Int. J. Nonlinear Anal. Appl. 14 (2023) 1, 1413–1436
ISSN: 2008-6822 (electronic)
http://dx.doi.org/10.22075/ijnaa.2022.7095

On the performance of intrusion detection systems for the internet of things: State-of-the-Art in Research

Chovin Usman Najam[a,*], Ahmed M. Fakhrudeen[b]

[a]*Computer Science Department, College of Computer Science and Information Technology, Kirkuk University, Kirkuk, Iraq*

[b]*Software Department, College of Computer Science and Information Technology, Kirkuk University, Kirkuk, Iraq*

(Communicated by Javad Vahidi)

Abstract

Nowadays, the IoT attracts a multitude of research and industrial interests. Smaller and smarter devices are being implemented daily in multiple IoT domains. However, protecting IoT devices from cyber-attacks is critical to their operation. Confidential data is leaked as a result of malicious acts. As a result, device performance becomes crucial. Security risks are frequently made in IoT-based structures that impact their standard work. Therefore, to eliminate and mitigate these issues (attacks), the Intrusion Detection System (IDS) was proposed to fulfill this purpose. This paper aims to study the state of the art of the proposed IDS. Moving on, we critically review the proposed IDS-based machine learning algorithms. Based on this evaluation criteria, the solutions covering architectures, intelligent prediction and algorithms are critically reviewed. To achieve our goals, the paper presents challenges and open research areas in IoT design.

Keywords: Internet of Things, IoT Security Challenges, Intrusion Detection System, Machine Learning based IDS
2020 MSC: 68M11, 68M25, 68Q04

1 Introduction

With the recent rapid development of high-speed networks and smart gadgets, the IoT system has quietly and gradually entered our lives [102]. A relatively recent analysis [58] predicts that after two years, machine-to-machine (M2M) connectivity will rise rapidly from 2016 to 2024 (5.6 to 27 billion). In addition, from 2018 to 2025, the IoT industry's revenue is projected to rise from $892 to $4 trillion [40]. IoT will therefore be crucial in the upcoming market generation inside the growing digital economy. Controlling the number of IoT devices remotely is essential for information sharing and performing the needed functionality [4]. As shown in Figure 1, people primarily use IoT devices because they offer a variety of lightweight and connected solutions. However, such devices typically have limited computing and memory abilities [61, 13]. Most IoT devices are heterogeneous low-power devices with limited storage and processing power [46]. IoT systems communicate with one another to exchange information and provide services. Communication in a dispersed network ought to happen as quickly as possible. Additionally vulnerable to security risks are distributed networks [92].

[*] Corresponding author
Email addresses: stcha007@uokirkuk.edu.iq (Chovin Usman Najam), dr.ahmed.fakhrudeen@uokirkuk.edu.iq (Ahmed M. Fakhrudeen)

Received: July 2022 *Accepted:* October 2022

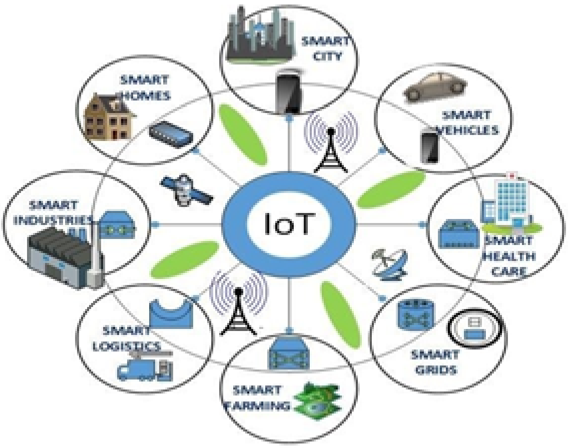

Figure 1: IoT devices connected to the internet

The IoT is still steadily spreading globally due to improved Internet and wireless access, wearable technology, the decreasing cost of embedded computers, advancements in storage technology, and cloud computing [3]. There are several academic and business interests currently drawn to the IoT. A growing number of IoT sectors, including housing, precision agriculture, infrastructure monitoring, personal healthcare, and autonomous vehicles, to name a few, are implementing smaller, smarter devices every day. However, several security risks try to take advantage of the flaws in the present IoT infrastructures and obtain sensitive and private data from IoT devices [4].

One of the significant security risks with IoT frameworks is the many devices connected to the network through sensors and actuators [6]. The majority of edge devices use outdated operating systems and are typically relatively small. As previously indicated, security is a concern in an IoT environment due to the limited resource nature of edge gadgets [5]. Gadgets at the edge layer need to answer components like correspondence, calculation, throughput, strength, power utilization, and heterogeneity. Supporting or improving the security of a framework must not compromise these critical requirements [89].

In current IoT systems, devices are connected and authenticated via a centralized server/client model. This approach would not be able to meet future IoT system expansion requirements [59]. In any case, such focused centralization has likewise caused a developing number of issues [110].

- Denial of service assaults is common in standard Internet service architectures, making services unavailable, as demonstrated by the global financial crisis (GFC) of 2008 [77].
- Most Internet services depend on centralized databases, creating one point of failure by providing assailants with one objective to infiltrate. For instance, when centralized frameworks like LinkedIn or When Google Services go down, all of the sites and projects that rely on them fall with them.
- Clients' personality data and errand arrangements are kept up within a concentrated dataset, which may now incorporate various parts of information security concerns. Clients have no clue about what happens behind the walls of centralized services. Subsequently, individuals have no clue about how much information these administrations gather approximately them and the way that information is utilized.

Besides, when a requester and provider debate, they require a reliable organization to give adjudication personnel. This can direct behavior referred to as “error reporting.” In summary, contemporary Internet administration executions accomplish decentralized data transmission and sharing. There has now no longer been enough scrutiny and motion in making sure transactional acceptance is true to guarantee the exchange of wealth or cost throughout the Internet [122, 45], differential privacy [118, 57], and encryption schemes [51, 52] are proposed to safeguard individual information security. Reputation-primarily based protection tools totally are meant to determine and foretell transaction integrity primarily based mostly on general use and reputation, all through a huge network of clients. To solve the failure issue, distributed architectures are offered. However, no existing work has addressed all issues at the same time. An intrusion detection system (IDS) can monitor network activity between linked devices and produce notifications when a breach is detected [107]. Because of its monitoring and alerting capabilities, an IDS is a vital defense tool for classical IP networks. Although IDS operates effectively in traditional networks, as yet evolving IDS for IoT networks is a difficult errand. This is due to the peculiarities of IoT networks. For example, the restricted processing and storage capacity of a network's IDS agent nodes [11]. An IDS is a protection factor that works predominantly inside the network layer of an IoT framework. IDSs can detect illegal network access to computer systems and take appropriate action based on security regulations. An IDS set up for a system of things ought to be the ability to evaluate information parcels and create real-time responses, examine facts packets in more than one layer of the IoT community by using numerous protocol stacks, and adapt to numerous IoT technologies [44]. The Security Operating Center (SOC) coordinates IDSs and computer hosts for attack countermeasures [81].

This chapter aims to study the state of the art of the proposed IDS. Moving on, we critically review the proposed IDS-based machine learning algorithms. Based on this evaluation criteria, the solutions covering architectures, intelligent prediction and algorithms are critically reviewed. To achieve our goals, the paper presents challenges and open research areas in IoT design.

This paper is organized as follows: Section 2 explains IoT's main architectures and characteristics. Section 3 presents the main challenges and concerns in IoT design and focuses on security concerns. At each layer, IoT attacks are detailed in Section 4. The taxonomy of IDSs is described in Section 5. Section 6 provides a critical literature review on implementing machine learning algorithms in IDS published in highly ranked journals, such as IEEE, Scopus, and Springer. Finally, we conclude the paper in Section 7. Figure 2 highlights the road map of this paper.

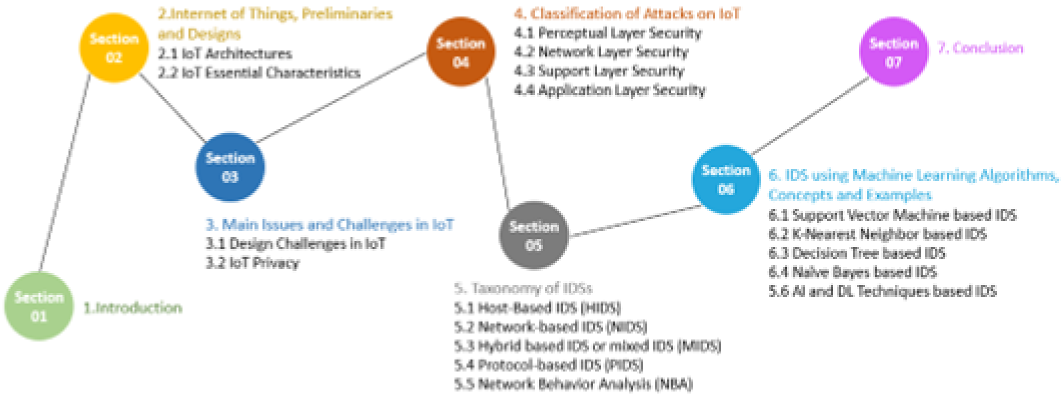
Section 02
2.Internet of Things, Preliminaries and Designs
2.1 IoT Architectures
2.2 IoT Essential Characteristics
Section 04
4. Classification of Attacks on IoT
4.1 Perceptual Layer Security
4.2 Network Layer Security
4.3 Support Layer Security
4.4 Application Layer Security
Section 07
7. Conclusion
Section 03
3. Main Issues and Challenges in IoT
3.1 Design Challenges in IoT
3.2 IoT Privacy
Section 06
6. IDS using Machine Learning Algorithms, Concepts and Examples
6.1 Support Vector Machine based IDS
6.2 K-Nearest Neighbor based IDS
6.3 Decision Tree based IDS
6.4 Naïve Bayes based IDS
5.6 AI and DL Techniques based IDS
Section 05
5. Taxonomy of IDSs
5.1 Host-Based IDS (HIDS)
5.2 Network-based IDS (NIDS)
5.3 Hybrid based IDS or mixed IDS (MIDS)
5.4 Protocol-based IDS (PIDS)
5.5 Network Behavior Analysis (NBA)
Section 01
1.Introduction

Figure 2: Organization of the paper

2 Internet of Things, Preliminaries and Designs

IoT devices can link and communicate with billions of things at the same time. It offers a variety of benefits to consumers that will alter how they interact with technology. Information from our environment may be collected using a variety of inexpensive sensors and connected gadgets, allowing us to improve our way of life [17].

