International Journal of Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: 10.31695/IJASRE.2024.7.5

Volume 10, Issue 7
July - 2024

A Study of an Intrusion Detection System in IoT Environment

Mohanad Ridha Ghanim[1], Rafal Naser Saleh[2], Farah Neamah Abbas[3]

Department of Computer Science

College of Education

Baghdad

Iraq

ABSTRACT

The fast development and widespread use of IoT gadgets in recent years have altered many aspects of our lives, from wearable technology and smart homes to healthcare systems and industrial automation. However, the extraordinary expansion of interconnected IoT devices also brings various security issues that open them to cyber threats. Intrusion Detection Systems (IDS) have become essential elements of IoT security systems to reduce these risks. To thoroughly grasp the subject's state, this literature review will examine the current research and technological developments in IoT IDS. This literature review covers the architecture of the IoT, various security issues and attacks in IoT, security mechanisms for IoT, IoT IDS, the role of AI in IoT data security, and hybrid IoT IDS.

Key Words: Internet of Things, Intrusion Detection System, Intrusion Prevention System, Machine Learning, Network Security.

1. INTRODUCTION

Artificial intelligence (AI) is an indispensable technique within the domain of computation. However, its functionality cannot be completed without the use of machine learning (ML). Indeed, ML is an emerging technology that permits computers to acknowledge information from experience and was emerged forth as an approach for artificial intelligence (AI) in the late 1950s [1]. Further, it is pertinent to mention that the ML algorithm uses computational techniques to learn from the dataset indirect way without concerning predetermined equations specified as a model. Numerous algorithms have been proposed within the domain of ML to develop the models for predictions using past data. The main feature of ML techniques is to improve the automatic learning from study or through previous experience and thus no need to be programmed explicitly [2-4]. Moreover, the fundamental working of ML algorithm entails receiving training or previous data as input and data inference rules are generated that subsequently renders the prediction for new outcomes. It is also an reality that by employing different training data on similar learning algorithms different models can be created. Even more, ML techniques render the computational process more authentic, cost-effective with high efficiency as well as the complexity of data can be analyzed automatically through ML with more accuracy. It has been revealed from extensive literature survey that in preceding decade ML techniques have been implemented to perform different tasks pertaining to classification and regression such as fraud and spam detection, speech recognition, and bioinformatics, etc. The ML techniques used to perform these varying tasks entails the knowledge from the realm of mathematics, medical, and computer engineering [3].

There are different learning strategies for ML algorithms but four strategies are widely used. These are: supervised, unsupervised, semi-supervised, and reinforcement learning [5, 6]. In supervised learning, a determined set of labeled data is used for the training model to predict the targeted variable from the given set of sample data [7]. In unsupervised learning, no output vector or labels are associated with the inputs and the learning model does not extract relationship by observing the data. Indeed, this learning strategy is used to classify the set of patterns into clusters [8]. The unsupervised learning strategy is used within the purview of Wireless Sensor Network (WSN) to tackle the different issues like problem pertaining to connectivity [9], anomaly detection [10], data aggregation [11-12], and routing [13-14]. Further, some ML algorithm shares hybrid characteristics of supervised and unsupervised mechanism. These hybrid algorithms are called semi-supervised learning. The semi supervised algorithms are considered as the

pre-classifiers with reduced softness [15]. In contrast, reinforcement learning enables or trains an agent over the duration to interact with a specific environment. The agent will follow a set of rules while interacting with the environment and after observing the environment some operation is performed regarding the present state of environment. Q-learning is a well-known reinforcement learning method [16]. A review of existing IDS proposals for the Internet of Things is done in this paper. Every work is classified in terms of attributes such as: Intrusion detection techniques, Security threat and Validation strategy. It examines the approaches taken by researchers to develop IDS for IoT and provides special emphasis on the proposed classification for intrusion detection in IoT.

2. NETWORK SECURITY

Security in an interconnected computer world is a prime concern for casual users to sophisticated scientific and research users. The presence of huge user sources operating with multivariate intentions emphasizes the need for robust network security. The availability of tools to intrude networks has seen a rapid growth. The ease of access to Intruding tools signifies the fact that developing an efficient Network Security tools to counter intrusions is anticipated.

The security threats emerge from not only external sources but also from Internal sources [17]. Intruders having super-user access can always carry out harmful actions, cause havoc, and destroy data system resources. Doubt mechanisms like Firewalls [18], Encryption [19], Authorization [20], Vulnerability checking and access control policies. [21] provide security, but they are not completely fool proof solutions. They are mainly vulnerable to Social Engineering attacks. Further computer systems that operate in isolation from public networks are also vulnerable to attacks from internal disgruntled employees [22]. These observations force researchers to lay more emphasis on IDS that protects the systems from intruders. Basically IDS [23] is defined as a security system ensuring monitoring activities on the networks and possess the ability to detect any attempts of compromise happening in the security policies. Importance of IDS is to stop stealing the network data by intruders and will be used to inspect the network activities for all the time.

3. DEFINITION AND TYPES OF INTRUSION DETECTION SYSTEM

Various emerging technologies focus on interfacing with computer systems randomly distributed among various fields of operation. The ability to identify the intrusion and to protect the information in real-time becomes crucial. An IDS properly supervise the network, detects unusual behaviour and sends out alarm about intrusion on successful detection. The term 'intrusion' refers to the misuse of a network. An intrusion can be characterized as the theft of important resources through the network. Intrusion detection methods include system files to unauthorized signature comparison, unethical scanning that identify indications of dangerous behaviours. The intrusion identification comprises tracing network monitoring and comprehension of that hostile behaviour. Different criteria can be used to categorize IDSs [24].

For example, there are mainly five kinds of IDS:

1. Active and passive IDS: The process of active IDS works on prevention and also detection of intrusion. It is set to keep track of network traffic and warns about possible threats and assaults; whereas passive is set up to simply monitor and analyse network traffic flow, alerting a user to potential security flaws and threats.
2. Network IDS: NIDS is a software program or a device that looks for suspicious attacks or policy deviations on a network. To report or gather any malicious activity or violation, an Information security and performance management system is frequently utilized.
3. Host IDS: Host-based IDS examines system activity for signals of suspicious behaviour and runs on the host. system registry unusual updates, several unsuccessful login, or the unlicensed installation are all examples. This IDSs often keep an eye on system objects, processes, and memory areas.
4. Knowledge-based IDS: To detect ongoing intrusion attempts, this IDS consults a database of prior threat profiles and also known as suspicious attacks. This IDS is more common than behaviour-based IDS at the moment. Its false alert rates are lower than those of behaviour-based IDS.

DOI: 10.31695/IJASRE.2024.7.

5. Anomaly Based IDS: This IDS often begin by establishing a baseline of the network's normal traffic and activity. They can compare the current condition of network traffic to this baseline in order to find patterns that aren't ordinarily present in traffic.

Figure 1 represents a scientific categorization of IDS according to the usage and learning methods.

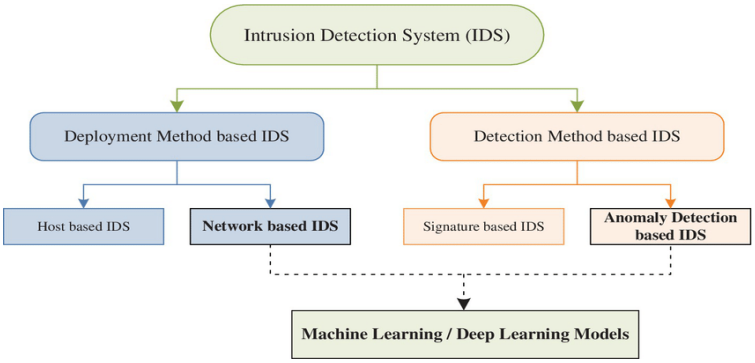

Figure 1: Taxonomy of IDS categories

The architecture of NIDS involved in intrusion detection is shown in Figure 2. NIDS inspects and captures the intrusion detection on a network. This device monitor the network to identify intrusion and send an alert to the NIDS server. There are different benchmark intrusion datasets used in recent research work. Port-Based Classification relies on the source and destination port numbers in IP traffic, assigned by IANA. While many applications have well-known registered port numbers, not all do. Peer-to-peer and online gaming applications, for instance, often use random port numbers, making them difficult to classify using this technique. In contrast, Protocol Anomaly Detection (PAD) examines application-level traffic for irregular commands and behaviors, blocking inappropriate actions. PAD can identify expected behaviours even without explicit identification, effectively intercepting new attacks .

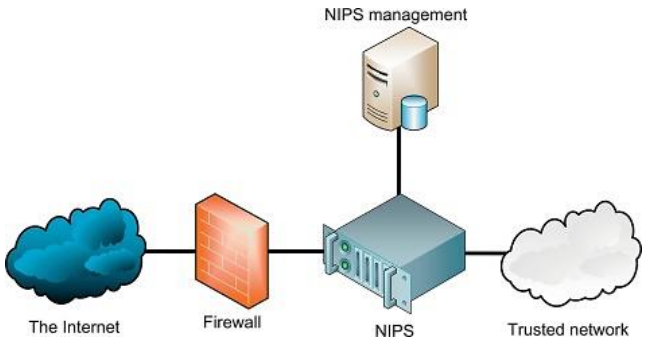

Figure 2: Architecture of NIDS

Payload statistical traffic characteristics aid in the identification and classification of network traffic. Unique statistical properties, such as flow duration distribution, flow idle time, packet inter-arrival time, and packet lengths, help distinguish different source applications from one another.

4. INTERNET OF THINGS

The Internet is a constantly evolving technology that since inception has transformed human lives in ways more than one can imagine. Beginning as Internet of Computers, it has gradually progressed towards the Internet of Things (IoT). IoT refers to a network of uniquely identifiable and intelligent physical objects with processing and communicating capabilities connected to the Internet. The exponential growth of IoT is driven by widespread Internet adoption and declining sensor technology costs and sizes. Contributing factors include cheap Internet access, built-in device sensors, the mobile revolution, and numerous companies developing IoT applications and software. By 2030, IoT is projected to reach 125 million connected smart devices, embedding itself in various domains and digitizing the physical world. However, this growth raises security and privacy concerns. IoT refers to a network of physical objects

DOI: 10.31695/IJASRE.2024.7.

connected to the Internet, equipped with sensing, actuating, processing, and communication capabilities . The objects or things in IoT interact among themselves as well as with systems on the Internet. These interactions between sensors, software, technologies, people, and processes gave birth to new applications and services. Mathematically, IoT can be expressed as an equation given in Figure 3.

