REVIEW ARTICLE

# A Review on Intrusion Detection Systems to Secure IoT Networks

A. Arul Anitha
Department of Computer Science, St. Joseph’s College (Autonomous) (Affiliated to Bharathidasan University),
Tiruchirappalli, Tamil Nadu, India
arulanita@gmail.com

L. Arockiam
Department of Computer Science, St. Joseph’s College (Autonomous) (Affiliated to Bharathidasan University),
Tiruchirappalli, Tamil Nadu, India
larockiam@yahoo.co.in

Received: 23 November 2021 / Revised: 08 January 2022 / Accepted: 13 January 2022 / Published: 28 February 2022

**Abstract – The Internet of Things (IoT) and its rapid advancements will lead to everything being connected in the near future. The number of devices connected to the global network is increasing every day. IoT security challenges arise as a result of the large-scale incorporation of smart devices. Security issues on the Internet of Things have been the most focused area of research over the last decade. As IoT devices have less memory, processing capacity, and power consumption, the traditional security mechanisms are not suitable for IoT. A security mechanism called an Intrusion Detection System (IDS) has a crucial role in protecting the IoT nodes and networks. The lightweight nature of IoT nodes should be considered while designing IDS for the IoT. In this paper, the types of IDS, the major attacks on IoT, the recent research, and contributions to IDS in IoT networks are discussed, and an analytical survey is given based on the study. Though it is a promising area for research, IDS still needs further refinement to ensure high security for IoT networks and devices. Hence, further research, development, and lightweight mechanisms are required for IDS to provide a higher level of security to the resource-limited IoT network.**

**Index Terms – Attack, IoT, Intrusion, IDS, RPL, Security.**

## 1. INTRODUCTION

The Internet of Things (IoT) is a robustly evolving trend that incorporates technical, scientific, social, and economic implications. It is essential to all facets of human life [1]. Healthcare, logistics, smart-cities, smart-homes, and agriculture are just a few of the applications for IoT. Due to its resource-constrained characteristics, the IoT tends to have more vulnerability that can be easily exploited by an attacker. The number of connected unsecured IoT devices on the global network is rapidly increasing [2]. Researchers are mainly focusing on various encryption and authentication mechanisms to ensure data confidentiality, authentication, and privacy among users and things. Most of the IoT devices have been developed without considering the fundamental security requirements [3].

The tools and techniques available for securing the IoT are inadequate because of the large number of interconnected devices. Moreover, the security mechanisms based on cryptography are mainly used to prevent external attacks such as eavesdropping and message alternation. When the cryptographic techniques hold the valid key and are compromised by the attack, they cannot detect the vulnerable nodes. Intruders can easily access the security details from the compromised nodes and immediately launch several internal attacks. Hence, to offer an extra level of security to the IoT, the Intrusion Detection System (IDS) acts as a tool [4].

Anthea Mayzaud et al. [5] categorized the Routing Protocol for Low Power Lossy Networks (RPL) attacks into three types: attacks targeting the topology, attacks on network resources, and attacks targeting the network traffic. Attacks on resources require more of the restricted devices' resources like processing requirements, power, and memory; attacks on topology induce isolation and sub-optimization in the topology, and attacks on traffic create security risks from the network's traffic. All these types of attacks have negative impacts on the RPL based IoT network. These attacks have to be detected and mitigated to ensure the security constraints of the IoT networks.

Intrusion Detection is an act of monitoring and possibly preventing the malicious activities of the intruders. Intrusion Detection System is a network security tool that consists of software or a combination of hardware and software to protect the traditional networks. It can be used to monitor all sorts of activities in the network. If there is any attack or unwanted activity in the network, the IDS detects the intrusions, alerts the administrator, logs the attacks for forensic activities, isolates the intruder, and also disconnects the connection path of the intruder [6]. The functionalities of Intrusion Detection System are illustrated in Figure 1.

As it is given in Figure 1, the IDS can monitor, analyse, assess, track, alert and mitigate attacks in IoT networks. IDSs are at a mature level in the traditional networks. Since IDS consumes more memory, processing capability and energy, the IDSs that are technologically advanced for the traditional and wireless networks are not suitable for IoT. Because of these constraints, finding IoT nodes with higher computing capability to support IDS agents is very difficult. So, there is a need for modelling lightweight IDS to adapt to the IoT constraints. The Figure 2 illustrates the typical centralized IDS for IoT networks.

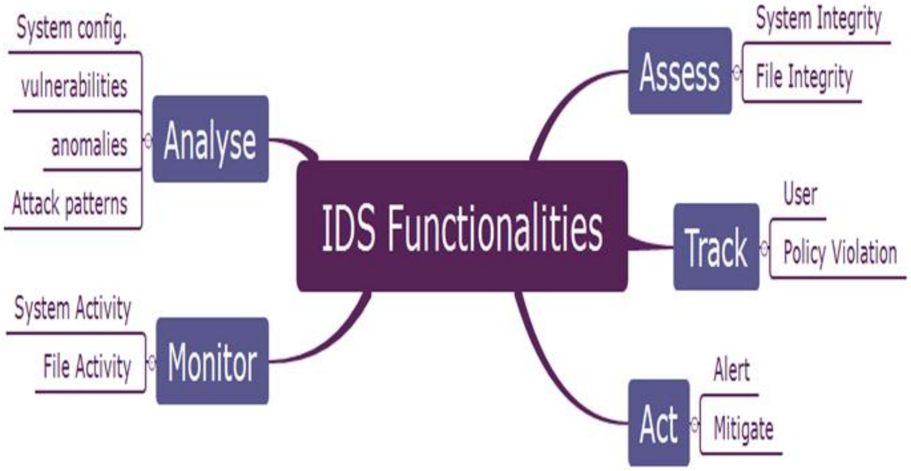

Figure 1 Functionalities of IDS

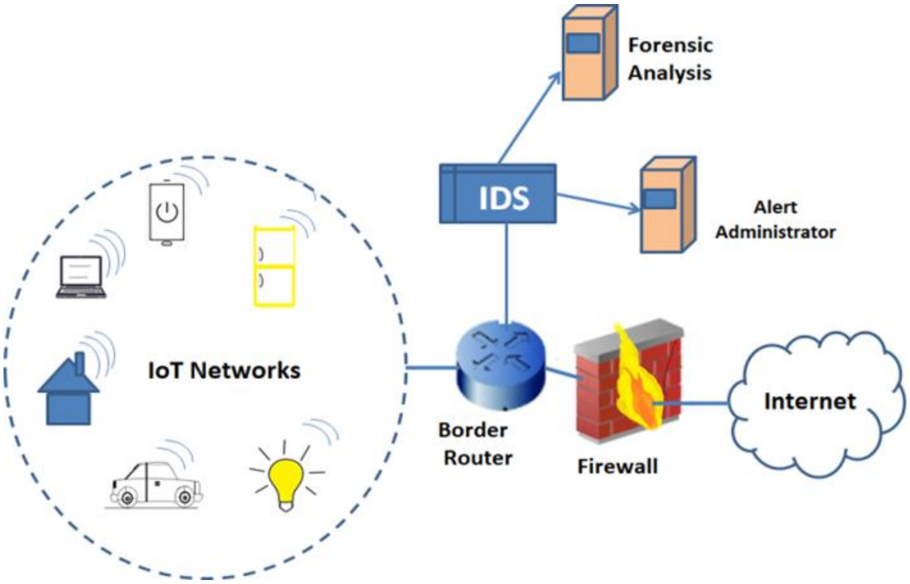

Figure 2 A Typical IDS for Internet of Things

Here, the smart gadgets are linked to the Internet through the gateway device called border router. As the Figure 2 indicates, the IDS tool is implemented in the gateway device. It monitors all IoT network-related activities and, whenever an intrusion arises, the IDS will alert the administrator. It also logs the events for forensic analysis.