The IoT concept is not new. The founder of the MIT auto-identification center, Ashton, stated in 1999, "The Internet of Things has the potential to revolutionize the world, just as the Internet did" Perhaps even more so [14].

A brief and basic example can demonstrate the Internet of Things in our daily life. Television is an example of an IoT display [10]. We can alternate the channel move by simply sitting at a specific location and not touching the television with a remote. The premise of IoT is similar; we may remotely operate nearly any electrical equipment in our surroundings [123]. IoT is a phenomenal innovation that influences us in light of how we respond to our conduct in daily routines [94]. Ranging from home electronics (such as refrigerators and air conditioners) to remote-controlled gadgets (such as televisions) to vehicles that take the shortest and safest path to us [27], Our watches and smartphones are capable of controlling everything. IoT is a broad organization, including associated gadgets [64]. The connected devices collect data, share how they are used, and carry out given tasks [97]. It's everything because of sensors. They are embedded in our phones and other electrical machines and sign-based devices related to the IoT association [41].

2.1 IoT Architectures

Researchers have not yet discovered a universal reference model appropriate for all IoT scenarios. Because of the absence of standardization of IoT items. Layered models and their targets/capabilities or objectives are discussed in other literature with slight variations. It depicts the results of a broad literature study conducted to discover distinct

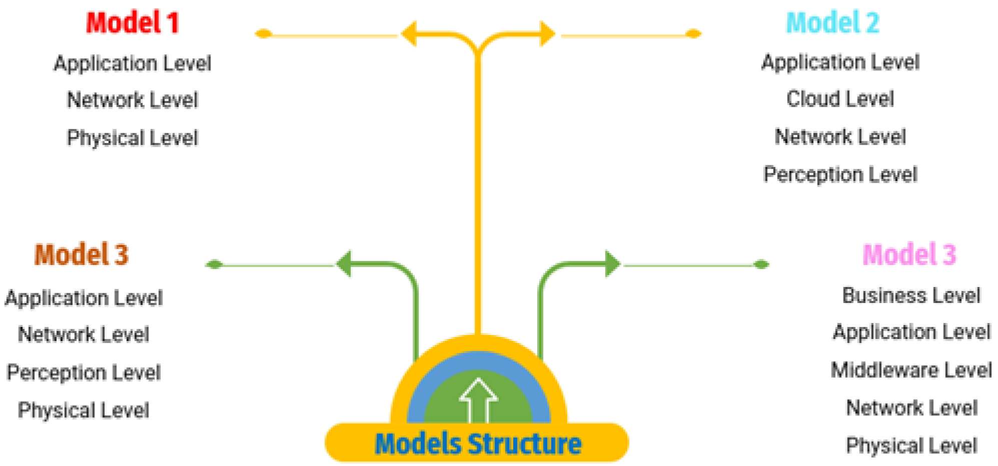

Figure 3: The layered architectures of IoT (three, four and five)

IoT architecture models. [72, 88, 65, 18, 113]. Generally, as illustrated in Figure 3, From the pool of suggested architectures, three- to five-tier are distinguished. The models, however, have parallels and essential differences, according to the study. Initially, a three-tiered model is shown.

- The physical layer comprises an assortment of IoT gadgets, like sensors (like remote for ecological observing, RFID labels, and cell phones [72, 88, 80]. This layer is in charge of establishing connections between different gadgets, replacing messages, and accumulating facts on the top level.
- The network layer is concerned with sending data that IoT devices have gathered or processed. Data are sent utilizing diverse exchange technology, which includes 4G, 5G, Wi-Fi, LPWaN, or Bluetooth [34, 83, 8].
- The application layer consists of numerous IoT applications that utilize enormous volumes of data gathered and handled in the preceding layers.

Since IoT innovation is constantly developing, a basic three-level model can't give a proper reflection. The following model viable is four-level. The Cloud Computing layer is the obvious distinction from the prior architecture. Some authors point out that cloud servers Can method considerable quantities of data more efficiently and quickly if they have the greater processing power, higher data evaluation tools, and bigger capacity storage. The fourth structure is a far extra distinct model from the first [72, 65]. Network and middleware are the two divisions of the network layer. The new network layer still manages data transport. In contrast, client needs are managed by the middle layer, prompt message, conveyance, data integration, and data formatting. Usually, there is a new level among IoT gadgets and IoT applications intending to resolve the interoperability issue. Furthermore, in this methodology, the creators have separated a business layer that is supposed to show a greater level of IoT biological system reflection. It is in responsible for the entire structure [65, 83].

2.1.1 Sensors

Sensors are critical components of intelligent devices. To gather information from nature, all IoT applications must include at least one sensor [76]. One of the fundamental bits of the IoT is the wake mode, which is senseless without sensor progression. IoT sensors are tiny in size, require negligible exertion, and consume lower power. Components like battery capacity and transmitting ease require them. Schmidt and Van Laerhoven present a diagram of the types of sensors used in the evolution of intelligent applications [100]. The list of several types of sensors utilized in IoT applications is provided in Figure 4.

2.1.2 Mobiles Sensor

Above all, take into account the ubiquitous personal phone, which has a variety of sensors. In particular, the personal phone is practical and easy to utilize, with several inherent correspondences and data preparation features.

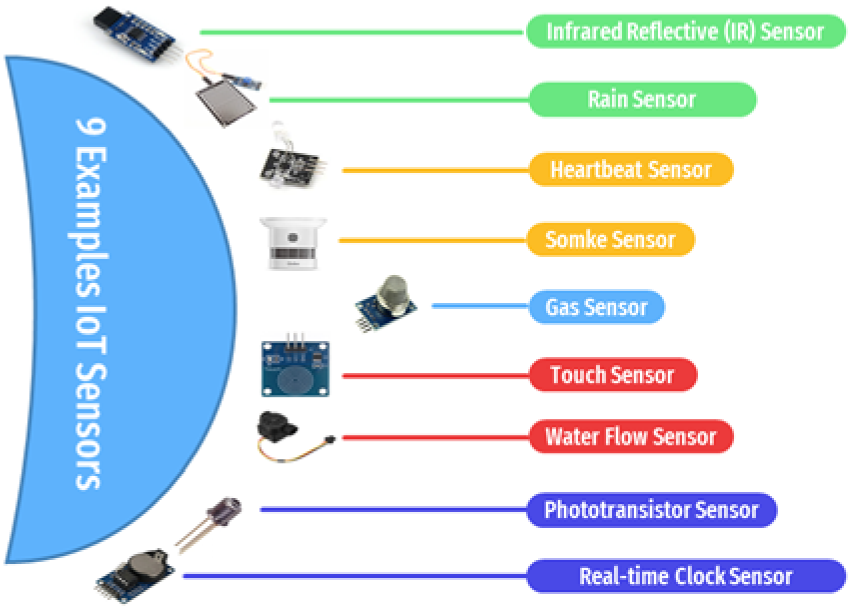

Figure 4: IoT Sensors

Due to the increased popularity of personal phones among people, researchers have expressed interest in developing more intelligent IoT preparations for using cell phones because of the incorporated sensors [62]. Depending on the situation, some other sensors may also be used. Applications for mobile devices that use sensor data to produce substantial results are possible [12].

2.1.3 Neural Sensors

The likelihood of identifying neurological symptoms in mind, assessing the condition of the brain, and educating it to improve thought and focus is much higher nowadays [26]. It is called Neurological observations. The development applied to monitor the alerts of the mind is called Electroencephalography (EEG), or the interface of a brain-computer [23]. The neurons' electronic transmission of internal ideas creates an electric field that may be quantified in terms of frequencies from the outside.

2.1.4 Actuator

An actuator is a gadget that could modify the earth by converting electrical vitality linked to a specific type of valuable vitality [112, 75]. These models include lighting, speakers, displays, cooling or heating components, and engines. Actuators can be characterized into three gatherings in light of their activities: electrical, pressure-driven, and pneumatic actuators. Mechanical movement powered by liquid or water is encouraged by pressure-driven actuators. Pneumatic actuators use the weight of packed air, and electrical ones use electrical energy.

2.1.5 Low Energy Bluetooth (LEB)

Also known as "Intelligent Bluetooth", Bluetooth Special Interest Group invented it [30]. Compared to competing conventions, it has a short reach and devours up low energy to some degree. The LEB convention stack is much like the stack applied in high-quality Bluetooth technology [109]. The controller host part is one of two. The controller is liable for the physical and association layer execution.

2.2 IoT Essential Characteristics

As illustrated in Figure 5, the essential characteristics of IoT are as follows:

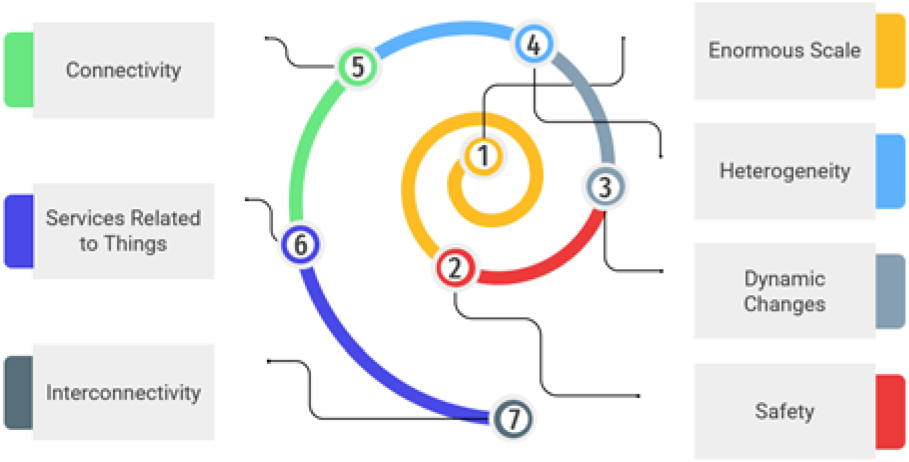

Figure 5: Characteristics of IoT

2.2.1 Enormous Scale

The number of IoT nodes that need to be handled and connected will be greater than those already connected to the Internet. The administration of the information generated and its analysis for application purposes will be critical. It is all about content semantics and content management.