Figure 1: IoT as Mathematical Equation

4.1 Security in the Internet of Things

This section highlights the security services essential for IoT. It also discusses the security aspects and later presents the different attacks targeting IoT networks. The IoT requires the following multi-faceted security solutions which involves securing the communication, the data, and the network (refer Figure 3). Data Security: The first aspect of securing the IoT is securing the sensitive data either stored on an IoT device or in transit from one device to another. This data can be data sensed from the environment or other cryptographic credentials like passwords, shared keys, certificates, and identities. In a conventional storage framework, data is often stored in an encrypted format along with its cryptographic hash value. When such data is requested by a remote system, it is first decrypted and integrity is confirmed, re-encrypted and then, transmitted securely. In this manner, the resource-intensive tasks of encryption, decryption, and hashing are performed two times. Apart from being treated upon by resource-intensive operations, IoT data is generated at a very fast pace and is highly heterogeneous. With developments in flash memory technology, IoT devices have vast flash memory sizes which can be used for increased storage and minimized energy consumption for performing cryptographic operations on the data. Further, the rapid generation of newer data signals towards a conceptually infinite storage solution for storing IoT data and its processing in real-time. Such an infrastructure could be the cloud computing or the fog computing. In addition, legal issues like who owns the data collected by an IoT device also exist that is, whether it is owned by the device owner, the device Original Equipment Manufacturer (OEM), or any third party. There is no generic advice on this issue and the best way is to stay aware of the responsibility and liability of the data generated by an IoT device [26]. Communication Security: The futuristic IoT devices will all be IP-enabled. As IoT will be the core of many services, the availability, and reliability of its operation are important. Hence, it is essential to address the conventional security requirements of authentication, non-repudiation, confidentiality, and integrity in the context of secure communication in the IoT. It is essential to achieve a secure E2E communication between devices with confidentiality and integrity and other cryptographic services. To secure IoT communication, three options are available: (i) adapt optimized protocols from WSNs, (ii) develop new protocols tailored to IoT constraints, or (iii) utilize existing Internet security protocols. WSN security mechanisms need modification to work with IP networks, complicating their deployment in IoT. While new lightweight security protocols might be efficient, they also require impractical modifications to the Internet's scale. Therefore, analyzing existing Internet security mechanisms for IoT is a practical approach [27]. Network Security: Even with the first line of defence mechanisms like communication security in place, an IoT network is vulnerable to several attacks against the availability services of the network. This happens when the first line of defense mechanisms is either broken or absent and cannot prevent intrusions. Most of such intrusions target routing, access control, and availability services in an IoT network. Therefore, contrary to WSN, IoT networks suffer from insider attacks as well as attacks originating from the Internet. The second line of defense mechanisms like firewall and Intrusion Detection System (IDS) protect against such intrusions. Though the available IDS proposed for WSN could be used in IoT, these approaches are based on the assumption that there is no central entity, nodes are uniquely identifiable only within the WSN, and messages are not secured. On the contrary, IoT networks have a central entity as the 6BR which is always available to ensure seamless connectivity of 6LoWPAN with the Internet. The nodes are globally identifiable with IP addresses and E2E security is also mandatory. Thus, newer approaches to secure IoT networks by considering the newer characteristics are mandatory. In addition, developing mechanisms to secure the IoT network is challenging due to resource constraints, lossy links, and the introduction of modern protocols like RPL [28].

DOI: 10.31695/IJASRE.2024.7.

4.2 Internet Of Things Architecture

The rapid growth of technology and mass usage of IoT conveyed considerable changes in the end user's daily lives. IoT can work with Wireless Sensor Networks (WSNs), Radio Frequency Identification (RFID) objects, and any network anywhere. The security and privacy of the IoT is a critical problem. With the help of RFID sensors or actuators, intelligent devices can make the self-decision and pass the information to the user safely [46]. According to various studies by Gartner, International Business Machines Corporation (IBM), and Cisco, the physical world will be thoroughly oriented in connected devices, which can make predictions, take appropriate solutions, improve processes and reduce human efforts very shortly [29].

Even though there exists no standardised format for IoT architecture, most existing architecture models follow the layered approach. Several stakeholders and research groups recommend layered architectures. The models are not from an entirely technical point of view, mixed with business and processes together. Table 1 shows a summary of the different layered architecture of IoT based on altered perspectives available in the literature. From this, it can be summarised that there are four types of layered architecture: three-layered, four-layered, five-layered, and seven-layered. Even though different authors give different names for each underlying layer in each category of layered architecture, functionalities remain the same. The following sections provide a detailed briefing about the various layered architectures in IoT.

Table 1: Summary of the different layered architecture of IoT

Sl. No	Number of Layers	Major Technologies	Article
1	Three Layers	WSN, Cloud Servers, Application.	[22]
		Perception, Network, Application.	[8] [18] [48] [49]
		Sensing, Transport, Application.	[50]
2	Four Layers	Sensing, Networking, Middleware, Application	[46] [23]
		Local environment, Transportation, Storage & Data Mining, Availability.	[47]
		Physical, Network, Perception, and Application.	[36] [48]
		Sensors and Actuators, Networking, Data Processing, Application.	[51] [49]
3	Five Layers	Physical, Data Link, Network, Transport, Application	[15] [48] [49]
		Edge Nodes, Object Abstraction, Service Management, Service Composition, Applications.	[22]
4	Seven Layers	Edge Nodes, communication, edge Computing, Data Accumulation, Data Abstraction, Applications, Users, and Centre	[22] [16] [52] [53]

The second layer, known as the network, transport, or cloud server layer, is the core of the entire network. It routes data from the sensing layer to appropriate destinations while ensuring data security. This layer primarily focuses on data routing and network security, encompassing core and local network security, various technologies, 3G/4G access security, ad hoc network security, and WiFi security.

The preceding layer is the application layer, offering diverse services to users. Its primary goal is to create smart environments, addressing areas such as structural health monitoring, waste management, air quality assessment, noise monitoring, traffic management, city energy consumption optimization, and smart lighting systems. Providing security to IoT applications is a key function of the application layer, ensuring data integrity, confidentiality, and authenticity. Application layer protocols establish interfaces with lower layer protocols to facilitate data transfer across the network [30].

DOI: 10.31695/IJASRE.2024.7.

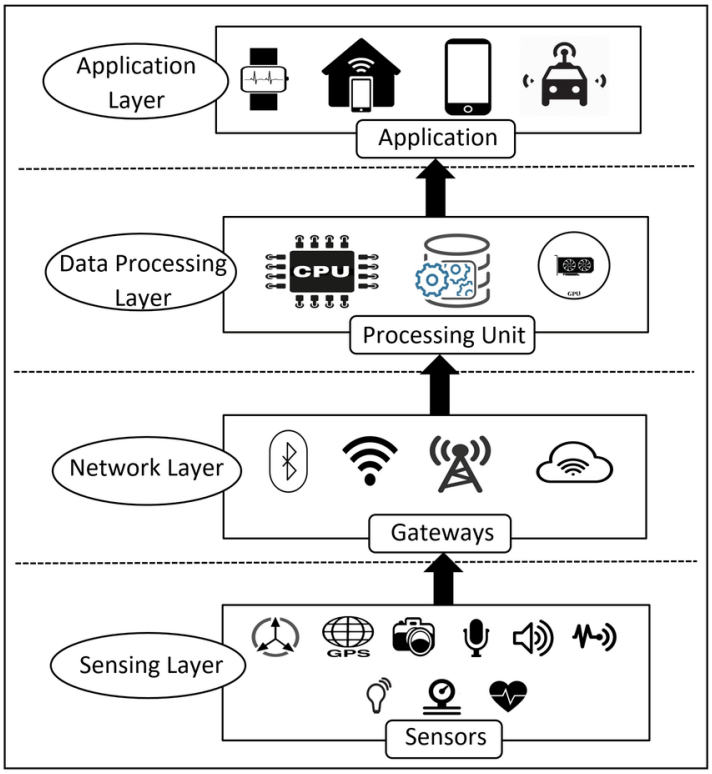

Figure 2: Three-layered IoT architecture

4.3 Security Vulnerabilities and Attacks in IoT

This section focuses on attacks in IoT and explores the proposals that provide security solutions to counter those attacks. A systematic process is followed to perform this literature review beginning with building a knowledge base of attacks on IoT and their countermeasures. [31] presented the lifecycle phases of a device in the IoT which starts with bootstrapping followed by iterative phases of operational, maintenance and re-bootstrapping. The authors concluded that securing all layers of the communication stack was important but may be challenging on resource constrained devices. So, cross-layer concepts like intrusion detection and other common security mechanisms should be considered for IoT security protocols. Stankovic [56] provided comprehensive insights into open problems like how the IoT data will be collected, used and stored, whether protocols like IPv6 and 6LoWPAN will suffice, development of interoperable hardware and software, secure code updates and even modelling human behaviour when interacting with IoT devices. However, some important topics like the development of standards, the impact of privacy laws, and the cultural impact on the use of these technologies were not discussed.

The necessity for defensive security systems in IoT is underscored by existing literature on IoT security . Studies such as [32] delve into IoT attacks and stress the importance of their detection within IoT networks. For instance, research outlined in [33] catalogued attacks in 6LoWPAN-based IoT communication environments, while [34] proposed a taxonomy of attacks on RPL, classifying them based on their targets, including network resources, topology, and traffic. Additionally, [35] surveyed Sybil attacks in IoT, categorizing them into three classes based on attacker capabilities and comparing detection schemes. Moreover, [36] outlined the deployment of Intrusion Detection Systems (IDS) for RPL intrusions as a second line of defence, complementing traditional cryptography. This research scrutinized various detection methodologies, data, system architectures, and Intrusion Response Systems (IRS) as a third line of defence.

Over the past decade, significant efforts have been directed towards proposing Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) for IoT. Various surveys have scrutinized these solutions, employing taxonomies of different depths and scopes. In a concise study, authors in [37] offered a comprehensive overview of IDS proposed for Wireless LAN (WLAN), Local Area Network (LAN), Wireless Sensor Networks (WSN), RFID, and mobile-based networks, distinguishing them from IoT solutions. They advocated for a hybrid, interoperable, and cross-layer IDS

DOI: 10.31695/IJASRE.2024.7.

integrated with anomaly-based intelligence into the 6LoWPAN protocol stack as a promising approach for IoT. Similarly, research outlined in [38] reviewed IDS-based countermeasures for insider attacks, proposing a lightweight IDS framework integrated with a firewall in the border router just above the adaptation layer in IoT. Furthermore, authors in [39] presented a thorough classification of IDS based on placement technique, security threat, detection method, and validation strategy, analyzing 18 papers dedicated to IDS in IoT. Expanding on prior research, [40] delved into machine and deep learning methods for intrusion detection in IoT. However, [41] later enhanced the taxonomy by incorporating additional characteristics such as performance metrics, IDS location, and usage frequency. In 2018, [42] critically reviewed recent advancements in intrusion detection approaches for IoT, with a focus on IoT architecture and protocols. Both [43] surveys referenced and summarized 22 papers, highlighting the necessity for lightweight and robust IDS for IoT. Despite this, these surveys overlooked factors like placement strategy, validation, and usage frequency in their taxonomies. Furthermore, [44] discussed two additional taxonomies of IDSs based on machine learning detection techniques, while [45] focused on IoT-related datasets, and [46] provided a detailed review of network intrusion detection solutions for IoT security, concluding with future research directions. However, these taxonomies were restricted to specific criteria of IDS classification, emphasizing certain points:

Literature presents a diverse array of intrusion detection methods, each varying in effectiveness and often tailored to specific attacks and protocols. However, validating these solutions with realistic IoT datasets remains a critical requirement. One recurring theme across surveys is the necessity for lightweight and robust IDS, as traditional approaches are ill-suited for IoT networks due to resource constraints and the proliferation of diverse traffic, expanding the attack surface beyond manageable limits. While much emphasis is placed on defending against attacks originating within the IoT network, there's a notable dearth of research addressing defenses against outsider attacks. Table 2 highlights the different criteria of IDS classification proposed as taxonomies in review papers on IDS in IoT. Most of these studies covered basic aspects of IDS, yet none specifically addressed specific IDS characteristics like data pre-processing techniques of feature extraction and feature selection algorithms which have direct impact on accuracy of machine learning based IDS.

