Hindawi
Journal of Sensors
Volume 2023, Article ID 6048087, 18 pages
https://doi.org/10.1155/2023/6048087

Review Article

A Systematic and Comprehensive Survey of Recent Advances in Intrusion Detection Systems Using Machine Learning: Deep Learning, Datasets, and Attack Taxonomy

Asadullah Momand,[1] **Sana Ullah Jan**,[2] **and Naeem Ramzan**[1]

[1] *School of Computing Engineering and Physical Sciences, University of the West of Scotland, Paisley, UK PA1 2BE*
[2] *School of Computing, Edinburgh Napier University, Edinburgh, UK EH10 5DT*

Correspondence should be addressed to Naeem Ramzan; naeem.ramzan@uws.ac.uk

Received 17 July 2022; Revised 6 February 2023; Accepted 18 February 2023; Published 28 February 2023

Academic Editor: Jesús Lozano

Recently, intrusion detection systems (IDS) have become an essential part of most organisations' security architecture due to the rise in frequency and severity of network attacks. To identify a security breach, the target machine or network must be watched and analysed for signs of an intrusion. It is defined as efforts to compromise the confidentiality, integrity, or availability of a computer or network or to circumvent its security mechanisms. Several IDS have been proposed in the literature to efficiently detect such attempts exploiting different characteristics of cyberattacks. These systems can provide with timely sensing the network intrusions and, subsequently, notifying the manager or the responsible person in an organisation. Important actions are then carried out to reduce the degree of damage caused by the intrusion. Organisations use such techniques to defend their systems from the network disconnectivity and increase reliance on the information systems by employing intrusion detection. This paper presents a detailed summary of recent advances in IDS from the literature. Nevertheless, a review of future research directions for detecting malicious operations and launching different attacks on systems is discussed and highlighted. Furthermore, this study presents detailed description of well-known publicly available datasets and a variety of strategies developed for dealing with intrusions.

1. Introduction

In today's environment, the Internet has evolved into a crucial tool and an integrated entity of human life. Individuals from all over the world have adopted it as a platform for communication and data exchange. The data carried through wireless Internet networks might vary from innocuous images or videos posted on social networking sites to sensitive material exchanged between government agencies. However, despite recent advances, the Internet still has limitations that must be resolved before it can be trusted, such as low resilience against cyberattacks. With the world's growing reliance on digital technologies, such as computers and the Internet, one of the key challenges that must be addressed is establishing secure and reliable applications, frameworks, and networks that are resistant to these assaults.

Developments in protocols for communication between interconnected smart devices and advances in the computational capabilities of these nodes have increased their usage in daily life activities. This combination of Internet services and smart devices has recently been termed as Internet of Things (IoT). It is made up of a wide range of smart sensors and devices that help to make the web an intelligent system. According to the growth rate usage of IoT device, presented by Intel, there were two billion interconnected devices in 2006, and 200 billion are predicted to increase by 2020 [1]. Primarily, it comprises of advanced digital devices that are incorporated in physical network. These devices are linked to each other via Internet, and they exchange large amounts of data on daily basis without the need for human intervention [2].

A generic architecture of IoT is given in Figure 1. It contains different types of nodes such as smart phones or personal devices which can communicate with different devices via Bluetooth, Wi-Fi, or cellular network. It can be a two-way communication such as the link between a smart phone and a smart watch, or it can be one-way traffic channel, such as a camera sending pictures and videos to the smart phone or a PC. Another category contains industrial nodes, for instance, industrial robots and robotic hands, that are continuously being monitored and operated through a PC. Such applications may require a two-way communication channel for sending instructions from the PC to the node and for sending the acknowledgements or observed readings from the node back to the PC. A third type of nodes in an IoT includes the routers and base stations which are typically used for routing the traffics. These devices are usually installed at fixed locations whereas the other devices are capable of mobile applications.

There have been many attempts by researchers in the field from around the world to achieve satisfactory level of safety and security of the Internet, each of these having respective pros and cons. This study is an attempt to review and summarize these efforts to provide a ground for researchers in the field. The studies have been classified according to dataset compositions and IDS capabilities via machine learning (ML) and deep learning (DL) techniques. The aim is to provide a detailed survey on data-driven IDS using advanced ML and DL techniques. Moreover, this paper provides a detailed overview of different types of attacks and their mitigating strategies proposed in the literature. Furthermore, a fine-grain taxonomy of ML- and DL-based IDS is also presented to provide deep insight into existing research. Hence, a thorough comparative analysis of the existing state-of-the-art ML and DL algorithms is presented. In addition, a comprehensive study of different datasets for intrusion detection along with their advantages and disadvantages is presented. Furthermore, this study also outlines the shortcoming in the existing literature and provides future research directions for efficient IDS using big data and ML. In brief, the motivation of this paper is to summarize recent developments in the sector of intrusion detection, highlight their shortcomings, spotlight the current challenges, and outline the future research direction.

The intrusion has been defined in the literature as “an unauthorised approach to the data within a network system to compromise the confidentiality of the system” [3]. The network intrusion has progressively been expanded in recent years, resulting in personal privacy theft and becoming a major attack platform [4]. The researchers have come up with the concept of IDS to tackle these issues that can be defined as “a network security device that monitors network traffic for unexpected patterns” [5].

It is believed that a good IDS is necessary to overcome the issue of network intrusion where unauthorised activities on a computer network result in a risk for end users [2]. Conventionally, to identify an intrusion, the IDS compares the user’s activities to previously recorded compromised data. A firewall, on the other hand, is a barrier that can control the traffic flow in both directions. The security policy defined in firewall determines how much traffic is permitted to flow in each direction. Therefore, the IDS and firewalls must be considered two different concepts as far as this study is concerned.

In this paragraph, this study is compared with the existing surveys in literature to highlight the essence of current review. Ahmed et al. [6] focuses on mainly intrusion detection techniques. Moreover, the different types of computer attacks are presented. Similarly, Buczak and Guven [7] explains the intrusion detection systems. Furthermore, it also focuses on the techniques of IDS and the datasets used by researchers to develop IDS. The studies [8–12] illustrate the comparative analysis of ML and DL approaches in intrusion detection. In articles [13–16], the authors comprehensively explain about the ML algorithms for intrusion detection along with the detailed explanation of the datasets and challenges for modern scenario. Thakkar and Lohiya [17] thoroughly described the taxonomy of IDS along with the techniques used for the evaluation of IDS. As per recent surveys in the field of intrusion detection using ML, no article comprehensively reviewed different types of IDS, publicly available datasets, IDS classifications, and different kinds of attacks altogether. As compared to the previous articles, our survey focuses on the majority areas of IDS which were not fully discussed in the previous surveys.

A rigorous and exhaustive assessment of the literature may aid in the community’s growth. Existing IDS may be classified according to their design, detection mechanism, decision-making process, localization, and reaction. We have gone through a large number of surveys focusing on the development of IDS using ML-based or DL-based approaches. Furthermore, we approach our study from a variety of angles. The intrusion detection methods are explored in detail, analysing their fundamental principles and relevant applications for each technology category. Additionally, we perform a comprehensive assessment of cybersecurity datasets to improve our understanding of them and their usefulness. Our survey also includes a detailed knowledge about the cyberattacks that can be useful for the readers or researchers in the field.

Bijone [18] presents a survey on security techniques for network. The intrusion detection and prevention approaches have been classified according to varying characteristics. Similarly, a survey of signature-based and statistical-based IDS techniques are presented by Dangra [19]. The study further discusses different ML and DL techniques applied for intrusion detection. Moreover, G. Meena and Choudhary [20] and Jose et al. [21] both present their surveys in terms of IDS based on varying features. Meena and Choudhary also discuss the IDS datasets and underlying shortcomings. Nevertheless, the current available surveys such as Khraisat et al. [22], Yu et al. [23], Leevy and Khoshgoftaar [24], and Lee et al. [25] focused on ML techniques, publicly available datasets, and different types of cyberattacks. As compared to these studies, the current survey covers and discusses majority of the areas of IDS in detail. Moreover, it also illustrates the challenges and classification of IDS. In addition, it

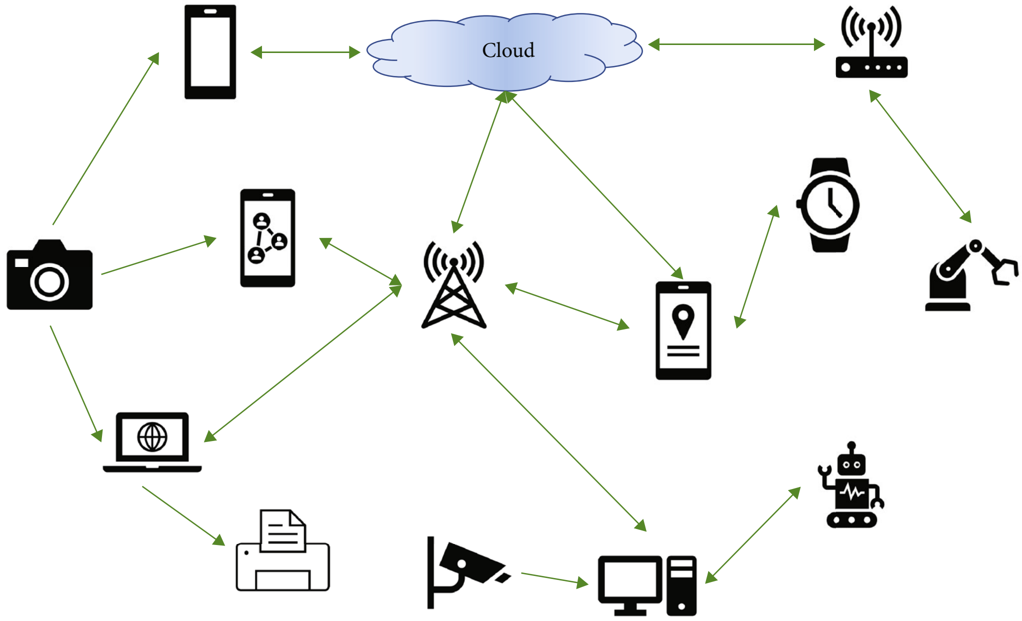

Figure 1: Visual representation of generic architecture of IoT with nodes connected to each other and to the cloud.

explains different aspects including ML, DL, datasets, and cyberattacks which are not presented in the previous surveys.