### 1.1. Objectives

The major aim of this paper is to explore systematically the IDSs that are available for protecting the IoT networks. The objectives are listed below.

- To analyse the need for IDS in securing the IoT networks,

- To explore the different types of existing IDS for IoT,
- To discuss the issues and challenges that direct to future research,
- To provide an analytical survey of the reviewed IDSs.

This paper is structured as follows: The section 2 discusses the recent IDS research in the IoT; section 3 explains the different types of attacks in IoT environment; section 4 describes the types of IDSs for IoT based on the placement strategy and technologies implemented; section 5 summarizes the reviewed works as an analytical survey; section 6 points out some issues and challenges while implementing the IDS in IoT environment and finally conclusion is presented in section 7.

## 2. LITERATURE REVIEW

The literature related to the security challenges of IoT and the IDS available for detecting malicious events/and attacks are presented below.

### 2.1. IoT and Security

In their article, Patel and Patel [7] discussed the definition, characteristics, technologies, architecture, and applications of IoT and also highlighted research issues and challenges regarding security, interoperability, data management, and energy issues in a nutshell. According to their survey, security and privacy issues are the most challenging tasks in the IoT. Among all the security issues, secure data communication and the quality of shared data are the predominant issues to be considered for research.

Adat and Gupta [8] conducted a thorough examination of the evolution of the Internet of Things, related works, IoT statistics, IoT architecture, and security concerns. The authors provided a set of layer-wise security challenges and security requirements for the IoT architecture. They also presented a classification of security issues and existing defence mechanisms for the IoT environment. As per the paper, network security issues and attacks cause more damage to the IoT eco-system.

Tewari, and Gupta [9] provided an overview of the security challenges associated with the IoT layered architecture. The security issues in traditional networks and IoT networks are compared and discussed. Heterogeneous integration of cross layers and their associated challenges are also analysed in this paper, and some future directions are highlighted. Though the aim of the paper is to present the security and privacy issues of the IoT, they have not been given much focus in this paper.

Sahay et al. [10] suggested an Attack Graph for identifying the susceptibilities of the rank of nodes. By mistreating these vulnerabilities, an intruder could invoke several attacks, compromising network traffic, optimizing and isolating the network, and consuming more resources. The impact of the attacks was claimed only by using some qualitative measures. The results are not quantified.

Based on the IoT architecture and layers, Deogirikar and Vidhate [11] classified all possible attacks related to IoT into physical layer-related attacks, network layer-related attacks, software-related attacks, and encryption-related attacks. A comparative analysis was also performed based on the harmful effects of the attacks, possibilities for detection, vulnerability, and location of the attacks. The layer-wise attacks and advantages and disadvantages of the attack detection techniques were also discussed elaborately. Security solutions are not considered in this paper.

Sfar et al. [12] offered an overview of the IoT security roadmap based on a systematic and cognitive approach. A case study is also given to explain this approach. Various research challenges are also classified based on access control, privacy, trust, and identification. The classified elements were not explained in this paper.

### 2.2. IDS for Internet of Things

Hemdan and Manjaiah [13] described how IoT and IDS are useful in cybercrime investigation, as well as how to use IDS data to analyse criminal behaviour and make decisions based on the findings. Here, the authors have explained only their theoretical views and ideas.

Fu et al. [14] proposed an innovative idea for IDS using Automata. The evaluation of this IDS was performed on a Raspberry Pi device with the help of an Android mobile phone. This IDS successfully detected the jam-attack, false-attack, and replay-attack. This Intrusion Detection System detected only these three types of attacks. Some problems may also arise while running the system out of resources.

Raza et al. [15] offered Hybrid-IDS suitable for the IoT environment to detect real-time sinkhole and selective forward attacks. It was named ‘SVELTE’. The authors attempted to improve performance in this study by balancing the costs associated with signature and anomaly-based IDS. In SVELTE, the border router processes intensive IDS modules by analysing the network data. The IoT devices are accountable for transmitting the data to the border router and alerting the router about the abnormal data they receive. Periodic updating of the database is required in order to make the IDS relevant to the current attack patterns.

The above work was extended by Shreenivas et al. [16] by including an IDS module that uses a metric called Expected Transmission Count (ETX) of RPL networks. They suggested the intruders’ activities in the 6LoWPAN network can be prevented and the location of the attacker nodes can be identified by monitoring the ETX metric. The true-positive rate is increased in their work by combining the ETX based rank mechanism with the rank-only approaches. Since there is an additional ETX module in this work, it requires more storage and computational overhead.

Mbarek et al. [17)] presented an Enhanced Network IDS protocol for the Internet of Things (ENIDS) to detect the clone attack. This protocol was evaluated with the performance of SVELTE and outperformed in terms of detection probability and energy consumption. This ENIDS is limited to clone attacks, and in the normal scenario it consumes more energy.

Ioulianou et al. [18] offered a Hybrid IDS using signature-based concepts for IoT architecture. Using the Version Number modification and 'hello-flood' attacks, a Denial of Service (DoS) attack was launched. The impact of the attacks was analyzed in terms of battery-power usage and reachability of nodes. The Intrusion Detection functionalities are not taken into account in this research work.

All possible attacks in the IoT environment are either passive or active. Passive attacks simply monitor the system activities and data traffic and eavesdrop to recover information. They are less dangerous and cause less damage to IoT devices and networks. Active attacks are dissimilar to passive attacks, and these attacks cause damage to the IoT infrastructure directly [19]. These attacks can circumvent smart devices and the IoT ecosystem, resulting in the loss of valuable data.

Using the IoT reference model, Abdul-Ghani et al. [20] conducted a thorough investigation on IoT attacks. Physical, protocol, data, and software attacks against IoT networks were characterised by the researchers. A detailed description of all conceivable attacks in these areas is provided. This article does not go through the security solutions. A summary of current research on security threats on IoT networks was provided by Lu and Xu [21]. Based on IoT devices, device location, access level, data damage degree, node capacity, and protocol, they created a taxonomy of cyber security attacks on IoT networks. They also eloborated the four-layer security architecture for IoT. The attacks on each layer, and the security solutions however, are not described in depth.

Ramakrishna et al. [22] conducted an analytical assessment on various forms of IoT threats and their security solutions. Physical, side-channel, cryptanalysis, software-based, and network-based attacks were all identified as IoT security attacks in this study.This paper only looked at a few attacks from each category, as well as available countermeasures.

### 2.3. Machine Learning and Deep Learning based IDS

For the Wireless Sensor Networks (WSN) nodes with low resources, Qu et al. [23] proposed a lightweight, fuzzy clustering-based Intrusion Detection System. The sensor data collected at the base stations were used to map the network state. To build this system, the authors combined the sliding window technique with fuzzy c-means and one-class SVM. This system was capable of quickly detecting the assaults. The EXata Network Simulator was used to test the system's efficacy. Although it is capable of identifying and detecting communication-destructive assaults, it might be enhanced in terms of recognising multiple attacks.