Table 1: Comparison of taxonomies proposed in review works on IDS in IoT

Criteria of IDS Classification	Review Works on IDS										
	[64]	[65]	[42]	[66]	[67]	[68]	[69]	[70]	[71]	[72]	[73]
Detection Technique	C	C	C	C	C	C	C	C	C	C	C
Placement Strategy/Architecture		C	C		C	C				C	C
Location/Visibility					C	C	C			C	
Usage Frequency					C						
Validation			C							C	C
IoT Attacks			C	C	C			C		C	C
Performance Evaluation Metrics					C		C		C	C	C
Dataset/ Database									C	C	C
Data Preprocessing and Feature Selection Technique											
IPS											

5. MACHINE LEARNING TECHNIQUES FOR INTRUSION DETECTION

The traditional first line of defines mechanisms are insufficient to secure IoT network and therefore, IDS as second line of defense are more suitable. An IDS is more adaptable and variated depending on the network needs. In addition to other technologies, the abilities of an IDS can be enhanced by learning logic like machine learning. Machine Learning (ML) techniques are the techniques that involve learning from data and making predictions based on data [47]. There has been a lot of research and development in ML-based IDS due to their ability to detect zero day attacks as well as their low false alarm rates. Machine learning can perform a variety of tasks, one of which is particularly

DOI: 10.31695/IJASRE.2024.7.

significant for intrusion detection: classification. Classification can categorize data into two classes, such as “benign” or “attack”, or even different classes of attacks. The development of any machine learning algorithm involves two stages: the training stage and the testing stage. The training of machine learning algorithms can be done in two different ways: in a supervised or unsupervised manner.

Supervised Machine Learning: Supervised ML models train on datasets where the input and the associated output both are known to the model and the algorithm learns to model the mathematical function associating the results with corresponding inputs. Classification and regression are supervised learning techniques and include algorithms like Decision Tree (DT), Logistic Regression (LR), k-Nearest Neighbors, Naive Bayes, Linear Regression, Neural Networks, Linear Support Vector Machine (SVM) and Random Forest (RF), among others.

Unsupervised Machine Learning: Unsupervised learning, on the other hand, is trained without the results and its aim is to look for interesting structures in the input data. Clustering and association are unsupervised learning techniques.

In addition to being supervised or unsupervised, there is another class of machine learning algorithms known as Ensemble Learning (EL). It is a special class of machine learning algorithms where multiple learning algorithms are generated and combined to improve the performance of a single model or reduce the probability to choose a poor one. EL involves combining decisions of several models where individual models must exhibit diversity among themselves. These decisions may be combined with three strategies: bagging, boosting and stacking. The individual error given by each model is strategically combined that the total error is minimum. Some of the other applications of ensemble learning include incremental learning, error correcting and optimal selection of features. Examples of ensemble algorithms include RF, Gradient Boosting Machine (GBM), AdaBoost etc. After the training stage, ML models are tested on new data to assess their performance. The testing is done on new data to avoid biasness in the model. Another way is to use a validation set which compares different values of parameter (for example, the number of layers, the depth, the learning rate, etc.). Following training, the model selects the best-performing value on the validation set, which is then applied to the model. Subsequently, the model undergoes testing on separate test data, often with a small portion of the training set reserved for this purpose. Designing a machine learning model typically involves utilizing frameworks such as scikit-learn [45], TensorFlow [46], Matlab, or Weka [47], each choice impacting algorithm optimization and parameter availability. ML algorithms necessitate substantial data for training, and their performance hinges on the quality and quantity of data available. Fundamentally, all ML problems are data-dependent: ample high-quality data can often outperform superior algorithms, underscoring their paramount importance. However, acquiring such datasets is costly and challenging. In the realm of intrusion detection, notable datasets like KDD Cup 99 [48], NSL-KDD [49], and CICIDS2017 [50] are frequently employed for evaluating IDS in conventional networks. Nonetheless, within IoT, there's a scarcity of explicitly designed datasets for intrusion detection, with much of the existing research relying on outdated datasets for evaluation purposes.

6. CLASSIFICATION OF INTRUSION DETECTION SYSTEMS

This section provides a comprehensive review of state-of-the-art IDS proposals in IoT, categorizing them based on various criteria such as detection techniques, placement strategy, information source, usage frequency, validation strategy, security threats, evaluation metrics, datasets, and feature selection techniques. Despite the abundance of surveys on IDS for IoT, their diversity underscores the necessity for thorough and extensive reviews concerning IDS characteristics and IoT. Consequently, only security solutions based on the standardized protocol stack of IoT are included, as outlined in [11]. Figure 5 visually depicts the different criteria used to classify IDS, which are elaborated upon in the subsequent discussion.

DOI: 10.31695/IJASRE.2024.7.

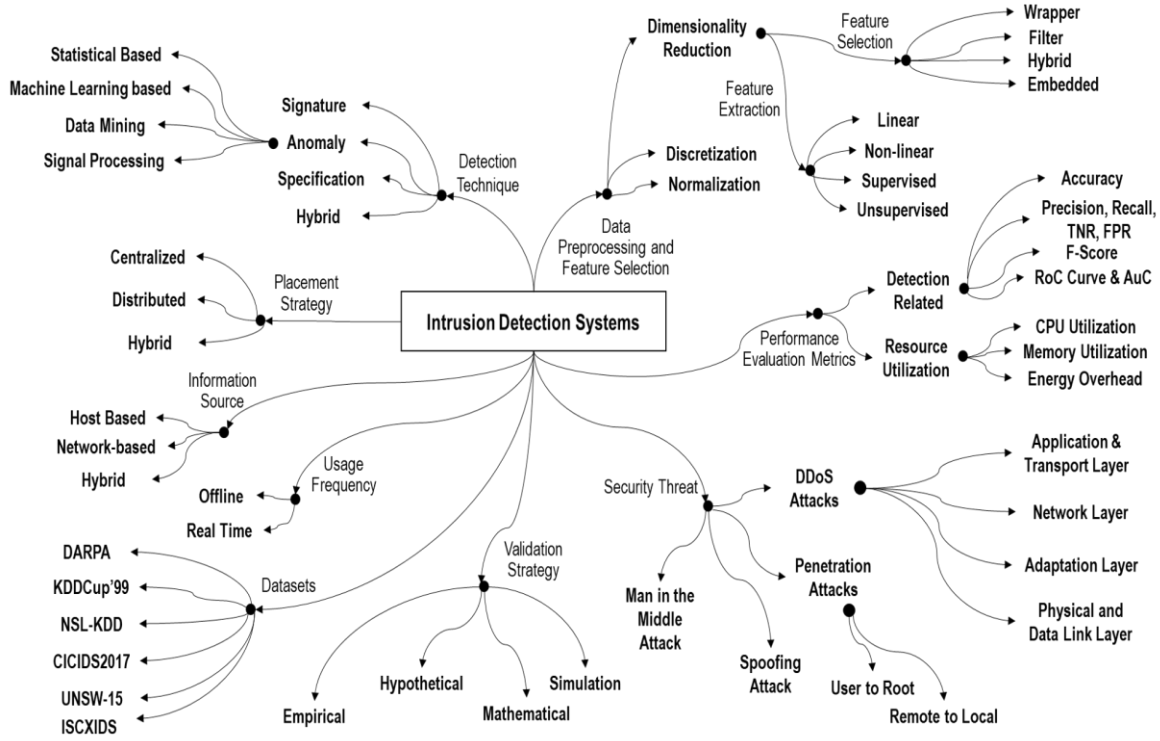

Figure 3: A Taxonomy of Intrusion Detection Systems

6.1 Security Frameworks for IoT

IoT security frameworks are crucial for addressing the growing concerns about the security and privacy of IoT networks and devices. These frameworks provide guidelines, best practices, and standards for creating, deploying, and maintaining secure IoT ecosystems. Table 3 gives glimpses of IoT security frameworks [51].

Table 2: IoT security frameworks Comparison

Sl. No	Name of the framework	The main area of attention
1	NIST Cybersecurity Framework, [79] NIST [80].	Incorporates industry standards and best practices to assist organizations in managing and reducing the cybersecurity risks associated with their critical infrastructure (threats, vulnerabilities, and impact) [81].
2	NIST	Control the risk to systems and
	Framework, [79] J. Task Force [82].	organisations from information security and privacy [82].
3	NIST SP 800-53, [79] [83].	Put energy into offering instructions for completing information systems risk assessment [83].
4	NIST Privacy Framework, [79] [84].	Accentuate the importance of enhancing privacy through corporate risk management [84].
5	HIPAA, [79] [85].	Concentrate on the privacy and security of sensitive health information, electronic health standards, and electronic health records [85].
6	Family Educational Rights and Privacy Act (FERPA), [79] [86].	Concentrate on the privacy and security of sensitive health information, electronic health standards, and electronic health records [86].
7	PCI-DSS, [79][87].	Protecting consumer financial information that is kept

DOI: 10.31695/IJASRE.2024.7.

		electronically should be a priority [87].
8	Cybersecurity Maturity Model Certification (CMMC), [79] [88].	Concentrate on enhancing and standardising cybersecurity preparation across the defence industrial base of the federal government (DIB) [88].
9	Cybersecurity Capability Maturity Model (C2M2), [79] [89].	Ensure that an organisation consistently assesses the state of its cybersecurity capabilities [89].
10	FFIEC Cybersecurity Assessment Tool, [79] [90].	Concentrate on identifying organisational threats and figuring out how equipped they are for cybersecurity [90].
11	NERC 1300 Standards,	Reduce the dangers that a breach of
	[79] [91].	crucial cyber assets poses to the overall stability of the electric grid [91].
12	ANSI/ISA 62443, [79] [92].	The main focus should be processes, methods, and specifications for Industrial Automation and Control Systems (IACS), including secure product development lifecycle specifications [92].
13	FISMA 2014, [79] [93].	Focus on the security specifications that can help government organizations improve them cybersecurity posture [93].
14	SOC 2, [79] [94].	Provide enterprises that gather and keep personally identifiable customer information in cloud services with advice on the security, availability, integrity, and privacy of sensitive user information [94].
15	Threat Assessment and Remediation Analysis (TARA), [79] [95].	Choose countermeasures that successfully mitigate such vulnerabilities, focusing on identifying and assessing cyber vulnerabilities [95].
16	Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), [79] [96].	Concentrate on locating and addressing information security concerns [96].
17	IASME Gouvernance, [79] [97].	Information assurance should be a priority for small and medium-sized businesses [97].
18	CIS v7, [79]	The emphasis should be on raising
	[98].	security requirements across organizations [98].
19	Control Objective for Information and Related Technologies (COBIT), [79] [99].	Priorities IT governance, management, and security [99].