Figure 2 shows the conceptual visual of an IDS applied for intrusion detection in IoT. As shown, it can be considered as an agent checking the data coming toward the IoT nodes. It allows the normal data to pass through it toward the IoT nodes. On the other hand, if the data is attacked, then it should block the data and raise the alarm.

Table 1 summarizes the previous and existing surveys published over the last decade. It shows the classification of IDS along the datasets covered in this survey as well as previous surveys with explanation about ML and DL techniques. In addition, different types of cyberattacks are very well explained in this survey.

The rest of the paper is organised as follows: Section 2 summarizes the types of intrusions reported in the literature so far. Section 3 presents classification of IDS as per the categories found in the literature including architecture, detection methods, decision-making, locality, and response. Section 4 highlights the difference between the concepts of IDS and closely related firewall; a taxonomy of machine learning algorithms is presented in Section 5; a list of publicly available datasets is provided in Section 6 along with different characteristics of those datasets to highlight the differences. Section 7 discusses the research gaps discovered as a result of this assessment, as well as possible future directions. Finally, Section 8 concludes the paper.

2. Types of Intrusions

There are several types of network attacks on the basis of purpose, severity of involvement, and network types as explained below. Figure 3 illustrates different cyberattacks with different domains of applications corresponding to the attacks.

2.1. Based on Purpose

2.1.1. Reconnaissance. The process of gathering or probing information to analyse a network's vulnerabilities and then using that information to execute a successful attack is known as reconnaissance. Such attacks include network port inspection and traffic analysis. In addition, packet sniffers and IP address queries are also included in this type of attack [26]. The following are examples of reconnaissance attacks.

(i) Scanning the port: an attacker attempting to get into a computer sends a series of messages to check and learn which computer services are associated with certain number of well-known ports

(ii) Packet sniffers: a special device listens in on networked computer traffic, addressed to other computers, capturing data, and storing it for further examination

(iii) Sweeping the ping: in this type of attack, the attacker tries different methods for determining the IP address range that is mapped to live hosts

2.1.2. Access Attacks. An unauthorised invader can obtain access to a device if they do not have access to an account or password [27]. Someone without access to the data can enter illegally and hack it or create a programme to exploit a hole in the hacked or attacked application. Unauthorised access to online accounts, private databases, and other sensitive data may be acquired by exploiting known vulnerabilities in authentication services, File Transfer Protocol (FTP)

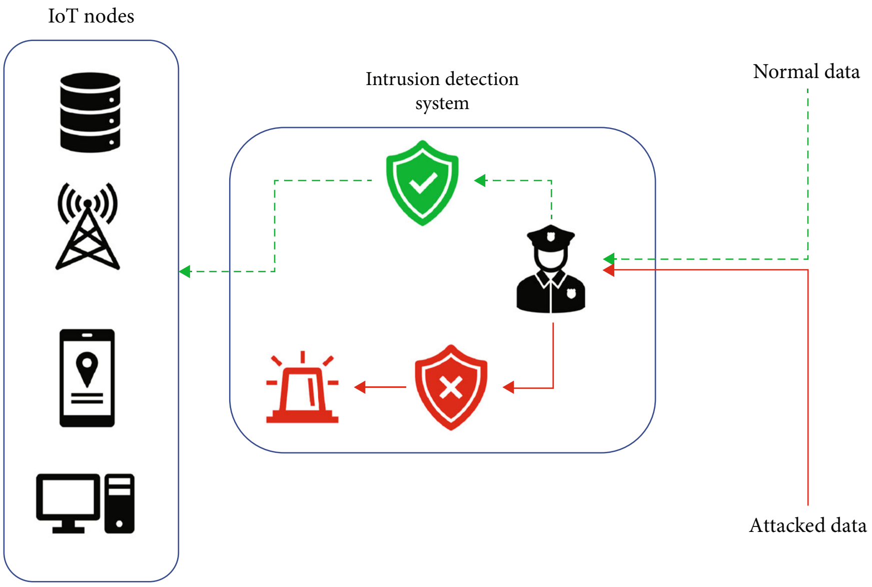

Figure 2: Intrusion detection system concept.

Table 1: Comparison of our survey with the past surveys in terms of IDS classification and machine learning techniques.

Ref.	Year	Datasets	ML	DL	Attacks	IDS classification
[18]	2016	✗	✗	✗	✓	✓
[19]	2016	✗	✓	✓	✗	✗
[20]	2017	✓	✗	✗	✗	✓
[21]	2018	✗	✗	✗	✗	✓
[22]	2019	✓	✓	✗	✓	✗
[23]	2019	✓	✗	✗	✓	✗
[24]	2020	✓	✓	✓	✗	✗
[25]	2021	✓	✓	✓	✗	✗
Our survey	2022	✓	✓	✓	✓	✓

services, and web services. The following are some examples of access attacks:

(i) Attacks on secret code: this attack, also known as dictionary attack, is initiated by an unauthorised user trying all possible password combinations in a small domain to get access to an account. Password resetting and password guessing are the two techniques which are commonly used in this attack

(ii) Port redirection: a type of attack where one trusted host is used by an attacker to get access to other hosts that are protected by a network firewall

(iii) Utilization of trust port: when an attacker takes control of one trusted host and uses it for launching attacks against another trusted host is known as utilization of trust port

(iv) Man-in-the-middle attacks: it, also known as Janus attack, is an active kind of surveillance where the attacker establishes independent connections with victims and transfers messages between them, creating the impression that they are having a private conversation

(v) Phishing: when an attacker sends a fraudulent email and pretend to be a reputable organisation to deceive the recipient into revealing personal data that will be utilised to commit identity theft

2.1.3. Denial-of-Service Attacks. Malicious cyber threat devices block authorised IoT devices from gaining access to information systems, servers, or other network services, leading in denial-of-service (DoS) assaults. This attack floods a target server or network with traffic until it becomes ineffective or fails, preventing genuine IoT devices from communicating with it [28].

2.2. Based on Severity of Involvement

2.2.1. Active Attacks. When the data is being sent to all parties by attacker or to stop transfer of the data in unidirectional or multidirectional directions is referred to as active attack. The examples are as follows:

(i) Distributed DoS attacks: a distributed DoS (DDoS) attack triggers several IoT devices to collaborate for launching attack on a single target. An attacker may utilise botnets to compromise a large number of IoT devices connected to the Internet by launching DDoS attacks on such devices. Attackers profit from security flaws or system shortcomings by controlling devices via multiple commands to hack IoT gadgets. DDoS attacks are growing increasingly serious as more and more IoT devices are connecting to networks. IoT systems frequently employ default keys that are not password-protected, leaving the system exposed to assaults and exploitation. IoT system penetration is often unknown to consumers, and an

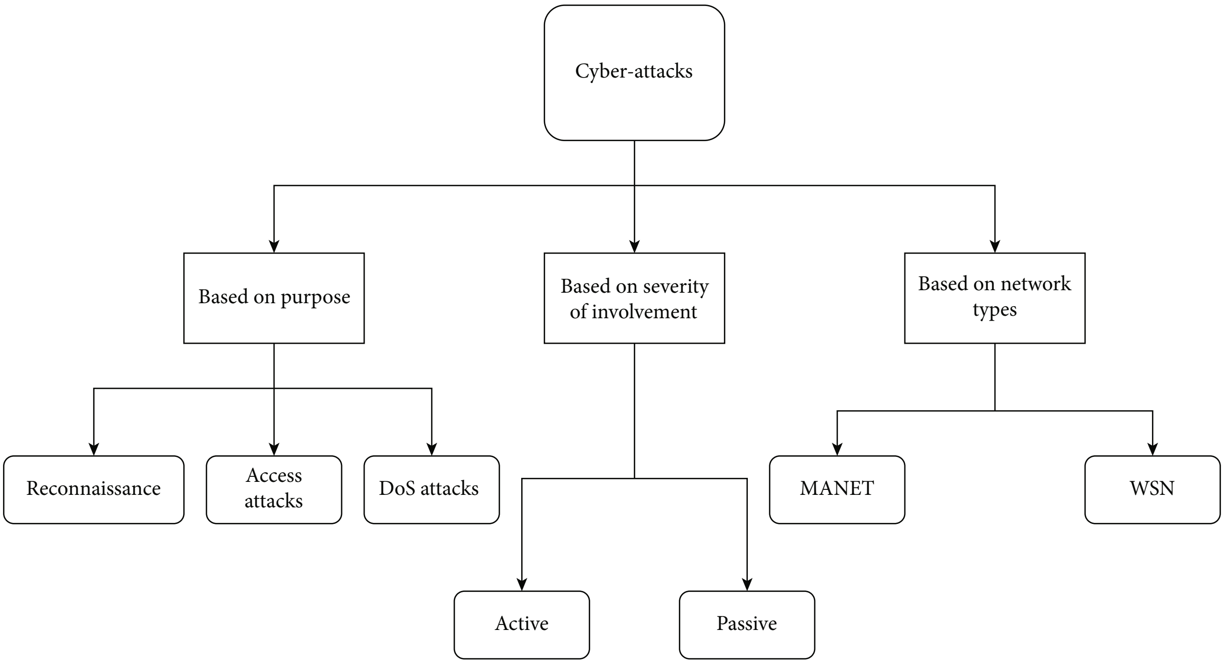

Figure 3: Types of cyberattacks and corresponding target applications.

attacker might potentially infiltrate a significant number of these networks to launch a wide-scale assault without informing the networks' administrators [26]

2.2.2. Passive Attacks. An unauthorised attacker wiretaps or otherwise intercepts the two parties' communication to steal data from a system.

