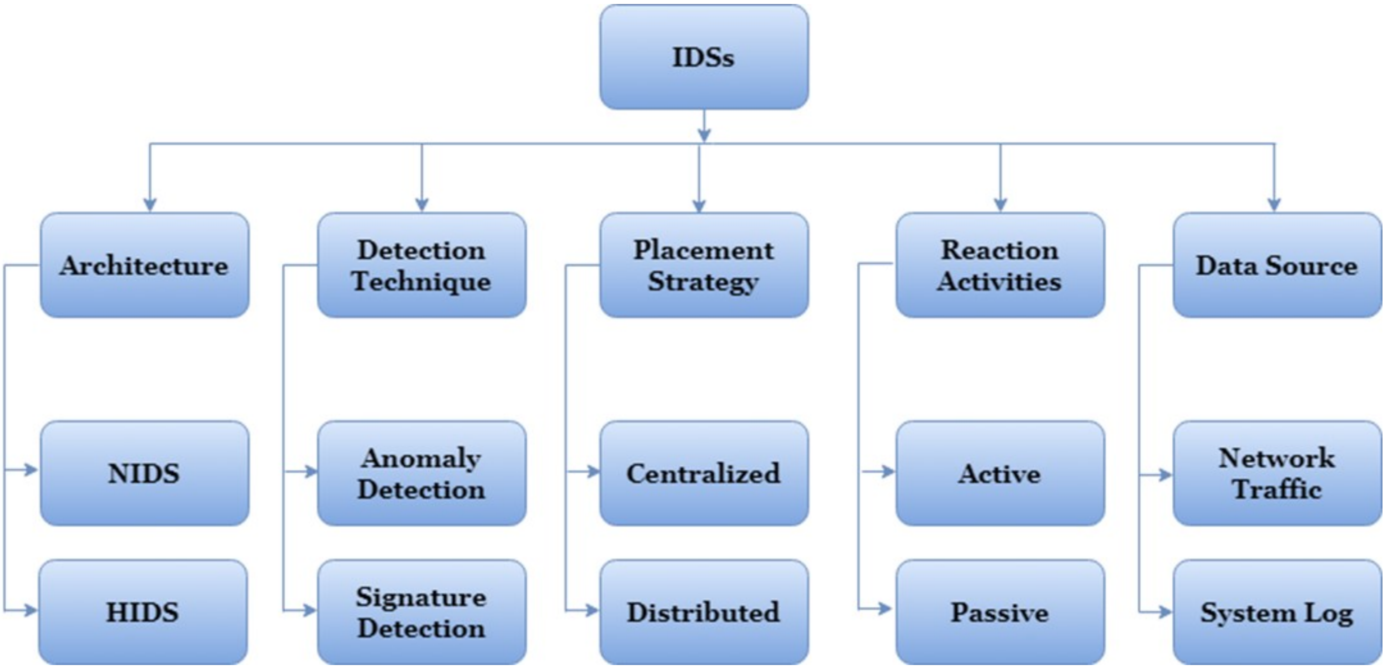

Figure 1: Taxonomy of Intrusion Detection Systems

responsible for collecting data and transmitting them to the central module. [4].

•Distributed IDS: In a distributed IDS, traffic analysis and intrusion detection are carried out by the collection agents. In this architecture, intrusion detection is done by the collector agents and by the manager modules. [4].

•Hierarchy IDS: In an IDS hierarchy, the protected system is configured in the form of subordination levels. This architecture allows distinct subordinations and the agents that collect information on the network (NIDS) can be subordinated to the network management module, and the same for the information collected in HIDS [4].

2.2 Internet of Things

The Internet of Things is the interconnection between the Internet and objects in which these objects can take on unique identifiers, communicate and exchange data without human intervention. The evolution of the Internet of Things began with Kevin Ashton, who was the first to use this term in 1999, and this evolution is initially based on technologies that already exist such as RFID, and M2M.

2.2.1 IoT Architecture

Standard Internet of Things architecture contains three main layers [5], and each layer is defined by its function and the devices used within it [6]. Figure 2, shows the architecture of the Internet of Things which is based on three layers:

•Perception Layer

It is the lowest layer in IoT architecture and is known as the sensor layer. This layer is implemented to detect, collect, and process data using sensors and finally transmit this data to the network layer via layer interfaces. Thus, the main objective of this layer is to transmit data from the environment to the IoT network.

•Network Layer

The network layer or transmission layer is the middle layer in the three-layer IoT architecture. This layer is intended to determine the correct routes to transmit the data received from the perception layer to the IoT devices. The network layer is considered the heart of the IoT architecture because it contains several devices such as hub, switch, router, and several technologies are integrated into it such as Wi-Fi, ZigBee, Bluetooth, 3G, and LTE. So, the objective of the network layer is to transmit data to IoT applications via the right routes using the right technology.

•Application Layer

The application layer (business layer) is located at the top of the IoT architecture. This layer takes the data sent by the previous layer to provide services or operations. It is in this stadium that we can say

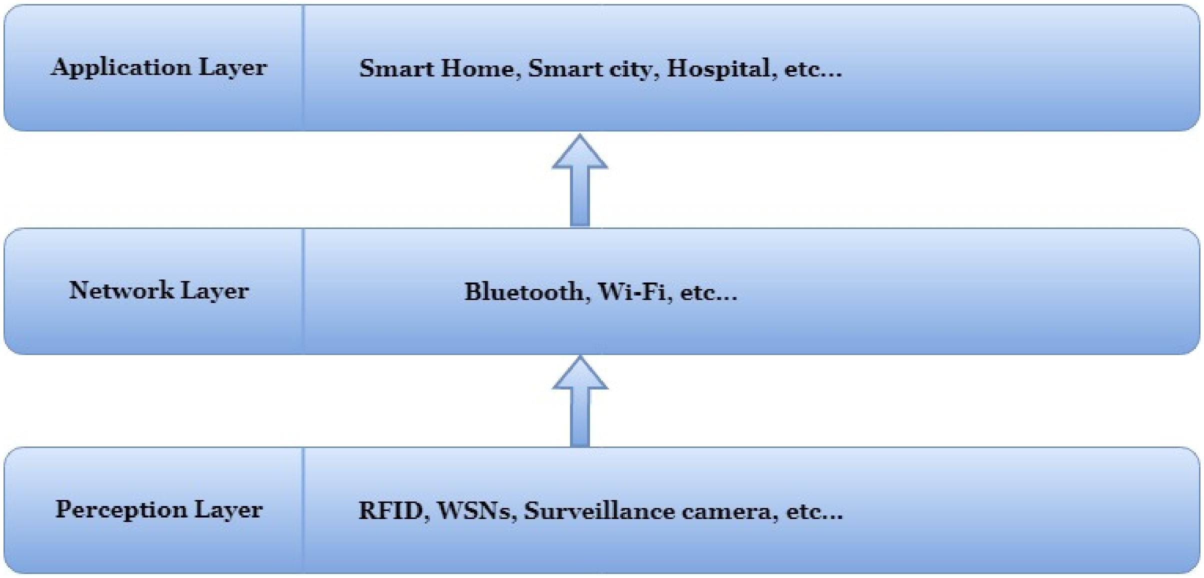
Application Layer
Smart Home, Smart city, Hospital, etc...
Network Layer
Bluetooth, Wi-Fi, etc...
Perception Layer
RFID, WSNs, Surveillance camera, etc...

Figure 2: IoT Architecture

that we have a smart environment. Thus, the main purpose of this layer is to provide services from data processing.

2.2.2 IoT threats

The rise in connected devices leads to an increase and development in the types of attacks. In this part, we will discuss the most well-known types of attacks and the functioning of each of them, and Figure 3, summarizes the types of attacks against IoT networks:

•Application Attacks

The first type of attack is attacks against IoT applications. In this category, there are several attacks, we will cite the main ones among them.

DoS Attack: It is an attack implemented to bring down a computer, server, website, or computer network, by sending the target a large number of service requests until the machine, site, or network victim cannot process normal traffic, which results in a denial of service. In our life, in the case of the Internet of Things, it is not only computers that are used to launch this attack, but all other objects connected to the Internet can be used.

Code Injection Attack: It is a type of attack intended for the application part. The cybercriminal in this attack attempts to inject malicious code to gain privileged access to the victim's machine. This implies that the attacker can damage the data or the functioning of the victim's system. In the case of an IoT system, this type of attack becomes very dangerous because the cybercriminal can damage, for example, a hospital system that contains information about the patient.

Traditional Subversion Attacks: several other attacks are also intended to damage computer systems or to steal information that exists in the victim system, among these attacks we cite, interception, manufacturing, modification, subversion, and phishing of messages, and the same thing that was said for the previous attacks, these types of attacks are also dangerous in the Internet of Things networks.

•Routing Attacks

Wormhole Attack: This is a dangerous type of attack where the attacker receives packets from one point on the network and sends them to another point on the network using wired or wireless links and replays them over the network. This type of attack is very dangerous in the case of wireless networks, and therefore dangerous in IoT networks because in the latter most objects are connected wirelessly.

Rank Attack: The RLP routing protocol in IoT networks is the main target of this attack. When a node changes its rank, it always informs its neighbors. The ranking information can be maliciously altered by an attacker so that it chooses the node with the lowest performing ranking to be its parent. This can therefore disrupt the network topology. As a result, there is a delay in normal transmission.