It is critical to consider the unique requirements and properties of the relevant networks and devices while deploying IoT solutions. To defend IoT ecosystems from potential threats and vulnerabilities, security frameworks can be a significant resource for enterprises. A significant obstacle to creating and implementing IoT security management measures is the need for standardized methodologies that can expand beyond traditional network requirements into IoT-based smart environments. Researchers and other stakeholders should consider creating new security standards and assessment frameworks to address existing and future IoT security issues.

6.2 IoT IDS

Any communication network must have efficient methods in place to address a variety of data security issues, such as confidentiality, integrity, and availability [52]. IDS are devices or procedures that are used to stop unauthorised entrance and identify attacks. Jim Anderson and Heberlein established the conceptualization of IDS starting in 1980

DOI: 10.31695/IJASRE.2024.7.

[53]. The three main parts of every IDS are sensors, an analytical engine, and a reporting system. The deployment strategy, detection techniques, security threats, occurrence, and utilisation of IoT IDS may all be broadly categorised [54]. IDS can be classified as centralised, distributed, or hybrid depending on placement approach. The categories for detection techniques are hybrid IDS, anomaly-based, signature-based, and specification-based IDS. Routing- specific and application-specific IDS are two examples of security threats. Host- based intrusion detection systems (HIDS) or network-based intrusion detection systems (NIDS) are the two different types of IDSs [55] [56]. It can be divided into frequency, continuity, and periodicity depending on how it is used [57]. Computer networks were the origin of the IDS idea for detecting aberrant traffic [58]. Different approaches based on Game Theory (GT), Complex Event Processing (CEP), Automata [59], data mining, statistical models, payload models, rule-based [60], and AI were employed for this implementation of IDS. IDS has the benefit of being able to filter specified information from every network packet, preventing attack data. They can analyse the data in light of the protocol in order to categorise and value the attacks. Table 4 gives an overview of the IoT IDS.

Table 3: An overview of the IoT IDS

Sl. No	References	Summary
1	[50]	the IoT are used in a survey of intrusion detection systems (IDS). To comprehend and demonstrate the distinctions across IDS platforms and the current research trend toward a universal and cross-platform
2	[51]	Various intrusion detection techniques and security attacks are deployed to mitigate threats. These encompass rule-based approaches, anomaly-based approaches, hierarchical energy-efficient approaches, distributed detection-based methods, cluster-based strategies, and hybrid systems, among others.
3	[52]	An inventive MapReduce-based architectural model for intrusion detection in the Internet of Things aims to facilitate distributed detection. This proposed model comprises anomaly-based and misuse-based intrusion detection agents leveraging supervised and unsupervised optimum-path forest models for multidimensional intrusion detection.
4	[53]	The suggested model dramatically improves the limitations of SVELTE and INTI, which combines a unique detection method with constraint-based specification. The effectiveness of the proposed plan is evaluated through comparison analysis and the use of the NS-2 simulation tool.
5	[54]	Kalis is a self-adapting, expert intrusion detection system with knowledge-driven capabilities to identify real-time attacks across various IoT platforms.
6	[55]	They have designed and tested a few IDS techniques for small, device-friendly IoT networks. They took advantage of a method for managing trust that enables devices to handle neighbor reputation data. With the help of this technique, it is feasible to identify maliciously acting units in a processing- and energy-efficient manner. The method is described in the healthcare industry.
7	[56]	A thorough rundown of WSNs. Additionally, it evaluates the capabilities and features of WSNs. Additionally, it offers an analysis of WSN and IoT applications.
8	[57]	A review of IoT IDS research initiatives. The survey encompasses detection technique, IDS placement strategy, security threat, and validation strategy as its attributes. It extensively covers various options for each aspect, providing detailed insights into studies proposing specific IDS schemes for IoT or developing attack detection tactics tailored to IoT .
9	[58]	Examining the literature, identifying current trends, presenting unresolved issues and future directions, and focusing on the current state of research are the key goals of this literature review on the IDS in IoT topic.

DOI: 10.31695/IJASRE.2024.7.

10	[59]	detection technologies, including new ones like the Internet of Vehicles (IoV). Existing systems regarding energy use, privacy consequences, and computational overhead are examined.
11	[60]	Improvements in IoT intrusion detection techniques. It thoroughly analyses the most recent Intrusion Detection Systems (IDS) for Internet of Things (IoT) technologies, concentrating on architecture kinds.
12	[61]	They created a mechanism for monitoring the virtual environment to stop invasions. It checks a virtual machine that has just joined for potential weaknesses, threats, and assaults. It recognizes possible attacks and their underlying system and network vulnerabilities. Additionally, it makes predictions about upcoming attacks using the vulnerabilities that have been analyzed.
13	[62]	By utilizing a unique deployment method that considers a realistic sensing model and the specific impacts of various network parameters on the detection probability, it is possible to get around the drawbacks of uniform and Gaussian deployments for energy-efficient and rapid detection.
14	[63]	E-Spion is an IoT intrusion detection system that profiles devices based on anomaly- based system information, detecting unusual behavior indicative of invasions. It offers three detection levels with higher effectiveness but higher overhead expenses.
15	[64]	Literature Review (SLR) of the IDSs in the IoT environment. Then, thorough categorizations of IDSs in the IoT have also been offered, utilizing common traits. The benefits and drawbacks of the chosen mechanisms are then addressed.
16	[65]	To examine and categories intrusion detection systems, this work proposes a taxonomy of such systems. The taxonomy comprises two components: the detection theory and a few operational features of the intrusion detection system.
17	[66]	This study analyses current intrusion detection algorithms for IoT systems, focusing on computational overhead, energy use, and privacy implications. It identifies barriers like resource limitations, attack complexity, experimental rigor, and security data. The study aims to improve the state-of-the-art and highlight important research topics.
18	[67]	This paper provides an overview of data mining methods used on intrusion detection systems to accurately detect known and unidentified attack patterns, assisting users in creating safe information systems.
19	[68]	To help researchers understand and address the most pressing challenges in the IoT ecosystem, we have studied and explained IoT technology in this article, along with its components, security features, security concerns, and risks tied to each IoT layer.

6.3 Role of AI in IOT Data Security

In today's world, Artificial Intelligence (AI) is very familiar to everybody. Artificial Intelligence is bringing human intelligence to machines, primarily through computer systems. Even though there are alternative methods, AI plays a significant part in intrusion detection. The limitations of the current conventional techniques can be overcome by AI-based IoT IDS. The majority of IoT IDS technologies now in use are static and unable to learn from an attack's history. AI is a potent tool for identifying assaults from routine traffic, learning from past attacks over time, and alerting the appropriate system. For IoT security requirements, AI techniques like Machine Learning (ML) and Deep Learning (DL) can offer strong capabilities [61] [62].

The following literature review shows the impact of machine learning algorithms in IoT IDS. Since the use of artificial intelligence in enhancing security has proven to be quite effective, numerous studies are being conducted in this field.

DOI: 10.31695/IJASRE.2024.7.

In a thorough analysis of ML-based IoT security solutions, [63] note that despite multiple machine learning algorithms, they are all expensive to run, necessitate large training datasets, and require challenging feature extractions. In an intriguing paper, Liang et al. discussed the benefits and drawbacks of employing machine learning for IoT security and potential vulnerabilities [64]. The authors focused more on the advantages of machine learning than the problems, such as faster attack detection and improved accuracy. Additionally, they made people aware of how adversarial networks might deceive the system.

The KDD Cup dataset is the most frequently used, according to an examination of the literature. The inability to obtain real-time datasets is the primary cause of the same. For their experimentation, the authors of [65] produced a fresh dataset using Wireshark. They had created a hybrid IDS using K-Means clustering and Support Vector Machines (SVM) [66]. Using the UNSW-NB15 and NIMS botnet datasets, Moustafa et al. developed a successful NIDS system. They suggested an AdaBoost ensemble method, which successfully detected aberrant traffic [67].

To efficiently detect anomalies, Bagga et al. created a scalable system employing software-defined networking, network function, and visualisation techniques [68] [69]. Liu et al. conducted a similar study for anomaly traffic identification using machine learning utilising a real-time dataset they produced. Hussain et al. conducted a thorough investigation to discover the many attack vectors and the application of machine learning and deep learning to improve the attack detection rate [70] [71].

To fix the shortcomings of the earlier ML models, Shafiq et al. suggested a novel feature selection strategy using machine learning algorithms [72]. Atam and Hariri

[73] developed an anomaly detection approach employing ngrams specifically for WIFI anomaly detection. All of these studies emphasize the value of ML in raising the rate of attack detection. A standard detection system won't be a workable option because the data supplied by IoT apps varies. Therefore, more study must be done.

Numerous cutting-edge solutions successfully stop innumerable attacks, including firewalls, antivirus software, and access control systems. Most researchers concentrate on intrusion detection to achieve better outcomes, utilizing various machine learning and DL algorithms. ML techniques are employed to identify assaults; however, they have some limitations. Pre-processing data requires specialized knowledge, and the attack detection rate could be better. To achieve better outcomes, vast amounts of training data are needed, which could be more practical, especially in a heterogeneous setting. DL is more effective because it can accurately estimate network traffic and spot unauthorized data invasions [74]. DL algorithms are more effective at detecting known and undiscovered assaults than conventional methods, especially in IoT networks where devices create enormous volumes of data [75] [76].

In an effort to improve the NSL-KDD dataset, researchers proposed employing a Stacked Denoising Autoencoder Supporting Vector, leveraging insights from the KDD Cup99 dataset . Their findings yielded significantly low false positive and false negative rates, accompanied by a notably high accuracy rate. Additionally, another study focused on developing a multi-class neural network model for rapid identification of IoT Botnet attacks [78]. The Mirai-RGU dataset and the MedBIoT dataset were compatible with the suggested model. To simplify and expedite the learning process, this research introduced the Fast GRNN algorithm. The other two models were examined with both datasets (LSTM and GRU). The proposed technique improved the F1 score while reducing training and detection times. The whole training of the suggested system required one minute for the MedBIoT dataset and two minutes for the Mirai-RGU dataset. Both datasets had a 29-second detection completion time. For the multi-classification of MedBIoT and Mirai-RGU, the F1 scores were 99.99% and 99.04%, respectively.

In their work, the authors introduced the BLSTM phishing detection model outlined in [79], aimed at identifying phishing attacks and elucidating information security functions. For this study, they utilized phishing website datasets comprising 2456 instances and 30 attributes. In comparison to the conventional random forest model, which yielded an attack rate of 87.53%, the experimental findings showcased robust network security, achieving an impressive attack detection rate of 95.47%.

DOI: 10.31695/IJASRE.2024.7.

Researchers introduced a novel deep learning strategy to classify the DDoS attack on the IoT in the paper referenced in [80]. Employing an emerging feature fusion method and a loss function grounded in category cross-entropy, the authors meticulously outlined a convolutional neural network (CNN) model. This innovative approach, utilizing GPU-enabled Tensor Flow, facilitated a put-ahead detection technique, evaluated on the widely accessible NSL-KDD dataset. Comparisons were drawn with established techniques including CNN, SVM, DT, Bayes, KNN, and RNN algorithms. The proposed system exhibited remarkable accuracy and a notably reduced false alarm rate in contrast to existing methodologies.