In a comparative study, Biswas [24] explained various feature selection techniques and machine learning classifiers for developing IDS. The classifiers used in this research are Decision Tree (DT), K-Nearest Neighbor (KNN), Support Vector Machine (SVM), Naive Bayes (NB), and Neural Networks (NN). The Correlation-based Feature Selection method (CFS), Information Gain Ratio (IGR), Minimum Redundancy Maximum Relevance method, and Principal Component Analysis (PCA) feature selection techniques were evaluated. The NSL-KDD dataset with 10,000 tuples with 40 attributes was used for this analysis. According to this study, K-NN (K-Nearest Neighbor) and information gain ratio-based feature selection (GIR) provided a better result. The NSL-KDD is one of the very old datasets for intrusion detection, so it is not suitable for IoT.

Using the AdaBoost ensemble approach, Moustafa et al. [25] created an IDS for detecting intrusions in IoT networks. To improve performance, ensemble models are created by integrating numerous classifiers. Three classifiers, namely Artificial Neural Network (ANN), Naive Bayes (NB), and Decision Tree (DT), are merged in an ensemble technique to produce this model.The botnet was mostly identified using this strategy against application layer protocols. It's also confined to the three protocols, and should be extended to include features from more IoT protocols.

Jan et al. [26] proposed a lightweight IDS based on an SVM classifier to detect attempts to inject unnecessary data into IoT networks. The packet arrival rate's Poisson distribution was used to differentiate the packets as benign or intrusive. A subset of the CICID2017 dataset was selected, obtaining a synchronized beget dataset from that subset, which was further utilized in this research. The packet arrival rate is the only attribute considered in this experiment. It supports the lightweight aspect of IDS, but only a single attribute from a huge dataset will not detect all possible attacks.

Eskandari et al. [27] suggested an anomaly-based IDS termed Passban IDS for detecting intrusions at the edge level based on security attacks. Real-time network traffic was gathered to detect the attacks, and the iForest ensemble technique was used in this methodology. This Passban IDS detected the port scanning, brute force attacks, and SYN flooding attacks. The attacks during the training phase were not considered in this research. The SYN Flood attacks in this work will consume more resources and will reduce the detection accuracy of the Passban IDS.

Alkadi et al. [28] recommended distributed IDS using Deep Blockchain technology and Bidirectional Long Short-Term Memory (BiLSTM). This system detected the DoS, DDoS, port scanning, and other attacks in UNSW-NB15 and BoT-IoT datasets effectively. It is suitable for IoT and cloud architecture. For real-world implementation, it requires further fine-tuning. The UNSW-NB15 dataset used in this research was not specific to IoT.

Cheema et al. [29] introduced a Blockchain based IDS for IoT using Machine Learning Algorithms. The IoT network is divided into number of Autonomous Systems (AS). The selected AS nodes are responsible for traffic monitoring in a distributed manner. The SVM algorithm is applied for training the dataset. This system detects the Botnets and routing attacks. Since the Blockchain module handles all attackers' associated details, it increases the computational complexity for each transaction. The lightweight features should be addressed before incorporating it into IoT networks.

Parra et al. [30] suggested a distributed attack detection technique for the IoT using Deep Learning algorithms using a cloud-based approach. It comprises two security mechanisms, such as a Distributed Convolutional Neural Network (DCNN) and a cloud-based temporal Long-Short Term Memory (LSTM) model. The proposed mechanism detects phishing attacks, DDoS attacks, and botnets. This method can detect the attack at both the node and the cloud level. The network layer-related attacks are not considered in this research.

Alsoufi et al. [31] investigated anomaly-based IDSs for the IoT using deep learning approaches. Different databases and journals having deep learning-based IDS were identified in this study. The algorithms used for anomaly-based IDS, such as supervised, unsupervised, and semi-supervised algorithms, were reviewed. Although the authors aimed to review anomaly attacks in the IoT, most of the datasets taken for the study are not specific to the Internet of Things.

Kumar et al. [32] offered an ensemble distributed IDS model to safeguard the IoT network from different types of security attacks. The Gaussian Naïve Bayes, KNN, Random Forest, and XGBoost algorithms were applied to develop the ensemble model. The UNSW-NB15 and DS2OS were the datasets used in this research to examine the IDS's performance. The model is built for detecting attacks in IoT environments. But in the experimented datasets, DS2OS is the only dataset specific to the IoT. Though there is much ongoing research and development in the security of IoT by implementing Intrusion Detection Systems, it is still needed to enhance the security level further by using innovative tools and techniques.

## 3. SECURITY ATTACKS IN IOT

The security related threats and vulnerabilities rise robustly as the connected devices in IoT increase. The IoT nodes create dynamic topology and the nodes perform their tasks without human intervention, so that, handling the security issues in IoT becomes more complex. The privacy and security challenges of IoT become more troublesome with the limited resources. Moreover, the enormous growth and adoption of IoT devices in all aspects of human life indicate the necessity of considering these security threats before the implementation of the countermeasures. The security market from 2019 to 2025 is given in Figure 3.

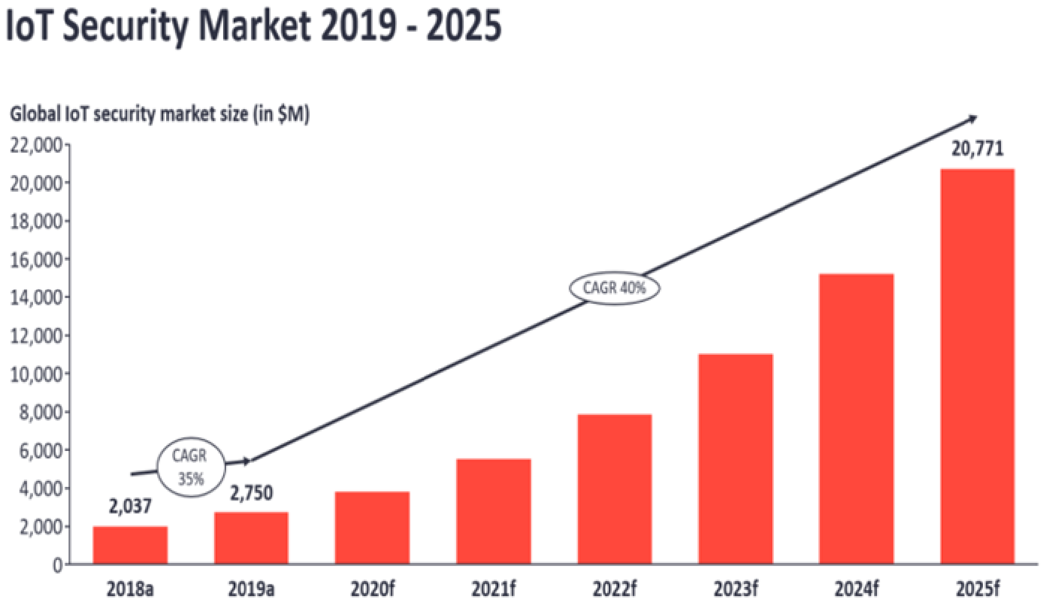

Figure 3 IoT Security Market (2019-2025) (Source: IoTAnalyticsResearch 2020)

According to IoT Analytics Research 2020, the IoT security market size was $2,750 million in 2019, and it is estimated to be the same as $20,771 million in 2025. The increase in the compound annual growth rate (CAGR) is 40% from the year 2019 to 2025. This emphasises the rapid growth of security challenges in IoT and the importance of securing the devices against various attacks. Intrusions or attacks on any network can be caused in three ways:

- Attacks are targeted by external attackers after gaining access to any network, and then the systems explore various malicious activities against the network.
- Internal attackers who have been granted a certain level of privilege but attempt to launch attacks using additional unauthorised access.
- Authorized internal attackers misuse the privileges given to them.

### 3.1. External Attacks

External attacks are initiated from outside of the networks. By acting as insiders, the external attackers inject malicious code during data communication. The attackers access the smart devices of the IoT devices remotely and attempt various types of attacks against the IoT networks.