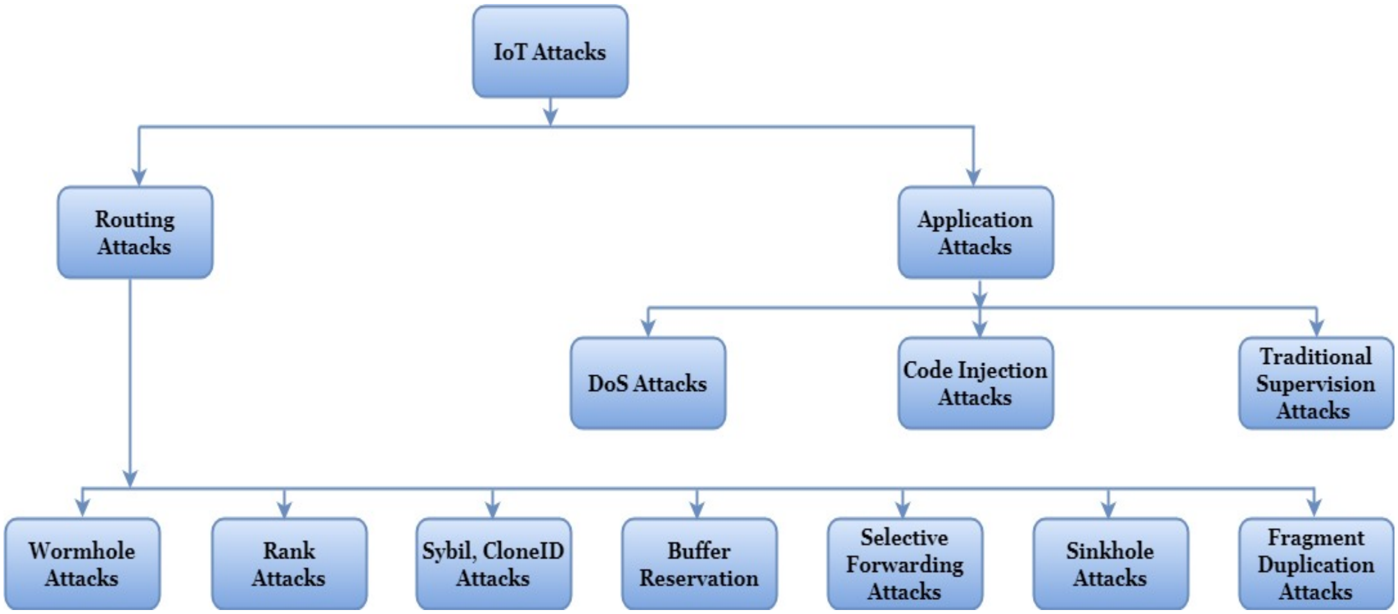

Figure3: Attacks against IoT

Sybil and CloneID Attack: The objective of both attacks is the same, which is to use spoofed logical identities without deploying physical devices. The Sybil attack is intended for peer-to-peer networks. In this attack, the cybercriminal attempts to take control of the network by creating several nodes. The CloneID attack is an attack in which the cybercriminal uses logical identities.

Buffer reservation Attack: This attack uses the fact that the recipient of a fragmented packet is unable to determine whether all fragments will be received correctly. Therefore, a recipient node reserves buffer space based on the information provided in the 6LoWPAN header, with every additional fragment being ignored. Taking advantage of this parameter, a malicious node can send to its victim the first fragment only to reserve arbitrary buffer space, thus consuming the rare memory of the node whose resources are limited. This type of attack also targets the fragment mechanism vulnerability used by 6LoWPAN networks. Buffer reservation Attack is linked to the Fragment Duplication attack.

Selective Forwarding Attack: In this attack, the cybercriminal (malicious node) tries to stop the packets by refusing to transfer them into the network, or also to delete the messages. In this type of attack, the attack can filter the packets that want to pass through [7].

Sinkhole Attack: In this attack, the attacker tries to compromise a network node. When the node is compromised, it tries to attract all traffic from neighboring nodes based on the routing metric used in the routing protocol [8]. So, the main objective of this attack is to attract node traffic via a designated node using illegitimate information.

Fragment Duplication Attack: This attack is based on a weak point in 6LoWPAN. This point is the method with which fragmented packets are received and assembled by an IoT node. A destination node cannot check whether two fragments of a packet were sent by the same source. The destination node is therefore unable to distinguish between legitimate and spoofed fragments. Therefore, a malicious node can exploit this vulnerability to block the reassembly of targeted packets such as connection establishment packets and that reveals a danger in the case of a connection between two machines in an IoT network [9].

3. RELATED WORKS

Several works are published as part of presenting a study, a taxonomy, or a state of art on the subject "Intrusion Detection System in the Internet of Things". In 2016, Sherasiya et al [10] presented a study on the different attacks against IoT and the different approaches to IDS that exist. In 2017, Zarpelao et al [11] presented a study and taxonomy of IDSs in IoT. In 2017, L.Santos et al [12], presented a literature review, and their work contains articles published between 2009 and 2017. In 2019, Hajiheidari et al [13] presented a

Systematic Literature Review on the term IoT security using IDSs. Also in 2019, Choudhary et al [14] presented a study on IDSs in IoT, and they also presented in their study cyberattacks against the 6LoWPAN and RPL protocols.

4. STATE OF THE ART

IoT security is one of the trending topics that attract the attention of cybersecurity researchers, and IDSs are essential tools to provide strong IoT security. In the field of scientific research, there are several works in which researchers try to increase the security level in Internet of Things networks using IDSs, and we will present these works in this subsection (Table1):

In 2009, Cho et al. [15] presented a centralized IDS for IoT where the packets that pass through the router, between IP network and 6LoWPAN, are analyzed to detect the botnet attack.

In 2011, Le et al. [16] proposed an IDS for IoT networks. The main objective is to detect RPL attacks, and they presented two new attacks against RPL, "rank attack" and "local repair attack" which damage the optimal network topology by breaking protocol operations. The researchers use a finite state machine (FSM) to specify the RPL behavior, which is used to detect malicious activity since the basic idea of specification-based IDS is to manually construct an abstract of normal network operations and then detect malicious behavior that breaks specifications.

Also, in 2011, Liu et al. [17] proposed a signature-based IDS that employs the mechanisms of the artificial immune system (AIS). The authors offer the basic theory of AIS to intrusion detection systems for IoT. In this work, the computational overhead needed to run the learning algorithms might be a weakness.

In their 2011 work, Misra et al. [18] proposed an IDS for IoT networks to prevent DDoS attacks over IoT middleware. They use « Learning Automata » concept to develop a DDoS attack prevention strategy in the context of SOA for IoT networks. The system generates an alert when the number of requests to a middleware layer exceeds the specified threshold. The authors also proposed an identical multi-layer module to prevent any DDoS attack attempt.

In 2013, Gupta et al. [19] presented an architecture for a Wireless IDS for IoT. In the work presented, the IDS placement strategy and the types of attacks to be detected by this solution were not mentioned by the authors. The proposed approach is based on computer intelligence algorithms to create profiles of the normal behavior of network devices. Therefore, a specific behavior profile would be for each device with an IP address assigned.

Also in 2013, Kasinathan et al. [20] proposed a centralized solution for IoT whose objective is to detect Denial of Service attacks in 6LoWPAN-based networks. To implement IDS, the authors use a known signature database, called SURICATA, and adapted to 6LoWPAN networks. The proposed solution is integrated into the platform currently under development within the Ebbits project.

In another 2013 paper, Kasinathan et al. [21] presented a centralized framework based on a signature-based detection method for IoT, more specifically for DoS attack detection. This work is considered an extension of the approach proposed by Kasinathan et al [20].

In their 2013 work, Raza et al. [22] presented a Real-Time Intrusion Detection System for Internet of Things. This approach also uses a hybrid placement strategy due to the participation of the router and the network nodes in the detection system. This IDS is named SVELTE, whose intention is to detect Sinkhole and Selective Forwarding attacks. In this IDS, all nodes transmit information to the router, send data from the RPL network, and notify about malicious traffic received. On the other hand, the router analyzes data from the RPL network to detect intrusions.

Also in 2013, Wallgren et al. [23] proposed an IDS for IoT networks where the objective is to detect routing attacks against the RLP protocol such as Sinkhole, Selective Forwarding, Hello Flood, Wormhole, Sybile, and CloneID. The authors installed their IDS in the router and did not use the router to monitor network traffic, but they suggested a heartbeat protocol to detect attacks within the physical domain.

In 2014, Amaral et al. [24] presented an IDS to protect IoT networks. The proposed approach is based on the following procedure: a group of selected nodes called "watchdogs" manages IDS aiming to identify intrusions by detecting the exchanged packets in their area. The watchdog node has a particular set of rules to decide whether a node is compromised or not. Each network area might have a different set of rules. When a rule is violated, the watchdog node send alerts to an Event Management System (EMS).