In [81], the model's performance was evaluated using both the NSL-KDD and ISCXIDS 2012 datasets. Employing Wireshark, the authors conducted visual traffic analysis and experiments to showcase the efficacy of their proposed approach. The results indicated the superiority of the proposed model over other pertinent machine learning techniques like RF, Decision Tree, Naive Bayes, Support Vector Machine, and Multi-Layer Perceptron Neural Network in terms of accuracy. In a separate study [82], deep learning techniques for intrusion detection were classified. The authors detailed the training and evaluation of four significant deep learning models—feed-forward ANN, AE, DBN, and LSTM—utilizing two legacy and two contemporary datasets. The findings highlighted that the deep feed-forward ANN achieved favorable assessment metrics across all four datasets.

In [83], an anomaly-based network IDS was suggested. The researchers proposed an effective IDS built around the pruning of the P-DNN deep neural network. Researchers developed an adequate attack detection performance using this technique after training a DNN with a compound system. Through the pruning operation, researchers could simplify this model's complexity. After that, they retrained the deep neural network to determine the best model. To evaluate the model, the researchers used the KDD Cup 99 dataset. The findings demonstrated that the new P-DNN model achieved a 99% attack identification rate for investigated assaults and a 1% attack identification rate for unidentified attacks. We may comprehend that the proposed model performs less well against novel attacks.

In an increasingly linked world, the role of AI in IoT data security is changing quickly and redefining the cyber defence landscape. Organizations may strengthen their defences against changing threats using AI's analytical skills, adaptability, and predictive capabilities. However, to fully realise the potential of AI in safeguarding IoT networks, a comprehensive strategy that considers privacy, collaboration, and continual innovation will be essential. As technology advances, ongoing research and development will be required to avoid new difficulties and build a safer and more secure IoT ecosystem for everyone.

7. IoT- IDS CLASSIFICATION BASED ON DATASETS

For the purpose of shrinking the feature subset search space, [84]adopted the filter feature selection approach, which combines Information Gain and Random Forest Importance. Then, using RFE as a wrapper feature selection approach redundant features were further removed recursively on the smaller feature subsets. The suggested strategy can increase the accuracy of anomaly identification while decreasing the feature dimension, based on experimental findings employing UNSW-NB15dataset. [85] designed a special network IDS that is essential to network security and protects against existing threats occurring in the networks employing the standard UNSW-NB15 dataset. The recommended approach is built as multiclass network IDS utilizing machine learning classifiers. It is broken down into a number of supervised machine learning-based phases. Prior to using the Extremely Randomized Trees Classifier for selecting the key attributes for each class that already exists within selected dataset in accordance with Gini Impurity criterion(Extra Trees Classifier), the dataset’s imbalanced classes are first addressed using the Synthetic Minority Oversampling Technique (SMOTE) method.

[86] proposed a features selection architecture for effective network anomaly detection employing several machine learning classifiers. By employing feature selection approaches for filters and wrappers, the framework employs several strategies. The objective of this framework is to choose the fewest features possible while still achieving the best level of accuracy.

[87] suggested a unique hybrid approach of classification constructed on the Artificial Bee Colony (ABC) along with Artificial Fish Swarm(AFS)algorithms. Here, the Fuzzy C-Means Clustering (FCM) along with Correlation-based

DOI: 10.31695/IJASRE.2024.7.

Feature Selection (CFS) techniques are used for separating the training dataset, which also removes the unnecessary features. Additional If-Then signatures are created using the CART technique in accordance with the chosen criteria to distinguish between regular as well as anomalous records. Similar to this, the generated rules are trained using the suggested hybrid approach.

A Feed-forward Neural Network (FNN) is optimized by [88] to accurately identify DoS attack with minimal resource use. The three main stages of the suggested technique are mentioned as follows: capturing the incoming network traffic, selecting the necessary attributes for DoS attack detection employing the unsupervised Correlation based Feature Selection (CFS) technique and classifying the incoming traffic from the network as anomalous traffic or ordinary traffic. When compared to cutting-edge DoS detection techniques, the results are satisfactory. A hybrid approach determined from the centres of features value centres as well as an association rule mining algorithm was presented by [89] to minimize the FAR. Here proposed strategy is planned to apply within a minimum computation time since it constructed upon central feature scores when splitting data samples equally into pieces. The proposed method adopts the highest ranked characteristics fromtheUNSW-NB15 as well as NSLKDD data sets.

According to the proposed results by [90], the multi-classification accuracy of MLP is increased from 82.25 percent to 84.24 percent while the feature dimension is decreased from 42 to 23. To minimize the uncertainty in cyberspace, [91] developed an ensemble classifier. The machine learning model was trained using the classification technique in MATLAB employing the UNSW-NB15 and datasets acquired locally. Here multiclass classification was carried out on the both the mentioned datasets, bachfisch contains distinct attack category subsets. Using an ensemble classifier in MATLAB's classification learner, the suggested model was examined on the datasets, with 30% of the datasets being kept for validation. Performance evaluation metrics included confusion matrix, receiver operating characteristic (ROC) curve and accuracy. The trials yielded good classification results with an accuracy as 99.1%as well as 99.4%respectively, on the combined csv files of UNSW-NB15 dataset along with self acquired dataset .Both the datasets used in the experiment showed that ensemble classification accuracy was superior to that of an artificial neural network classifier. The proposed ensemble model helped to resolve the classification of attack problems in network settings and cyberspace uncertainty with the help of its findings. The suggested strategy will effectively safeguard user interaction and cyberspace infrastructures.

[92] concentrate on a vital aspect of computer networking with their discussion of network security and the possibility for automation in this area. Upon the benchmark dataset UNSW-NB15, an exploratory data analysis was performed. Due to its more uniform pattern distribution, this dataset is a more recent replacement for the outdated KDD'99 dataset. The system uses a range of ensemble approaches, such as Random Forest, AdaBoost, Extra Trees as well as XGBoost to get ideas about information so as to produce usable conclusions. The commonly used performance parameters were calculated in order to assess all of the employed classifiers. The paper provides details, considers challenges and potential strategies for machine learning in networking in the future.

A unique Routing Technology over Lightweight and Lossy Channels whichsupportsIPv6 was put forth as per [93] Depending on the application, vital, sensitive information is transferred between these networks' nodes, which are located in hazardous areas. As a result, a network's security is essential. Intrusion detection systems, which are important in securing these kinds of networks, are computationally expensive because of the constrained capabilities of nodes carrying sensors. To make best possible use of the electric power coming from each of the sensor nodes, a rule-based approach is used within the base location. Empirical findings prove that the suggested technique performs well in identifying multiple intrusions.

For RPL-based IoT networks, [94] proposal to enhance ANIDS performance was made. The recommended voting ensemble classifier integrates outcomes from various base classifiers, such as logistic regression, support vector machines, decision trees, bidirectional long short-term memories, and K-nearest neighbors, to accurately identify anomalies through majority voting rules. Optimal sizes for core classifiers are determined using the simulated annealing-based improved salp swarm algorithm (SA-ISSA), a feature selection approach that combines the salp swarm algorithm, opposition-based learning, and particle swarm optimization. The study is conducted utilizing the RPL-NIDDS17 dataset, encompassing seven distinct types of attack events. The efficacy of the proposed strategy is

DOI: 10.31695/IJASRE.2024.7.

evaluated and compared against state-of-the-art feature selection and classification methods in terms of accuracy, attack detection rate (ADR), false alarm rate (FAR), and other metrics. The suggested ensemble classifier achieves superior results, with higher accuracy (96.4%), higher ADR (97.7%), and lower FAR (3.6%), showcasing its effectiveness in intrusion detection.

[95] introduced a methodology for botnet detection employing machine learning algorithms. The model investigated potential anomalies indicative of a botnet in a collection of Internet of Things gadgets trying to establish a network connection. This paper showed how to leverage information generated by Internet of Things (IoT) devices at the transport layer, specifically via the User Datagram Protocol (UDP). A new intelligent model based on Random Forest Classifier and Independent Component Analysis (ICA) has been developed for botnet detection among IoT gadgets. Machine learning techniques of varying types were also applied to the results for further comparison. Experimental findings of the proposed algorithm yielded cutting-edge results for all three separate datasets, with accuracy as much as 99.99 percent achieved efficiently considering the shortest prediction time of 0.12 seconds with no overfitting. To effectively and efficiently detect botnets in IoT devices, this study combines ICA along with Random Forest Classifier, a basic machine learning algorithm.

In order to detect botnet attacks within IoT networks. [96] proposed ELBA-IoT, a model of ensemble learning that monitors characteristics of Io network behaviour and utilises ensemble learning for recognizing abnormal traffic on the network via compromised IoT gadgets. Here suggested IoT-based botnet detection method is also characterized by an examination of three distinct machine learning classifiers, all of which are decision tree techniques (Adaboost, RUS Boosted, and bagged). With subject to this evaluation, ELBA-IoT was applied to the N-BaIoT-2021dataset, that records typical IoT network traffic as well as botnet attack traffic from compromised IoT devices. The experimental findings demonstrate that the ELBA-IoThas an outstanding detection accuracy (99.6%) and minimal inference overhead(40-seconds) for detecting botnet attacks accomplished from compromised Io gadgets. To further demonstrate ELBA-IoT's efficiency the authors compared their findings to those of competing approaches.

Two LSTM-based classification algorithms for botnet categorization were described by [97] with greater than 98 percent accuracy. The adversarial attacks then suggested, which lowers the accuracy to roughly 30%. The defense approach is the suggested to raise the accuracy to roughly 70% by looking at the methods for computing uncertainty. The uncertainty of the accuracy of the suggested methods has been evaluated utilising the deep ensemble and stochastic weight averaging quantification methods. [98] proposed using a integrated machine learning technique called XGB-RF to detect intrusions. The suggested hybrid strategy was used to test on the N-BaIoT dataset, which includes assaults from malicious botnets. Researchers used the Random Forest (RF) feature selector as well as the Extreme Gradient Boosting (XGB) classifier to look for intrusions into IoT environments. Several metrics are used to evaluate the XGB-RF proposal, and the results demonstrate that it can accurately predict 99.94%of attacks. When contrasted with the most recent algorithms, the proposed model consistently produce superior results. The proposed method is effective at detecting botnet attacks, which is a major cause for concern when it comes to the security of IoT systems.

[99] devised a strategy employing a variety of classifier approaches, including K-Nearest Neighbor, Naive Bayes, Adaboost with Decision Tree, Support Vector Machine, Random Forest, and Artificial Intelligence, to discern representations of botnet attacks across the CSE-CIC-IDS2018 cyber dataset. The classification results are presented in terms of precise precision for each classifier. Furthermore, the proposed framework utilizes calibration curves, a common analytical tool, to generate performance diagrams, which are subsequently utilized to assess the accuracy of predicted probabilities generated by various classifiers. The final graph displays how well the AI method performs in comparison to other classifiers and includes reliability diagrams for checkingthe accuracy of the predicted probabilities of various classifiers.