### 3.2. Internal Attacks

Internal attacks are initiated by the authorized people of the IoT network. They misuse their given privileges as well as pretend that they have other privileges which they may not be granted. In this attack, the attacker tries to inject and run abnormal codes on the nodes without the user's awareness in this attack. IDSs protect the IoT network and devices in real-time from external and internal security threats and attacks [33].

## 4. TYPES OF IDS FOR IOT

Intrusion Detection Systems are used to discover intrusions, attacks, and malicious activities in the IoT environment. IDSs are networking security components that are widely used to protect network environments from attacks and malicious activities. They normally monitor the behaviour of the individual device or the network. Intrusion Detection Systems for the Internet of Things are classified into two categories:

- IDS types based on their positions
- IDS types based on their techniques

The classifications of IDS used in this review are illustrated using Figure 4.

The first category is based on where the Intrusion Detection System is located in the IoT network. The second category of classification is based on the techniques used for implementing the IDS. Each type is explained in detail.

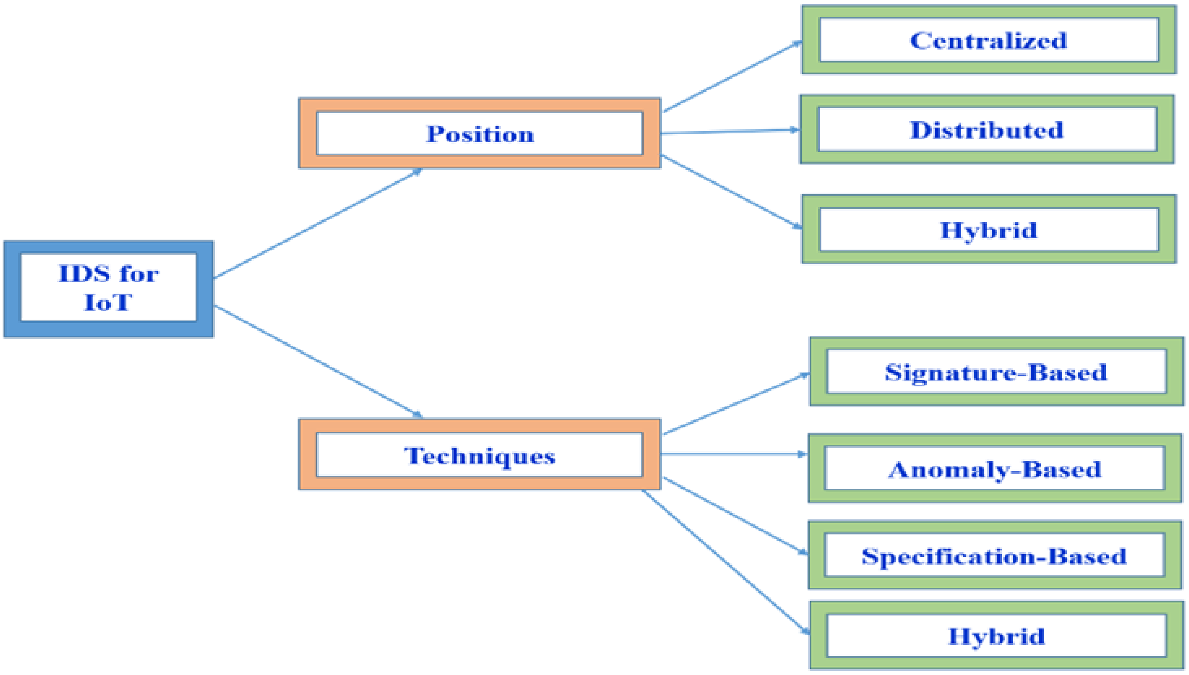

Figure 4 Types of IDS for IoT

### 4.1. IDS Types Based on its Position in the Network

There are several types of IDSs, each of which is classified differently. The IDS can be installed on the border router, selected nodes, or every node in the IoT network in the IoT ecosystem. Intrusion detection systems are classified into three types based on this deployment strategy: distributed IDS, centralized IDS, and hybrid IDS.

#### 4.1.1. Distributed IDS (Host-based IDS)

Each node in the IoT network is responsible for monitoring and detecting the attacks in this distributed deployment method. As a result, the intrusion detection system is installed on nearly all nodes in the network. The attacks are detected in a distributed manner by the IDSs [34]. The resource-constrained properties of the IoT should be examined and optimised since the intrusion detection system is installed on each node. To deal with this problem, a variety of approaches have been devised.

Oh et al. [35] devised a lightweight approach for identifying assaults by comparing packet payloads and attack patterns. Auxiliary shifting and early decision, according to the authors, are required to minimize the number of matches required to identify attacks. This attack detection system skips a large volume of data that are not relevant for detecting the attacks.

The authors claim it is a lightweight system since it reduces the memory requirements and computational costs. Sometimes, the reduction of memory for pattern matching also degrades the detection accuracy of the system.

Lee et al. [36] suggested a lightweight distributed IDS for detecting Denial of Service (DoS) attacks in 6LowPAN networks. In this approach, the malicious node is identified using the battery power consumption of an IoT device. The authors considered only a single node as the parameter in their research work.

In distributed IDS settings, some nodes also have an additional responsibility to monitor their neighbours and such nodes are called watchdogs.

Mehmood et al. [37] developed a multi-agent IDS using Naïve Bayesian algorithm for detecting the probable distributed Denial of Service (DDoS) attacks in IoT layered architecture. In this work, the multi-agents along with Naïve Bayesian algorithm were implemented in selected IoT devices throughout the network. The agents were classified as system monitoring, communicating, collector, and actuator agents. The distributed multi-agents in this approach share the responsibility of intrusion detection and reduce the workload of the individual nodes. The agent nodes could communicate with other agents too, whenever required. The authors used sensors to gather the information, and the collected information was analyzed to check whether there were any attacks on the network. Malicious nodes and their activities were monitored and reported to the administrator or to the IoT objects. The authors did not consider low-capacity systems in their approach. Though the authors claim that it is suitable for IoT, it is only relevant for Wireless Sensor Networks (WSN) and Mobile Ad-hoc Networks (MANET) as they implemented these networks only in the NS2 Simulator and gave the simulated results.

Cervantes et al. [38] proposed a distributed solution named "Intrusion Detection of Sinkhole Assaults on 6LoWPAN for InterneT of Things (INTI)" that monitors, detects, and mitigates the attacks by merging the concepts of trust and status with watchdogs. Different types of nodes, such as associated, leader, and member nodes, were used to create a hierarchical structure. A change in the network, such as network reconfiguration or the occurrence of an attack, might cause the node to change its role. After then, each node keeps track of a superior node's incoming and departing traffic. When a node detects an attack, it notifies the other nodes, and the attacker node is isolated. The effectiveness of the tool in low capacity nodes is not deliberated by the authors. Since the distributed IDSs have a hierarchy among themselves, this type of IDS can be termed as Hierarchical Intrusion Detection System.

By deploying the open-source Snort tool on the Raspberry Pi device, Sforzin and Conti [39] developed a distributed IDS termed RpiDS. The Raspberry Pi is considered the core commodity for this system. It was implemented in a smart home. The performance of the Raspberry Pi is evaluated as a host of the snort tool. Though this RpiDS is capable of hosting Snort, due to its constrained nature, it is very hard to monitor and manage the attacks in a large-scale implementation.