2.2.2 Safety

Customers should remember security even as they enjoy the benefits of IoT. They should make security plans as IoT senders and receivers. It is a global message that stands for creating a measurable safety model. It involves the protection of networks and endpoints, as well as the security of consumer information and welfare.

2.2.3 Dynamic Changes

Device status varies significantly, including sleep and alertness, connection and disconnection, and IoT node content (speed and position). Additionally, the number of IoT nodes can change energetically.

2.2.4 Heterogeneity

Different IoT nodes rely on diverse hardware platforms and networks. They should use different networks to link to other nodes.

2.2.5 Connectivity

IoT can be compatible and easy to use as a result. Compatibility offers the same capabilities for utilizing and producing information and makes the network easier to access.

2.2.6 Services Related to things

IoT can offer various services relating to things inside the bounds of things. Both global and data will change ways to provide services connected to items within constraints.

2.2.7 Interconnectivity

Anything could be connected to universal data and make contact with the fundamental IoT organizational and physical structures [90].

3 Main Issues and Challenges in IoT

IoT is important in many areas of life; however, some problems and difficulties must be resolved. A diverse environment, growth in data storage, privacy concerns, and security concerns are among the most prevalent problems [111].

3.1 Design Challenges in IoT

As shown in Figure 6, the main issues of the IoT systems are categorized as follows.

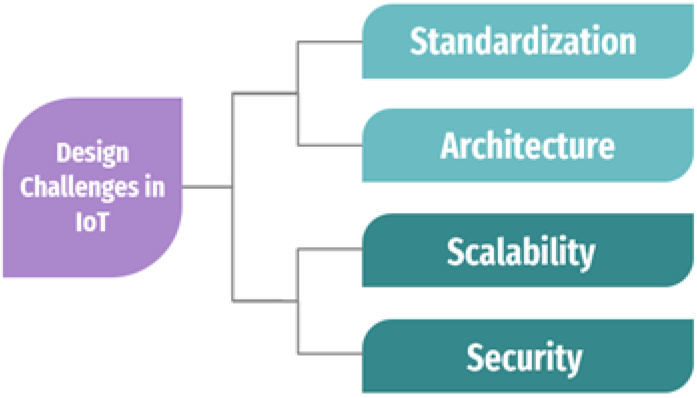

Figure 6: Main issues and challenges in IoT

3.1.1 Standardization

One of the most significant and crucial issues in IoT applications is standardization, which is also the foundation for IoT growth. The framework for IoT development includes participation from the most significant standardization bodies, including ETSI, ITU, IETF, IEEE, etc. The standardization activity is distinct from creating a seamless process and open standards, and integrating different standards to be consistent presents some challenges. Future integration of diverse IoT technology types will need to take into account all these difficulties [3, 111, 21].

3.1.2 Architecture

IoT architecture is essential for the IoT system since it can integrate various technologies. It supports the continuation of services. The most critical and significant IoT system challenge is using the integrated architecture for a separate application. Extensibility, transparency, and reliability in all varieties of milieus are necessities for this model. It should provide easy, scalable, and possible cross-domain integration and automation in the IoT. The IoT architecture has many group types, including hardware, software, networks, and general [111].

3.1.3 Scalability

Scalability in IoT alludes to the ability to add new gadgets and administrations to existing execution. It upholds a large number of gadgets with shifting limitations. A structure and design are required to carry out the scaling system. The fundamental problem with scalability is adding extra gadgets to the Internet of Things [111, 74].

3.1.4 Security

To link devices and things, security is a critical component of IoT. Many threats can disrupt our network, compromise data, and gain access to personal information. With today's technologies, it is challenging to provide security [111, 87].

3.2 IoT Privacy

Since the greater part of the data in an IoT framework might be private information, ensuring the user's anonymity and the treatment of restricted access to personal information is essential. IoT privacy refers to permitting safeguarded information to be put away, handled, and exchanged without third-party access to the information content. Several sectors demand advancement [73, 117]. Techniques that support the notions of privacy by design include data glorification, validation, commendation, confirmation and obscurity. Some security issues are coming from the inescapability and universality of IoT gadgets, including:

- Maintaining region privacy in situations where the region can be found from things connected with individuals.
- Keeping an eye on IoT-related exchanges prevents the inference of personal data that individuals need to keep private.
- Using decentralized computing and key administration to keep data as local as possible.

As stated in our guiding principles, guaranteeing the security, dependability, versatility, and soundness of Internet applications and administrations is imperative to fostering trust and utilization of the Internet. As Internet clients, we should have a high degree of confidence in the Internet, its applications, and the gadgets that interface with it to understand the type of exercises we wish to do on the web, no matter what risks are associated with such tasks. The IoT is no exception; IoT security is tied to users' capacity to trust their environment.

As we interface more devices to the Internet, there are more chances to exploit potential security holes. Poorly protected IoT devices could operate as entry points for a cyber-attack by enabling malicious actors to reprogram or make a device malfunction. Poorly constructed gadgets might leave user data vulnerable to theft, leaving data streams unprotected. Failing or malfunctioning gadgets can potentially lead to security flaws. These issues are just as serious, if not more so, for the small, inexpensive, and ubiquitous savvy devices of the Internet of Things as they are for the PCs that have historically served as Internet access endpoints. IoT device manufacturers are challenged by competitive pricing and technical limits to effectively layout security measures into those devices, probably creating security and long-term maintainability dangers extra than their conventional pc equivalents.

The sheer boom in the amount and variety of IoT gadgets may grow the opportunity for attacks in addition to any security design flaws. Every insecure device linked to the Internet can damage the security and flexibility of the Internet worldwide, not simply locally, given the IoT devices' high degree of interconnection. For instance, utilizing the owner's home WiFi Internet connection, a malware-infected refrigerator or television in the US may send numerous perilous spam messages to users worldwide [95].

4 Classification of Attacks on IoT

IoT networks are susceptible to attacks from both the outside and the inside when an attacker initiates an attack from outside the network (without having access to the cryptographic network keys); this is known as an external attack on IoT networks. To start an internal attack, on the other hand, it is expected that the attacker has control over a reliable network object. Therefore, the assault originates from within the network. This attack can happen when a reliable device turns rogue after earning network confidence, making it more challenging to identify. An attacker may pursue multiple objectives, such as transmitting false information to influence decisions or prevent system functions [50, 15, 24].

4.1 Perceptual Layer Security

The perceptual layer comprises resource-limited IoT gadgets, including sensors, RFID tags, Bluetooth, and Zigbee. Increase the possibility of cyber-attacks on these gadgets. Because a massive number of IoT devices are physically distributed in open fields, they may be susceptible to several physical attacks, including [7] (see Figure 7):

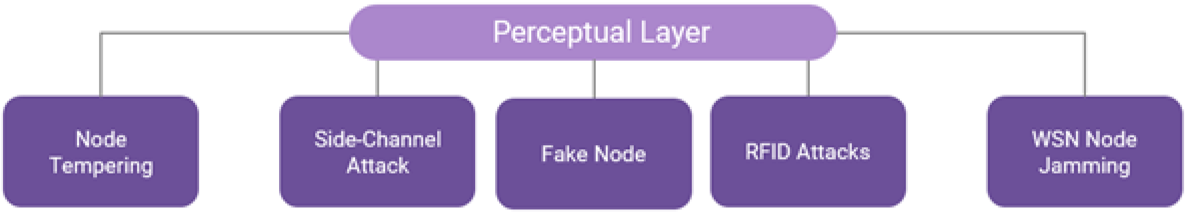

Figure 7: Security issues in the perceptual layer

4.1.1 Node Tempering

If an attacker gets actual admittance to a sensor node, they can exchange the whole node, a part of its equipment, or associate straightforwardly to it to change delicate information [85]. Cryptographic keys or routing table routes could be sensitive data.

4.1.2 Side-Channel Attack

Due to its ease of usage and low power consumption, a side-channel assault is perhaps the most significant one that could happen during data exchange on the IoT. In 1965, the primary authoritative data about side-channel assaults were delivered. Side-channel assaults, which may be ciphertext-just, plaintext-just, or chosen plaintext attacks, rely on side-channel data. Timing assaults, electromagnetic attacks, and ecological assaults are examples of side-channel attacks [37].

4.1.3 Fake Node

The assailant can insert a bogus or pernicious network node between network nodes [121]. It can make the hub quit sending real information and subsequently ruin the whole organization. Accordingly, the aggressor accesses the organization and has unlimited authority over the organization's data stream.

4.1.4 RFID Attacks

Radio Frequency Identification (RFID) attacks, like the WSN network, operate through radio signals. The distinction is that signal jamming is not necessary for attackers. The hacker can build the nodes to reject services by transmitting noise signals across the network [67]. This distortion meddles with the RFID signal, causing a stumbling block in node connectivity.

4.1.5 WSN Node Jamming

Radio frequency is what a wireless sensor network uses to operate. This prevents communication between IoT network nodes. Noise signals across the network or through jamming on WSN signals, a Dos can be produced. The attacker continues to jam the signals, which prevents the IoT from providing its services [68].

4.2 Network Layer Security

Despite the core network's adequate security protections, several vulnerabilities persist. Data integrity and confidentiality issues might result from conventional security issues. As shown in Figure 8, The network layer is still vulnerable to numerous network assaults [7].