(i) Theft attack: an assault in which the hacker attempts to seize control of the IoT system's security to obtain access to sensitive information is known as a theft attack. Data leaking and keylogging are two types of theft attacks. During data theft assaults, an attacker attempts to hack into a remote IoT device to acquire unauthorised access to data that can be sent to a distant attack computer. During keylogging operations, the attacker connects to a remote computer to collect user inputs and extract private information [26]

2.3. Based on Network Types. Wireless sensor networks (WSN) [29] and mobile ad hoc networks (MANET) [30] are two network types where attacks are categorised. The attacks on WSNs and MANET are explained as follows.

2.3.1. Attacks in MANET

(i) Byzantine attack: this is a MANET attack in which information leakage compromises an authenticating device or set of devices that normally offers security, making it hard to distinguish between a genuine device and a hostile user

(ii) The black hole attack: it is defined as routing all network traffic to a specific node as if that node does not exist, causing all data sent to disappear. In this case, the node is referred to as a black hole. The Route Request (RREQ) and Route Reply (RREP) protocols will be used to construct this assault

(iii) Flood rushing: a race between legitimate flood opponents and valid flood opponents will occur in this attack. Something happens when there is propagation. An adversarial free route will not be established using the authentication methods used

2.3.2. Attacks on WSN

(i) Black hole attack: in terms of the routing method, it creates an alliance node that appears to be highly appealing in that it encourages zero-cost paths for neighboring nodes. As a result, the traffic to these false nodes is at its peak. Nodes that are close to these dangerous nodes use a lot of bandwidth, causing resource congestion and message destruction

(ii) Flooding: flooding occurs at the network layer as well. An opponent sends connection requests to the targeted node on a regular basis. The targeted node allocates specific resources to the opponent to fulfil each request. The memory and energy resources of the flooded node may be expended because of this attack

(iii) Sybil attack: in this scenario, a bad node in a network has more than one character. It was first described as a method for bypassing the redundancy features of distributed data storage systems in peer-to-peer networks. Other fault tolerance systems such as disparity, multipath routing, routing algorithms, data aggregation, voting, fair resource allocation, topology maintenance, and malfunction detection are all vulnerable to Sybil's attack

(iv) Wormhole attack: a pair of terrible nodes initially detects a wormhole on the network layer in the wormhole assault. All network traffic is tunnelled in one way to a remote point, preventing data from being received in other sections of the network. These packets are then locally replayed. This generates the false impression that the sender is only a few nodes away from the remote location. This might result in packet resend and congestion, draining energy from innocent nodes. The wormhole attack on the network of wireless sensors is further discussed in [31]

3. Taxonomy of IDS

An IDS is a network security system that watches for unusual network activity. It determines if a user's behaviour is normal and reports on it [32]. A comparison of the user's actions to previously recorded intrusion records is used to identify the intrusion. In addition, IDS learns patterns from training data which is the concept of one of the intrusion detection techniques called signature-based detection. Sometimes called misuse-based detection, it can only identify known attacks and cannot detect new ones. Anomaly-based IDS, on the other hand, look for regular activity and treat any data that mismatch to regular patterns as an anomaly. This type of IDS can identify new threats that cannot be identified using signature-based methodology.

IDS can be applied for variety of applications, which includes the following:

(i) Keeping track of users and system activity

(ii) Recognising attack patterns in system activity

(iii) Identifying configuration errors in the system

(iv) Keeping records about intruders

3.1. IDS Classification Based on Architecture. Host-based IDS (HIDS), network-based IDS (NIDS), and hybrid IDS are the three forms of IDS depending on their architecture. The following sections go through each of them.

3.1.1. Host-Based IDS. A piece of software that is installed on a computer and monitors just the action of that specific computer is known as HIDS. It communicates with the operating system directly and is indifferent about the network traffic which is low level. To identify intrusions, majority of the HIDS are dependent on information that comes from system log files [33]. They can also keep track of system files, resources, and data received from programmes. A host-based IDS can generate most of the data and add to the administrative burden; it is normally only used on critical systems.

3.1.2. Network-Based IDS. The packets that transit across a network link are monitored by a NIDS. It might be a standalone hardware device or a software programme operating on a networked computer. The system is protected from an entire class of attacks, such as the "ping-of-death" attack, which may disable a host without ever activating a HIDS, since the packets monitored by the NIDS are not directed to the host on which the NIDS is placed. Furthermore, a NIDS is not able to identify attacks conducted on a host through an interface other than the network. It can only monitor traffic in its own network segment unless it uses sensors [33]. In switched and routed networks, a sensor is required in each segment (collision domain) where network traffic is to be monitored. When a sensor detects a possible intrusion, it alerts a central management console, which takes care of the appropriate passive or active response. Communication between the remote sensor and the management console should be secure to avoid interception or manipulation by the intruder. If a local attack is carried out, the system's authorised user who seeks to acquire further benefits will not be removed. A system user that is authorised could be able to establish a secure encrypted channel when accessing the computer remotely [33].

Zhao et al. [34] propose a support vector machine- (SVM-) based NIDS with k-fold cross-validation to increase the system's identification capabilities through attributes of attacks. The results show that the false-negative (FN) and the false-positive (FP) rates are high for both anomaly-based and signature-based methods. Similarly, Khan et al. [35] outline the difficulties of delivering fresh intrusion detection models utilising ML techniques. The KDD dataset is used to create and test a solution that merges the softmax algorithm with a convolutional neural network- (CNN-) based NIDS. It is a more efficient model for intrusion detection than the SVM and DBN (deep belief network) algorithms, according to the experimental analysis.

3.1.3. Hybrid IDS. Hybrid intrusion detection systems, which include both HIDS and NIDS, are the current trend in intrusion detection paradigm. It is generally believed that a flexible hybrid intrusion detection system boosts security as compared to HIDS and NIDS. It combines the locations of IDS sensors and generates information on attacks targeting specific network segments or the whole network. The research [36] utilises a modified kernel function called the radial basis function (RBF) and incremental SVM training methods to develop hybrid IDS. The authors utilised KDD Cup 1999 as a baseline dataset for their investigations.

3.2. IDS Classification Based on Detection Methods

3.2.1. Signature-Based IDS. The signature detection or misuse detection technique relies on a database containing a set of patterns, attacks, or intrusion signatures, among other things [18]. When an intrusion occurs or someone tries to attack, IDS compares the incursion's signatures to a database of predetermined signatures. When a match is made, the system raises an alarm. To detect misuse, the IDS analyses the data it collects and later compares it to vast databases of threat signatures. The IDS is looking for a specific type of attack that has been disclosed earlier. Misuse detection is based on the concept of utilising an expert system to detect intrusions using a comprehensive knowledge base. As a result, misuse systems can accurately detect even slight intrusions in their expert knowledge base. In addition, if this expert knowledge base is updated, misuse systems can detect even minor incursions with high accuracy. Because they are correctly constructed, misuse detection systems have a low percentage of false positives. One disadvantage of this design is that a misuse detection system will be unable to detect those intrusions which are not available in its knowledge base. Dangra describes how tiny variants of well-known attacks can go unnoticed if a misuse system is not properly created [19]. As a result, the system's accuracy is heavily reliant on the building of this knowledge base.

3.2.2. Anomaly-Based IDS. One of the most important characteristics of anomaly detection systems is their capability to detect new as well as previously unknown attacks. Several techniques have been examined as feasible answers to the anomaly detection problem, including statistical modelling and neural networks. Each of these anomaly-based techniques follows the same basic principles: abnormal behaviour shows an attempted attack, and the correct collection of features may identify anomalies from regular system usage. In anomaly detection, the system administrator establishes the baseline, or normal, condition of the network's traffic load, breakdown, protocol, and usual packet size. The anomaly detector compares the condition of network segments to the typical baseline to look for abnormalities [18]. It does not require specialised knowledge of computer attacks because the process of developing a baseline model of typical behaviour is frequently automated. This method is not without flaws, since anomaly detection may miss even well-known and well-understood attacks if they do not deviate much from what the system's normal behaviour.

Song et al. [37] developed a unique anomaly detection approach that may be automatically adjusted and improved without the need of predefined parameters. Furthermore, the author uses real traffic data from Kyoto University honeypots to assess this approach as a dataset. Hu et al. [38] describe a new approach to anomaly detection over noisy data based on robust SVM (RSVM). The overfitting problem caused by noise in the training dataset is efficiently addressed by these models. The use of an averaging strategy in typical SVM creates a smoother decision surface and automatically adjusts the level of regularisation with RSVM. Furthermore, when compared to regular SVM, the number of support vectors in RSVM is substantially lower. As a result, RSVM take less time to test. This approach is tested using DARPA BSM data from 1998. RSVM are compared to normal SVM and the k-nearest neighbors (kNN) classifier. Experiments demonstrate that RSVM are superior not just in terms of intrusion detection accuracy and minimal false positives but also in terms of generalisation ability and running duration in the presence of noise.

3.2.3. Stateful Protocol Analysis Detection. In contrast to anomaly-based detection, stateful protocol analysis detection is based on vendor-developed universal profiles that govern how individual protocols should and should not be utilised. It may identify unusual command sequences, such as issuing the same command many times or issuing a command without first issuing a command that it relies on. Another advantage of stateful protocol analysis is that it allows an IDS to maintain track of the authenticator used for each session and record the authenticator used for suspicious behaviour [39]. Overview of the classification of IDS is shown in Figure 4.

3.3. IDS Classification Based on Decision-Making

3.3.1. Cooperative IDS. Cooperative intrusion detection systems (COIDS) are active MANET with specific current protocol, services, and applications. MANET is considered to be the most cooperative as well as pleasant network; however, it does not include security. In the event, a node detects any abnormality or comes across evidence that is not assessed properly in COIDS. The process then works out to ensure the global intrusion detection action while coordinating with other nodes. In such systems, even if a single node is agreed upon having committed a crime, the decision-making is subjected to cooperation because a node deciding by itself would be malevolent. MANET are unstructured wireless networks, and their security is supposed to be substantially more effective and efficient since they hold differentiating characteristics of ad hoc networks. Based on cooperative strategy, an approach to establish an IDS, which would be used in MANET while utilising the fundamental game theories, has been discussed in [30]. Shams et al. [40] suggests about an active IDS (AIDS), which is not only a flexible cooperative detection system but also is an effective intrusion detection framework. Moreover, this research is to design and construct an IDS that does not interfere with MANET's normal packet routing process while retaining good performance.