#### 4.1.2. Centralized IDS (Network IDS)

In this strategy, intrusion detection systems are installed on a centralized router or a dedicated server. Because of the centralized edge node, i.e., border router, which connects the IoT network to the Internet, implementing centralized IDS in IoT is very simple. Because data packets from the outside enter the IoT environment through the border router, external attackers may be quickly recognised by the centralised IDS. Hence, when the intrusion detection system is deployed in the border router, it can easily monitor, analyze, and drop the malicious data packets when it detects any attacks. Contrarily, internal attack detection is difficult in this approach since it necessitates thorough monitoring and analysis of all internal nodes connected to the border router.

Midi et al. [40] developed a centralized Intrusion Detection System for an IoT environment called “Knowledge-driven Adaptable Lightweight Intrusion Detection System (KALIS)”.

It can be deployed as a standalone tool on any specialized external device or in a centralised installation setting like a router. KALIS acquires knowledge about the characteristics of network entities on its own and uses it to dynamically create a set of detection algorithms. In compared to standard intrusion detection systems, KALIS excelled in identifying DoS, routing, and conventional attacks, according to the authors. This system is not tied to any particular protocol or architecture. Though the KALIS system outperforms traditional IDS in terms of performance, it requires more memory to deploy than the traditional IDS.

Wani and Revathi [41] recommended an innovative IDS using Software Defined Networking (SDN). It is programmable, so it makes the network flexible. Here, a centralized controller is moved to develop a global control system. The authors implemented their work in Mininet2.0. They achieved 99% accuracy in their result. In this research, the authors considered only the flooding attack. The NSL-KDD dataset is used in this research, which is a very old dataset and it is not specific to Internet of Things related attacks. The experiment and methodology are not explained in detail.

#### 4.1.3. Hybrid IDS

By analysing the pros and cons of the centralized and distributed placement strategies, the hybrid placement strategy is developed. In this hybrid IDS, the strengths of both strategies are included and the drawbacks are excluded.

Using the hybrid strategy, Amaral et al. [42] proposed a hybrid intrusion detection system. In this work, selected nodes act as watchdogs (Distributed IDS) to detect intrusions caused by eavesdropping on their neighbours. According to the defined security rules, the watchdogs determine whether there is any attack on the network. Each watchdog has a different rule-set based on the behaviour of the components in the network. According to the security rule-sets in the centralized IDS, the patterns are identified from the monitored messages. Thus, a hybrid approach is used in this work. The flexibility of using a different set of rules is the main advantage of this system. The rule-set has to be updated very often in order to make the system up-to-date for new attacks. Dynamic attack detection is not possible in this IDS as it has some predefined set of rules..

Thanigaivelan et al. [43] developed a hybrid attack detection system for internal anomalous activities. It was used to monitor and evaluate their neighbors within a one-hop distance and to report them to their parents only when it detected an anomaly. When an intrusion is detected, the monitoring node is isolated, and data packets are discarded in the link layer to avoid unnecessary network overhead. The system also included a fingerprinting function that allowed the border router to detect network changes and locate the source of the threats. The router and other nodes were given different tasks and they were coordinated. This system is capable of detecting and banning flooding attacks, selective forwarding attacks, and clone attacks. This system is quite complex to handle, and it mainly focuses on limited types of attacks only.

### 4.2. IDS Types Based on its Techniques

There are many algorithms for detecting intrusions and improving the performance of the IDS. These algorithms and techniques can be applied in various stages of intrusion detection. Based on the techniques and methods implemented along with it, the IDSs are grouped into four types: signature-based, anomaly-based, specification-based, and hybrid IDSs.

#### 4.2.1. Signature-Based IDS

This kind of intrusion detection system is also termed as a "Misuse-based IDS". All possible known attack patterns are stored in the IDS database. These IDSs analyse the generated information and find out whether there is any match with the known attack. This type of IDS is very effective against known attacks. It needs a periodic update because the efficiency of this system depends on attack signatures available in the database [44]. Although it gives a higher true-positive rate, it is incapable of detecting new patterns of attacks.

Kumar et al. [45] proposed a unified IDS (UIDS) for detecting DoS attacks, probe attacks, generic attacks, and exploit attacks. The decision tree algorithm is applied to the UNSW-NB15 dataset. Various forms of rule sets are defined in order to develop the system. This signature-based IDS detects the attacks more effectively than the existing research work. It needs further refinement to detect new attacks. The dataset used in this research is not specific to IoT. It is difficult to detect unknown attacks using this approach.

#### 4.2.2. Anomaly-Based IDS

This kind of IDS can classify the behavior of the system as abnormal or anomalous. This categorization is based on rules or heuristics rather than patterns or signatures. First, the IDS should be trained to understand the normal behavior of the system. If there is any activity that violates the normal behavior, then the IDS can identify it as an attack. This type of IDS detects unknown attacks effectively. However, it considers everything an intrusion, which means it is deviating from the normal behavior. Therefore, anomaly-based intrusion detection systems normally have higher false-positive rates than other types of IDSs [46]. In general, to train the normal behavior of the systems, machine learning algorithms can be used. But implementing machine learning for the resource-constrained IoT nodes is a challenging research issue. The lightweight aspects should be considered in such cases.

Ulla and Mahmoud [47] proposed an anomaly detection system for IoT networks using deep learning. The Convolutional Neural Network algorithm was the backbone of this research. The proposed IDS model was evaluated using IoT-related IDS datasets such as BoT-IoT, IoT-DS-2, IoT-23, and MQTT-IoT-IDS2020. This multiclass model detects various attacks like DoS, DDoS, flooding attacks, OS Scan, Port Scan, Mirai, etc. efficiently in terms of accuracy and other metrics. Multiple IDS datasets were combined in this research for the purpose of developing the model. The deep learning approach and the multiple data sources require more training time and computational costs.

### 4.2.3. Specification-Based IDS

This kind of intrusion detection system is also called "Rule-based IDS". These IDSs contain a rule-set and some thresholds associated with the rule-set. These rules are defined by the experts regarding the normal and abnormal activities of the nodes and protocols in the networks. Like anomaly-based IDS, these IDSs also detect attacks whenever there is a deviation from the specified thresholds and rules. In specification-based IDS, the rules and thresholds are set by the human experts, but in anomaly-based IDS, the system should be trained. This is the difference between these two types of IDSs. Since there is human involvement in these IDSs, they have a lower false-positive rate compared to the anomaly-based IDSs [48]. The specification-based IDSs are not flexible and error-prone due to the manually defined specifications. Periodic upgrading of the rules and thresholds is essential to make the system relevant for current needs.

Astillo et al. [49] recommended a specification-based system to detect the malicious acts of an implanted Artificial Pancreas System (APS) which maintains the blood glucose level of the human body. In this research, the security challenges and associated risks related to patients’ health and safety were studied. The behavior-rules of the APS were defined. The UVa/Padova simulator was used to emulate the functionalities of APS. SVM and kNN are the classifiers used in this research to validate the proposed model. The recommended system monitors the components of the APS continuously, and abnormal glucose levels are identified with better accuracy. Since it is related to human life, better refinements should be required. The behavior-rules of the APS have to be updated in order to include new symptoms that lead to abnormalities in blood glucose levels.

### 4.2.4. Hybrid IDS

Hybrid IDSs are developed by combining one or more of the aforementioned types of IDSs. These IDSs are established to optimize the performance by minimizing the drawbacks and maximizing the advantages of these IDSs. By merging the merits of such IDSs, the detection accuracy and the performance of the hybrid IDS are enhanced.