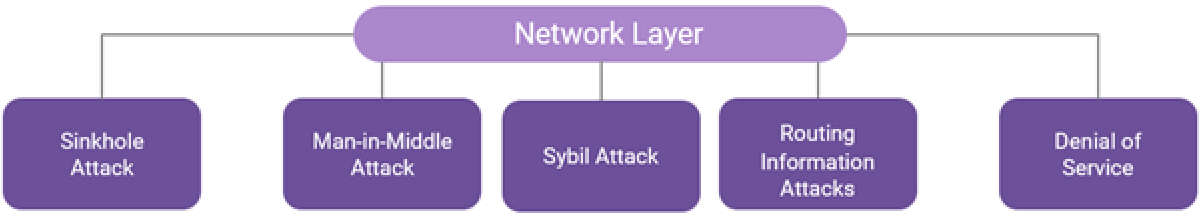

Figure 8: Security issues in the network layer

4.2.1 Sinkhole Attack

This attack terminated data security and rejected all packets instead of appropriately delivering them to their destination since the assailant through all transmissions from a remote sensor network node to a constant point, which is very dangerous in the IoT environment [91].

4.2.2 Man-in-Middle Attack

The attacker in this assault is not required to show up at the target network physically. As a result, to access sensitive information, the IoT connection protocol interfered with the two sensor nodes [91].

4.2.3 Sybil Attack

In this attack, a malicious node steals the identities of other nodes and assumes their identities. For instance, a single node in a wireless sensor network voting system can cast several votes [38].

4.2.4 Routing Information Attacks

In this assault, the assailant can impersonate, change, or send directing data to make the organization complex. It allows or rejects packets, sends inaccurate data, or splits the network [36].

4.2.5 Denial of Service

The services are unavailable to the intended users because an attacker floods the network with a lot of traffic [114].

4.3 Support Layer Security

The security of the support layer is independent of the security of the other levels; what's more, distributed computing security is a considerable space of safety. Cloud Security Alliance (CSA) is establishing a high-level security architecture for clouds. In addition, Security Content Automation Protocol (SCAP) [16] is being developed as a means for ongoing cloud audits, as is Trusted Computing (TCG) [16]. This layer hosts the data and applications of IoT users; therefore, both should be secure. As illustrated in Figure 9, security vulnerabilities at this layer include:

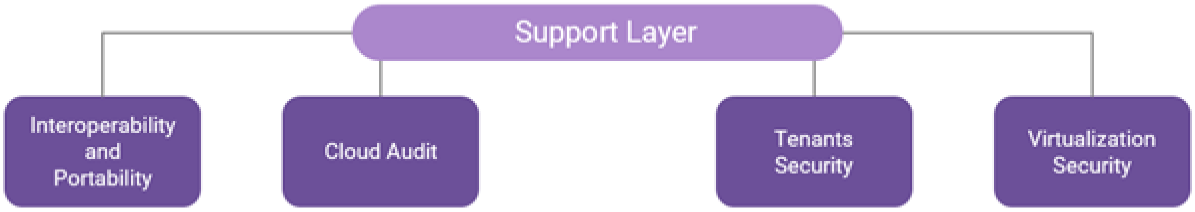

Figure 9: Security vulnerabilities at the support layer

4.3.1 Interoperability and Portability

A significant issue nowadays is cloud companies' lack of interoperability and portability. Users who want to switch from one cloud to another have issues since different vendors utilize different proprietary standards. Additionally, this heterogeneity exposes security [7].

4.3.2 Cloud Audit

For cloud vendors, the CSA establishes several standards. To increase user confidence, it is necessary to conduct ongoing audits to ensure that these security criteria are being followed [7].

4.3.3 Tenants Security

Different clients' information might be stored on the same disk in the cloud, or IaaS client users may share the same physical storage. Tenants are the name given to such users. Because the data shares the same physical media, the adversary can steal the tenant's data [7].

4.3.4 Virtualization Security

Virtualization security is critical. Virtual machine connections can occasionally sidestep network security restrictions [79]. The security of virtualization is significant since it can be a barrier in cloud audits. Various cloud vendors used different virtualization methods.

4.4 Application Layer Security

Before attacks occur, data must be protected by attack software. Utilizing Trojan pony programs, worms, viruses, spyware and vindictive content, programming assaults can foster a framework that can hurt IoT System gadgets, suitable data, mess with information and refuse service [2]. The main Security issues in the application layer are as follows (see Figure 10).

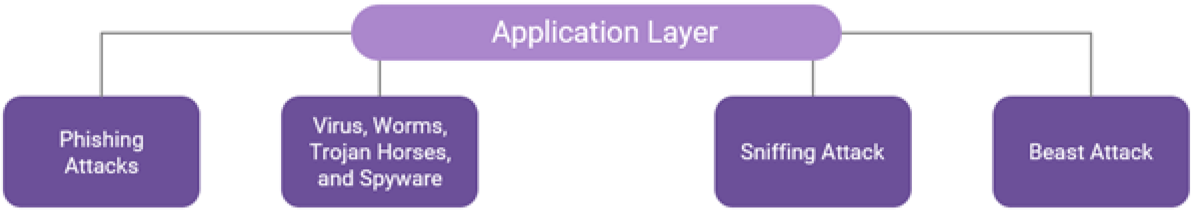

Figure 10: Security issues in the application layer

4.4.1 Phishing Attacks

A hacker can obtain private information via a compromised website or email by Spoofing the users' confirmation ID [106].

4.4.2 Virus, Worms, Trojan Horses, and Spyware

Adversaries can infect the system with malicious software that can steal data, mess with it, or even perform denial of service [115].

4.4.3 Sniffing Attack

Sniffer applications might help sniff or check the organization's traffic to get close enough to delicate information, mainly if application protocols have been executed without a security system, for example, CoAP with no-security mode [105].

4.4.4 Beast Attack

The monster assault relies vigorously upon taking advantage of the weaknesses in TLS 1.0, as it executes Cipher Block Chaining (CBC). Having utilized HTTP to run over TLS, the assailant can utilize the CBC to decode either part of the message or HTTP treats [1].

Finally, Table 1 summarizes the attacks in each layer of IoT.

Table 1: Summary of the attacks in each layer in IoT

Attacks	Perceptual Layer	Network Layer	Support Layer	Application Layer
Node Tempering	√	-	-	-
Sid Channel	√	-	-	-
Fake Node	√	-	-	-
RF interference	√	-	-	-
WSN Node Jamming	√	-	-	-
Sinkhole attack	-	√	-	-
Interoperability and Portability	-	-	√	-
Phishing Attack	-	-	-	√
Man-in-Middle attack	-	√	-	-
Cloud Audit	-	-	√	-
Sniffing attack	-	-	-	√
Sybil Attack	-	√	-	-

Beast Attack	-	-	-	√
Routing Information	-	√	-	-
Denial of Service	-	√	-	-
Tenants Security	-	-	√	-
Virtualization Security	-	-	√	-
Virus, Worms, Trojan Horses, and Spyware	-	-	-	√

5 Taxonomy of IDSs

IDS is among the most well-known security frameworks. It safeguards computer systems and network infrastructure from malicious activity and illegal use. It recognizes the various risks. Users and network administrators can utilize it to assist them in taking preventative action. IDS is crucial for protecting IT infrastructure. To identify suspicious behavior, intrusion detection systems record and examine network traffic [19, 35, 53]. IDS primarily employs two distinct approaches:

- Anomaly detection: Using a variety of characteristics, network transport or administrator operating system conduct is studied and compared to expected behavior in this technique. The warning is raised whenever the system notices departures from typical behavior.
- Misuse/Signature detection: This method looks for a particular example of conduct previously distinguished as an assault. The IDS signature database stores all dangerous styles and behaviors recognized as attacks. These signature databases are regularly updated.

As illustrated in Figure 11, IDS are often differentiated in taxonomies.

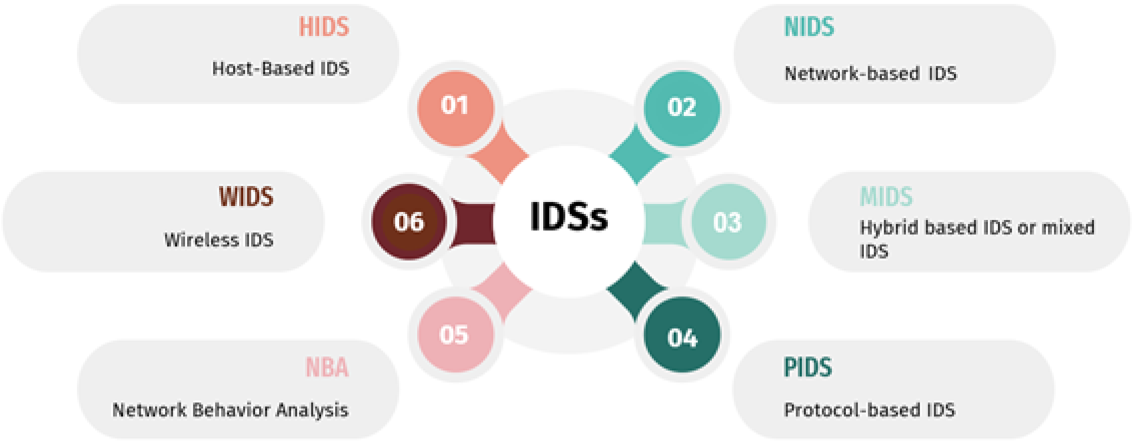

Figure 11: Categories of IDSs

5.1 Host-Based IDS (HIDS)

Host-based IDS refers back to the detection of intrusion on one system. It is mostly a software-based total deployment wherein an agent is deployed on the local host to monitor and report application behavior. HIDS monitors system and application access and alerts for unexpected activity [42]. It continuously monitors event logs, application logs, client strategy authorization, rootkit discovery, and other framework invasions. It constantly looks at these data and lays out a benchmark. At the point when another log section shows up, HIDS compares the information to the benchmark; assuming any passages are found that are beyond this pattern, HIDS issues caution. According to the policy set up on the system, HIDS can notify, prohibit the activity, or take any other action if any unauthorized behavior is discovered [42].