Table 01: IDSs in IoT

R	Year	Title	Detection method	Detected attack
15	2009	Attack Model and Detection Scheme for Botnet on 6LoWPAN	Anomaly-based	Botnet
16	2011	Specification-based IDS for securing RPL from topology attacks	Specification-based	Routing attack
17	2011	Research on Immunity-based Intrusion Detection Technology for the Internet of Things	Signature-based	-
18	2011	A Learning Automata-Based Solution for Preventing Distributed Denial of Service in Internet of Things	Specification-based	DoS
19	2013	Computational Intelligence based Intrusion Detection Systems for Wireless Communication and Pervasive Computing networks	Anomaly-based	-
20	2013	Denial-of-Service detection in 6LoWPAN-based Internet of Things	Signature-based	DoS
21	2013	DEMO: An IDS Framework for Internet of Things Empowered by 6LoWPAN	Signature-based	-
22	2013	SVELTE: Real-time intrusion detection in the internet of things	Hybrid	Routing attack
23	2014	Routing Attacks and Countermeasures in the RPL-Based Internet of Things	-	Routing attack
24	2014	Policy and Network-based Intrusion Detection System for IPv6-enabled Wireless Sensor Networks	Specification-based	-
25	2014	Integration and Evaluation of Intrusion Detection for CoAP in Smart City Applications	Hybrid	Routing attack Man-in-the-middle
26	2014	Design of Complex Event-Processing IDS in Internet of Things	Specification-based	-
27	2014	A Lightweight Intrusion Detection Scheme Based on Energy Consumption Analysis in 6LowPAN	Anomaly-based	DoS
28	2015	A Malicious Pattern Detection Engine for Embedded Security Systems in the Internet of Things	Signature-based	Multiple Conventional attacks
29	2015	Detection of Sinkhole Attacks for Supporting Secure Routing on 6LoWPAN for Internet of Things	Hybrid	Routing attack
30	2015	Real-Time Intrusion and Wormhole Attack Detection in Internet of Things	Anomaly-based	Routing attack
31	2016	Ultra-Lightweight Deep Packet Anomaly Detection for Internet of Things Devices	Anomaly-based	Conventional
32	2016	A Specification-Based IDS for Detecting Attacks on RPL-Based Network Topology	Specification-based	Routing attack
33	2016	Distributed Internal Anomaly Detection System for Internet-of-Things	Anomaly-based	-
34	2017	Kalis - A System for Knowledge-driven Adaptable Intrusion Detection for the Internet of Things	Hybrid	
35	2017	Intrusion Detection in the RPL-connected 6LoWPAN Networks	Hybrid	Routing attack
36	2018	Intrusion Detection in Internet of Things: The Review of Taxonomy	-	-
37	2019	Efficient Physical Intrusion Detection in Internet of Things: A Node Deployment Approach	-	-
38	2019	Toward a Lightweight Intrusion Detection System for the Internet of Things	-	DDoS
39	2019	A Heuristic Intrusion Detection System for Internet-of-Things (IoT)	-	-
40	2019	A Novel Ensemble of Hybrid Intrusion Detection System for Detecting Internet of Things Attacks	Hybrid	well-know zero-day
41	2019	A Survey: Intrusion Detection Techniques for Internet of Things	-	-
42	2019	Intrusion detection systems in the Internet of things: A comprehensive investigation	-	-
43	2019	ELNIDS: Ensemble Learning based Network Intrusion Detection System for RPL-based Internet of Things	-	Sinkhole, Blackhole, Sybil, Clone ID, Selective Forwarding, Hello Flooding, and Local Repair
44	2019	Design of Intrusion Detection System for Internet of Things Based on Improved BP Neural Network	-	DoS, R2L, U2L, and Probing attack

45	2019	Intrusion Detection Techniques Used For Internet of Things	-	-
46	2019	A Real-Time Intrusion Detection System for Wormhole Attack in the RPL-based Internet of Things	-	Wormhole attack
47	2019	Recent Advancements in Intrusion Detection Systems for the Internet of Things	-	
48	2020	Hybrid Intrusion Detection System for Internet of Things (IoT)	Hybrid	-
49	2020	Enhanced Network Intrusion Detection System Protocol for Internet of Things	-	-
50	2020	Intrusion Detection System for the Internet of Things Based on BlockChain and Multi-Agent Systems	-	-
51	2020	A Literature Review: Intrusion Detection Systems in Internet of Things	-	-
52	2021	A Flow-based intrusion detection framework for internet of things networks	Specification-based	-
53	2021	AS‑IDS: Anomaly and Signature-Based IDS for the Internet of Things	Hybrid	DoS, Probe, U2R, R2L
54	2021	Towards building data analytics benchmarks for IoT intrusion detection	-	-
55	2021	Feature selection for intrusion detection system in Internet-of-Things (IoT)	-	DoS, DDoS
56	2021	A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges	-	-
57	2022	An IoT-Based Intrusion Detection System Approach for TCP SYN Attacks	anomaly-based	DoS
58	2022	Intrusion Detection Systems in Internet of Things and Mobile Ad-Hoc Networks	-	-
59	2022	MidSiot: A Multistage Intrusion Detection System for Internet of Things	-	-
60	2022	Realguard: A Lightweight Network Intrusion Detection System for IoT Gateways	-	multiple
61	2022	A Review on Intrusion Detection Systems to Secure IoT Networks	-	-
62	2023	Lightweight Intrusion Detection Model of the Internet of Things with Hybrid Cloud-Fog Computing	-	-
63	2023	An Anomaly Detection Method for Wireless Sensor Networks Based on the Improved Isolation Forest	Anomaly-based	-
64	2023	A Deep Learning Method for Lightweight and Cross-Device IoT Botnet Detection	Anomaly-based	Botnet
65	2023	Deep learning in distributed denial-of-service attacks detection method for Internet of Things networks	-	DDoS
66	2023	Deep Learning Approach for SDN-Enabled Intrusion Detection System in IoT Networks	-	-
67	2023	Deep Learning-Based Malicious Smart Contract and Intrusion Detection System for IoT Environment	-	Data injection
68	2023	Efficient Intelligent Intrusion Detection System for Heterogeneous Internet of Things (HetIoT)	-	DDoS
69	2023	An Anomaly Intrusion Detection for High-Density Internet of Things Wireless Communication Network Based Deep Learning Algorithms	Anomaly-based	-
70	2023	Real-Time Intrusion Detection and Prevention System for 5G and Beyond Software-Defined Networks	-	-
71	2023	Transfer Learning Approach to IDS on Cloud IoT Devices Using Optimized CNN	-	-
72	2023	Intelligent approaches toward intrusion detection systems for Industrial Internet of Things: A systematic comprehensive review	-	-
73	2023	Multi-Zone-Wise Blockchain-Based Intrusion Detection and Prevention System for IoT Environment	-	DDoS, IP Spoofing, Replay attack, Data Tampering
74	2023	Hybrid Deep Learning Based Attack Detection for Imbalanced Data Classification	-	-
75	2023	Optimal Fuzzy Logic Enabled Intrusion Detection for Secure IoT-Cloud Environment	-	-

Also in 2014, Krimmling et al. [25], proposed an IDS for IoT to detect attacks such as routing attacks, and Man-in-the-Middle attacks in IoT networks. In this article, researchers applied the CoAP protocol as a communication protocol used for smart cities application. The authors' goal is to provide a framework for developers to evaluate proposed IDS techniques for planned smart city applications. They study the possibility of applying IDSs to smart city applications that use the CoAP protocol. The authors concluded that the hybrid IDS approach is a favorable candidate for detecting a higher number of attacks such as routing and Man-in-the-Middle attacks, and consequently increases the rate of Internet security items.

In another 2014 work, Jun et al. [26] proposed an IDS for IoT networks. To create this approach, the authors used Complex Event Processing (CEP) techniques in which the rules are stored in the rules model repository and adopt Esper's EPL and SQL as references. According to the authors, the results showed that the proposed approach is better in terms of computational resources and processing time consumption compared to traditional IDS.

Also in 2014, Lee et al. [27] proposed an IDS for IoT where the objective is to detect intrusions such as DoS attacks. The idea of this approach is to monitor the node energy consumption i.e., each node monitors its energy consumption, and when the normal value changes, IDS classifies this node as malicious and removes it from the routing table in 6LoWPAN. The results performed by the authors showed that the proposed IDS is more efficient and accurate, and the detection rate of DoS attacks by this approach is 100%.

In 2014, Oh et al. [28] presented a lightweight IDS for Internet of Things to detect the main classic attacks. The basic idea of this approach is that each node will send packet payloads using an algorithm designed to skip irrelevant matching operations aimed at reducing the computational cost of comparing packet payloads and attack signatures. This article presented a new "pattern-matching" algorithm for the security of embedded systems.

In 2015, Cervantes et al. [29] proposed a distributed IDS for IoT networks whose objective is to detect Sinkhole attack in IoT networks and more precisely in 6LoWPAN. The proposed IDS is named INTI and its main task is to monitor upper node that has its traffic patterns. When a node detects a Sinkhole attack, the IDS broadcasts a message to alert other nodes. Finally, the authors declared that the proposed IDS detects the Sinkhole attack with an accuracy of 92% for the fixed scenarios and with an accuracy of 75% for the mobile scenarios.

Also in 2015, Pangle et al. [30] proposed an Intrusion Detection system for the Internet of Things where the objective is to detect the Wormhole attack. This approach is based on the idea that network nodes detect changes in their neighborhoods and send information to centralized models installed in the router. The obtained results showed that the proposed solution is suitable for IoT systems since its memory and energy consumption is low. The detection rate of this solution declared by the authors is 94%.

Another 2015 work presented by Summerville et al. [31] proposed an IDS for the Internet of Things. This IDS uses the detection method that is based on deep packet anomalies, without indicating the placement strategy. Their detection method used a technique called "bit-pattern matching" to select feature selection. The results showed that the false positive rate for classic attacks was very low.

In 2016, Le et al. [32] proposed an IDS for Internet of Things. The objective is to detect attacks on the network topology against the RPL protocol. The idea of this approach is to divide the network into clusters, and each cluster has a head node that communicates with the other nodes in the cluster. The role of the head node is to control other nodes, and the role of other nodes is to report the information to the head node.

Also in 2016, Thanigaivelan et al. [33] presented an IDS for IoT. The principle proposed in this article is that each node monitors these neighborhoods and sends notifications of possible attacks to the IDS module installed on the router. The IDS module receives these notifications and decides whether there is an intrusion or not.

In 2017, Midi et al. [34] presented a centralized IDS for the Internet of Things. The proposed IDS is called Kalis (Knowledge-driven Adaptable Lightweight Intrusion Detection System). The basic idea is that Kalis is a self-adaptive and knowledge-based IDS for IoT systems running different communication protocols. Kalis collects information about the functionalities of IoT networks and monitored entities and exploits them to dynamically configure the most effective set of detection techniques.

Also in 2017, Shreenivas et al. [35] proposed an IDS solution for IoT. This work is an extension of IDS SVELTE proposed by Raza et al [22]. This

IDS aims to detect the RPL attack in 6LoWPAN networks. Intending to improve the security level, the authors extended SVELTE with an intrusion detection module that uses the ETX (Expected Transmission) metric.