By using the Map Reduce approach and the unsupervised Optimum-Path Forest (OPF) algorithm, Bostani et al. [50] developed a hybrid IDS with anomaly and specification- IDS. Based on their experimental results, the authors defend that their IDS performed well by reducing false-positives and increasing true-positives. This hybrid system is suitable for detecting sinkhole and selective forwarding attacks in IoT networks. This system has its own limitations in unsupervised learning and the Map-Reduce approach. The raw data packets from the simulated Wireless Sensor Networks (WSN) are used in this research. Hence, the dataset used in this research is not specific to the Internet of Things.

## 5. ANALYTICAL SURVEY OF IDS FOR IOT

The Table 1 shows the summary of the reviewed literature. Here, IDS research work, the type of IDS it belongs to, techniques used in the IDS, advantages, and the research gaps of these IDSs are briefly given.

| Research | IDS Type | Techniques/Tools | Attack Detection | Required Refinements |
|---|---|---|---|---|
| Fu et al. [14] | Centralized | Automata | jam-attack false-attack replay-attack | State-space problem |
| Raza et al. [15] | Hybrid | SVELTE | Sink-hole attacks | Additional Control overhead due to 6Mapper module |
| Shreenivas et al. [16] | Hybrid | Extension to SVELTE using ETX metric, the geographical detection algorithm | ETX and Rank attack | Maximum 8 nodes only used. |
| Mbarek et al. [17] | Centralized | ENIDS protocol | Clone attacks | Consumes more energy in normal scenario |
| Ioulianou et al. [18] | Hybrid | Cooja Simulator, | DoS | IDS functionalities are |

| | | | | |
|---|---|---|---|---|
| | | Pattern Matching Algorithm | | not considered |
| Qu et al. [23] | Hybrid | Sliding window Protocol, One-Class SVM, Fuzzy C-Means | Anomalous events and routing attacks | Refinements required for diversity of attacks |
| Moustafa et al. [25] | Centralized | AdaBoost ensemble method | Botnet attacks | Limited to three IoT application layer protocols |
| Jan et al. [26] | Centralized | SVM classifier | DDoS attacks | Single attribute only used |
| Eskandari et al. [27] | Centralized | Passban IDS, iForest | Port Scanning, Brute force, flooding attack | Not considered the attacks in the training phase, flooding attack reduces the detection rate |
| Alkadi et al. [28] | Distributed | Blockchain, Bidirectional Long Short-Term Memory (BiLSTM) | DoS, DDoS, Port Scanning, OS Scan etc. | Need further refinement for real-time implementation |
| Cheema et al. [29] | Distributed | Blockchain, Spectral Partitioning | Routing attacks and Botnet | Real-world conditions should be addressed |
| Parra et al.[30] | Distributed | Deep Learning | Phishing, DDoS,<br>Botnet | More training time |
| Kumar et al. [32] | Distributed | Ensemble | Backdoor, Reconnaissance, DoS | Real-time deployment requires lightweight mechanisms for IoT nodes |
| Oh et al. [35] | Distributed | auxiliary shifting,<br>early decision | Conventional attacks using signatures | Single device only |
| Lee et al. [36] | Distributed | Energy consumption models | Routing attacks, DoS | Single device only |
| Mehmood et al. [37] | Distributed | Naïve Bayes Algorithm, Multi-agent | DDoS Attack | Low capacity systems are not considered |
| Cervantes et al. [38] | Hierarchical - Distributed | INTI | Sinkhole attacks | Low capacity systems are not considered |
| Sforzin and Conti [39] | Distributed | Snort tool | Conventional Attacks | Single Node is considered |
| Midi et al. [40] | Centralized | KALIS | DoS, Routing attacks | Complex functionalities |
| Wani and Revathi [41] | Centralized | Software-Defined Networking (SDN) | Flooding attacks | Only flooding attack is considered |
| Amaral et al. [42] | Hybrid | Watchdogs | Routing attacks based on a different set of rules | Requires optimization in enforcing and storing new security rules |

| | | | | |
|---|---|---|---|---|
| Thanigaivelan et al. [43] | Anomaly-based, Hybrid | Network fingerprinting | Clone, Flooding, selective forward | Complex to handle |
| Kumar et al, [45] | Centralized Specification-based IDS | Decision Tree | Exploit, DoS, Probe, Generic | Requires refinement for detecting new attacks. |
| Ulla and Mahmoud [47] | Anomaly-based | Convolutional Neural Networks | Dos, DDoS, Mirai, Flooding, Port Scan | Training takes more time |
| Astillo et al. [49] | Centralized<br>Specification-based | UVa/Padova simulator,<br>SVM, KNN | Abnormal blood glucose level | Human life related. Periodic update required |
| Bostani et al. [50] | Hybrid | Optimum-Path Forest (OPF), Map Reduce Algorithm | Sinkhole, wormhole, selective forward attack | Simultaneous different types of attacks reduce the performance |

Table 1 Intrusion Detection Systems for IoT

According to this review, when machine learning algorithms are deployed, the performance and efficiency of the intrusion detection systems will be better and the hybrid IDS will provide better accuracy, which reduces false positives and improves the true positives.

## 6. RESEARCH DIRECTIONS BASED ON THE REVIEW

The IoT has evolved from the traditional network architecture. Hence, it also incorporates all the vulnerabilities and threats associated with traditional networks. As IoT is connected to the global network, all the security issues that lie on the Internet also propagate to the IoT environment. The following are the reasons for various security-related issues in the IoT environment:

- The devices in IoT networks are resource-constrained; they have less memory, processing power, and limited energy.
- Voluminous IoT devices from heterogeneous sources are linked to the Internet, which tends to make the IoT more vulnerable.
- IoT devices use different technologies and platforms. Hence, providing interoperability among such devices is a challenging issue.

These issues make the IoT vulnerable and cause serious damage like data breaches and tampering of IoT nodes. If the nodes are compromised, then the security risk will rise to a higher level. Cryptography is one of the technologies used to secure data. Here, secure keys are the core elements. But, when the attacker compromises the internal nodes to get the security keys, preventing the network from attacks is not possible. In such a scenario, IDSs are a boon for providing security to the IoT networks. Therefore, it is essential to have an intrusion detection system to monitor the IoT network and detect the attacker and compromised IoT devices.

IDSs have been used in traditional network and information systems for more than two decades. The usage of IDS and its implementation in IoT compared to traditional networks is still in the initial stage. Moreover, current IDS solutions for the IoT are not sufficient. The research gaps for deploying intrusion detection systems in IoT networks are given below:

- The intrusion detection systems used in traditional networks are heavyweights, which mean they will not be suitable for resource-constrained IoT networks. The lightweight aspects in terms of processing, memory, and battery power consumption should be considered for developing IDS for the IoT.
- In traditional network, once the connection is established, there will be an end-to-end data transmission. But in the IoT network, the data packets traverse multi-hops from the sender to the receiver. Hence it is more vulnerable. The connectivity and link stability issues of the IoT network should be kept in mind when designing IDS for IoT.
- The IoT uses advanced protocols and technology that have their own vulnerabilities in the networks. So, the IDS developed for traditional networks are not applicable in the IoT environment.
- The sensors generate voluminous data. The security aspects of such data and managing such voluminous data also lead to research challenges.

The above facts summarize the issues and challenges of implementing IDS while deploying them in IoT networks.

## 7. CONCLUSION

One of the most important security tools deployed in traditional networks is the IDS. While implementing the IDS in an IoT environment, the characteristics of the IoT should be considered. The deployment of IDS in the IoT has a lot of emerging scope and challenges for research. In this paper, the security issues in the IoT, the need for IDS in the IoT, and the different types of IDS for the IoT are reviewed. An analytical survey based on the review is also given. The analysis clearly shows that they did not reach a consensus, implying that additional research and development for IDS in IoT networks is still required. The intrusion detection systems also necessitate periodic refinement to keep the systems suitable for current needs. Hence, it provides a wider scope for IoT security researchers.