Hybrid deep learning was presented by [100] to detect botnet assaults like BASHLITE as well as Mirai on nine commercial IoT devices. This has been accomplished by combining the long short-term memory (CNN-LSTM) method with convolutional neural network. Detailed experimental research was carried out using real world N-BaIoT collection that was taken from a functioning device and also which included both safe and unsafe patterns. The testing

DOI: 10.31695/IJASRE.2024.7.

results demonstrated that the CNN-LSTM approach is most effective having accuracies around 90.88%and 88.61%atrecognising botnet assaults from doorbells, while the suggested method performed well (88.53 percent) when applied to thermostat devices. The proposed solution was able to identify botnet attacks using security cameras with an accuracy of 87.19%, 89.23%, 87.76%, and89.64%, respectively. For the most part, the CNN-LSTM approach proved to be effective at observing botnet attacks originating from different kinds of IoT gadgets. [101] updated the identification process for intrusion detection methods by using a new dataset. In order to prove that Random Forests provide the highest accuracy, the proposed simple method makes use of various algorithms.

[102] presented a DL based botnet attack detection framework of dealing with highly asymmetric network traffic data. Whenever Deep Recurrent Neural Networks (DRNNs) learn structured feature representations using balanced network traffic information techniques. Using the Bot-IoT dataset, researchers have created DRNN plus SMOTE-DRNN models. While the baseline model had accuracy of 99.50%, recall of 99.75%, F1score of 99.62%, AUC of 99.87%, GM of 99.74%, and MCC of 99.62%, where as the SMOTE-DRNN model had accuracy of 99.60%, recall of 99.75%, F1 score of 99.62%, AUC of 99.87%, and MCC of 99.62%. Even state-of-the-art ML and DL models were not comparable with SMOTE-DRNN.

Here, IDS work is summarized by various researchers for three IoT based IDS Datasets, UNSW-NB15, RPL-NIDDS17 and N-BaIoT18. In UNSW-NB15 dataset, most of authors used binary and multiclass classification scheme to predict the intrusion, in which most of them have employed supervised machine learning algorithms with various feature extraction technique. In the scenario of RPL-NIDDS17 dataset, classification is performed by machine learning algorithms with supervised approach having binary and multiclass prediction. In N-BaIoT18 dataset, deep learning along with machine learning are used for prediction of IDS through random feature selection. Performance evaluation of all prediction system is evaluated using accuracy, precision, recall, f-score, sensitivity and specificity. It has been observed that still most of researchers have not achieved better performance with their respective proposed system, hence it is necessary to build the system which overcome the drawback of existing system and improve the efficiency of system.

Table 4: IDS proposals for IoT - Security threats

Data Set	Author/Reference	Machine Learning Approach	Feature Selection Approach	Performance Parameters
UNSW-NB15	[26]	Genetic-Fuzzy	Genetic-Fuzzy Algorithm, Ranking technique	Accuracy 90.24% FAR 13.04%
UNSW-NB15	[50]	Support Vector Machine ,Logistic Regression, Gradient Boost Machine	Random Forests and Recursive Feature Elimination	Accuracy 86.04%
UNSW-NB15	[70]	Decision Tree, Naive Bayes, Random Forest, SVM	Random Forest	Accuracy 97.49% Sensitivity 93.53%
UNSW-NB15	[87]	Ensemble classifier	K-means	Accuracy 90%
UNSW-NB15	[91]	Random forest	Random forest RF800, Ensemble Classifier	Accuracy 95.5% FAR 7.22%
RPL-NIDS-17	[14]	Ensemble ML (SVM DT KNN LR Bi- LSTM)	Novel feature selection technique (SA-improved SSA)	Accuracy 0.88 Precision 0.69 ADR 0.79 F-measure 0.73 Specificity 0.91 FAR 0.088
RPL-NIDS-17	[28]	Lightweight intrusion detection algorithm	Population-based algorithm and an optimization technique	Accuracy 0.94 Sensitivity 0.95 Specificity. 0.85 F-Score 0.89

DOI: 10.31695/IJASRE.2024.7.

8. GAPS IN THE RESEARCH LITERATURE

The following research gaps have been identified from the review of the literature which needs to be addressed.

1. IDS Detection Technique: It has been observed from the literature that the huge diversity of IoT devices makes it difficult to develop specific signature or specifications for each intrusion and attack type. Therefore, the machine learning techniques are highly effective to continuously monitor and analyze vast amount of IoT network and sensing data for intrusions. However, there are limitations in existing literature on machine learning based IoT network intrusion detection. Some of these schemes [93, 96,98,99] have been validated experimentally and lack evaluations on any dataset. On the other hand, most of the schemes [78] have been evaluated on outdated datasets which are not explicitly designed for use in IoT networks. While, a few of them [52] have been trained on IoT datasets, their performance is low and they incur large overhead on the IoT network. So, there is a need for machine learning techniques that are trained and tested on IoT datasets and make accurate predictions while incurring zero or low overhead on the IoT network and devices.
2. Lack of IoT Dataset for IDS Evaluation: Machine learning based IDS requires a realistic and high-quality dataset to produce an unbiased result in the training and testing phase. From literature review, it has been observed that researchers seldom use datasets applicable for IoT networks. As can be seen from Table 2.13, most of the works used KDDCup [48], NSL-KDD [49], CICIDS [50] and ISCXIDS [24] datasets to evaluate and test the proposed solutions. These datasets are outdated, created in different environment and not explicitly designed for IoT network. In addition, these datasets are based on different set of protocols, architecture and attacks to those used in IoT networks. Other synthetic datasets like [52] are based on common IoT routing protocol, the RPL and include only the traces of routing attacks. UNSW- NB15 [38] dataset contains traces of single IoT protocol, the MQTT while others represent particular scenarios like botnet malware [28] or smart cities network [10]. A common limitation with these datasets is the lack of multi-layer attacks on standard IoT protocols like RPL for routing, UDP for transport communication, ICMPv6 and IPv6 for network and CoAP for application layer. The non-availability of these dataset in public domain for further research is yet another challenge. Therefore, creating a dataset with these protocols in public domain is significant to produce accurate results.
3. IoT Targeted Attacks: The majority of existing IDSs primarily target routing layer attacks on RPL within IoT networks. However, there is a notable absence of studies focusing on other well-known attacks affecting different layers of the IoT stack, which could potentially lead to catastrophic consequences for IoT networks. In [21], researchers surveyed machine learning techniques for detecting ICMPv6-based DDoS attacks and emphasized the necessity for ML-based solutions in IoT to detect such attacks. Moreover, none of the existing studies address the concept of cross-layer attacks that can impact multiple layers of the IoT communication stack simultaneously. Hence, the development of a cross-layer solution that considers attacks across various layers is imperative for bolstering IoT network security.
4. Lack of multi-attacker scenarios: A notable limitation identified in the literature is the tendency for most proposals to solely address single attacker scenarios, overlooking the possibility of a realistic IoT network being compromised by multiple attackers concurrently. Evaluations have predominantly been conducted in a constrained manner, often with a single malicious node. Therefore, it becomes imperative to consider the impact of multiple attackers on the network while evaluating IDS effectiveness .
5. Scalability: Scalability is important factor to measure the performance of system in a large and dynamic network. Unfortunately, most of the studies in literature evaluate their IDS on smaller IoT networks with few nodes. Only works in [52] generate extensive dataset with hundreds of nodes in IoT network. So, evaluation of IDS on scalable IoT network is an open area of research.
6. Limited Evaluation Parameters and Lack of Lightweight Solutions: It is quite evident from the literature that most of the schemes do not perform any evaluation on their proposed IDS while others lack evaluation with resource utilization metrics to visualize whether the IDS or IPS has any detrimental effect on the resources of IoT network. For instance, any additional network overhead can cause depletion of energy resources of the

DOI: 10.31695/IJASRE.2024.7.

IoT device. Thus, security solutions that are lightweight should be explored that do not impose any burden on resources of IoT networks.

7. Limited IPS solutions: A discernible trend in the literature is the limited discussion on effective preventive measures to safeguard IoT networks from internal and external attacks, with only a few proposals addressing this aspect . Conversely, host-based Intrusion Prevention Systems (IPS) introduce significant performance issues and drain the resources of IoT devices . In light of these considerations, deploying and evaluating IPS for IoT could be prioritized on gateways or critical hosts housing sensitive information. IPS techniques such as limiting the number of request/response packets, implementing pushback protocols, real-time packet filtering, and conducting deep packet investigation for IoT systems warrant further research attention.

9. CONCLUSION

The rapid development and widespread adoption of IoT devices in recent years have significantly impacted various aspects of life, including healthcare, smart homes, and industrial automation. However, this expansion also introduces multiple security challenges, making IoT devices vulnerable to cyber threats. Intrusion Detection Systems (IDS) have become vital for IoT security, addressing risks like device susceptibility to viruses, denial-of-service attacks, and unauthorized intrusions. The literature reviewed for this research study delves into the current state of IoT IDS, exploring the IoT architecture, security issues, and the role of AI in IoT data security. It highlights different layered architectures (three-layered, four- layered, five-layered, and seven-layered) in IoT, each with specific functionalities across layers like perception, network, and application. It also examined various security concerns, including risks, threats, vulnerabilities, and different types of attacks like physical, network, software, and encryption attacks. Furthermore, the review emphasized the critical role of AI, particularly Machine Learning (ML) and Deep Learning (DL), in enhancing IoT data security. AI-based IoT IDS can learn from past attacks and adapt to new threats, offering a more dynamic defense mechanism compared to static traditional systems. The use of AI and ML in IoT security solutions, despite challenges like the need for large training datasets and specialized knowledge for data pre-processing, shows promising results in improving attack detection rates and addressing security vulnerabilities in IoT networks. From the literature it can be inferred that as IoT continues to evolve, it becomes increasingly important to develop robust security frameworks and leverage AI advancements to safeguard against a broad spectrum of cyber threats, ensuring the safe and secure operation of IoT systems.

In this paper, the extant literature on Intrusion Detection Systems (IDS) in IoT has been systematically classified according to various criteria, including detection techniques, placement methodologies, information sources, validation strategies, and evaluation metrics, among others. This paper aims to outline all the research contributions made toward the development of IDS for IoT. Additionally, it provides a comprehensive review of datasets available for evaluating IDS in the IoT domain, along with an analysis of preprocessing techniques applied to these datasets. A discussion on proposal implementing IPS in IoT has been presented. Towards the end, some of the gaps existing in the literature have been presented which need to be addressed.

REFERENCES LIST

[1] I. Markit, “The internet of things: a movement, not a market,” tech. rep., IHS Markit, London, 2018. [Online]. Available:https://cdn.ihs.com/www/pdf/ IoT ebook.pdf. [Accessed on 02-Jan-2020]. [2] Q. Stafford-Fraser, “On site: The life and times of the first web cam,” Communications of the ACM, vol. 44, pp. 25–26, July 2001.

[2] K. Ashton, “That ‘internet of things’ thing,” RFID journal, vol. 22, no. 7, pp. 97–114, 2009. [4] C. Bormann, M. Ersue, and A. Keranen, “Terminology for constrained-node networks,” RFC 7228, IETF, May 2014.