In 2018, Babu et al. [36], the authors presented a taxonomy on Intrusion Detection Systems in IoT networks. This taxonomy contains the architecture of IoT infrastructures, the concept of IoT, the technologies used in IoT networks with their standards, and finally, the authors talked about existing attacks against IoT environments.

In 2019 work presented by Halder et al. [37] proposed a new approach for intrusion detection in IoT. In their work, they studied the problem of physical intrusion detection and examined the various network parameters.

In 2019, Jan et al [38] proposed a design of a Lightweight IDS to detect DDoS attacks in IoT networks using Machine Learning techniques, precisely the supervised learning technique: Support Vector Machine (SVM). According to the researchers, the proposed system focuses on two essential factors. The first is the receiving data attribute used to classify the signal. The researchers take a single attribute which is the packet arrival rate at the node. The second factor is the Machine Learning classifier, and the researchers take the SVM classifier.

In 2019, Qureshi et al [39] developed a Random Neural Network (RNN) based Heuristic Intrusion Detection System using the feed-forward nature for IoT networks. To estimate the performances relative to a different number of inputs, the researchers adopted two methods: in the first method, the IDS RNN-IDS model proposed 29 Input Layer Neurons that are connected by 21 Hidden Layer Neurons. In the second method, RNN-IDS uses all features of NSL-KDD data set; it has 41 Input Layer Neurons that are connected by 21 Hidden Layer Neurons.

In 2019, Khraisat et al [40] proposed a hybrid IDS. The proposed system is based on a combination of two classifiers C5 and SVM on the one hand, and a combination of the advantages of signature-based IDS and anomaly-based IDS. To increase the performance of the proposed system, the authors divided the system into two phases: the 1st phase is the AIDS phase in which the researchers use the C5 classifier. The 2nd phase is the SIDS phase, in which the SVM classifier was used. The proposed IDS aims to detect well-known attacks and zero-day attacks.

In 2019, Choudhary et al [41] first presented a study on Intrusion Detection Systems and their types according to architecture, analysis strategy, and source of information. Second, the architecture of the Internet of Things infrastructure. Third, the work contained an explanation of the existing cyber-attacks against both 6LOWPAN and RPL protocols. Finally, the researchers presented some articles on the use of Intrusion Detection Systems for Internet of Things. These articles were published between 2009 and 2016.

In 2019, Hajiheidari et al [42] presented a Systematic Literature Review on the use of Intrusion Detection Systems in IoT infrastructures. The researchers also presented a detailed study on Intrusion Detection Systems based on their types and categorization. Moreover, they presented the published articles concerning each category of IDS. The categories covered in this article are Detection techniques, Location, Assessment techniques, and Types of attacks. The advantages and disadvantages of IDS are also discussed. Finally, the researchers gave numerical statistics on the use and implementation of each category, and these statistics came from the analysis of more than 324 articles by the researchers.

In 2019, Verma et al [43] proposed an architecture of Ensemble Learning based Network Intrusion Detection System named ELNIDS for detecting a set of attacks against IoT networks such as Sinkhole, Blackhole, Sybil, CloneID, Selective Forwarding, Hello Flooding, and Local Repair Attacks. The proposed model uses four different types of set-based classifiers: Boosted Trees, Bagged Trees, Subspace Discriminant, and RUSBoosted Trees. To evaluate the presented architecture, the RPL-NIDDS17 dataset is used.

In 2019, Yang et al [44], proposed an Intrusion Detection System based on LM-BP Neural Network Model. The architecture of the proposed IDS is divided into the following stages: Network Data Collection, Data Preprocessing, the Rule Base Definition, the part of detecting intrusion behavior that is carried out by the Improved Neural Network Model, and an update of the rule base using the LM-BP Neural Network Model. In this work, the researchers use the KDD CUP 99 dataset to test the detection of the following attacks: DoS, R2L, U2L, and Probing attacks. According to the authors, the detection rate of the proposed model is more effective compared to the PSO-BP and Traditional BP models.

In 2019, M. Bhargavi et al [45] presented a study on Intrusion Detection Systems for IoT networks. This study contains an introduction to the Internet of Things, the main attacks against IoT networks, the definition, the importance of Intrusion Detection Systems, and the techniques and approaches used in the development of Intrusion Detection Systems.

In 2019, Deshmukh-Bhosale et al [46] proposed an Intrusion Detection System for IoT networks, precisely an Intrusion Detection System to detect Wormhole Attacks against the RPL routing protocol in Internet of Things networks.

In 2019, Ali Khan et al [47] presented an overview on Intrusion Detection Systems for IoT networks. First, researchers gave a classification of IDS. They, in this classification, talked about existing attacks against IoT networks. Furthermore, a description of the IDS implementation strategy was presented. Finally, the authors presented an analysis of some articles on the use of IDS for MANET, WSN, CPS and IoT networks based on the implementation technique, the detection method, and the detected attacks.

In 2020, S. Smys et al [48] proposed an intrusion detection system to detect attacks in IoT networks using Hybrid Convolutional Neural Network model. In the proposed model, Long Short-Term Memory (LSTM) is used in combination with Recurrent Neural Network (RNN). This model is divided into 4 steps: Data Collection, Data Pre-Processing, the network Training, and attack Identification.

In 2020, Mbarek et al [49] proposed an ENIDS protocol augmented with an algorithm to detect replicas for the security of IoT networks against Clone attacks. To test the performance of the proposed model, the researchers compared their work with the SEVELTE intrusion detection protocol in terms of energy consumption and the probability of replica detection. In terms of the probability of replica detection, the results show that the proposed protocol ENIDS is more efficient than SEVELTE. Regarding energy consumption, if the number of compromised nodes is minimal, then the ENIDS model consumes more energy compared to SEVELTE Protocol. However, when the number of compromised nodes increases, the energy consumption of ENIDS becomes optimal compared to SEVELTE.

In 2020, Liang et al [50] proposed an IDS based on multi-agents, BlockChain and Deep Learning. According to the researchers, the proposed system contains four models which are: Data Collection, Data Management, Data Analysis and Response. To test their system, the researchers used the NSL-KDD dataset. The authors concluded that Deep Learning algorithms are effective in attack detection and are suitable for intrusion detection in IoT environments.

In 2020, Chauhan et al [51] presented a literature review on the use of Intrusion Detection Systems in IoT networks. In this article, the researchers first presented a classified IDS for IoT according to the placement strategy, detection method and validation strategy. In the next section, attack classification against IoT was also presented, and researchers divided these attacks into two classes application-specific attacks and routing-specific attacks. Finally, the researchers gave an overview of IDS for IoT devices based on an analysis of 16 articles, specifying for each article the placement strategy, the detection method, and the detected attack.

In 2021, Santos et al [52] proposed an Intrusion Detection System (IDS) Framework for IoT networks. This Framework is based on IP-Flow, i.e., it collects and analyzes IP Flows from an IoT network to detect attacks. For the placement strategy used, the researchers implemented their Framework based on a Hybrid architecture that contains a part of distributed data collection and a part of centralized intrusion detection and analysis. Regarding the detection method, the researchers used a specification-based approach.

In 2021, Otoum et al [53] proposed an IDS model (known as "AS-IDS") to detect attacks in IoT networks. The proposed model has three phases: traffic filtering, Data Pre-processing, and the Hybrid IDS which has two IDS subsystems, the first is based on signatures that investigate packets to group traffic into the intruder, normal or unknown traffic. The second is based on anomalies that identify the unknown attacks and categorize them into 5 categories (DoS, U2R, R2L, Probe, or normal). To evaluate the proposed model, the researchers used five parameters (DR, FAR, Specificity, F-measure, and Computation time) using NSL-KDD datasets.

In 2021, Ahmad et al [54] presented a study of several models of IoT Intrusion Detection Systems to build data analytics benchmarks for IoT intrusion detection. The authors began their paper with a literature review in which they presented the most used datasets, detection techniques, and Deep Learning models for IDSs, and performance metrics. They also presented a comparison between several detection techniques using the data presented. Finally, they illustrated a data analytics benchmark model.

In 2021, Nimbalkar et al [55] proposed an Intrusion Detection System for the Internet of Things. The main objective of the proposed system is to detect DoS and DDoS attacks. This system is focused on feature selection based on two factors: Information Gain -IG- and Gain Ratio -GR-. The IDS proposed by the researchers consists of three main parts: Data Pre-processing, Feature Selection, and JRip Classifier. To evaluate the proposed system, the authors used the two datasets IoT-BoT and KDD Cup 1999.

In 2021, Khraisat et al [56] presented a review of Intrusion Detection Systems in the Internet of Things. First, the authors presented a classification of IoT SDIs according to Placement Strategy, Detection Method, and Validation Strategy. Second, a State-of-the-art is presented. Then, they presented a taxonomy of IoT attacks. A set of the most used datasets in the IDS domain in IoT is presented as well. Finally, they got their hands on some challenges of setting up IDSs in IoT.

In 2022, Berguiga et al [57] proposed an anomaly-based Intrusion Detection System for the Internet of Medical Things networks. The main purpose of the proposed system is to detect Denial of Service attacks performed by TCP SYN flooding attacker nodes.

In 2022, Ponnusamy et al [58] presented a study on the architectures of Intrusion Detection Systems for wireless networks. They began their article with a presentation of the taxonomy of IDSs. Then, they compared the IDS architectures for filial and wireless networks. Finally, architectural design challenges for WSNs, IoT, and Mobile Ad-Hoc networks and recommendations as well were suggested.