3.3.2. Autonomous IDS. A software agent that performs a specific security monitoring function on a host is referred to as an autonomous agent. It can be evaluated separately because they are self-contained entities; they may be added, deleted, or changed without impacting other components or requiring the IDS to be restarted. Before making node-level judgments, network nodes make decisions and gather evidence and criteria of anomalies or intrusion activities from the network independently [18]. Other network nodes are not involved in the decision-making process. Furthermore, Kholidy et al. [41] discuss about HA-CIDS, a cloud-based intrusion detection system that is hierarchical and autonomous. The framework analyses and monitors system events in real time, as well as computing security and risk factors. The framework computes security parameters, and an autonomous controller picks the appropriate reaction to defend the cloud from identified threats and recover any damaged data or compromised services.

3.4. IDS Classification Based on Locality

3.4.1. Centralized IDS. The centralized IDS is made up of numerous monitors that keep an eye on the behaviour of

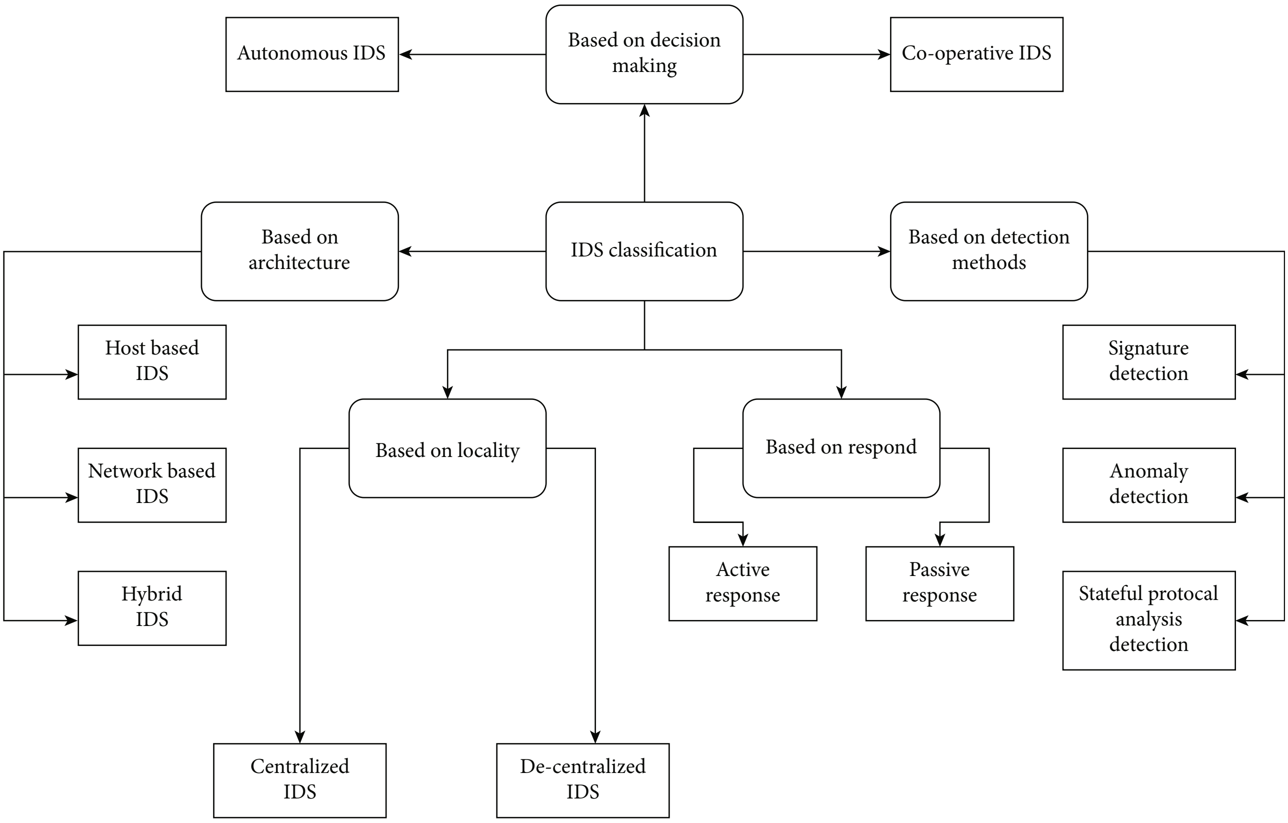

Figure 4: Classification of IDS.

their hosts or the network traffic that flows through. These monitors provide data to a central processing unit, which can be triggered by a local detection or regained from local network traffic. As a result, the analysis unit either receives alerts using alert correlation methods or receives network traffic data using conventional detection techniques [42]. A centralized intrusion detection system analyses data in a set number of locations, independent of the number of monitored hosts.

3.4.2. Decentralized IDS. A hierarchical system of monitoring sites or numerous self-contained IDS deployments are common components of decentralized IDS. They employ preprocessing and correlation of the monitored data throughout the hierarchy until the data converge to a central analysis unit on top of the hierarchy to overcome the performance of centralized IDS [42]. Data analysis is conducted in various places proportionate to the number of monitored hosts in a distributed IDS. We only consider the number and location of data analysis components, not the number of data gathering components.

3.5. IDS Classification Based on Response

3.5.1. Active Response. An active attack tries to change or disturb the system's resources. It involves modifying data streams or creating a false stream [43]. To acquire additional information about the attack and intruder, increasing the sensitivity level of the IDS is a common active reaction. When an intrusion is identified, active response IDS takes automated action. The severity and type of attack determine the specific action. Another preventative measure is to modify the system or network device configuration, such as routers and firewalls, to stop the intrusion and prevent the attacker from gaining access. It may be necessary to block the attacker's source address, restart a server or service, terminate connections or ports, or reset TCP sessions.

3.5.2. Passive Response. An IDS detects a possible security breach in a passive system, logs the data, and sends out an alarm. Furthermore, the intrusion is not actively tried to be stopped with passive reaction intrusion detection. It simply records the intrusion and sends an email notification to a designated recipient. For connectivity with a central administration console, some passive response IDS enable plug-ins. This enables to use the passive response product in a distributed active response system, where the passive IDS reports to a central console, which may then operate the network devices and systems involved. Intrusion notifications can be sent through pager, mobile phone, email, or a message box on the administrator's PC in today's IDS. To prevent an attacker from intercepting or manipulating the alerts, it is vital that they are transmitted securely. Communication surveillance or monitoring is part of the passive attack. A passive attack is one that tries to learn or use information from the system without causing any damage to the system's resources. The purpose of the attacker is to get the information being delivered [43].

4. Concepts of IDS

4.1. Difference between IDS and Firewall. The terms IDS and firewall are often confused; however, they are not the same thing. While both are concerned with network security, an IDS varies from a firewall in that a firewall detects intrusions and can also filter harmful traffic, whereas an IDS detects intrusions and attempts to prevent them by reporting the network. A firewall is a barrier that must allow traffic in both directions to pass through. The traffic that is allowed to travel in either direction is determined by a firewall security policy [44]. It also restricts the amount of data sent and received between private networks. An IDS and firewall concept is presented in Figure 5 to highlight the difference. Primarily, the firewall blocks network access to prevent infiltration, but it does not detect attacks from within the network.

5. Taxonomy of Machine Learning

5.1. Machine Learning Algorithms. The section below discusses two types of ML algorithms including supervised and unsupervised.

5.1.1. Supervised Learning. These types of algorithms learn from labelled data. After analysing the data, the algorithm decides which label to apply to new data based on patterns and connects the patterns to unlabelled new data.

(1) Naïve Bayes. The Naive Bayes algorithm is a simple way to predict outcomes based on the likelihood of each class's attributes. The supervised learning technique is used to simulate a predictive modelling problem. Naive Bayes is one of the most effective learning algorithms. It simplifies probability calculations by assuming that the probability of each attribute belonging to a specific class value is independent of all other attributes [45]. Conditional probability is the probability of a class value given an attribute value. Because ratios are simple to define and calculate, Naive Bayes is frequently discussed with categorical data.

(2) Decision Tree. A decision tree is a supervised machine learning method capable of performing both regression and classification problems. The decision tree method has a basic concept yet is quite powerful. The approach may be used to categorise nonlinearly separable data and requires less time to train [46]. It is significantly faster and more efficient than kNN and other classification algorithms.

(3) Logistic Regression. Logistic regression seeks to find the best-fitting model for establishing a link or dependency between the class variable and the characteristics [46]. It predicts a number between 0 and 1, which is the probability that the class is 1 given the observation, for a test case with just two classes: 0 and 1. The simple logistic regression model is good for binary classification, but it may be expanded to multiclass classification with some extra work.

(4) k-Nearest Neighbors. The kNN approach is a machine learning methodology that is used to solve classification problems. The kNN is a nonparametric and slow learning algorithm that makes no assumptions about basic data distribution. The absence of assumptions about the underlying data distribution is referred to as "nonparametric." The number of nearest neighbors is identified by k in kNN, the most crucial deciding factor is the quantity of neighbors. It determines the distance between the input and its test data before generating the appropriate forecast.

(5) Support Vector Machine. The SVM has been favoured as the framework since it is both interesting in terms of ML and embedded systems. It is a mathematical function that can distinguish between two categories of objects in both linear and nonlinear cases. It is a well-known ML algorithm that can still be applied to large-scale data classification challenges. It is very beneficial in a big data environment for multidomain applications.

(6) Artificial Neural Networks. A variety of neurons can be used to create artificial neural networks (ANN). The sizes of ANNs, or the number of neurons, in applications vary from tens of thousands to fewer than 10. ANNs can have a single layer of neurons or even more layers of neurons [47].