[3] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of things: A survey on enabling technologies, protocols, and applications,” IEEE communications surveys & tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.

DOI: 10.31695/IJASRE.2024.7.

[4] R. D. Pietro, L. V. Mancini, C. Soriente, A. Spognardi, and G. Tsudik, "Catch me (if you can): Data survival in unattended sensor networks," in Proceedings of 6th Annual IEEE International Conference on Pervasive Computing and Communications, (Hong Kong, China), pp. 185–194, IEEE, 2008.

[5] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the internet of things: perspectives and challenges," Wireless Networks, vol. 20, no. 8, pp. 2481–2501, 2014.

[6] T. Borgohain, U. Kumar, and S. Sanyal, "Survey of security and privacy issues of internet of things," arXiv preprint arXiv:1501.02211, 2015.

[7] B. Glover and H. Bhatt, RFID essentials. Sebastopol, California: O'Reilly Media, Inc., 2006. [10] F. Javed, M. K. Afzal, M. Sharif, and B. Kim, "Internet of things (iot) operating systems support, networking technologies, applications, and challenges: A comparative review," IEEE Communications Surveys Tutorials, vol. 20, pp. 2062– 2100, thirdquarter 2018.

[8] M. R. Palattella et al., "Standardized protocol stack for the internet of (important) things," IEEE Communications Surveys and Tutorials, vol. 15, no. 3, pp. 1389–1406, 2013.

[9] S. Raza, L. Wallgren, and T. Voigt, "Svelte: Real-time intrusion detection in the internet of things," Ad hoc networks, vol. 11, no. 8, pp. 2661–2674, 2013.

[10] M. Alam, "Cloud algebra for handling unstructured data in cloud database management system," International Journal on Cloud Computing: Services and Architecture (IJCCSA), vol. 2, pp. 01–08, sep 2018.

[11] C. Maple, "Security and privacy in the internet of things," Journal of Cyber Policy, vol. 2, no. 2, pp. 155–184, 2017.

[12] W. Stallings, Cryptography and Network Security: Principles and Practice. India: Prentice Hall, 1999.

[13] J. Ye, X. Cheng, J. Zhu, L. Feng, and L. Song, "A ddos attack detection method based on svm in software defined network," Security and Communication Networks, vol. 2018, pp. 1–8, 2018.

[14] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "Ddos in the iot: Mirai and other botnets," Computer, vol. 50, no. 7, pp. 80–84, 2017.

[15] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures," in Proceedings of the IEEE International Workshop on Sensor Network Protocols and Applications, (Anchorage, AK, USA), pp. 113–127, IEEE, May 2003.

[16] A. Mayzaud, R. Badonnel, and I. Chrisment, "A taxonomy of attacks in rpl-based internet of things," International Journal of Network Security, vol. 18, no. 3, pp. 459 – 473, 2016.

[17] A. Abdollahi and M. Fathi, "An intrusion detection system on ping of death attacks in iot networks," Wireless Personal Communications, vol. 112, no. 4, pp. 2057–2070, 2020.

[18] Z. Inayat, A. Gani, N. B. Anuar, M. K. Khan, and S. Anwar, "Intrusion response systems: Foundations, design, and challenges," Journal of Network and Computer Applications, vol. 62, pp. 53–74, 2016.

[19] N. Moustafa, J. Hu, and J. Slay, "A holistic review of network anomaly detection systems: A comprehensive survey," Journal of Network and Computer Applications, vol. 128, pp. 33–55, 2019.

[20] F. Y. Yavuz, D. Unal, and E. G ¨ ul, "Deep learning for detection of routing attacks in ¨ the internet of things," International Journal of Computational Intelligence Systems, vol. 12, no. 1, pp. 39–58, 2018.

[21] M. N. Napiah, M. Y. I. B. Idris, R. Ramli, and I. Ahmedy, "Compression header analyzer intrusion detection system (cha-ids) for 6lowpan communication protocol," IEEE Access, vol. 6, pp. 16623–16638, 2018.

DOI: 10.31695/IJASRE.2024.7.

[22] E. Canbalaban and S. Sen, "A cross-layer intrusion detection system for rpl-based internet of things," in Proceedings of International Conference on Ad-Hoc Networks and Wireless, (Bari, Italy), pp. 214–227, Springer, 2020.

[23] M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, and M. Guizani, "A survey of machine and deep learning methods for internet of things (iot) security," arXiv preprint arXiv:1807.11023, 2018.

[24] J. Arshad, M. A. Azad, K. Salah, W. Jie, R. Iqbal, and M. Alazab, "A review of performance, energy and privacy of intrusion detection systems for iot," arXiv preprint arXiv:1812.09160, 2018.

[25] E. Benkhelifa, T. Welsh, and W. Hamouda, "A critical review of practices and challenges in intrusion detection systems for iot: Toward universal and resilient systems," IEEE Communications Surveys & Tutorials, vol. 20, no. 4, pp. 3496–3509, 2018.

[26] M. F. Elrawy, A. I. Awad, and H. F. Hamed, "Intrusion detection systems for iot-based smart environments: a survey," Journal of Cloud Computing, vol. 7, no. 1, p. 21, 2018.

[27] S. Choudhary and N. Kesswani, "A survey: Intrusion detection techniques for internet of things," International Journal of Information Security and Privacy (IJISP), vol. 13, no. 1, pp. 86–105, 2019.

[28] K. A. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. C. de Albuquerque, "Internet of things: A survey on machine learning-based intrusion detection approaches," Computer Networks, vol. 151, pp. 147–157, 2019.

[29] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, "Network intrusion detection for iot security based on learning techniques," IEEE Communications Surveys & Tutorials, vol. 21, pp. 2671 – 2701, 2019.

[30] 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," Cybersecurity, vol. 4, no. 1, pp. 1–27, 2021.

[31] L. Johansson and O. Olsson, "Improving intrusion detection for iot networks," Master's thesis, University of Gothenburg, Gothenburg, Sweden, 2018.

[32] J. Granjal and A. Pedroso, "An intrusion detection and prevention framework for internet-integrated coap wsn," Security and Communication Networks, vol. 2018, pp. 1–14, 2018.

[33] A. M. da Silva Cardoso, R. F. Lopes, A. S. Teles, and F. B. V. Magalhaes, "Real- ˜ time ddos detection based on complex event processing for iot," in Proceedings of IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation, (Orlando, USA), pp. 273–274, IEEE, 2018.

[34] V. H. Bezerra, V. G. T. da Costa, S. B. Junior, R. S. Miani, and B. B. Zarpelao, "Oneclass classification to detect botnets in iot devices," in Proceedings of 18th Brazilian Symposium on Information Security and Computer Systems, (Natal, Brazil), pp. 43– 56, SBC, 2018.

[35] S. U. Jan, S. Ahmed, V. Shakhov, and I. Koo, "Towards a lightweight intrusion detection system for the internet of things," IEEE Access, 2019.

[36] J. Granjal, J. Silva, and N. Lourenc¸o, "Intrusion detection and prevention in coap wireless sensor networks using anomaly detection," Sensors, vol. 18, no. 8, pp. 1–17, 2018.

[37] A. Abbas, M. A. Khan, S. Latif, M. Ajaz, A. A. Shah, and J. Ahmad, "A new ensemble-based intrusion detection system for internet of things," Arabian Journal for Science and Engineering, vol. 47, pp. 1805–1819, 2021.

[38] P. Verma et al., "A novel intrusion detection approach using machine learning ensemble for iot environments," Applied Sciences, vol. 11, no. 21, pp. 1–21, 2021.

DOI: 10.31695/IJASRE.2024.7.

[39] A. Verma and V. Ranga, "Elnids: Ensemble learning based network intrusion detection system for rpl based internet of things," in Proceedings of 4th International Conference on Internet of Things: Smart Innovation and Usages, (Ghaziabad, India), pp. 1–6, IEEE, 2019.

[40] E. Aydogan, S. Yilmaz, S. Sen, I. Butun, S. Forsstrom, and M. Gidlund, "A central ¨ intrusion detection system for rpl-based industrial internet of things," in Proceedings of 15th IEEE International Workshop on Factory Communication Systems, (Sundsvall, Sweden), pp. 1–5, IEEE, 2019.

[41] A. A. Diro and N. Chilamkurti, "Distributed attack detection scheme using deep learning approach for internet of[137] M. Ahmad, Q. Riaz, M. Zeeshan, H. Tahir, S. A. Haider, and M. S. Khan, "Intrusion detection in internet of things using supervised machine learning based on application and transport layer features using unsw-nb15 data-set," EURASIP Journal on Wireless Communications and Networking, vol. 2021, no. 1, pp. 1–23, 2021. things," Future Generation Computer Systems, vol. 82, pp. 761–768, 2018.

[42] Faek, R., Al-Fawa'reh, M., & Al-Fayoumi, M. (2021). Exposing bot attacks using machine learning and flow level analysis. International Conference on Data Science, E-Learning and Information Systems 2021.

[43] Shinan, K., Alsubhi, K., Alzahrani, A., & Ashraf, M. U. (2021). Machine learning-based botnet detection in software-defined network: A systematic review. Symmetry, 13(5), 866.

[44] Wang, H., Muñoz-González, L., Eklund, D., & Raza, S. (2021). Non-IID data re-balancing at IoT edge with peer-to-peer federated learning for anomaly detection. Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks.

[45] Bagui, S., Department of Computer Science, University of West Florida, Pensacola, FL 32514 USA, Wang, X., & Bagui, S. (2021). Machine learning based intrusion detection for IoT botnet. International Journal of Machine Learning and Computing, 11(6), 399–406.

[46] Mihret, Estifanos. (2021). # Intrusion Detection System - IDS - Journal - by Sci-Tech with Estif.

[47] Popoola, S. I., Adebisi, B., Ande, R., Hammoudeh, M., Anoh, K., & Atayero, A. A. (2021). SMOTE-DRNN: A Deep Learning algorithm for botnet detection in the Internet-of-Things networks. Sensors (Basel, Switzerland), 21(9).

[48] [25] Özer, E., İskefiyeli, M., & Azimjonov, J. (2021). Toward lightweight intrusion detection systems using the optimal and efficient feature pairs of the Bot-IoT 2018 dataset. International Journal of Distributed Sensor Networks, 17(10), 155014772110522.

[49] Elhefnawy, R., Abounaser, H., & Badr, A. (2020). A hybrid nested genetic-fuzzy algorithm framework for intrusion detection and attacks. IEEE Access: Practical Innovations, Open Solutions, 8, 98218–98233.

[50] Verma, A., & Ranga, V. (2020). Mitigation of DIS flooding attacks in RPL-based 6LoWPAN networks. Transactions on Emerging Telecommunications Technologies, 31(2). https://doi.org/10.1002/ett.3802

[51] Murali, S., & Jamalipour, A. (2020). A lightweight intrusion detection for Sybil attack under mobile RPL in the internet of things. IEEE Internet of Things Journal, 7(1), 379–388.

[52] Foley, J., Moradpoor, N., & Ochen, H. (2020). Employing a machine learning approach to detect combined internet of things attacks against two objective functions using a novel dataset. Security and Communication Networks, 2020, 1–17.