In 2022, Dat-Thinh et al [59] proposed a distributed Intrusion Detection System (IDS), namely, MidSiot. The proposed IDS consists of three stages: (1) classifying the types of IoT devices, (2) differentiating between benign and malicious traffic, (3) identifying the types of attacks targeting IoT devices. This IDS is deployed at both local gateways that manage the first stage and internet gateways that manage the second and third stages. To evaluate their System, researchers used three datasets (IoTID20, CIC-IDS-2017 and Bot-IoT). According to researchers, IDS proposed can detect up to seven attacks with an average accuracy of 99.68%.

In 2022, Nguyen et al [60] proposed NIDS (Named Realguard), a DNN-based network, using a lightweight feature extraction algorithm. This proposed system is operated on IoT network gateways. According to the researchers, this IDS can detect multiple cyberattacks in real-time. The results show that Realguard can process up to 10,600 packets in a second with an average detection accuracy of 99.57%.

In 2022, Anitha et al [61] presented a review on IDSs in the context of securing IoT networks. The authors first gave the features of the IDSs. Then, they presented a literature review on IoT security generally and IoT security based on IDSs specifically. Attacks against IoT and types of IDSs are also presented. Finally, the researchers proposed an analytical Survey on IDSs for IoT and according to this survey they proposed research directions for future research work on the subject of "Security IoT based on IDSs Techniques".

In 2023, Zhao et al [62] proposed a lightweight model of an Intrusion Detection System for IoT networks. The proposed model is based on ConvNeXt-Sf. The intrusion detection model of IoT with hybrid cloud and Fog Computing can be summarized in 3 phases: first, Fog Node receives data packets from normal users or abnormal users. Second, data pre-processing will be done by LE-MMN. Finally, the pre-processed data is classified with ConvNeXt-Sf.

In 2023, Chen et al [63] proposed an anomaly detection method for IoT networks and more specifically for Wireless Sensors Networks (WSN). The proposed method, named “BS-iForest”, is a combination between the Box-Plot method and the Isolation Forest (iForest) algorithm. To evaluate the performance of the proposed method, the researchers adopted the three parameters ACC, AUC, and F1-score using the two datasets BreastW and Campus-CRS.

In 2023, Catillo et al [64] proposed a Botnet attack detection method for IoT devices using Deep Learning Techniques. The model proposed by the researchers is based on Deep Neural Network and an all-in-one Autoencoder. To evaluate the performance of the proposed method, the authors adopted the parameters Recall, Precision, False Positive Rate, and F1-score using the N-BaIoT dataset.

In 2023, Aswad et al [65] proposed a model of an Intrusion Detection System to detect DDoS attacks in IoT networks. The proposed model, CNN-BiLSTM, is based on a combination of three Deep

Learning algorithms which are: RNN, CNN and LSTM. The experiment procedure carried out by the researchers can be summarized in five steps: Data collection, data preparation, data processing with RNN, CNN and LSTM and also with CNN-BiLSTM, training and testing and finally evaluation.

In 2023, Chaganti et al [66] proposed an approach of an Intrusion Detection System based on Deep Learning for the prevention and detection of attacks in SDN IoT networks. The researchers selected the LSTM technique from three possible choices which are CNN, DNN and LSTM. The architecture of the proposed Deep Learning LSTM model consists Firstly of an input layer and secondly of four LSTM hidden layers and each layer contains 64 units, Third of a dense layer and finally of an output layer.

In 2023, Shah et al [67] proposed an Intrusion Detection System model and malicious smart contracts based on artificial intelligence techniques such as Deep Learning to secure IoT environments. The architecture of the proposed system is composed of 4 layers: The First layer is the Deployment Layer which is a layer of IoT applications that can also contain malicious users. The second layer is Malicious User Detection Layer which allows to check if a user is malicious or not by using a Machine Learning model. The Third layer is the Blockchain Layer which allows the validation of the smart contracts issued by the user. The Fourth and last layer is the Application Layer which contains IoT applications such as smart watches, smart homes…Etc.

In 2023, Mahadik et al [68] proposed an Intelligent Intrusion Detection System (IDS) for Internet of Things environments. The proposed system is based on CNN and named HetToT-CNN IDS. The architecture of this system contains 5 layers: The convolution Layer allows to extract the input entities. The Pooling Layer allows to extract the characteristics after convolution and which allows to reduce the calculation time and the errors. The Dropout Layer allows for over-adjustment during training process. Flatten Layer which allows to flatten all the information into a suitable format, Fully Connected Dense Layer allows to perform the same job of ANN. In the evaluation of the proposed model, the researchers used Binary Classification and multi-class classification in two boxes 8 classes and 13 classes.

In 2023, Salman et al [69] proposed two Intrusion Detection models for IoT networks, specifically for Wireless networks. The first model is based on both CNN and LSTM techniques. The second model is an ANN which is constructed from dense layers of different sizes. To evaluate the two models, the researchers used the UNSW-NB15 dataset and the evaluation parameters that are used are accuracy, precision, F1-score and Recall.

In 2023, Bocu et al [70] proposed An Intrusion Detection and Prevention System based on Machine Learning, specifically on CNN for the security of IoT networks, and more specifically for 5G networks. The proposed system architecture is divided into 3 layers: the first layer is Forwarding Layer which collects and transfers data to the second layer which is Management and Control Layer which identifies anomalies by analyzing the data received starting from the first layer, and the last layer is Data and Intelligence Layer which is the Intrusion Detection layer.

In 2023, Daniel Okey et al [71] proposed a Transfer Learning IDS using CNN for the security of CloudIoT environments. The proposed IDS is named ELETL-IDS (Efficient Lightweight Ensemble Learning Transfer Intrusion Detection System), and its objective is to detect attacks: Bot, DoS, DDoS, and Infiltration) using the two datasets: CIC-IDS2017 and CSE-CICIDS2018. The architecture of the proposed model can be divided into 4 phases, the first phase is Data Preparation which is also divided into two sub-stages: Data Cleaning and Data Transformation. The second phase is Splitting data into Training Set and Testing Set. The third phase is CNN model optimization and the last phase is data classification.

In 2023, Nuaimi et al [72] presented a study on the use of intelligent techniques in Intrusion Detection Systems for industrial Internet of Things security. In this study, the authors presented the IoT architecture, gave and overview of attacks against IIOT, cited the techniques of machine learning and deep learning in IDSs for the security of IoT. Moreover, the presented the architecture of Ids based on machine learning and deep learning techniques and as well as a comparison between the old research works that have been carried out on the use of intelligent techniques in IDSs to propose security solutions for IIoT. Finally, the researchers presented the remaining problems and the possible future directions of research.

In 2023, Kably et al [73] proposed an Intrusion Detection and Prevention System based on Blockchain technology for the security of IoT environments. The proposed system is named

“MSWB” (Multi-Zone-Wise Blockchain). It consists of three layers: First, the Perception layer which contains IoT devices. Second, the Edge layer on which the first level of IDS exists. Third, the Blockchain layer and on this layer there is the second level of IDS where the Multi-Zone Blockchain structure is applied.

In 2023, Almarshdi et al [74] proposed a model of an Intrusion Detection System based on Deep Learning CNN and LSTM algorithms. We can divide the proposed model into 3 phases: Data Pre-processing, Data Imbalanced, and finally training and testing. The researchers divided this model into 3 layers: CNN, LSTM and the dense layer. A comparison between the proposed model and CNN model, Decision Tree and Random Forest with balanced and unbalanced data was presented in this research work.

In 2023, S. Alrayes et al [75] proposed an Intrusion Detection System based on Fuzzy Logic with a Metaheuristics Feature Selection. The proposed model is named MFSFL-IDS and is intended for Internet of Things Environments. The approach proposed by the researchers is divided into 4 essential phases: Pre-Processing of Data, Feature Selection with the HGSO algorithm (Henry Gas Solubility Optimization), the intrusion classification phase with the ANFIS technique (Adaptive Neuro Fuzzy Inference System), and finally the adjustment of the parameters of the ANFIS model. In this phase, the researchers used the BBA (Bat Binary Algorithm) algorithm.

5. ANALYSIS AND DISCUSSION

Intrusion detection systems are considered one of the most important security techniques used in the search for effective solutions to protect the Internet of Things. Researchers interest in these techniques is due to their flexibility and ability to adapt to different types of networks, including the Internet of Things which is considered one of the most complex types of networks because they have a heterogeneous structure. As part of presenting IoT network security solutions using IDSs, several research projects have been proposed in recent years (see Table 1).

First Point: To properly extract solid ideas on the state of progress of our subject which is the use of IDSs in the security of Internet of Things networks, the analytical charts of the collected work and summaries will be presented in the following:

In our work, we have collected more than 60 research works that address our subject of study. These works were published between 2009 and 2023 and the Figure 4 shows the distribution of these articles by the years of publication:

From the analysis of this diagram, we see that the number of research works that address the subject of IDSs in IoT has increased in the last 4 years since 2019, and this can be interpreted by the rapid evolution of IoT applications in the different areas.

Intrusion detection techniques are considered the main building block in all IDSs. There are four intrusion detection approaches: Anomaly-based, Specification-based, Signature-based, and finally the Hybrid approach. The Figure 5 presents a comparison of the detection methods used in the analyzed research works:

By analyzing this diagram, we found that the most used method is anomaly-based, followed by hybrid solutions, Specification-based, and finally signature-based. Several research works do not mention the detection method.

As presented in the Background section, several attacks can impact the Internet of Things networks, and each of these attacks has its characteristics. In the Figure 6, we will present the frequency of the attacks most discussed in the articles analyzed:

The first remark is that most articles do not mention targeted attacks. Secondly, we find that the routing attack is the most targeted, and finally, we note the lack of solutions to detect new attacks.