5.2 Network-based IDS (NIDS)

A NIDS reviews network traffic parcels for intrusions and malignant attempts [43]. A NIDS can be either software or hardware-based [39]. As networks grow and traffic quantities increase, IDSs must be executed as equipment frameworks, for example, intelligent sensor engineering [71]. Field-programmable gate arrays (FPGAs), for example, can act as the underpinning of an equipment-based NIDS. FPGAs' unique qualities, like their support for rapid connections and exceptionally high-volume data handling, make them reasonable for NIDSs [86].

5.3 Hybrid based IDS or mixed IDS (MIDS)

MIDS combines at least two types of IDS to reap the benefits of IDS during completing a precise detection [70], for example, Double Guard [101], which utilizes IDS and organization IDS. MIDS, on the other hand, takes a long time to analyze data.

5.4 Protocol-based IDS (PIDS)

PIDS watches and validates specific protocol actions and statuses, such as HTTP [124]. PIDS might be customized to monitor application protocols (known as APIDS) [124]. It centers around events that occur in a particular application by watching and monitoring records [84]. Some studies have presented PIDS, including Danish et al. [33]. The proposition of an IDS for discovery jammer assaults in a LoRaWAN organization. The framework has been executed in light of the LoRaWAN protocol.

5.5 Network Behavior Analysis (NBA)

NBA screens and looks at network traffic to distinguish gambles that produce strange traffic designs, for example, DDOS assaults, malware, and strategy breaks [98, 96]. The NBA framework analyzes network traffic to distinguish attacks with strange traffic streams [70]. NBA systems are typically deployed on an organization's internal networks, occasionally deployed where they may keep an eye on traffic moving between an organization's network and outside networks [78].

5.6 Wireless IDS (WIDS)

WIDS watches and investigates remote interchanges to distinguish assaults [70]. Wireless networks are susceptible to various attacks, including sinkholes, floods, Sybil, and route-altering spoofing attacks [103].

Table 2: Advantages and disadvantages of IDS Type

IDS Type	**Advantages**	**Disadvantages**
HIDS	• The HIDS can encrypt and analyze data and communications. • HIDS informs us of the success or failure of an attack. • Simple to deploy because it doesn't call for new hardware and doesn't interfere with the existing architecture.	• If the attack causes the OS to malfunction, HIDS will fail. • Network scans or DOS cannot be detected by HIDS • HIDS can require a lot of resources.

NIDS	• Because NIDS operate independently of their operating environment, hosts' performance is unaffected.	• Does not indicate whether the attack was successful or no. • Cannot Analyze Encrypted Traffic. • NIDS is has very limited visibility inside the host machine.
MIDS	• more adaptable. • More effective. • MIDS benefit from the advantages of the combined type.	• Depending on the combined approaches, the monitored system will have high overhead. • Processor utilization of the hybrid agent is much great.
PIDS	• APIDS focus on observing and analyzing operations particular to the application. • More easier to define the normal and the abnormal behavior.	• System overhead is higher. • Particular development [66]. • It does not detect attacks below the application layer.
NBA	• Superior detection reconnaissance scanning, reconstruct malware infections and DDoS attacks • Effective at detecting zero-day exploits or novel attacks without a signature in the IDS database.	• Delay in detecting attacks. • Some attacks may not be detected until they have already damaged systems especially attacks that occur quickly.
WIDS	• More accurate. • It can manage wireless protocol activity	• Sensors has limited computational resource and limited energy [28].

6 DS using Machine Learning Algorithms, Concepts and Examples

Machine learning (ML) algorithms are quite effective at performing prediction tasks across various application domains. They are regularly used to determine the correlation among several inputs to approximate a result function and to find intriguing data structures. For these reasons, we decided to discover the use of ML algorithms in the context of automotive cyber-physical assaults and intrusion detection [60].

Contingent upon the learning procedure, AI algorithms can be parted into two significant classes:

- Supervised learning: A supervised learning strategy is utilized by an AI algorithm when the training set contains both the algorithm's input and output data. In this sense, the algorithm learns a mapping function by minimizing a predetermined cost function. The trained algorithm is then tested on some situations that weren't included in the training set. The generalization of an algorithm is said to be successful if it performs similarly on the test set as it did on the training set.

- Unsupervised learning: The ML technique uses unsupervised learning if the training set only comprises the input data and not the expected output. Finding intriguing data structures is the aim of the ML algorithm in this approach [60].

ML is used in real-world intrusion detection systems (IDS). In this research, we investigate algorithms that can be used to fulfill such a paradigm. The following are the benefits of using machine learning in intrusion detection. Such IDSs may adapt to the system and network environments, allowing them to identify and respond to abnormal system behavior [81].

ML and Deep Learning (DL) methods are utilized in numerous IoT applications and frameworks. These strategies are employed for assault categorization in the Internet of Things because they have the quality of learning via experience networks [89]. ML techniques have because of the improvement of the latest algorithms, generation of a massive quantity of data, and a low calculation cost [47]. Over time, ML and DL approaches have demonstrated advancement in the empirical assessment of various applications [47]. This paper investigates ML and DL approaches for detecting and classifying assaults in IoT networks. Utilizing feature engineering, ML techniques classify attacks on IoT networks by extracting pertinent information. Contrarily, DL approaches employ a variety of linear and non-linear processing layers to abstract discriminative or generative characteristics and carry out pattern analysis [54]. ML and DL techniques will be covered in detail to give a thorough overview of how they are utilized to secure IoT organizations.

ML and DL algorithms solve a specified application problem by learning from a dataset. The dataset is separated into two sections: training and testing. For learning and studying different dataset characteristics, the training set is employed. For example, given an intrusion detection dataset, the algorithms employ attributes from the training dataset to categorize a sample as an attack or normal. ML and DL algorithms aim to increase the system's classification accuracy by performing. Analysis of the network's ordinary and assault site visitors from a behavioral perspective.

Classification and clustering algorithms are two categories of ML algorithms. Classification algorithms work with labeled data samples to build prediction models by studying the input parameters and applying them to the desired output [47]. As a result, these strategies establish a link between input and output parameters. During the training phase of a classification method, the learning model is taught using a training set. The learning during the training phase is then applied to forecast and categorize new data [99]. Input, output, and one or more hidden layers are all present in a multi-layer network using supervised DL methods. These layers are made up of nodes called neurons, and every layer is related via edges. At the beginning weights, the neurons are assigned random weights and multiplied with the input variables to produce the result [48, 104].

Classification techniques are acknowledged for learning through data representation and labeling. Comparatively, clustering methods are widely recognized for learning through unlabeled datasets [108]. Data pre-labeling is unnecessary for learning using clustering algorithms and creating unique groups of unlabeled data based on their shared traits. Reinforcement Learning (RL) is another popular ML approach [47, 99]. The environment for learning data works in conjunction with RL approaches. Its goal is to evaluate the environment and choose the appropriate approach for any agents that may be present [25]. Trial-and-error methods are used in RL. A set of actions is defined based on input parameters and ambient factors.

Finally, in this section, several IDS implementations that are currently in use are conducted. The benefits and drawbacks of these systems are evaluated when conducting the survey.

6.1 Support Vector Machine based IDS

In [49], Halimaa et al. utilized a machine learning method to present the IDS model. Support Vector Machine (SVM) and Naive Bayes classifiers are employed as two machine learning classifiers. The results show that SVM provides more accuracy than naive Bayes. These precision results are solely applicable to known assault recognition. The lack of timeliness is another critical issue not addressed in this study.

In [119], Yang et al. introduced the job of SVM and its performance. The findings show that SVM is a speedier AI technique. Three types of indicators are used in the analysis sensitivity, specificity, and time consumption.

In [56], Jha et al., SVM was used to construct the intrusion detection system. NSL KDD dataset was utilized for model training and testing, The best features are chosen via feature selection using the k Means algorithm criterion. The amount of time needed to execute the SVM is decreased with a decrease in the number of characteristics. SVM's flaw, however, is that it is a classification approach that necessitates previous knowledge of the events and data. As a result, SVM models in intrusion detection systems only work when detecting known assaults and are ineffective when trying to identify a new attack.

When the efficient feature selection approach is used, SVM performs admirably. In [116], the SVM is utilized to build a model for the cloud IDS (CIDS) with the Correlation-based feature selection (COFS), which assisted in accomplishing achieving better outcomes.

6.2 K-Nearest Neighbor based IDS

Cover et al. proposed the closest neighbor design category technique called K-Nearest Neighbor (KNN) category in [31]. The distance among the numerous data items of different types is used for characterized the data items. The data item is categorized based on the category of data items with the shortest distance when contrasted with other classes' data points concerning the data items from various classifications, whose distance is the smallest. As per the research, the 1-NN classification has the least conceivable blunder, while the KNN arrangement can have the most minimal conceivable mistake. It's the classification method, which is a speedier pattern categorization method.

The particulars of the KNN algorithm's implementation for various datasets have been introduced by Ali et al. in [9]. The Euclidian and Manhattan distance recipes are used to assess the KNN execution. It has been discovered that the Euclidian distance (ED) equation doesn't give better KNN results. Additionally, for heterogeneous datasets, the KNN algorithm's execution doesn't seem to vary significantly.

Li et al. in [69] proposed the KNN categorization IDS for remote sensor networks. Flooding assault kinds are the assault type that is being targeted for location. The model has been demonstrated to classify flooding attacks using KNN effectively. The problem is that when various attack kinds or novel assault types need to be identified, KNN is ineffective.

In [22], Benaddi et al. The strong IDS model was suggested by utilizing Principal Component Analysis (PCA)—Fuzzy Clustering— KNN. For setting up the IDS model, the NSL-KDD dataset is used. To increase the efficiency and effectiveness of the IDS, it is assumed that the important thing is to reduce the set of characteristics in the dataset. The model could successfully categorize the various assault types input, thanks to the inclusion of KNN. Regardless, the issue is the precision of the KNN should be checked appropriately. Similarly, the supplied IDS model's temporal complexity is an area of concern.