[53] Verma, A., & Ranga, V. (2020a). Machine learning based intrusion detection systems for IoT applications. Wireless Personal Communications, 111(4), 2287–2310.

[54] Qurashi, M. A., Angelopoulos, C. M., & Katos, V. (2020). An architecture for resilient intrusion detection in IoT networks. ICC 2020 - 2020 IEEE International Conference on Communications (ICC).

DOI: 10.31695/IJASRE.2024.7.

[55] C. N. F. D. Jenny, "IoT-Botnet Detection using Long Short-Term Memory Recurrent Neural Network," Int. J. Eng. Res., vol. V9, no. 08, pp. 531–536, 2020.

[56] "TheUNSW-NB15dataset description." https://www.unsw.adfa.edu.au/unswcanberra-cyber/cybersecurity/ADFA-NB15-Datasets/ (accessed Feb. 15, 2021).

[57] K. Rai, M. S. Devi, and A. Guleria, "Decision Tree Based Algorithm for Intrusion Detection," Int. J. Adv. Netw. Appl., vol. 07, pp. 2828–2834, 2016.

[58] R. Hadidi, J. Cao, M. S. Ryoo, and H. Kim, "Toward collaborative inferencing of deep neural networks on internet-of-things devices," IEEE Internet Things J., vol. 7, no. 6, pp. 4950–4960, 2020,

[59] Q. A. Al-Haija and S. Zein-Sabatto, "An efficient deep-learning-based detection and classification system for cyber-attacks in iot communication networks," Electron., vol. 9,pp. 1–26, 2020, doi: 10.3390/electronics9122152.

[60] R. Panigrahi and S. Borah, "A detailed analysis of CICIDS2017 dataset for designing Intrusion Detection Systems," Int. J. Eng. Technol., vol. 7, no. 24, pp. 479–482, 2018.

[61] Kurniabudi, D. Stiawan, Darmawijoyo, M. Y. Bin Bin Idris, A. M. Bamhdi, and R. Budiarto, "CICIDS-2017 Dataset Feature Analysis with Information Gain for Anomaly Detection," IEEE Access, vol. 8, pp. 132911–132921, 2020.

[62] H. Dhillon and A. Haque, "Towards network traffic monitoring using deep transfer learning," in 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2020, pp. 1089–1096. doi: 10.1109/TrustCom50675.2020.00144.

[63] G. Van Houdt, C. Mosquera, and G. Nápoles, "A review on the long shortterm memory model," Artif. Intell. Rev., vol. 53, no. 8, pp. 5929–5955, 2020.

[64] R. Vinayakumar, M. Alazab, K. P. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep Learning Approach for Intelligent Intrusion Detection System," IEEE Access, vol. 7, pp. 41525–41550, 2019

[65] J. Shara, "Deep Learning Methods for Cybersecurity," in ICSNS XV-2021, 2021, pp. 1–18.

[66] J. P, J. Shareena, A. Ramdas, and H. A P, "Intrusion Detection System for IOT Botnet Attacks Using Deep Learning," SN Computer Science, vol. 2, no. 3. 2021.

[67] J. Kim, N. Shin, S. Y. Jo, and S. H. Kim, "Method of intrusion detection using deep neural network," in IEEE International Conference on Big Data and Smart Computing, BigComp 2017, 2017, pp. 313–316.

[68] Z. Ahmad et al., "Anomaly Detection Using Deep Neural Network for IoT Architecture," Appl. Sci., vol. 11, no. 15, pp. 1–19, 2021.

[69] R. C. Staudemeyer, "Applying long short-term memory recurrent neural networks to intrusion detection," South African Comput. J., vol. 56, pp. 136– 154, Jul. 2015.

[70] Supriya Shende, "Long Short-Term Memory (LSTM) Deep Learning Method for Intrusion Detection in Network Security," Int. J. Eng. Res., vol. V9, no. 06, pp. 1615–1620, 2020.

[71] Y. Li et al., "Robust detection for network intrusion of industrial IoT based on multi-CNN fusion," Measurement, vol. 154, pp. 1–10, 2020.

[72] X. Zhang, J. Ran, and J. Mi, "An Intrusion Detection System Based on Convolutional Neural Network for Imbalanced Network Traffic," in 2019 IEEE 7th International Conference on Computer Science and Network Technology, 2019, pp. 456–460.

[73] M. Azizjon, A. Jumabek, and W. Kim, "1D CNN based network intrusion detection with normalization on imbalanced data," in 2020 International Conference on Artificial Intelligence in Information and Communication (ICAIIC), 2020, pp. 218–224.

DOI: 10.31695/IJASRE.2024.7.

[74] B. Susilo and R. F. Sari, "Intrusion detection in IoT networks using deep learning algorithm," Information, vol. 11, no. 5, pp. 1–11, 2020.

[75] M. A. Al-Garadi, A. Mohamed, A. Al-Ali, X. Du, and M. Guizani, "A Survey of Machine and Deep Learning Methods for Internet of Things (IoT) Security," IEEE Commun. Surv. Tutorials, vol. 22, no. 3, pp. 1646–1685, 2020.

[76] M. A. Khan, "HCRNNIDS: Hybrid Convolutional Recurrent Neural Network-Based Network Intrusion Detection System," Processes, vol. 9, no. 5, pp. 1–14, 2021.

[77] "IoT network intrusion dataset | IEEE DataPort." https://ieeedataport.org/open-access/iot-network-intrusion-dataset (accessed Mar. 04, 2022).

[78] H. Hanan, T. Christos, A. Robert, B. Ethan, and B. Xavier, "MQTT-IoTIDS2020: MQTT Internet of Things Intrusion Detection Dataset," IEEE Dataport, 2020.

[79] Y. H.-K. Vanlalruata Hnamte, Hong Nhung-Nguyen, Jamal Hussain, "A Novel Two-Stage Deep Learning Model for Efficient Network Intrusion Detection," IEEE Access, vol. 11, pp. 37131–37148, 2023.

[80] Ž. Đ. Vujović, "Classification Model Evaluation Metrics," Int. J. Adv. Comput. Sci. Appl., vol. 12, no. 6, pp. 599–606, 2021, Accessed: May 03, 2023. [Online]. Available: www.ijacsa.thesai.org

[81] Y. Zhang, P. Li, and X. Wang, "Intrusion Detection for IoT Based on Improved Genetic Algorithm and Deep Belief Network," IEEE Access, vol. 7, pp. 31711–31722, 2019.

[82] M. Roopak, G. Yun Tian, and J. Chambers, "Deep learning models for cyber security in IoT networks," in 2019 IEEE 9th Annual Computing and Communication Workshop and Conference, CCWC 2019, 2019, pp. 452–457.

[83] R. Anushiya and V. S. Lavanya, "A Comparative Study on Intrusion Detection Systems for Secured Communication in Internet of Things," ICTACT J. Commun. Technol., vol. 12, no. 03, pp. 2527–2537, 2021.

[84] W. Yung-Chung, H. Yi-Chun, C. Han-Xuan, and T. Shu-Ming, "Network Anomaly Intrusion Detection Based on Deep Learning Approach," Sensors, vol. 23, no. 2171, pp. 1–21, 2023.

[85] X. Jun, H. Zunwen, and Z. Yan, "CNN-LSTM Combined Network for IoT Enabled Fall Detection Applications," in 2019 3rd International Conference on Artificial Intelligence, Automation and Control Technologies (AIACT 2019), 2019, pp. 1–7.

[86] K. Praanna, S. Sruthi, K. Kalyani, and A. S. Tejaswi, "A CNN-LSTM Model for Intrusion Detection System from High Dimensional Data," J. Inf. Comput. Sci., vol. 10, no. 3, pp. 1362–1370, 2020.

[87] A. Alferaidi et al., "Distributed Deep CNN-LSTM Model for Intrusion Detection Method in IoT-Based Vehicles," Math. Probl. Eng., pp. 1–8, 2022.

[88] R. A. Ramadan and K. Yadav, "A novel hybrid intrusion detection system (IDS) for the detection of internet of things (IoT) network attacks," Ann. Emerg. Technol. Comput., vol. 4, no. 5, pp. 61–74, 2020.

[89] S. Smys, Abul Basar, and Haoxiang Wang, "Hybrid Intrusion Detection System for Internet of Things (IoT)," J. ISMAC, vol. 2, no. 4, pp. 190–199, 2020.

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

[91] X. Zhang, Y. Zhou, S. Pei, J. Zhuge, and J. Chen, "Adversarial Examples Detection for XSS Attacks Based on Generative Adversarial Networks," IEEE Access, vol. 8, pp. 10989–10996, 2020.

[92] A. K. Sahu, S. Sharma, M. Tanveer, and R. Raja, "Internet of Things attack detection using hybrid Deep Learning Model," Comput. Commun., vol. 176, pp. 146–154, 2021.

DOI: 10.31695/IJASRE.2024.7.

[93] Z. E. Huma et al., "A Hybrid Deep Random Neural Network for Cyberattack Detection in the Industrial Internet of Things," IEEE Access, vol. 9, pp. 55595–55605, 2021.

[94] I. Ullah, A. Ullah, and M. Sajjad, "Towards a Hybrid Deep Learning Model for Anomalous Activities Detection in Internet of Things Networks," IoT, vol. 2, no. 3, pp. 428–448, 2021.

[95] M. Mahmoud, M. Kasem, A. Abdallah, and H. S. Kang, "AE-LSTM: Autoencoder with LSTM-Based Intrusion Detection in IoT," in International Telecommunications Conference, ITC-Egypt 2022, 2022, pp. 1–6.

[96] E. Mushtaq, A. Zameer, M. Umer, and A. A. Abbasi, "A two-stage intrusion detection system with auto-encoder and LSTMs," Appl. Soft Comput., vol. 121, pp. 108–768, May 2022

[97] A. Binbusayyis and T. Vaiyapuri, "Unsupervised deep learning approach for network intrusion detection combining convolutional autoencoder and oneclass SVM," Appl. Intell., vol. 51, no. 10, pp. 7094–7108, Oct. 2021.

[98] Z. Wu, H. Zhang, P. Wang, and Z. Sun, "RTIDS: A Robust TransformerBased Approach for Intrusion Detection System," IEEE Access, vol. 10, pp. 64375–64387, 2022.

[99] M. B. Umair et al., "A Network Intrusion Detection System Using Hybrid Multilayer Deep Learning Model," Big Data, pp. 1–10, Jun. 2022.

[100] A. Sardar, A. Issa, and Z. Albayrak, "DDoS Attack Intrusion Detection System Based on Hybridization of CNN and LSTM," Acta Polytech. Hungarica, vol. 20, no. 2, pp. 105–123, 2023.

[101] H. C. Altunay and Z. Albayrak, "A hybrid CNN+LSTM-based intrusion detection system for industrial IoT networks," Eng. Sci. Technol. an Int. J., vol. 38, pp. 101–113, Feb. 2023.

[102] E. Calik Bayazit, K. Sahingoz, and B. Dogan, "Deep Learning based Malware Detection for Android Systems: A Comparative Analysis," Tech. Gaz., vol. 30, no. 3, pp. 787–796, 2023

DOI: 10.31695/IJASRE.2024.7.