Second point: Several methods, techniques, and models are proposed to develop more efficient Intrusion Detection Systems to protect Internet of Things networks. Among the techniques proposed, we find: Finite State Machine (FSM) [16], is a mathematical model that consists of designing and describing the behavior of a system, and this system has a finite number of states. This technique has advantages such as the speed of development of systems based on it and their reliability. However; systems based on this technique can become complex and difficult to manage when the number of states and transactions increases. In [17], the researchers propose an IDS that is based on the techniques of the artificial immune system (AIS) which is a computer model that takes its principles and characteristics from the human immune system. The Artificial Immune System (AIS) model is a

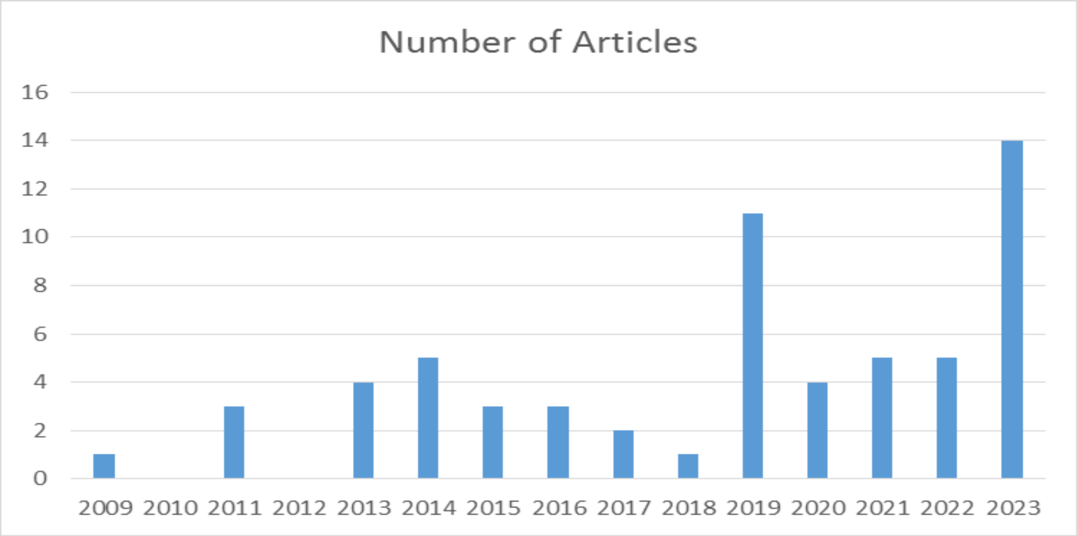

Figure 4: Number of articles

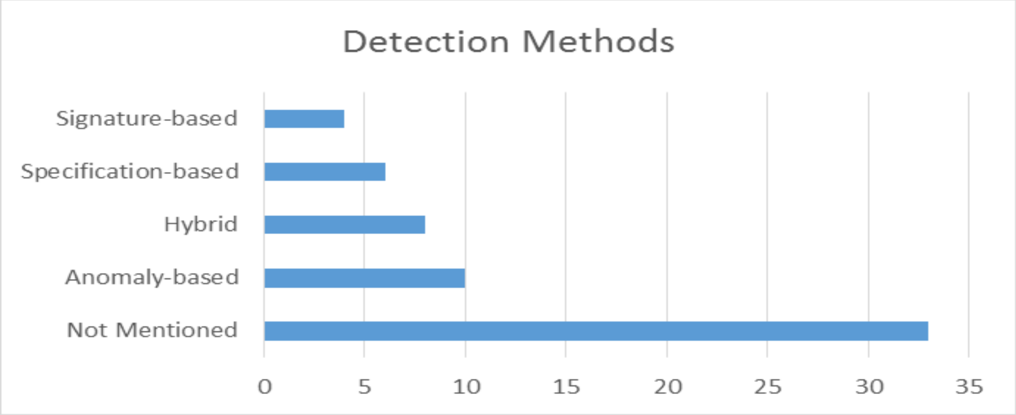

Figure 5: Detection methods

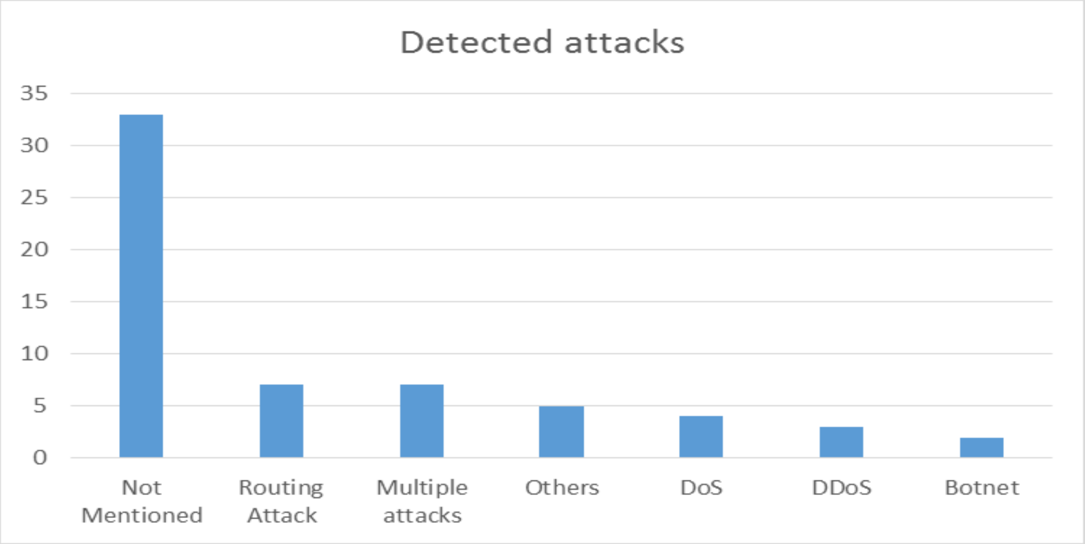

Figure 6: Detected attacks

very strong model due to the large number of computing nodes and the number of detectors and their distributed architecture, however, it has disadvantages such as the possibility of autoimmune reaction, and difficulty in detecting new attacks. Another technique proposed in [26] is the Complex Event Processing technique, CEP, which is a computer science concept that allows the discovery of complex events through the analysis, deduction, and correlation of elementary events. Systems based on the CEP technique enable collecting information in real time and these systems can also evolve quickly. However, the difficulty of implementing these systems in complex cases remains a weakness of systems based on this technique. The researchers in the article [27] propose an IDS with the idea of monitoring the energy consumption in each node of the network. When the normal consumption value of a node changes, the IDS detects this node as a node malicious and removes it from the routing table in 6LowPAN. This idea may be considered innovative, but this solution may only be valid for attacks based on the amount of data traffic. Among other techniques, we have the heuristic model proposed in [39]. The heuristic model is a problem-solving methodology based on practical knowledge experience (quick solution). We can cite two main advantages of Heuristic models. The first advantage is the speed of finding a solution whereas the second is the use of minimal memory space by these models. On the other hand, among the disadvantages of the Heuristic model is that the solution proposed by a Heuristic algorithm is not always optimal, and it faces difficulty in solving new problems.

By comparing our work with similar works mentioned in the “Related works” section. Firstly, we find that the study on the Internet of Things and the attacks on this technology are more profound than the other articles and the presented taxonomy of Intrusion Detection Systems is more detailed. Second, our state-of-the-art contains a significant number of works which amounts to 60 articles and were published between 2009 and 2023 in indexed journals, and according to our knowledge, no other article does this type of work by this volume in this field. Third, we presented a state-of-the-art that contains a detailed analysis of all the articles collected (summary of each article, the detection methods, the attacks detected, etc.) and contains a discussion of the existing problems and the limitations of the suggested solutions. Moreover, we presented some important open research issues for the future researches.

6. PROBLEMS AND OPEN RESEARCH

Several researchers in cybersecurity have started in recent years to try to present security solutions for Internet of Things technology and among the techniques most adapted by researchers is Intrusion Detection Systems. Since 2009, several scientific works have been published to increase the effectiveness of Intrusion Detection Systems for the Internet of Things. Despite all this, and according to our work, we have found that several problems still exist. Among these problems we mention firstly centralization, that is to say, we find that all the tasks of an IDS are centralized in a single node, and this has an impact on the consumption of system resources and needs more time to perform the detection. Second, most existing IDSs detect only one type of attack and familiar attacks. Finally, Real-time problems, the existing IDS solutions do not detect malicious Events in real time which implies the non-applicable IDS.

The problems cited above have provided insights into new avenues of research in the field of Internet of Things security. We will, in what follows, list some open research issues:

Distribution: among the points that can be addressed in future work is the distribution of IDS solutions for networks and IoT applications, because distributed solutions can give good detection time and can also reduce resource consumption. Among the technologies that can be integrated in IDSs to resolve the problems of centralization, we mention Blockchain and Multi-Agent Systems.

Real-Time: Such IDSs must monitor, collect, and analyze data traffic in real time, and minimizing detection time is one of the main points to be resolved to present effective and applicable IDSs in IoT networks.

New Attacks Detection: the operation of detecting known attacks is generally easy. The difficulty or challenge for IDSs in recent years is to detect new attacks and to achieve this goal, the techniques of artificial intelligence can be effective.

7. CONCLUSION

The security of the Internet of Things is a major point for the confidential and sustainable use of this technology in various fields. Among the security techniques used to secure the Internet of Things are intrusion detection systems. In this article, we presented a taxonomy of IDSs, the architecture of IoT, the threats against IoT, and a detailed state of the art on the use of IDSs for securing networks and

IoT applications. This work is considered a starting point to understand the existing solutions and their limitations to present more effective solutions. Our future work will focus on the integration of Machine Learning techniques and distributed artificial intelligence into IDS solutions to secure IoT networks and applications.