6.3 Decision Tree based IDS

Yihunie et al. presented their work on anomalous intrusion detection using AI methods in [120]. As part of the model, the five categorization strategies are compared. The dataset used for preparing the evaluation system is the NSL-KDD. The outcomes showed that arbitrary woodland had better precision when contrasted with different methods. It is crucial to highlight that this accuracy is significant even for known assaults. It is vital to remember that this precision is only applicable for detecting known attacks. What is important to consider is that this work does not include the discovery of unbeknown assaults. Furthermore, the paper does not discuss the framework's quickness, discovery punctuality, or fault-tolerance nature of IDS. Subsequently, this IDS structure needs improvement pondering these properties, which should be updated with further developed techniques.

In [29], using SVM and random forest, Chang et al. introduced the IDS. The random forest provides options to improve performance, precision and time. Out of 41 elements, 14 are selected using random forest, providing a high degree of precision when contrasted with precision by utilizing 41 attributes. These outcomes are for known information; consequently, the precision can't be generalized for new assault-type input.

In [63], Kumar et al. introduced the IDS utilizing the decision tree. The produced results provide high-quality numbers. The decision tree utilizes the prior information for model structure and gives further developed results for the known input sorts. It can't work well for obscure input types and should be utilized with other strategies to improve outcomes.

6.4 Naïve Bayes based IDS

Panda et al. introduced the IDS in [82] utilizing the naïve Bayes method. The outcomes obtained by the model are superior to the neural network architectures. The distance among data nodes is minimized, and the model is created with two levels. The outcomes further demonstrated that the Bayes technique provides great outcomes quicker than expected and with minimal expense. The system's flaw, however, is that it produces more false positives than other systems. Subsequently, Bayes should be involved alongside different strategies for improved results and decreased bogus up-sides.

In [55], Sharmila et al. have introduced the IDS utilizing PCA-based naïve Bayes design. The outcomes have demonstrated that, compared to traditional nave Bayes, PCA-based naïve Bayes design achieves superior precision. As the information increases, the precision decreases and the system's velocity slowly. This approach likewise assists with giving helpful outcomes even when the datasets lack values. Subsequently, credulous Bayes can be utilized with different methods to improve results.

6.5 AI and DL Techniques based IDS

Rassam et al. in [93] proposed an approach for IDS based on intelligent and general rule building. The standards designed as one instead of two or three rules, which may discover various attacks, are intelligent principles. Data preprocessing is the first stage in the previous job, after which intelligent and general rules are constructed, and constructed rule learning and then implementation. The system's benefit is that, owing to the intelligent rules' design, fewer rules aid in discovering the highest number of attacks, resulting in reduced power consumption. In any event, this solution is designed with the assumption that the majority of network assaults originate from the network's inward systems. Consequently, it cannot be utilized to detect outside assaults because it is challenging to detect incoming attacks from outside due to the network's vastness.

A thorough analysis of the architecture of an IDS utilizing AI methods.is provided by Zamani in [32]. The AI strategies are parceled into two segments: AI and Computational Intelligence. These strategies have a lot of similar qualities. It can make it possible to construct a precise, error-tolerant, productive framework, and so forth. The work asserts that an ML technique may be used to create an efficient IDS.

Bahlali et al. used AI systems to complete research based on IDS in [20]. The paper presents a deep learning approach alongside ANN. It utilizes the USNW-NB15 dataset, which has problems with imbalanced classes. In any scenario, using these classifiers will produce results with the needed precision. The ANN is regarded as the optimal design among those in use for the exactness of the IDS model. The IDS model has an execution problem in terms of timing; velocity isn't seen as an important factor in the task. Additionally, because the dataset is outdated and does not accurately reflect recent assaults, the results cannot be really used to compare the models.

Finally, the properties of the studies reviewed here are summarized and evaluated in Table 3

Table 3: A summary of the selected papers in Section 5.

Ref.	System	Results	Challenges
[49]	SVM based IDS	The results show that SVM provides more accuracy than naive Bayes.	1. The precision results are solely applicable to known assault recognition. 2. The lack of timeliness is another critical issue not addressed in this study.
[119]		Three types of indicators are used in the analysis sensitivity, specificity, and time consumption.	A classification approach that necessitates previous knowledge of the events and data.
[56]		The amount of time needed to execute the SVM is decreased with a decrease in the number of characteristics.	They only work when detecting known assaults and are ineffective when identifying new attacks.
[116]		Using the COFS, the model achieved better outcomes.	Timeliness has not been addressed.

[31]	KNN based IDS	1. 1-NN classification has the least conceivable blunder. 2. Speeding the pattern categorization method.	KNN arrangement likewise can have the most minimal conceivable mistake
[9]		The ED equation doesn't give better KNN results.	For heterogeneous datasets, the KNN algorithm's execution doesn't seem to vary significantly
[69]		The model has been demonstrated to be effective in classifying flooding attacks.	In any event, the problem is that when various attack kinds or novel assault types need to be identified, KNN is ineffective
[22]		The model could successfully categorize the various assault types input.	1. The issue is the precision of the KNN should be checked appropriately. 2. Complexity.
[120]	Decision Tree-based IDS	1. Arbitrary woodland has given better precision when contrasted with different methods. 2. The accuracy is significant even for known assaults.	1. The detection of unbeknown assaults has not been included. 2. No discussions of the framework's quickness, discovery punctuality, or fault-tolerance nature of IDS.
[29]		A high degree of precision has been provided compared to precision by utilizing 41 attributes.	The precision can't be generalized for new assault-type input.
[63]		The decision tree utilizes the prior information for model structure and gives further developed results for the known input sorts	It can't work well and should be utilized with other strategies to improve outcomes.
[82]	Naïve Bayes based IDS	The outcomes demonstrated that the Naïve Bayes provides excellent outcomes quicker than expected and with minimal expense.	Bayes should be involved alongside strategies for improved results and decreased bogus up-sides.
[55]		The outcomes have demonstrated that, when compared to traditional nave Bayes, PCA-based naïve Bayes design achieves superior precision	As the number of information increases, the precision decreases and the system's velocity slowly
[93]	AI and DL based IDS	Reduced power consumption	It cannot be utilized to detect outside assaults because it is challenging to detect incoming attacks from outside due to the network's vastness
[32]		It can make it possible to construct a framework that is precise, error-tolerant productive.	The complexity of the model has not been addressed.
[20]		In different scenarios, using these classifiers will produce results with the needed precision.	1. The model has an execution problem in terms of timing; velocity isn't seen as an important factor in the task. 2. Because the dataset is outdated and does not accurately reflect recent assaults, the results cannot be really used to compare the models.

7 Summary

To conclude, we have conducted a state of the art of IDS, along with their main features and characteristics, as well as technical working principles. The IDS is critical to any network safety since it can detect infiltration before and after an attack. As a defense mechanism for networks and systems, it is crucial. A system's data is tracked and analyzed by an ID to look for any attacks. With more recent, cutting-edge technologies, intrusion detection has significantly improved. In this study, IDS types implemented in various platforms or contexts were reviewed in general, along with comparisons between them. This study gave an overview of IDS-based machine learning algorithms deployed in various scenarios or platforms and compared them. Then, it described each type's characteristics, benefits, and drawbacks.

References

[1] H.A. Abdul-Ghani, D. Konstantas, and M. Mahyoub, *A comprehensive IoT attacks survey based on a building-blocked reference model*, Int. J. Adv. Comput. Sci. Appl. **9** (2018), no. 3.

[2] M.M. Ahemd, M.A. Shah, and A. Wahid, *IoT security: A layered approach for attacks and defenses*, IEEE, 2017, pp. 104–110.

[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 Commun. Surveys Tutorials **17** (2015), no. 4, 2347–2376.

[4] F.A. Alaba, M. Othman, I.A.T. Hashem, and F. Alotaibi, *Internet of Things security: A survey*, J. Network Comput. Appl.s **88** (2017), 10–28.

[5] T. Alam, *Blockchain and its role in the internet of things (IoT)*, arXiv preprint arXiv:1902.09779 (2019).

[6] M. Alamri, N.Z. Jhanjhi, and M. Humayun, *Blockchain for internet of things (IoT) research issues challenges and future directions: A review*, Int. J. Comput. Sci. Netw. Secur **19** (2019), no. 1, 244–258.

[7] I. Ali, S. Sabir, and Z. Ullah, *Internet of things security, device authentication and access control: A review*, April 2022.

[8] J. Ali, T. Ali, S. Musa, and A. Zahrani, *Towards secure IoT communication with smart contracts in a blockchain infrastructure*, arXiv preprint arXiv:2001.01837 (2020).

[9] N. Ali, D. Neagu, and P. Trundle, *Evaluation of k-nearest neighbour classifier performance for heterogeneous data sets*, SN Appl. Sci. **1** (2019), no. 12, 1–15.

[10] G. Aloi, G. Caliciuri, G. Fortino, R. Gravina, P. Pace, W. Russo, and C. Savaglio, *Enabling IoT interoperability through opportunistic smartphone-based mobile gateways*, J. Network Comput. Appl. **81** (2017), 74–84.

[11] I. Andrea, C. Chrysostomou, and G. Hadjichristofi, *Internet of things: Security vulnerabilities and challenges*, IEEE, 2015, pp. 180–187.

[12] L.J.B. Andrews, L. Raja, and S. Shanmugasundaram, *Mobile android-based remote patient monitoring system through wearable sensors*, J. Discrete Math. Sci. Crypto. **22** (2019), no. 4, 557–568.

[13] J. Arshad, M.A. Azad, M. Mahmoud Abdellatif, M.H. Ur Rehman, and K. Salah, *COLIDE: A collaborative intrusion detection framework for internet of things*, IET Networks **8** (2019), no. 1, 3–14.

[14] K. Ashton, *That 'internet of things' thing*, RFID J. **22** (2009), no. 7, 97–114.