5.1.2. Unsupervised Learning. This method is used to analyse the structure of data, extract useful insights, find patterns, and increase efficiency; it incorporates this information into its operation.

(1) K-Means Clustering. K-means clustering is an unsupervised approach for dividing data into k-clusters [46]. The letter "K" stands for an iterative clustering process that supports in the determination of the greatest value for each iteration. The required number of clusters is decided initially. Using this clustering procedure, the data points are divided into K groups.

5.2. Deep Learning. A subset of ML techniques is known as deep learning (DL); that is, a combination of several linked layers can form a deep learning network, where the first layer is being considered an input and the final one is the output layer, and all levels in between are being referred to as hidden layers. The signal intensity of a neuron is influenced by characteristics such as activation function and weight, and each buried layer is made up of multiple neurons [48]. Table 2 shows a comparison between ML and DL methodologies.

The taxonomy of ML is shown in Figure 6. As indicated in the diagram, deep learning techniques are divided into supervised and unsupervised learning methods, including supervised learning methods such as deep neural network (DNN), CNN, DBN, and recurrent neural network (RNN) and unsupervised learning methods such as restricted Boltzmann machine (RBM), generative adversarial network (GAN), and autoencoder (AE).

5.2.1. Deep Neural Network. A deep neural network (DNN) is an ANN with numerous hidden layers between the input and output layers. DNNs, like shallow ANNs, may simulate

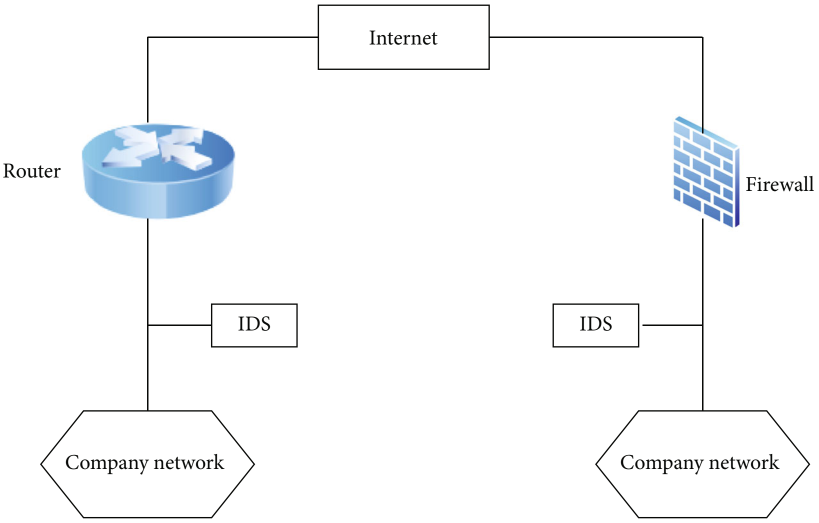

Figure 5: Concepts of IDS and firewall.

Table 2: Comparison of ML and DL techniques.

No.	Machine learning	Deep learning
1	To train machine learning methods, small datasets can be used.	The training of deep learning networks necessitates a huge dataset.
2	To supply the necessary input, external involvement is required.	Deep learning networks can extract characteristics from unprocessed data.
3	Retraining machine learning algorithms need human interaction.	Human involvement is not required in deep learning.
4	Approaches of machine learning are faster in implementation.	It takes longer to process in deep learning networks.
5	The outcomes of machine learning approaches are numerical in nature.	Deep learning techniques may provide a wide range of outcomes.

nonlinear interactions that are complicated. The fundamental goal of a neural network is to take a collection of inputs, conduct more calculations on them, and then outputs to solve real-world issues like categorisation. DNNs are multilayer variants of regular ANNs. Due of their high learning performance, DNN models have lately gained popularity [49].

5.2.2. Convolutional Neural Network. Convolutional neural networks (CNNs) are DL networks that are generally used for image processing. In addition, it can be used for intrusion detection as well as other applications. To extract characteristics from raw data, CNNs are often utilised in the intrusion detection sector. To recognise the output, a CNN takes a 2D picture as input and assigns priority to various areas of the image. There are several hidden layers in a CNN, including a fully connected layer and a convolutional layer. Moreover, a pooling layer and a nonlinearity layer are also presented in it where the first two of are parametric and the other two are not [50]. A detailed explanation about the advantages and disadvantages of the existing machine learning models and techniques is discussed in Table 3.

5.2.3. Deep Belief Networks. A probabilistic generative models comprised of RBM modules stacked on top of each other is known as deep belief networks (DBNs). Each RBM's output is fed into the next RBM in a DBN. Furthermore, neurons in the DBN layers communicate with neurons in the next layer but not with neurons in the same layer. DBNs can help with ANN training problems like delayed training and slipping into a local minimum. Natural language processing, intrusion detection, and picture identification are just a few of the applications that DBNs are utilised for [51].

5.2.4. Recurrent Neural Networks. Because recurrent neural networks (RNNs) can recall data processed at each time step and use it to calculate subsequent outcomes, an upgraded form of feed forward ANNs might be considered as RNNs. For this reason, the input of neurons in the other layer is connected to the output of each layer's neurons, as well as to itself, in an RNN. As a result, these models can deal with variable-length input sequences like times series and learn a data sequence to generate new members by using their internal memory. In RNNs, for complete information exchange, the neurons in the hidden layers are bidirectionally connected to themselves and all other neurons in the next layer. RNNs can be used successfully to simulate the temporal correlations of security threats and malicious activities [23]. RNNs have a wide range of applications, including computer vision, natural language processing (NLP), semantic comprehension, speech recognition, language modelling, translation, picture description, and human action recognition [52, 53].

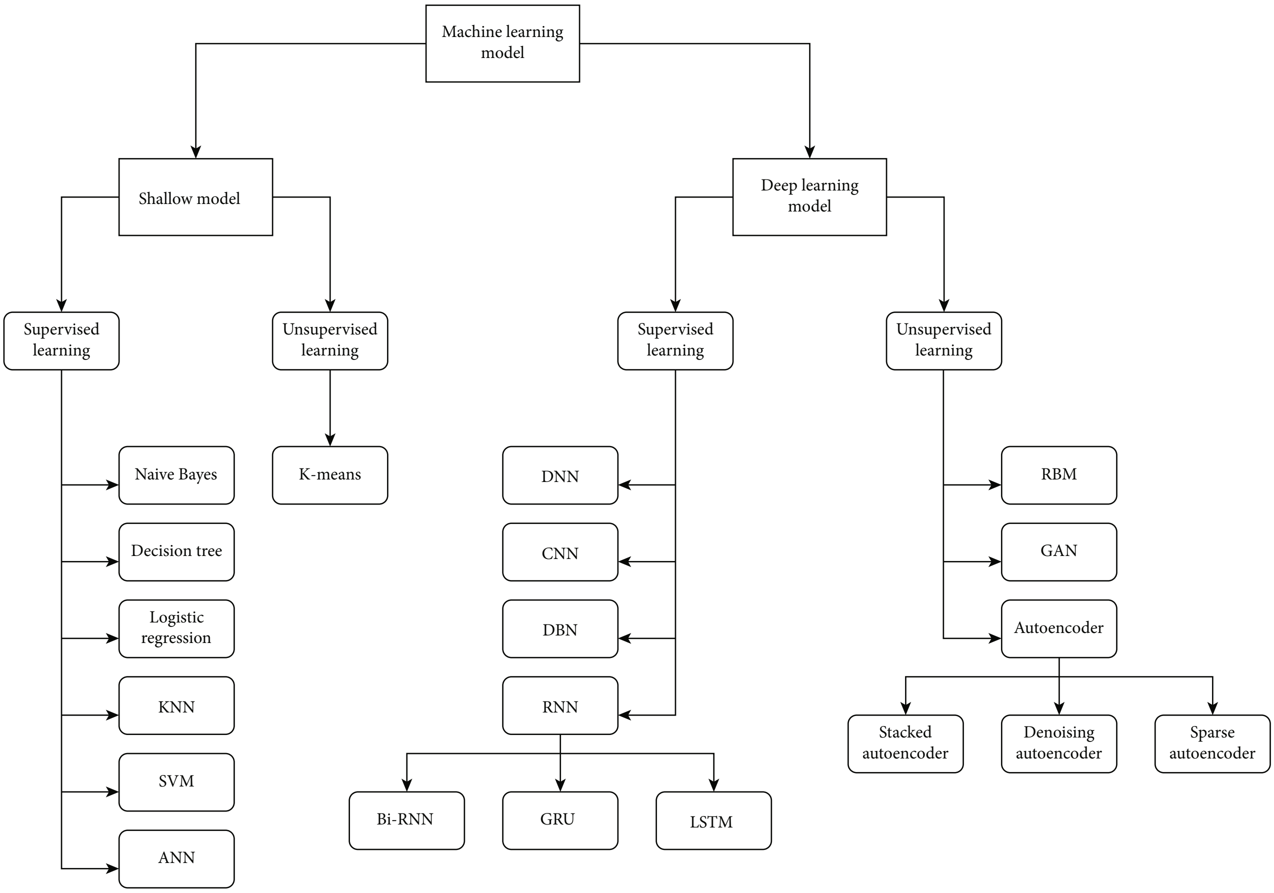

FIGURE 6: Taxonomy of machine learning.

TABLE 3: Advantages and disadvantages of the existing machine learning models and techniques.

Machine learning techniques	Advantages	Disadvantages
kNN	Simple and effective classification performance in many domain.	It shows poor run time performance upon large training set.
SVM	It gives high accuracy and low computational cost.	Lack of transparency in results.
ANN	It can learn without the need to be programmed.	High processing time is required for a large neural network.
Naïve Bayes	It requires little space during classification and training.	It can be oversensitive to irrelevant attributes.
Decision tree	Decision trees are very simple and fast.	It has long training time.
K-means	Implementation is easy.	It is very difficult to predict K-value.
DNN	It has a capability of processing unrecognised data.	Highly dependent on the data made available to them.
CNN	High accuracy in image recognition problems.	High computational cost.
RNN	RNN can model a collection of records.	Gradient exploding and vanishing problems.
GAN	Images generated by GAN are very realistic.	Poor interpretability of neural networks.