REFERENCES

[1] https://www.techopedia.com
[2] https://searchsecurity.techtarget.com
[3] Mr Mohit Tiwari, Raj Kumar, Akash Bharti, Jai Kishan, "Intrusion detection system", International Journal of Technical Research and Applications, Volume 5, Issue 2, 2017, pp. 38-44.
[4] Al-Sakib Khan Pathan, "The state of the art in intrusion prevention and detection", Auerbach Publications, CRC Press, 2014.
[5] Leonel Santos, Carlos Rabadão, Ramiro Gonçalves, "Intrusion detection systems in internet of things A literature review", Proceedings of the 13th Iberian Conference on Information Systems and Technologies (CISTI), IEEE Xplore, 13-16 June, 2018, pp. 1-7.
[6] Rwan Mahmoud, Tasneem Yousuf, Fadi Aloul, Imran Zualkernan, "Internet of things (IoT) security: current status, challenges and prospective measures", International Journal for Information Security Research (IJISR), Volume 5, Issue 4, 2015, pp. 608-616.
[7] Wazir Zada Khana, Yang Xiangb, Mohammed Y Aalsalema, and Quratulain Arshad, "The selective forwarding attack in sensor networks: detections and countermeasures", I.J. Wireless and Microwave Technologies, Vol. 2012, No. 2, 2012, pp. 33-44.
[8] Camilius Sanga, George W. Kibirige, "A survey on detection of sinkhole attack in wireless sensor network", International Journal of Computer Science and Information Security, 2015, pp. 1-9.
[9] Junaid Arshad, Muhammad Ajmal Azad, Khaled Salah, Wei Jie, Razi Iqbal, Mamoun Alazab, "A review of performance, energy and privacy of intrusion detection systems for IoT", Electronics, Volume 9, Issue 4, 2020, pp. 1-24.
[10] Tariqahmad Sherasiya, Hardik Upadhyay and Hiren B Patel, "A survey: intrusion detection system for internet of things", International Journal of Computer Science and Engineering (IJCSE), Vol. 5, Issue 2, 2016, pp. 91-98.
[11] Bruno Bogaz Zarpelão, Rodrigo Sanches Miani, Cláudio Toshio Kawakani, Sean Carlisto de Alvarenga, "A survey of intrusion detection in internet of things", Journal of Network and Computer Applications, Volume 84, 2017, pp. 25-37.
[12] Leonel Santos, Carlos Rabadão, Ramiro Gonçalves, "Intrusion detection systems in internet of things A literature review", Proceedings of the 13th Iberian Conference on Information Systems and Technologies (CISTI), IEEE Xplore, 13-16 June, 2018, pp. 1-7.
[13] Somayye Hajiheidari, Karzan Wakil, Maryam Badri and Nima Jafari Navimipour,"Intrusion detection systems in the internet of things: A comprehensive investigation", Computer Networks, Vol. 160, 2019, pp. 165-191.
[14] Sarika Choudhary and Nishtha Kesswani, "A survey: intrusion detection techniques for internet of things", International Journal of Information Security and Privacy, Vol. 13, Issue. 1, 2019, pp. 86-105.
[15] Eung Jun Cho, Jin Ho Kim, and Choong Seon Hong, "Attack model and detection scheme for botnet on 6LoWPAN", Management Enabling the Future Internet for Changing Business and New Computing Services, Lecture Notes in Computer Science, Vol 5787, 2009, pp. 515–518.
[16] Anhtuan Le, Jonathan Loo, Yuan Luo, and Aboubaker Lasebae, "Specification-based IDS for securing RPL from topology attack", Proceedings of the IFIP Wireless Days (WD), Niagara Falls, ON, Canada, 2011, PP. 1-3.
[17] Caiming Liu, Jin Yang, Run Chen, Yan Zhang, Jinquan Zeng, "Research on immunity-based intrusion detection technology for the internet of things", Proceedings of the Seventh International Conference on Natural Computation, Shanghai, China, 2011, pp. 212-216.
[18] Sudip Misra, P. Venkata Krishna, Harshit Agarwal, Antriksh Saxena, Mohammad S. Obaidat, "A Learning automata based solution for preventing distributed denial of service in internet of things", Proceedings of the International Conference on Internet of Things and 4th International Conference on Cyber, Physical and Social Computing, Dalian, China, 2011, pp. 114-122.
[19] Abhishek Gupta, Om Jee Pandey, Mahendra Shukla, Anjali Dadhich, Samar Mathur, and Anup Ingle, "Computational intelligence based intrusion detection systems for wireless communication and pervasive computing networks", Proceedings of the IEEE

International Conference on Computational Intelligence and Computing Research, Enathi, India, 2013, pp. 1-7.

[20] Prabhakaran Kasinathan, Claudio Pastrone, Maurizio A. Spirito, and Mark Vinkovits "Denial-of-service detection in 6LoWPAN based internet of things" Proceedings of the IEEE 9th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Lyon, France, 2013, pp. 600-607.

[21] Prabhakaran Kasinathan, Gianfranco Costamagna, Hussein Khaleel, Claudio Pastrone, Maurizio A. Spirito, "DEMO: An IDS framework for internet of things empowered by 6LoWPAN", Proceedings of the ACM SIGSAC conference on Computer & communications security (CCS '13), 2013, pp. 1337–1340.

[22] Shahid Raza, Linus Wallgren, and Thiemo Voigt, "SVELTE: Real-time intrusion detection in the internet of things", Ad Hoc Networks, Volume 11, Issue 8, 2013, pp. 2661-2674.

[23] Linus Wallgren, Shahid Raza, and Thiemo Voigt, "Routing attacks and countermeasures in the RPL-Based internet of things", International Journal of Distributed Sensor Networks, Vol 9, Issue 8, 2013, pp. 1-11.

[24] João P. Amaral, Luís M. Oliveira, Joel J. P. C. Rodrigues, Guangjie Han, and Lei Shu, "Policy and network-based intrusion detection system for IPv6-enabled wireless sensor networks", Proceedings of the IEEE International Conference on Communications (ICC), Sydney, NSW, Australia, 2014, pp. 1796-1801.

[25] Jana Krimmling, Steffen Peter, "Integration and evaluation of intrusion detection for CoAP in smart city applications", Proceedings of the IEEE Conference on Communications and Network Security, San Francisco, CA, USA, 2014, pp. 73-78.

[26] Chen Jun, Chen chi, "Design of complex event-processing IDS in internet of things" Proceedings of the Sixth International Conference on Measuring Technology and Mechatronics Automation, Zhangjiajie, China, 2014, pp. 226-229.

[27] Tsung-Han Lee, Chih-Hao Wen, Lin-Huang Chang, Hung-Shiou Chiang and Ming-Chun Hsieh, "A lightweight intrusion detection scheme based on energy consumption analysis in 6LowPAN", Proceedings of the Advanced Technologies, Embedded and Multimedia for Human-centric Computing, Lecture Notes in Electrical Engineering, vol 260, 2014, pp. 1205–1213.

[28] Doohwan Oh, Deokho Kim and Won Woo Ro, "A malicious pattern detection engine for embedded security systems in the internet of things", sensors, Vol 14, Issue 12, 2014, pp. 24188-24211.

[29] Christian Cervantes, Diego Poplade, Michele Nogueira and Aldri Santos, "Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for internet of things", Proceedings of the IFIP/IEEE International Symposium on Integrated Network Management (IM), Ottawa, ON, Canada, 2015, pp. 606-611.

[30] Pavan Pongle Gurunath Chavan, "Real time intrusion and wormhole attack detection in internet of things", International Journal of Computer Applications, Vol 121, Issue 9, 2015, pp.1-9.

[31] Douglas H. Summerville, Kenneth M. Zach and Yu Chen, "Ultra-lightweight deep packet anomaly detection for internet of things devices", Proceedings of the IEEE 34th International Performance Computing and Communications Conference (IPCCC), Nanjing, China, 2015, pp. 1-8.

[32] Anhtuan Le, Jonathan Loo, Kok Keong Chai, and Mahdi Aiash, "A specification-based IDS for detecting attacks on RPL-Based network topology", Information, Vol 7, Issue 2, 2016, pp. 1-19.

[33] Nanda Kumar Thanigaivelan, Ethiopia Nigussie, Rajeev Kumar Kanth, Seppo Virtanen and Jouni Isoaho, "Distributed internal anomaly detection system for internet-of-things" Proceedings of the 13th IEEE Annual Consumer Communications & Networking Conference (CCNC), Las Vegas, NV, USA, 2016, pp. 319-320.

[34] Daniele Midi, Antonino Rullo, Anand Mudgerikar, Elisa Bertino, "Kalis - A system for knowledge-driven adaptable intrusion detection for the internet of things", Proceedings of the IEEE 37th International Conference on Distributed Computing Systems, Atlanta, GA, USA, 2017, pp. 656-666.

[35] Dharmini Shreenivas, Shahid Raza, and Thiemo Voigt, "Intrusion detection in the RPL-connected 6LoWPAN networks", Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security (IoTPTS '17), Association for Computing Machinery, New York, NY, USA, 2017, pp. 31–38.

[36] M. Jagadeesh Babu, A. R Reddy, "Intrusion detection in internet of things: The review of taxonomy", International Journal of Applied Engineering Research, Volume 13, Issue 16, 2018, pp. 12805-12812.

[37] Subir Halder, Amrita Ghosal and Mauro Conti, "Efficient physical intrusion detection in internet of things: A Node Deployment Approach", The International Journal of Computer and Telecommunications Networking, Volume 154, Issue C, 2019, pp. 28–46.

[38] Sana Ullah Jan, Saeed Ahmed, Vladimir Shakov and Insoo Koo, "Toward a lightweight intrusion detection system for the internet of things", IEEE Access, Vol 7, 2019, pp. 42450-42471.