[15] S. Asiri and A. Miri, *A sybil resistant IoT trust model using blockchains*, IEEE, 2018, pp. 1017–1026.

[16] M. Aslam, C. Gehrmann, and M. Björkman, *ASArP: automated security assessment and audit of remote platforms using TCG-SCAP synergies*, J.Inf. Secur. Appl. **22** (2015), 28–39.

[17] H. Atlam, A. Alenezi, R. Walters, and G. Wills, *An overview of risk estimation techniques in risk-based access control for the internet of things*, 2017, pp. 254–260.

[18] H.F. Atlam, M.A. Azad, A.G. Alzahrani, and G. Wills, *A review of blockchain in internet of things and AI*, Big Data Cognitive Comput. **4** (2020), no. 4, 28.

[19] S. Axelsson, *Intrusion detection systems: A survey and taxonomy*, Technical Report (2000).

[20] A.R. Bahlali, *Anomaly-based network intrusion detection system: A machine learning approach*, vol. 10, Biskra University, 2019.

[21] D. Bandyopadhyay and J. Sen, *Internet of things: Applications and challenges in technology and standardization*, Wireless Personal Commun. **58** (2011), no. 1, 49–69.

[22] H. Benaddi, K. Ibrahimi, and A. Benslimane, *Improving the intrusion detection system for NSL-KDD dataset*

based on PCA-fuzzy clustering-KNN, IEEE, 2018, pp. 1–6.

[23] A. Benitez-Andonegui, R. Burden, R. Benning, R. Möckel, M. Lührs, and B. Sorger, *An augmented-reality fNIRS-based brain-computer interface: A proof-of-concept study*, Front. Neurosci. **14** (2020), 346.

[24] R. Boncea, I. Petre, and V. Vevera, *Building trust among things in omniscient internet using blockchain technology*, Roman. Cyber Secur. J. **1** (2019), no. 1, 17–24.

[25] L. Breiman, J.H. Friedman, R.A. Olshen, and C.J. Stone, *Classification and regression trees*, Routledge, 2017.

[26] D. Brevers, G. Sescousse, P. Maurage, and J. Billieux, *Examining neural reactivity to gambling cues in the age of online betting*, Current Behav. Neurosci. Rep. **6** (2019), no. 3, 59–71.

[27] R.W. Brown and A.M. Haslett, *Method and system of monitoring appliance usage*, U.S. Patent Appl. (2018).

[28] O. Can and O.K. Sahingoz, *A survey of intrusion detection systems in wireless sensor networks*, IEEE, 2015, pp. 1–6.

[29] Y. Chang, W. Li, and Z. Yang, *Network intrusion detection based on random forest and support vector machine*, vol. 1, IEEE, 2017, pp. 635–638.

[30] W. Cheng, H. Wu, T. Dayong, E. Zhang, L. Cao, and R. Shi, *Method and apparatus for reducing continuous-wakeup delay of bluetooth loudspeaker, and bluetooth loudspeaker*, U.S. Patent (2022).

[31] T. Cover and P. Hart, *Nearest neighbor pattern classification*, IEEE Trans. Inf. Theory **13** (1967), no. 1, 21–27.

[32] Q.-V. Dang, *Studying machine learning techniques for intrusion detection systems*, Springer, 2019, pp. 411–426.

[33] S.M. Danish, A. Nasir, H.K. Qureshi, Ay.B. Ashfaq, S. Mumtaz, and J. Rodriguez, *Network intrusion detection system for jamming attack in lorawan join procedure*, IEEE, 2018, pp. 1–6.

[34] P. Danzi, A.E. Kalor, C. Stefanovic, and P. Popovski, *Analysis of the communication traffic for blockchain synchronization of IoT devices*, IEEE, 2018, pp. 1–7.

[35] H. Debar, M. Dacier, and A. Wespi, *Towards a taxonomy of intrusion-detection systems*, Comput. Networks **31** (1999), no. 8, 805–822.

[36] J. Deogirikar and A. Vidhate, *Security attacks in IoT: A survey*, IEEE, 2017, pp. 32–37.

[37] M. Devi and A. Majumder, *Side-channel attack in internet of things: A survey*, Applications of Internet of Things, Springer, 2021, pp. 213–222.

[38] M.U. Farooq, M. Waseem, S. Mazhar, A. Khairi, and T. Kamal, *A review on internet of things (IoT)*, Int. J. Comput. Appl. **113** (2015), no. 1, 1–7.

[39] M. Ford, C. Mallery, F. Palmasani, M. Rabb, R. Turner, L. Soles, and D. Snider, *A process to transfer Fail2ban data to an adaptive enterprise intrusion detection and prevention system*, IEEE, 2016, pp. 1–4.

[40] G. Safety, *Privacy and Security*, 2019.

[41] M.M. Gaber, A. Aneiba, S. Basurra, O. Batty, A.M. Elmisery, Y. Kovalchuk, and M.H.U. Rehman, *Internet of things and data mining: From applications to techniques and systems*, Wiley Interdiscip. Rev.: Data Min. Knowledge Discovery **9** (2019), no. 3, e1292.

[42] V. Ganesh and M. Sharma, *Intrusion detection and prevention systems: A review*, Inventive Communication and Computational Technologies (G. Ranganathan, J. Chen, and Á. Rocha, eds.), vol. 145, Springer Singapore, Singapore, 2021, pp. 835–844.

[43] S.K.r Gautam and H. Om, *Computational neural network regression model for host based intrusion detection system*, Perspect. Sci. **8** (2016), 93–95.

[44] A.A. Gendreau and M. Moorman, *Survey of intrusion detection systems towards an end to end secure internet of things*, IEEE, 2016, pp. 84–90.

[45] G. Ghinita, P. Karras, P. Kalnis, and N. Mamoulis, *A framework for efficient data anonymization under privacy and accuracy constraints*, ACM Trans. Database Syst. (TODS) **34** (2009), no. 2, 1–47.

[46] T. Golomb, Y. Mirsky, and Y. Elovici, *CIoTA: Collaborative IoT Anomaly Detection via Blockchain*, April 2018.

[47] I. Goodfellow, Y. Bengio, and A. Courville, *Deep learning*, MIT Press, 2016.

[48] D. Gunning, *Explainable artificial intelligence (xai)*, Defense Adv. Res. Projects Agency (DARPA), nd Web **2** (2017), no. 2, 1.

[49] A. Halimaa and K. Sundarakantham, *Machine learning based intrusion detection system*, IEEE, 2019, pp. 916–920.

[50] M.T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, *Bubbles of Trust: A decentralized blockchain-based authentication system for IoT*, Comput. Secur. **78** (2018), 126–142.

[51] W. He, D. Akhawe, S. Jain, E. Shi, and D. Song, *Shadowcrypt: Encrypted web applications for everyone*, Proc. 2014 ACM SIGSAC Conf. Comput. Commun. Secur., 2014.

[52] F. Heuer, T. Jager, S. Schäge, and E. Kiltz, *Selective opening security of practical public-key encryption schemes*, IET Inf. Secur. **10** (2016), no. 6, 304–318.

[53] M.D. Holtz, B. David, and R.T. de Sousa Júnior, *Building scalable distributed intrusion detection systems based on the mapreduce framework*, Revista Telecommun **13** (2011), no. 2, 22.

[54] T. Hothorn, *CRAN task view: Machine learning and statistical learning*, Comprehensive R Archive Network (CRAN) (2022).

[55] A.D. Jadhav and V. Pellakuri, *Highly accurate and efficient two phase-intrusion detection system (TP-IDS) using distributed processing of HADOOP and machine learning techniques*, J. Big Data **8** (2021), no. 1, 1–22.

[56] J. Jha and L. Ragha, *Intrusion detection system using support vector machine*, Int. J. Appl. Inf. Syst. **3** (2013), 25–30.

[57] P. Kairouz, S. Oh, and P. Viswanath, *Extremal mechanisms for local differential privacy*, Adv. Neural Inf. Process. Syst. **27** (2014).

[58] R. Kandaswamy and D. Furlonger, *Blockchain-based transformation: A gartner trend insight report*, Gartner IT Glossary (2018).

[59] E. Karafiloski and A. Mishev, *Blockchain solutions for big data challenges: A literature review*, IEEE, 2017, pp. 763–768.

[60] K. Karray, J.-L. Danger, S. Guilley, and M.A. Elaabid, *Prediction-based intrusion detection system for in-vehicle networks using supervised learning and outlier-detection*, Springer, 2018, pp. 109–128.

[61] M.A. Khan and K. Salah, *IoT security: Review, blockchain solutions, and open challenges*, Future Gen. Comput. Syst. **82** (2018), 395–411.

[62] F. Khelifi, A. Bradai, A. Benslimane, P. Rawat, and M. Atri, *A survey of localization systems in internet of things*, Mobile Networks Appl. **24** (2019), no. 3, 761–785.

[63] M. Kumar, M. Hanumanthappa, and T.V.S. Kumar, *Intrusion detection system using decision tree algorithm*, IEEE, 2012, pp. 629–634.

[64] A.A. Laghari, K. Wu, R.A. Laghari, M. Ali, and A.A. Khan, *A review and state of art of internet of things (IoT)*, Arch. Comput. Meth. Engin. (2021), 1–19.

[65] L. Lao, Z. Li, S. Hou, B. Xiao, S. Guo, and Y. Yang, *A survey of IoT applications in blockchain systems: Architecture, consensus, and traffic modeling*, ACM Comput. Surveys (CSUR) **53** (2020), no. 1, 1–32.

[66] A. Lazarevic, *Managing cyber threats: issues, approaches, and challenges*, Springer Science+ Business Media, Incorporated, 2005.

[67] L. Li, *Study on security architecture in the internet of things*, vol. 1, IEEE, 2012, pp. 374–377.

[68] M. Li, I. Koutsopoulos, and R. Poovendran, *Optimal jamming attack strategies and network defense policies in wireless sensor networks*, IEEE Trans. Mobile Comput. **9** (2010), no. 8, 1119–1133.