5.2.5. Generative Adversarial Networks. A generative adversarial network (GAN) is comprised of two ANNs competing within a zero-sum game. The loss of one ANN is considered a gain of another. GAN can work both on supervised as well as on unsupervised [54]. GANs are frequently employed in several fields, including speech, video, and picture production, as well as intrusion detection.

5.2.6. Autoencoders. An autoencoder, which may have many hidden layers, is aimed at building its inputs in such a way that the difference between its inputs and outputs is as small as possible. By training the network to avoid signal noise, autoencoders provide unsupervised learning of dataset encoding for dimensionality reduction. An encoder consists of two steps: encoder transforms the data into code while the decoder reconstructs the data from the code [55].

5.2.7. Staked Autoencoder. In [56], the authors present a two-staged IDS system that uses a stacked autoencoder with two hidden layers and a softmax classifier in each stage. The hidden layers are trained on unlabelled network traffic characteristics using a semisupervised learning approach. In first phase, the network is divided into two states such as normal and abnormal whereas the second phase allows you to distinguish between different types of attacks.

(1) Denoising Autoencoder. The denoising autoencoder (DAE) expands the data stream method's ability to utilise unlabelled samples. Nonetheless, the practicality of DAE for data stream analytic warrants further investigation because it denotes a fixed network capacity that is unable to adapt to quickly changing surroundings. A deep evolving denoising autoencoder (DEVDAE) which consists of two phases is described in [57]. In both phases, the generating and the discriminative phases, DEVDAE proposes an incremental learning strategy for DAE that uses a fully open and single pass working model. It has the ability to begin its generative learning process from scratch, without any prior structure. Its hidden nodes can be automatically produced and trained. Note that while this study focuses on the most difficult case of starting from scratch, the principle is immediately applicable in the existence of basic structure. The discriminative model is based on a softmax layer that generates DNN's end output and has the same online and evolving characteristics as the generative phase.

(2) Sparse Autoencoder. An IDS approach that combines a support vector regression (SVR) classifier with a sparse autoencoder (SAE) has been proposed in [58]. SVR prediction accuracy is improved using the SAE with a minimum amount of training time. The tests are conducted out on the NSL-KDD dataset using Python programming language. Moreover, TensorFlow tool is used in these tests. The SAE-SVR model reduces the training time of SVR and increases prediction rates by taking down error rates, according to the findings. The authors employ training time, root mean squared error, and mean absolute error as metrics.

5.2.8. Restricted Boltzmann Machine. The restricted Boltzmann machine (RBM) is a two-layer undirected graphical model with a complete set of connections between an observed layer and a hidden layer of random variables. It is a generative framework for modelling a distribution over visible variables using a set of stochastic features. To construct an effective NIDS, the authors of [59] employed unsupervised DL techniques. RBM is very useful for dimension reduction and extraction of feature. After that, just three remaining characteristics are clustered using the K-means clustering approach, and intrusions are detected using the unsupervised extreme learning machine. The author used KDD Cup 1999 dataset for this method and obtained 92.12 percent detection accuracy for RBM.

Table 4 illustrates IDS techniques throughout the last 6-7 years, along with evaluation metrics and detected attacks. It also reveals the dataset and algorithm that were used.

6. Datasets of IDS

This section presents an analysis of commonly used and important datasets for the research and development in the sector of IDS.

6.1. KDD-99. A DARPA dataset, namely, KDD-99, comprises of a network traffic trace of seven weeks. Moreover, it contains five million records in the form of binary data which is nearly four gigabytes. Several security attacks are included in this dataset such as U2R (user to root), DoS, probing, and R2L (remote to local). U2R is a type of attack in which an intruder gets root access of the host by gaining access to a user account [20]. A cyberattack on information systems or devices that stops authorised users from entering the system is known as DoS whereas in probing, the attacker tries to scan a network and gather information about it. An attacker uses an R2L attack to obtain access to a remote host by delivering data packets to it. This dataset contains 4.90 million single connection vectors along with its 41 features that can describe it as an attack or normal.

6.2. NSL-KDD. It is developed to address the shortcomings in the KDD Cup 1999 dataset. However, it also has low number of observations in training as well as testing subsets. This removes the requirement to pick a restricted selection of the data and enables the newly created IDS approaches to be tested over the whole of the dataset. Previously, this would have required selecting a subset of the data. Furthermore, this dataset is favoured due to very few redundant records. This also helps in reducing bias in the classification step caused by redundant data records that helps improve performance. However, there are some errors reported in this data that may limit its ability of reflecting real-world network activities [20].

6.3. ISCXIDS2012. It is a profile-based dataset that includes distribution models for network entities and applications at a lower level. User behaviour is simulated using the profiles. In the proper testbed, these profiles are utilised to build a dataset. The anomalous component of this dataset was created using various multistage attack scenarios. Agents are then utilised to simulate user action and run these profiles. This dataset covers malicious and nonmalicious network behaviour over the course of seven days [25].

6.4. CIDDS. CIDDS (Coburg intrusion detection datasets) are supplied for testing network intrusion detections in a virtual environment utilising OpenStack and comprise tagged flows. The CIDDS-001 dataset considers a tiny network with only a few servers and clients. In addition, Python scripts are used to generate innocuous user activity, such as web surfing, in this dataset. Each user works according to a fixed timetable, and his or her attributes are given in a configuration file to ensure realistic user behaviour. Security attacks includes DDoS, port scans, and brute force [80].

6.5. UNSW-NB15. To trace network traffic and test NIDS, this dataset is used. There are nine different types of security attacks such as fuzzers, shellcode, analysis, and worms. It

Table 4: IDS schemes used in last decade.

Ref.	Year	Algorithms	Evaluation metrics	Datasets	Detected attacks	Accuracy
[60]	2015	*K*-means kNN	Accuracy, detection rate	KDD-99	DoS U2R Probing R2L	99.76%
[61]	2015	SVM	—	GureKdd-Cup	R2L	96.08%
[62]	2016	ANN	—	Simulated dataset	Dos/DDos	99.4%
[63]	2016	PCA SVM	—	KDD-99	Attack Normal	—
[64]	2017	*K*-means R-tree SVM KNN	—	KDD-99	DoS U2R Probing R2L	—
[65]	2017	DNN	Accuracy, *F*1-score, recall, and precision	KDD-99, NSL-KDD	DoS U2R Probing R2L	KDD Cup 1999 = 81.29%, NSL − KDD = 83.28%
[66]	2018	Deep autoencoder-ANN	Accuracy, detection rate, and FPR	UNSW-NB15 NSL-KDD	DoS Probing R2L U2R	UNSWNB15 = 92.4% NSL − KDD = 98.6%
[67]	2018	GRU-RNN	Accuracy, *F*1-score, recall, and precision	NSL-KDD	—	89%
[68]	2018	GRU-RNN	Accuracy, detection rate, *F*1 -score, and precision	NSL-KDD KDD-99	DoS Probing R2L U2R	NSL − KDD = 99.24% KDD − 99 = 99.84%
[69]	2019	RNN GRU LSTM	Accuracy, detection rate	NSL-KDD ISCX	DoS U2R Probing R2L	NSL − KDD = 94% ISCX = 99.5%
[70]	2019	DNN	Accuracy, *F*1-score, recall, and precision	UNSW-NB15 NSL-KDD	DoS U2R Probing R2L	UNSW − NB15 = 89.1% NSL − KDD = 85.9%
[71]	2020	DNN	Accuracy, *F*1-score, recall, and precision	NSL-KDD	DoS U2R Probing R2L	87.7%
[72]	2020	—	Precision, *F*1-score, and recall	NSL-KDD	DoS U2R Probing R2L	—
[73]	2020	LSTM	Accuracy, FPR, and detection rate	NSL-KDD	DoS U2R Probing R2L	84.25%
[74]	2020	—	Accuracy, *F*1-score, recall, and precision	NSL-KDD	DoS U2R Probing R2L	87%
[75]	2021	CNN	Accuracy, *F*1-score	KDD-99 UNSW-NB15 CICIDS2017	—	KDD − 99 = 93.6% UNSW − NB15 = 93.5% CICIDS2017 = 98%

Table 4: Continued.

Ref.	Year	Algorithms	Evaluation metrics	Datasets	Detected attacks	Accuracy
[76]	2021	CNN	Accuracy, recall, and precision	CICIDS2017	Dos/DDos	98%
[77]	2021	CNN LSTM	Accuracy, recall, precision, ROC, and F-measure	UNSW-NB15 CIDDS-001	—	UNSW – NB15 = 99.1% CIDDS – 001 = 99.8%
[78]	2021	Kernel-based extreme learning machine	Accuracy, recall, and precision	NSL-KDD KDD-99 UNSW-NB15 CICIDS2017	DoS U2R Probing R2L	NSL – KDD = 98.6% KDD – 99 = 98.6% UNSW – NB15 = 93.42% CICIDS2017 = 97.15%
[79]	2021	—	Detection rate, error rate	Dapra NSL-KDD	DoS U2R Probing R2L	—

Table 5: Detailed explanation of IDS datasets.

Datasets	Number of records	Created by	Categories of attacks	Year of creation
KDD99	5 million	Dapra	DoS U2R Probe R2L	1999
NSL-KDD	5 million	University of New Brunswick (UNB)	DoS U2R Probe R2L	2000
ISCXIDS2012	2.4 million	Information Security Centre of Excellence (ISCX) (UNB)	DoS, brute force, and distributed denial of service (DDoS)	2012
CIDDS	33 million flows	Markus Ring et al.	Brute force, DDoS, and port scans	2017
UNSW-NB15	2.54 million	University of New South Wales (UNSW), Canberra. Australian Centre for Cyber Security (ACCS)	Fuzzers, shellcode, analysis, worms, backdoors, reconnaissance, dos, generic, and exploits	2015
CICIDS2017	2.8 million	Canadian Institute of Cyber Security (CIC)	Brute force FTP, Heartbleed, brute force SSH, DDoS, infiltration dos, web attack, and botnet	2017
CSE–CIC–IDS2018	16.2 million	Communications Security Establishment (CSE). Joined with ISCX and CIC	Brute force, DDoS, and web attacks	2018
Ton_IoT	22.3 million	School of Engineering and Information technology (SEIT), University of New South Wales (UNSW), Canberra	DDoS, ransomware, data injection, DoS, password attack, cross-site scripting (XSS), backdoor, man-in-the-middle (MITM), and scanning	2020

contains 2.5 million of records, and it has been created by university of New South Wales. *Tcpdump* is also used to record 100 GB of network traffic for 16 hours [81]. A brief description of IDS datasets is discussed in Table 5.