## REFERENCES

[1] A. Khraisat and A. Alazab, "A critical review of intrusion detection systems in the Internet of Things: techniques, deployment strategy, validation strategy, attacks, public datasets and challenges", Cyber Security 4(18), 2021, DOI: 10.1186/s42400-021-00077-7

[2] A. Colakovi and M. Hadziali, "Internet of Things (IoT): A Review of Enabling Technologies, Challenges, and Open Research Issues", Computer Networks, 2018, DOI: 10.1016/j.comnet.2018.07.017.

[3] E. C. Ugwuabonyi and E.Z. Orji, "Issues and Challenges in Security and Privacy of Internet of Things (IoT)", International Journal of Latest Technology in Engineering, Management & Applied Science (IJLTEMAS), 7(12), 2018, ISSN 2278-2540.

[4] B. B. Zarpaelo, R.S. Miani, C.T. Kawakani and S. C. Alverenga, "A Survey of Intrusion Detection in Internet of Things", Journal of Network and Computer Applications, 2017, DOI: 10.1016/j.jnca.2017.02.009.

[5] A. Mayzaud, R. Badonnel and I. Chrisment, "A Taxonomy of Attacks in RPL-based Internet of Things", International Journal of Network Security", ACEEE a Division of Engineers Network, 18 (3), pp.459-473, 2016, DOI:10.6633/IJNS.201605.18(3), hal-01207859.

[6] T. A. Tchakoucht and M. Ezziyyani, "Building A Fast Intrusion Detection System For High-Speed Networks: Probe and DoS Attacks Detection", Procedia Computer Science, 127, pp. 521–530, 2018.

[7] K.K. Patel and S.M. Patel, "Internet of Things-IoT: Definition, Characteristics, Architecture, Enabling Technologies, Application and Future Challenges", International Journal of Engineering Science and Computing, 6(5), ISSN 2321- 3361, 2016, DOI: 10.4010/2016.1482.

[8] V. Adat and B. B. Gupta, "Security in Internet of Things: issues, challenges, taxonomy, and architecture", Telecommunication System, 2017, DOI: 10.1007/s11235-017-0345-9.

[9] A. Tewari and B.B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework", Future Generation Computer Systems, 108, ISSN: 0167-739X, pp: 909-920, 2020, DOI: 10.1016/j.future.2018.04.027

[10] R. Sahay, G. Geethakumari and K. Modugu, "Attack Graph based Vulnerability Assessment of Rank property in RPL-6LowPAN in IoT", IEEE Explore, 2018, DOI: 10.1109/WF-IoT.2018.8355171

[11] J. Deogirikar and A. Vidhate, "Security Attacks in IoT: A Survey. International Conference on IoT in Social, Mobile, Analytical and Cloud", I-SMAC- 2017, IEEE, 2017.

[12] A. R. Sfar, E. Natalizio, Y. Challal and Z. Chtourou, "A Roadmap for Security Challenges in the Internet of Things", Digital Communications and Networks, 4, pp.118-137, 2018.

[13] E E. Hemdan and D.H. Manjaiah, "Cybercrimes Investigation and Intrusion Detection in Internet of Things based on Data Science Methods", Cognitive Computing for Big Data Systems over IoT, 2018, DOI: 10.1007/978-3-319-70688-7_2.

[14] Y. Fu, C. Yan, J. Cao, O. Kore and X. Cao, "An Automata based Intrusion Detection method for Internet of Things", Mobile Information Systems, Hindawi Publications, 2017(1750637), 2017, DOI: 10.1155/2017/1750637.

[15] S. Raza, L. Wallgren and T. Voigt, "SVELTE: real-time intrusion detection in the Internet of Things", Ad Hoc Network, 11(8), ISSN: 2661-2674, 2013, DOI:10.1016/j.adhoc.2013.04.014.

[16] D. Shreenivas, S. Raza and T. Voigt, "Intrusion Detection in the RPL connected 6LoWPAN Networks", Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, IOTPTS'17, Abu Dhabi, United Arab Emirates, 2017.

[17] B. Mbarek, M. Ge and T. Pitner, "Enhanced Network Intrusion Detection System Protocol for Internet of Things", Proceedings of ACM SAC Conference (SAC'20), ACM, New York, Article 4, 2020, DOI: 10.1145/3341105.3373867.

[18] P. P. Ioulianou, V. G. Vassilakis, I.D. Moscholios and M. D. Logothetis, "A Signature-based Intrusion Detection System for the Internet of Things", International Conference on Information and Communication Technology Forum (ICTF-2018) ,Graz, Austria, 2018, https://www.researchgate.net/publication/ 326376629.

[19] P. Wanda and H. J. Jie, "A survey of Intrusion Detection System", International Journal of Informatics and Computation (IJICOM) 1(1), ISSN: 2685-8711, 2019.

[20] H. Abdul-Ghani, D. Konstantas and M. Mahyoub, "A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model", International Journal of Advanced Computer Science and Applications, Springer, 9(3), 2018.

[21] Y. Lu and L.D. Xu, "Internet of Things (IoT) Cyber Security Research: A Review of Current Research Topics", IEEE Internet of Things Journal, 2018, DOI: 10.1109/JIOT.2018.2869847.

[22] C. Ramakrishna, G.K. Kumar, A.M. Reddy and P. Ravi, "A Survey on various IoT Attacks and its Countermeasures", International Journal of Engineering Research in Computer Science and Engineering (IJERCSE), 5(4), ISSN: 2394-2320, 2018.

[23] H. Qu, L. Lei, X. Tang and W. Ping, "A Lightweight Intrusion Detection Method Based on Fuzzy Clustering Algorithm for Wireless Sensor Networks", Advances in Fuzzy Systems, Article ID: 4071851, 2018, DOI: 10.1155/2018/407185.

[24] S. K. Biswas, "Intrusion Detection Using Machine Learning: A Comparison Study", International Journal of pure and Applied Mathematics, 118 (19), pp.101-114, ISSN: 1311-8080 (print); ISSN: 1314-3395 (online), 2018.

[25] N. Moustafa, B. Turnbull and K. R. Choo, "An Ensemble Intrusion Detection Technique based on proposed Statistical Flow Features for Protecting Network Traffic of Internet of Things", IEEE Internet of Things Journal, 2018, DOI:10.1109/JIOT.2018.2871719.

[26] S. U. Jan, S. Ahmed, V. Shakov and I. Koo, "Toward a Lightweight Intrusion Detection System for the Internet of Things", IEEE Access, 2019, DOI: 10.1109/ACCESS.2019.2907965.

[27] M. Eskandari, Z. H. Janjua, M. Vecchio and F. Antonell, "Passban IDS: An Intelligent Anomaly Based Intrusion Detection System for IoT Edge Devices", IEEE Internet of Things Journal, pp. (99):1-1, 2020, DOI: 10.1109/JIOT.2020.2970501.

[28] O. Alkadi, N. Moustafa, B. Turnbull and K. R. Choo, "A Deep Blockchain Framework-enabled Collaborative Intrusion Detection for Protecting IoT and Cloud Networks", IEEE Internet of Things Journal, 2020, DOI:10.1109/JIOT.2020.2996590.

[29] M. A. Cheema, H. K. Qureshi, C. Chrysostomou and M. Lestas, "Utilizing Blockchain for Distributed Machine Learning based Intrusion Detection in Internet of Things", 16th International Conference on Distributed Computing in Sensor Systems (DCOSS-2020), IEEE Xplore, 2020, DOI: 10.1109/DCOSS49796.2020.00074.