[69] W. Li, P. Yi, Y. Wu, L. Pan, and J. Li, *A new intrusion detection system based on KNN classification algorithm in wireless sensor network*, J. Electric. Comput. Engin. **2014** (2014).

[70] H.-J. Liao, C.-H.R. Lin, Y.-C. Lin, and K.-Y. Tung, *Intrusion detection system: A comprehensive review*, J. Network Comput. Appl. **36** (2013), no. 1, 16–24.

[71] F. Maciá-Pérez, F.J. Mora-Gimeno, D. Marcos-Jorquera, J.A. Gil-Martínez-Abarca, H. Ramos-Morillo, and I. Lorenzo-Fonseca, *Network intrusion detection system embedded on a smart sensor*, IEEE Trans. Ind. Electron. **58** (2010), no. 3, 722–732.

[72] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, *Blockchain's adoption in IoT: The challenges, and a way forward*, J. Network Comput. Appl. **125** (2019), 251–279.

[73] F. Mattern and C. Floerkemeier, *From the internet of computers to the internet of things*, From active data management to event-based systems and more, Springer, 2010, pp. 242–259.

[74] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, *Internet of things: Vision, applications and research challenges*, Ad hoc networks **10** (2012), no. 7, 1497–1516.

[75] K. Mohamed, *IoT physical layer: sensors, actuators, controllers and programming*, The Era of Internet of Things, Springer, 2019, pp. 21–47.

[76] C.M. de Morais, D. Sadok, and J. Kelner, *An IoT sensor and scenario survey for data researchers*, J. Brazil. Comput. Soc. **25** (2019), no. 1, 1–17.

[77] S. Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*, Decentr. Bus. Rev. (2008), 21260.

[78] T. Nitin, S.R. Singh, and P.G. Singh, *Intrusion detection and prevention system (idps) technology-network behavior analysis system (nbas)*, ISCA J. Engin.Sci. **1** (2012), no. 1, 51–56.

[79] P. Oberoi and S. Mittal, *Survey of various security attacks in clouds based environments*, Int. J. Adv. Res. Comput. Sci. **8** (2017), no. 9.

[80] A. Ometov, Y. Bardinova, A. Afanasyeva, P. Masek, K. Zhidanov, S. Vanurin, M. Sayfullin, V. Shubina, M. Komarov, and S. Bezzateev, *An overview on blockchain for smartphones: State-of-the-art, consensus, implementation, challenges and future trends*, IEEE Access **8** (2020), 103994–104015.

[81] C.-M. Ou, *Host-based intrusion detection systems inspired by machine learning of agent-based artificial immune systems*, IEEE, 2019, pp. 1–5.

[82] M. Panda and M.R. Patra, *Network intrusion detection using naive bayes*, Int. J. Comput. Sci. Network Secur. **7** (2007), no. 12, 258–263.

[83] S.S. Panda, B.K. Mohanta, M.R. Dey, U. Satapathy, and D. Jena, *Distributed ledger technology for securing IoT*, IEEE, 2020, pp. 1–6.

[84] A. Patel, M. Taghavi, K. Bakhtiyari, and J.C. Júnior, *An intrusion detection and prevention system in cloud computing: A systematic review*, J. Network Comput. Appl. **36** (2013), no. 1, 25–41.

[85] A. Perrig, J. Stankovic, and D. Wagner, *Security in wireless sensor networks*, Commun. ACM **47** (2004), no. 6, 53–57.

[86] S. Pontarelli, G. Bianchi, and S. Teofili, *Traffic-aware design of a high-speed FPGA network intrusion detection system*, IEEE Trans. Comput. **62** (2012), no. 11, 2322–2334.

[87] R. Porkodi and V. Bhuvaneswari, *The internet of things (IOT) applications and communication enabling technology standards: An overview*, IEEE, 2014, pp. 324–329.

[88] G.S. Ramachandran and B. Krishnamachari, *Blockchain for the IoT: Opportunities and challenges*, May 2018.

[89] ———, *A reference architecture for blockchain-based peer-to-peer IoT applications*, May 2019.

[90] L.K. Ramasamy and S. Kadry, *Blockchain in the Industrial Internet of Things*, IOP Publishing, 2021.

[91] T.A. Rao and E.U. Haq, *Security challenges facing IoT layers and its protective measures*, Int. J. Comput. Appl. **179** (2018), no. 27, 31–35.

[92] M.A. Rashid and H.H. Pajooh, *A security framework for IoT authentication and authorization based on blockchain technology*, IEEE, 2019, pp. 264–271.

[93] M.A. Rassam, M.A. Maarof, and A. Zainal, *A novel intrusion detection framework for wireless sensor networks*, IEEE, 2011, pp. 350–353.

[94] D. Rose, *Enchanted objects: Design, human desire, and the Internet of things*, Simon and Schuster, 2014.

[95] K. Rose, S. Eldridge, and L. Chapin, *The internet of things: An overview*, Internet Society (ISOC) **80** (2015), 1–50.

[96] F. Sabahi and A. Movaghar, *Intrusion detection: A survey*, IEEE, 2008, pp. 23–26.

[97] Y. Sahni, J. Cao, S. Zhang, and L. Yang, *Edge mesh: A new paradigm to enable distributed intelligence in internet of things*, IEEE Access **5** (2017), 16441–16458.

[98] K. Scarfone and P. Mell, *Guide to intrusion detection and prevention systems (idps)*, NIST Special Pub. **800** (2007), no. 2007, 94.

[99] J. Schmidhuber, *Deep learning in neural networks: An overview*, Neural Networks **61** (2015), 85–117.

[100] A. Schmidt and K. Van Laerhoven, *How to build smart appliances?*, IEEE Personal Commun. **8** (2001), no. 4, 66–71.

[101] D. Seethalakshmi and G.M. Nasira, *Detecting and preventing intrusion in multi-tier web applications using double guard*, IEEE, 2016, pp. 3124–3127.

[102] S. Sun, R. Du, S. Chen, and W. Li, *Blockchain-based iot access control system: Towards security, lightweight, and cross-domain*, IEEE Access **9** (2021), 36868–36878.

[103] M.V. Suramwar and S.M. Bansode, *A survey on different types of intrusion detection systems*, Int. J. Comput. Appl. **122** (2015), no. 16.

[104] I. Sutskever, R. Jozefowicz, K. Gregor, D. Rezende, T. Lillicrap, and O. Vinyals, *Towards Principled Unsupervised Learning*, December 2015, arXiv:1511.06440 [cs].

[105] S.N. Swamy, D. Jadhav, and N. Kulkarni, *Security threats in the application layer in IOT applications*, IEEE, 2017, pp. 477–480.

[106] A. Tewari, A.K. Jain, and B.B. Gupta, *Recent survey of various defense mechanisms against phishing attacks*, J. Inf. Privacy Secur. **12** (2016), no. 1, 3–13.

[107] A. Thakkar and R. Lohiya, *Role of swarm and evolutionary algorithms for intrusion detection system: A survey*, Swarm Evol. Comput. **53** (2020), 100631.

[108] S. Thrun and M.L. Littman, *Reinforcement learning: An introduction*, AI Magazine **21** (2000), no. 1, 103–103.

[109] J. Tournier, F. Lesueur, F. Le Mouël, L. Guyon, and H. Ben-Hassine, *A survey of IoT protocols and their security issues through the lens of a generic IoT stack*, Internet Things **16** (2021), 100264.

[110] B. Van Schewick, *Internet architecture and innovation*, Mit Press, 2012.

[111] A. Čolaković and M. Hadžialić, *Internet of things (IoT): A review of enabling technologies, challenges, and open research issues*, Comput. Networks **144** (2018), 17–39.

[112] R. Vijaya Saraswathi, S. Nalluri, S. Ramasubbareddy, K. Govinda, and E. Swetha, *Brilliant corp yield prediction utilizing internet of things*, Data Engineering and Communication Technology, Springer, 2020, pp. 893–902.

[113] W. Viriyasitavat, T. Anuphaptrirong, and D. Hoonsopon, *When blockchain meets internet of things: Characteristics, challenges, and business opportunities*, J. Ind. Inf. Integr. **15** (2019), 21–28.

[114] A. Wahid and P. Kumar, *A survey on attacks, challenges and security mechanisms in wireless sensor network*, Int. J. Innov. Res. Sci. Technol. **1** (2015), no. 8, 189–196.

[115] J. Wan, *Malware detection using pattern classification*, U.S. Patent Trademark Office (2012).

[116] W. Wang, X. Du, and N. Wang, *Building a cloud IDS using an efficient feature selection method and SVM*, IEEE Access **7** (2018), 1345–1354.

[117] R.H. Weber, *Internet of things–New security and privacy challenges*, Comput. Law Secur. Rev. **26** (2010), no. 1, 23–30.

[118] X. Xiao, G. Wang, and J. Gehrke, *Differential privacy via wavelet transforms*, IEEE Trans. Knowledge Data Engin. **23** (2010), no. 8, 1200–1214.

[119] Y. Yang, J. Li, and Y. Yang, *The research of the fast SVM classifier method*, IEEE, 2015, pp. 121–124.

[120] F. Yihunie, E. Abdelfattah, and A. Regmi, *Applying machine learning to anomaly-based intrusion detection systems*, IEEE, 2019, pp. 1–5.

[121] K. Zhao and L. Ge, *A survey on the internet of things security*, IEEE, 2013, pp. 663–667.

[122] B. Zhou, J. Pei, and W. Luk, *A brief survey on anonymization techniques for privacy preserving publishing of social network data*, ACM Sigkdd Explor. Newsletter **10** (2008), no. 2, 12–22.

[123] W. Zhou, Y. Jia, A. Peng, Y. Zhang, and P. Liu, *The effect of iot new features on security and privacy: New threats, existing solutions, and challenges yet to be solved*, IEEE Internet Things J. **6** (2018), no. 2, 1606–1616.

[124] R. Zuech, T.M. Khoshgoftaar, and R. Wald, *Intrusion detection and big heterogeneous data: A survey*, J. Big Data **2** (2015), no. 1, 1–41.