6.6. CICIDS2017. Records for a security attack have been discussed in this dataset. It creates natural benign traffic by profiling human behaviour using the B-profile method. Email, HTTP, HTTPS, SSH, and FTP are among the protocols included in this dataset, which comprises the actions of 25 individuals. Additionally, some security attacks of data such as web attack, DDoS, and several others are included [82].

6.7. CSE–CIC–IDS2018. This dataset could be used for the characteristics of agents or human operators for different network protocols when producing network traffic events. Nearly 16 million of records can be found in this dataset. Two types of profiles are used in this dataset namely "M" and "B." The M-profile outlines a security attack scenario for attacks, for instance, DDoS and brute force included in CSE–CIC–IDS2018. On the other hand, B-profiles summarize user behaviour for protocols including HTTP, HTTPS, and FTP. Several types of distribution are included in this dataset such as packet size distributions and request time distribution [24].

6.8. ToN-IoT. ToN-IoT includes telemetry data from connected devices, Linux and Windows operating system records, and industrial IoT network traffic, among other data sources acquired from the entire IIoT system. A medium-scale IoT network supplied a wide range of information. The UNSW Canberra IoT Labs and the Cyber Range collaborated to create ToN-IoT. The network ToN-IoT dataset is available in the ToN-IoT repository [83]. Furthermore, ToN-IoT datasets were represented in CSV format with a labelled column indicating attack or normal behaviour and a subcategory attack type, which indicates the various types of attacks, such as DoS, DDoS, data injection, ransomware, password attack, backdoor, cross-site scripting (XSS), scanning, and MITM attack. These attacks were launched and targeted various IoT and industrial IoT sensors.

7. Research Gap and Future Direction

From the papers [84–88], it can be concluded that a majority of existing research and development on intrusion detection adopted the centralized model training approach which require transferring a large chunk of data from several end devices to a central server. However, it causes serious issues in terms of security and privacy. Even in circumstances in which all the necessary data is readily accessible, relying on a centralized dataset for the purposes of maintenance and retraining may be an expensive and time-consuming endeavour. Furthermore, the cloud-centric approaches have the challenges of delays due to data propagation leading to latency which make it unsuitable for real-world deployment. In practice, the data comes from sources located away from the cloud in state-of-the-art systems, and a growing number of researchers are directed to exploring solutions exploiting mobile edge computing (MEC) architecture. It is developed on top of the intrinsic storage and computing capabilities of end nodes and edge servers. A similar mechanism can be developed for intrusion detection to improve the robustness of the model applied to identify the anomalies in the network. Even with centralized setup, some of the challenges are the following:

(i) In actual environment, ML model training with labelled dataset may have a low performance which will risk the security of network

(ii) The existing research uses the data cleaning mechanism and employs complicated model which leads to low efficiency in real deployment

8. Conclusion

Detecting and responding to intrusions is a critical component of computer security measures. In this work, classification of IDS has been discussed and highlighted based on architecture, detection methods, decision-making, and locality. Several machine learning-based IDS schemes are discussed. A detailed description of deep learning models along with its types is presented. Additionally, publicly available datasets are discussed for carrying out any IDS-based research. It is evident from the literate that an IDS plays an important role in detecting different types of attacks and securing networks/systems. However, two problems have been identified in this survey: (i) efficiency and (ii) performance. Most of the existing research is around few available datasets, and one can conclude that with the ever-improving AI-based models, the networks are more prone to cyberattack. Therefore, the datasets are needed to be upgraded to meet the modern-day requirements.

Conflicts of Interest

The authors declare no conflict of interest associated with this work.

References

[1] A. Thakkar and R. Lohiya, "A review on machine learning and deep learning perspectives of IDS for IoT: recent updates, security issues, and challenges," *Archives of Computational Methods in Engineering*, vol. 28, no. 4, pp. 3211–3243, 2021.

[2] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of Things: vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, 2012.

[3] Z. K. Maseer, R. Yusof, N. Bahaman, S. A. Mostafa, and C. F. M. Foozy, "Benchmarking of machine learning for anomaly-based intrusion detection systems in the CICIDS2017 dataset," *IEEE Access*, vol. 9, pp. 22351–22370, 2021.

[4] Akashdeep, I. Manzoor, and N. Kumar, "A feature reduced intrusion detection system using ANN classifier," *Expert Systems with Applications*, vol. 88, pp. 249–257, 2017.

[5] R. Patgiri, U. Varshney, T. Akutota, and R. Kunde, "An investigation on intrusion detection system using machine learning," in *2018 IEEE Symposium Series on Computational Intelligence (SSCI)*, pp. 1684–1691, Bangalore, India, November 2018.

[6] M. Ahmed, A. N. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," *Journal of Network and Computer Applications*, vol. 60, pp. 19–31, 2016.

[7] A. L. Buczak and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016.

[8] Y. Rbah, M. Mahfoudi, Y. Balboul et al., "Machine learning and deep learning methods for intrusion detection systems in IoMT: a survey," in *2022 2nd International Conference on Innovative Research in Applied Science, Engineering and Technology (IRASET)*, pp. 1–9, Meknes, Morocco, March 2022.

[9] K. Albulayhi, A. A. Smadi, F. T. Sheldon, and R. K. Abercrombie, "IoT intrusion detection taxonomy, reference architecture, and analyses," *Sensors*, vol. 21, no. 19, p. 6432, 2021.

[10] A. Das and S. G. Balakrishnan, "A comparative analysis of deep learning approaches in intrusion detection system," in *2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT)*, pp. 555–562, Bangalore, India, August 2021.

[11] C. Sekhar, K. Pavani, and M. S. Rao, "Comparative analysis on intrusion detection system through ML and DL techniques: survey," in *2021 International Conference on Computational*

Intelligence and Computing Applications (ICCICA), pp. 1–5, Nagpur, India, November 2021.

[12] A. Arqane, O. Boutkhoum, H. Boukhriss, and A. El Moutaouakkil, “A review of intrusion detection systems: datasets and machine learning methods,” in *NISS2021: Proceedings of the 4th International Conference on Networking, Information Systems & Security*, pp. 1–6, Kenitra, Morocco, April 2021.

[13] V. Hnamte and J. Hussain, “An extensive survey on intrusion detection systems: datasets and challenges for modern scenario,” in *2021 3rd International Conference on Electrical, Control and Instrumentation Engineering (ICECIE)*, pp. 1–10, Kuala Lumpur, Malaysia, November 2021.

[14] S. Mirlekar and K. P. Kanojia, “A comprehensive study on machine learning algorithms for intrusion detection system,” in *2022 10th International Conference on Emerging Trends in Engineering and Technology - Signal and Information Processing (ICETET-SIP-22)*, pp. 01–06, Nagpur, India, April 2022.

[15] O. M. Surakhi, A. M. Garcia, M. Jamoos, and M. Y. Alkhanafseh, “A comprehensive survey for machine learning and deep learning applications for detecting intrusion detection,” in *2021 22nd International Arab Conference on Information Technology (ACIT)*, pp. 1–13, Muscat, Oman, December 2021.

[16] D. N. P. Suthishni and K. S. S. Kumar, “A review on machine learning based security approaches in intrusion detection system,” in *2022 9th International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 341–348, New Delhi, India, March 2022.

[17] A. Thakkar and R. Lohiya, “A survey on intrusion detection system: feature selection, model, performance measures, application perspective, challenges, and future research directions,” *Artificial Intelligence Review*, vol. 55, no. 1, pp. 453–563, 2022.

[18] M. Bijone, “A survey on secure network: intrusion detection & prevention approaches,” *American Journal of Information Systems*, vol. 4, no. 3, pp. 69–88, 2016.

[19] M. B. J. Dangra, *A Survey of Signature Based & Statistical Based Intrusion Detection Techniques*.

[20] G. Meena and R. R. Choudhary, “A review paper on IDS classification using KDD 99 and NSL KDD dataset in WEKA,” in *2017 International Conference on Computer, Communications and Electronics (Comptelix)*, pp. 553–558, Jaipur, India, July 2017.

[21] S. Jose, D. Malathi, B. Reddy, and D. Jayaseeli, “A survey on anomaly based host intrusion detection system,” *Journal of Physics: Conference Series*, vol. 1000, no. 1, p. 012049, 2018.

[22] A. Khraisat, I. Gondal, P. Vamplew, and J. Kamruzzaman, “Survey of intrusion detection systems: techniques, datasets and challenges,” *Cybersecurity*, vol. 2, no. 1, p. 20, 2019.

[23] Y. Yu, X. Si, C. Hu, and J. Zhang, “A review of recurrent neural networks: LSTM cells and network architectures,” *Neural Computation*, vol. 31, no. 7, pp. 1235–1270, 2019.

[24] J. L. Leevy and T. M. Khoshgoftaar, “A survey and analysis of intrusion detection models based on cse-cic-ids2018 big data,” *Journal of Big Data*, vol. 7, no. 1, p. 104, 2020.

[25] S.-W. Lee, H. M. Sidqi, M. Mohammadi et al., “Towards secure intrusion detection systems using deep learning techniques: comprehensive analysis and review,” *Journal of Network and Computer Applications*, vol. 187, article 103111, 2021.

[26] P. Kumar, R. Kumar, G. P. Gupta, and R. Tripathi, “A distributed framework for detecting DDoS attacks in smart contract-based blockchain-IoT systems by leveraging fog computing,” *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 6, article e4112, 2021.