[39] Ayyaz-ul-Haq Qureshi, Hadi Larijani, Jawad Ahmad, and Nhamoinesu Mtetwa, "A heuristic intrusion detection system for internet-of-things (IoT)", Proceedings of the Computing Conference, Advances in Intelligent Systems and Computing book series, Vol 997, 2019, pp. 86-98.

[40] Ansam Khraisat, Iqbal Gondal, Peter Vamplew, Joarder Kamruzzaman and Ammar Alazab, "A novel ensemble of hybrid intrusion detection system for detecting internet of things attacks", Electronics, Vol 8, Issue 11, 2019, pp. 1-18.

[41] Sarika Choudhary, Nishtha Kesswani, "A survey: Intrusion detection techniques for internet of things", International Journal of Information Security and Privacy, Vol 13, Issue 1, 2019, pp. 86-105.

[42] Somayye Hajiheidari, Karzan Wakil, Maryam Badri, Nima Jafari Navimipour, "Intrusion detection systems in the internet of things: A comprehensive investigation", The International Journal of Computer and Telecommunications Networking, Vol 160, Issue C, 2019, pp. 165–191.

[43] Abhishek Verma, Virender Ranga, "ELNIDS: Ensemble learning based network intrusion detection system for RPL based internet of things", Proceedings of the 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019, pp. 1-6.

[44] A. Yang, Y. Zhuansun, C. Liu, J. Li and C. Zhang, "Design of Intrusion Detection System for Internet of Things Based on Improved BP Neural Network", IEEE Access, vol 7, 2019, pp. 106043-106052.

[45] M.Bhargavi, M.Nandha Kumar, N. Venkata Meenakshi, and N.Lasya, "Intrusion detection techniques used for internet of things", International Journal of Applied Engineering Research, Volume 14, 2019, pp. 4462-4466.

[46] Snehal Deshmukh-Bhosale, Santosh S. Sonavane, "A real-time intrusion detection system for wormhole attack in the RPL based internet of things", Procedia Manufacturing, Volume 32, 2019, pp. 840-847.

[47] Zeeshan Ali Khan and Peter Herrmann, "Recent advancements in intrusion detection systems for the internet of things", Hindawi, Security and Communication Networks, Volume 2019, 2019, pp. 1-19.

[48] S. Smys, Abul Basar, Haoxiang Wang, "Hybrid intrusion detection system for internet of things (IoT)", Journal of IoT in Social, Mobile, Analytics, and Cloud (ISMAC), Volume 4, Issue 2, 2020, pp. 190-199.

[49] Bacem Mbarek, Mouzhi Ge, Tomás Pitner, "Enhanced network intrusion detection system protocol for internet of things", Proceedings of the 35th ACM/SIGAPP Symposium on Applied Computing, 2020, pp. 1156-1163.

[50] Chao Liang, Bharanidharan Shanmugam, Sami Azam, Asif Karim, Ashraful Islam, Mazdak Zamani, Sanaz Kavianpour and Norbik Bashah Idris, "Intrusion detection system for the internet of things based on blockchain and multi-agent systems", Electronics, Vol 9, Issue 7, 2020, pp. 1-27.

[51] Anamika Chauhan, Rajyavardhan Singh and Pratyush Jain, "A literature review: Intrusion detection systems in internet of things", Journal of Physics Conference Series, Vol 1518, Issue 1, 2020, pp. 1-9.

[52] Leonel Santos, Ramiro Gonçalves, Carlos Rabadao, José Martins, "A flow-based intrusion detection framework for internet of things networks", Cluster Computing, Vol 26, 2021, pp. 37–57.

[53] Yazan Otoum, Amiya Nayak, "AS IDS: Anomaly and signature based IDS for the internet of things", Journal of Network and Systems Management, Vol 29, Issue 23, 2020, pp. 1-26.

[54] Rasheed Ahmad, Izzat Alsmadi, Wasim Alhamdani, Lo'ai Tawalbeh, "Towards building data analytics benchmarks for IoT intrusion detection", Cluster Computing, Vol 25, Issue 3, 2021, pp. 2125–2141.

[55] Pushparaj Nimbalkar, Deepak Kshisagar, "Feature selection for intrusion detection

system in internet-of-things (IoT)", ICT Express, Volume 7, Issue 2, 2021, pp. 177-181.

[56] Ansam Khraisat, Ammar Alazab, "A critical review of intrusion detection systems in the internet of things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges", Cybersecurity, Vol 4, Issue 18, 2021, pp. 1-27.

[57] Abdelwahed Berguiga, Ahlem Harchay, "An IoT-based intrusion detection system approach for TCP SYN attacks", Computers, Materials & Continua, Vol 71, Issue 2, 2022, pp. 3839-3851.

[58] Vasaki Ponnusamy, Mamoona Humayun, N. Z. Jhanjhi, Aun Yichiet and Maram Fahhad Almufareh, "Intrusion detection systems in internet of things and Mobile Ad-Hoc Networks", Computer Systems Science and Engineering, Vol 40, Issue 3, 2022, pp. 1199-1215.

[59] Nguyen Dat-Thinh, Ho Xuan-Ninh and Le Kim-Hung, "MidSiot: A multistage intrusion detection system for internet of things", Wireless Communications and Mobile Computing, Vol 2022, Issue 4, 2022, pp. 1-15.

[60] Xuan-Ha Nguyen, Xuan-Duong Nguyen, Hoang-Hai Huynh and Kim-Hung Le, "Realguard: A lightweight network intrusion detection system for IoT gateways", Sensors, Vol 22, Issue 2, 2022, pp. 1-18.

[61] A. Arul Anitha, L. Arockiam, "A review on intrusion detection systems to secure IoT networks", International Journal of Computer Networks and Applications (IJCNA), Volume 9, Issue 1, 2022, pp. 38-50.

[62] Guosheng Zhao, Yang Wang, and Jian Wang, "Lightweight intrusion detection model of the internet of things with hybrid cloud-fog computing", Security and Communication Networks, Volume 2023, 2023, pp. 1-16.

[63] Junxiang Chen, Jilin Zhang, Ruixiang Qian, Junfeng Yuan, and Yongjian Ren, "An anomaly detection method for wireless sensor networks based on the improved isolation forest", Applied Sciences, Volume 13, Issue 2, 2023, pp. 1-18.

[64] Marta Catillo, Antonio Pecchia and Umberto Villano, "A deep learning method for lightweight and cross device IoT botnet detection", Applied Sciences, Volume 13, Issue 2, 2023, pp. 1-21.

[65] Firas Mohammed Aswad, Ali Mohammed Saleh Ahmed, Nafea Ali Majeed Alhammadi, Bashar Ahmad Khalaf, and Salama A. Mostafa, "Deep learning in distributed denial-of-service attacks detection method for internet of things networks", Journal of Intelligent Systems, Vol 32, Issue 1, 2023, pp. 20220155.

[66] Rajasekhar Chaganti, Wael Suliman, Vinayakumar Ravi, and Amit Dua, "Deep learning approach for SDN-Enabled intrusion detection system in IoT networks", Information, Vol 14, Issue 1, 2023, pp. 1-21.

[67] Harshit Shah, Dhruvil Shah, Nilesh Kumar Jadav, Rajesh Gupta, Sudeep Tanwar, Osama Alfarraj, Amr Tolba, Maria Simona Raboaca, and Verdes Marina, "Deep learning-based malicious smart contract and intrusion detection system for IoT environment", Mathematics, Vol 11, Issue 2, 2023, pp. 1-22.

[68] Shalaka Mahadik, Pranav M. Pawar, Raja Muthalagu, "Efficient intelligent intrusion detection system for heterogeneous internet of things (HetIoT)", Journal of Network and Systems Management, Volume 31, Issue 2, 2023, pp. 1-27.

[69] Emad Hmood Salman, Montadar Abas Taher, Yousif I. Hammadi, Omar Abdulkareem Mahmood, Ammar Muthanna and Andrey Koucheryavy, "An anomaly intrusion detection for high-density internet of things wireless communication network based deep learning algorithms", Sensors, Vol 23, Issue 1, 2023, pp. 1-14.

[70] Razvan Bocu and Maksim Iavich, "Real-time intrusion detection and prevention system for 5G and beyond software-defined networks", Symmetry, Volume 15, Issue 1, 2023, pp. 1-15.

[71] Ogobuchi Daniel Okey, Dick Carrilo Melgarejo, Muhammed Saadi, Renata Lopes Rosa, Joâo Henrique Kleinschmidt and Demostenes Zegarra Rodrîguez, "Transfer learning approach to IDS on cloud IoT devices using optimized CNN", IEEE Access, Vol 11, 2023, pp. 1023-1038.

[72] Mudhafar Nuaimi, Lamia Chaari Fourati, Bassem Ben Hamed, "Intelligent approaches toward intrusion detection systems for Industrial internet of things: A systematic comprehensive review", Journal of Network and Computer Applications, Volume 215, 2023, pp. 103637.

[73] Salaheddine Kably, Tajeddine Benbarrad, Nabih Alaoui and Mounir Arioua, "Multi-zone-wise blockchain based intrusion detection and prevention system for IoT environment", Computers Materials & Continua, Vol 74, Issue 1, 2023, pp. 253-278.

[74] Rasha Almarshdi, Laila Nassef, Etimad Fadel and Nahed Alowidi, "Hybrid deep learning

based attack detection for imbalanced data classification", Intelligent Automation & Soft Computing, Vol 35, Issue 1, 2023, pp. 297-320.

[75] Fatma S. Alrayes, Nuha Alshuqayran, Mohamed K Nour, Mesfer Al Duhayyim, Abdullah Mohamed, Amgad Atta Abdelmageed Mohammed, Gouse Pasha Mohammed and Ishfaq Yaseen, "optimal fuzzy logic enabled intrusion detection for secure IoT-cloud environment", Computers, Materials & Continua, Volume 74, Issue 3, 2023, pp. 6737-6753.