[30] G. D. L. T. Parra, P. Rad, K. R. Choo and N. Beebe, "Detecting Internet of Things Attacks using Distributed Deep Learning", Journal of Network and Computer Applications, 163(102662), ScienceDirect, 2020, DOI: 10.1016/j.jnca.2020.102662.

[31] M. A. Alsoufi, S. Razak, M. M. Siraj, I. Nafea, F. A. Ghaleb, F. Saeed and M. Nasser, "Anomaly-based Intrusion Detection Systems in IoT using Deep Learning", Applied Sciences, 11(18), 8383, 2021,DOI:10.3390/app11188383.

[32] P. Kumar, G. P Gupta and R. Tripathi, “A distributed ensemble design based intrusion detection system using fog computing to protect the Internet of Things networks”, Journal of Ambient Intelligence and Humanized Computing, 12, pp. 9555–9572, 2020, DOI:10.1007/s12652-020-02696-3

[33] L. Santos, R. Gonçalves, C. Rabadao and J. Martins, “A flow-based intrusion detection framework for internet of things networks”, Cluster Computing, Springer, 2021, DOI: 10.1007/s10586-021-03238-y

[34] E. Benkhelifa, T. Welsh and W. Hamouda, “A Critical Review of Practices and Challenges in Intrusion Detection Systems for IoT: Towards Universal and Resilient Systems”, IEEE, 2018, DOI:10.1109/COMST.2018.2844742.

[35] D. Oh, D. Kim and W. W. Ro, “A Malicious Pattern Detection Engine for Embedded Security Systems in the Internet of Things”, Sensors, 14 (12), ISSN: 24188–24211, 2014, DOI: 10.3390/s141224188.

[36] T. H. Lee, T. H. Wen, L. H. Chang, H. S. Chiang and M.C. Hsieh, “A lightweight Intrusion Detection Scheme based on Energy Consumption Analysis in 6LowPAN”, Advanced Technologies, Embedded and Multimedia for Human-centric Computing, Lecture Notes in Electrical Engineering 260, Springer Netherlands, pp. 1205–1213, 2014.

[37] A. Mehmood, M. Mukherjee, S. H. Ahmed, H. Song and M. M. Malik, “NBC-MAIDS: Naïve Bayesian classification technique in multi-agent system-enriched IDS for securing IoT against DDoS attacks”, Journal of Supercomputers, Springer Science+Business Media, LLC, Springer Nature, 2018, DOI:10.1007/s11227-018-2413-7

[38] C. Cervantes, D. Poplade, M. Nogueira and A. Santos, “Detection of sinkhole attacks for supporting secure routing on 6LoWPAN for Internet of Things”, IFIP/IEEE International Symposium on Integrated Network Management (IM), pp.606–611, 2015.

[39] A. Sforzin and M. Conti, “RpiDS: Raspberry Pi IDS-A fruitful Intrusion Detection System for IoT”, International IEEE Conference on Ubiquitous Intelligence and Computing, Advanced and Trusted Computing, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People and Smart World Congress, 2016, DOI:10.1109/UIC-ATC-Scalcom-CBDCom-IOP-SmartWorld.2016.114.

[40] D. Midi, A. Rullo, A. Mudgerikar and E. 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 (ICDCS’17), 2017.

[41] A. Wani and S. Revathi, “Analyzing Threats of IoT Networks Using SDN Based Intrusion Detection System (SDIoT-IDS)”, Smart and Innovative Trends in Next Generation Computing Technologies (NGCT-2017), Springer, CCIS 828, pp. 536–542, 2018.

[42] J. Amaral, L. Oliveira, J. Rodrigues, G. Han and L. Shu, “Policy and Network-based Intrusion Detection System for IPv6-enabled Wireless Sensor Networks”, IEEE International Conference on Communications (ICC-2014), pp. 1796–1801, 2014.

[43] N. K. Thanigaivelan, E. Nigussie, S. Virtanen and J. Isoaho, “Hybrid Internal Anomaly Detection System for IoT: Reactive Nodes with Cross-Layer Operation”, Security and Communication Networks, Article ID: 3672698, 2018, DOI: 10.1155/2018/3672698.

[44] O. A. Okpe, O. A. John and S. Emmanuel, “Intrusion Detection in Internet of Things”, International Journal of Advanced Research in Computer Science, 9(1), ISSN: 0976-5697, 2018, DOI:10.26483/ijarcs.v9i1.5429.

[45] V. Kumar, A. K. Das and D. Sinha, “UIDS: A Unified Intrusion Detection System for IoT Environment”, Evolutionary Intelligence, 14, pp. 47–59, 2021, DOI: 10.1007/s12065-019-00291-w

[46] L. Santos, C. Rabadão and R. Gonçalves, “Intrusion Detection Systems in Internet of Things: A Literature Review”, ResearchGate, 2018, DOI: 10.23919/CISTI.2018.8399291.

[47] I. Ulla and Q. H. Mahmoud, “Design and Development of a Deep Learning-Based Model for Anomaly Detection in IoT Networks”, IEEE Access, 9, e-ISSN: 2169-3536, pp. 103906–103926, 2021, DOI: 1109/ACCESS.2021.309402.

[48] R. Mitchell and I. Chen, “A Survey of Intrusion Detection Techniques for Cyber-physical Systems”, ACM Computing Surveys (CSUR), 46 (4), 55, 2014.

[49] P. V. Astillo, J. Jeong, W. C. Chien, B. Kim, J. S. Jang, I. You, “SMDAps: A Specification-based Misbehavior Detection System for Implantable Devices in Artificial Pancreas System”, Journal of Internet Technology, 22(1), e-ISSN:2079-4029, 2021, DOI: 10.3966/160792642021012201001

[50] H. Bostani and M. Sheikhan, “Hybrid of Anomaly-Based and Specification-Based IDS for Internet of Things Using Unsupervised OPF Based on MapReduce Approach”, Computer Communications, 98(15), pp. 52-71, 2017, DOI:10.1016/j.comcom.2016.12.001.

Authors

**A. Arul Anitha** is pursuing her Doctoral Degree at St. Joseph’s College (Autonomous), Tiruchirappalli, Tamil Nadu, India, affiliated to the Bharathidasan University, Tiruchirappalli. She received her Master’s degree in Computer Applications (MCA) from Manonmaniam Sundaranar University, Tirunelveli, India and her B.Sc in Computer Science from Madurai Kamaraj University, Madurai, India. Her research interests are in computer networking and security, intrusion detection systems, the Internet of Things (IoT), and machine learning. She has published six research articles in reputed journals. She has cleared the National Eligibility Test (NET) for Assistant Professors.

**Dr. L. Arockiam** is working as an Associate Professor in the Department of Computer Science at St. Joseph’s College (Autonomous), Tiruchirappalli, Tamil Nadu, India. He has published four books and 359 research articles in reputed journals. He has guided more than 34 M.Phil Research Scholars and 30 Ph.D. Research Scholars, and at present he is guiding eight Ph.D. Research Scholars. He received various awards for his academic excellence. His research interests are in the Internet of Things, Cloud Computing, Big Data, Data Mining, Software Engineering, Web Services, and Mobile Networks.

**How to cite this article:**

A. Arul Anitha, L. Arockiam, “A Review on Intrusion Detection Systems to Secure IoT Networks”, International Journal of Computer Networks and Applications (IJCNA), 9(1), PP: 38-50, 2022, DOI: 10.22247/ijcna/2022/211599.