[27] R. K. Das, J. Yang, and H. Li, “Data augmentation with signal companding for detection of logical access attacks,” in *ICASSP 2021 - 2021 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, pp. 6349–6353, Toronto, ON, Canada, June 2021.

[28] P. Kumar, G. P. Gupta, and R. Tripathi, “TP2SF: a trustworthy privacy-preserving secured framework for sustainable smart cities by leveraging blockchain and machine learning,” *Journal of Systems Architecture*, vol. 115, article 101954, 2021.

[29] D. Kandris, C. Nakas, D. Vomvas, and G. Koulouras, “Applications of wireless sensor networks: an up-to-date survey,” *Applied System Innovation*, vol. 3, no. 1, p. 14, 2020.

[30] O. I. Khalaf, F. Ajesh, A. A. Hamad, G. N. Nguyen, and D. N. Le, “Efficient dual-cooperative bait detection scheme for collaborative attackers on mobile ad-hoc networks,” *IEEE Access*, vol. 8, pp. 227962–227969, 2020.

[31] R. A. Prakash, W. R. S. Jeyaseelan, and T. Jayasankar, “Detection, prevention and mitigation of wormhole attack in wireless adhoc network by coordinator,” *Applied Mathematics & Information Sciences*, vol. 12, no. 1, pp. 233–237, 2018.

[32] Z. Yu and J. J. P. Tsai, “A framework of machine learning based intrusion detection for wireless sensor networks,” in *2008 IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (sutc 2008)*, pp. 272–279, Taichung, Taiwan, June 2008.

[33] L. Litty, *Hypervisor-Based Intrusion Detection*, University of Toronto, 2005.

[34] G. Zhao, J. Song, and J. Song, “Analysis about performance of multiclass SVM applying in IDS,” in *Proceedings of the 2013 International Conference on Information, Business and Education Technology (ICIBET-2013)*, Beijing, China, March 2013.

[35] R. U. Khan, X. Zhang, M. Alazab, and R. Kumar, “An improved convolutional neural network model for intrusion detection in networks,” in *2019 Cybersecurity and Cyberforensics Conference (CCC)*, pp. 74–77, Melbourne, VIC, Australia, May 2019.

[36] Y. Yi, J. Wu, and W. Xu, “Incremental SVM based on reserved set for network intrusion detection,” *Expert Systems with Applications*, vol. 38, no. 6, pp. 7698–7707, 2011.

[37] J. Song, H. Takakura, Y. Okabe, and K. Nakao, “Toward a more practical unsupervised anomaly detection system,” *Information Sciences*, vol. 231, pp. 4–14, 2013.

[38] W. Hu, Y. Liao, and V. R. Vemuri, “Robust support vector machines for anomaly detection in computer security,” in *ICMLA*, pp. 168–174, Los Angeles, California, June 2003.

[39] S. Thakare, P. Ingle, and B. B. Meshram, “IDS: intrusion detection system the survey of information security,” *International Journal of Emerging Technology and Advanced Engineering*, vol. 2, no. 8, pp. 86–90, 2012.

[40] E. A. Shams, A. Rizaner, and A. H. Ulusoy, “Trust aware support vector machine intrusion detection and prevention system in vehicular ad hoc networks,” *Computers & Security*, vol. 78, pp. 245–254, 2018.

[41] H. A. Kholidy, A. Erradi, S. Abdelwahed, and F. Baiardi, “HA-CIDS: a hierarchical and autonomous IDS for cloud systems,” in *2013 Fifth international conference on computational intelligence, Communication Systems and Networks*, pp. 179–184, Madrid, Spain, June 2013.

[42] E. Vasilomanolakis, S. Karuppayah, M. Mühlhäuser, and M. Fischer, "Taxonomy and survey of collaborative intrusion detection," *ACM Computing Surveys*, vol. 47, no. 4, pp. 1–33, 2015.

[43] S. N. Kumar, "DecenCrypto cloud: decentralized cryptography technique for secure communication over the clouds," *Journal of Computer Sciences and Applications*, vol. 3, no. 3, pp. 73–78, 2015.

[44] S. N. Kumar, "Review on network security and cryptography," *International Transaction of Electrical and Computer Engineers System*, vol. 3, no. 1, pp. 1–11, 2015.

[45] Z. Muda, W. Yassin, M. N. Sulaiman, and N. I. Udzir, "Intrusion detection based on K-means clustering and Naïve Bayes classification," in *2011 7th International Conference on Information Technology in Asia*, pp. 1–6, Sarawak, Malaysia, July 2011.

[46] R. R. Devi and M. Abualkibash, "Intrusion detection system classification using different machine learning algorithms on KDD-99 and NSL-KDD datasets - a review paper," *International Journal of Computer Science & Information Technolog y (IJCSIT)*, vol. 11, no. 3, pp. 65–80, 2019.

[47] W. He, B. Ruhani, D. Toghraie et al., "Using of artificial neural networks (ANNs) to predict the thermal conductivity of zinc oxide–silver (50%–50%)/water hybrid Newtonian nanofluid," *International Communications in Heat and Mass Transfer*, vol. 116, article 104645, 2020.

[48] I. H. Sarker, "Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective," *SN Computer Science*, vol. 2, no. 3, p. 154, 2021.

[49] J. Karhunen, T. Raiko, and K. H. Cho, "Chapter 7 - Unsupervised deep learning: a short review," in *Advances in Independent Component Analysis and Learning Machines*, pp. 125–142, Academic Press, 2015.

[50] S. Albawi, T. A. Mohammed, and S. Al-Zawi, "Understanding of a convolutional neural network," in *2017 International Conference on Engineering and Technology (ICET)*, pp. 1–6, Antalya, Turkey, August 2017.

[51] M. A. Keyvanrad and M. M. Homayounpour, "A brief survey on deep belief networks and introducing a new object oriented toolbox (DeeBNet)," 2014, https://arxiv.org/abs/1408.3264.

[52] X. Peng, L. Wang, X. Wang, and Y. Qiao, "Bag of visual words and fusion methods for action recognition: comprehensive study and good practice," *Computer Vision and Image Understanding*, vol. 150, pp. 109–125, 2016.

[53] W. Nie, A. Liu, W. Li, and Y. Su, "Cross-view action recognition by cross-domain learning," *Image and Vision Computing*, vol. 55, pp. 109–118, 2016.

[54] A. Aggarwal, M. Mittal, and G. Battineni, "Generative adversarial network: an overview of theory and applications," *International Journal of Information Management Data Insights*, vol. 1, no. 1, article 100004, 2021.

[55] H.-T. Chiang, Y.-Y. Hsieh, S.-W. Fu, K.-H. Hung, Y. Tsao, and S.-Y. Chien, "Noise reduction in ECG signals using fully convolutional denoising autoencoders," *IEEE Access*, vol. 7, pp. 60806–60813, 2019.

[56] F. A. Khan, A. Gumaei, A. Derhab, and A. Hussain, "TSDL: A two-stage deep learning model for efficient network intrusion detection," *IEEE Access*, vol. 7, pp. 30373–30385, 2019.

[57] A. Ashfahani, M. Pratama, E. Lughofer, and Y. S. Ong, "DEVDAN: deep evolving denoising autoencoder," *Neurocomputing*, vol. 390, pp. 297–314, 2020.

[58] D. Preethi and N. Khare, "Sparse auto encoder driven support vector regression based deep learning model for predicting network intrusions," *Peer-to-Peer Networking and Applications*, vol. 14, no. 4, pp. 2419–2429, 2021.

[59] M. Z. Alom and T. M. Taha, "Network intrusion detection for cyber security using unsupervised deep learning approaches," in *2017 IEEE National Aerospace and Electronics Conference (NAECON)*, pp. 63–69, Dayton, OH, USA, June 2017.

[60] W. C. Lin, S. W. Ke, and C. F. Tsai, "CANN: an intrusion detection system based on combining cluster centers and nearest neighbors," *Knowledge-Based Systems*, vol. 78, pp. 13–21, 2015.

[61] B. W. Masduki, K. Ramli, F. A. Saputra, and D. Sugiarto, "Study on implementation of machine learning methods combination for improving attacks detection accuracy on intrusion detection system (IDS)," in *2015 International Conference on Quality in Research (QiR)*, pp. 56–64, Lombok, Indonesia, August 2015.

[62] E. Hodo, X. Bellekens, A. Hamilton et al., "Threat analysis of IoT networks using artificial neural network intrusion detection system," in *2016 International Symposium on Networks, Computers and Communications (ISNCC)*, pp. 1–6, Yasmine Hammamet, Tunisia, May 2016.

[63] P. Nskh, M. N. Varma, and R. R. Naik, "Principle component analysis based intrusion detection system using support vector machine," in *2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)*, pp. 1344–1350, Bangalore, India, May 2016.

[64] B. Xu, S. Chen, H. Zhang, and T. Wu, "Incremental k-NN SVM method in intrusion detection," in *2017 8th IEEE International Conference on Software Engineering and Service Science (ICSESS)*, pp. 712–717, Beijing, China, November 2017.

[65] C. Yin, Y. Zhu, J. Fei, and X. He, "A deep learning approach for intrusion detection using recurrent neural networks," *IEEE Access*, vol. 5, pp. 21954–21961, 2017.

[66] M. AL-Hawawreh, N. Moustafa, and E. Sitnikova, "Identification of malicious activities in industrial Internet of Things based on deep learning models," *Journal of Information Security and Applications*, vol. 41, pp. 1–11, 2018.

[67] T. A. Tang, L. Mhamdi, D. McLernon, S. A. R. Zaidi, and M. Ghogho, "Deep recurrent neural network for intrusion detection in sdn-based networks," in *2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft)*, pp. 202–206, Montreal, QC, Canada, June 2018.

[68] C. Xu, J. Shen, X. Du, and F. Zhang, "An intrusion detection system using a deep neural network with gated recurrent units," *IEEE Access*, vol. 6, pp. 48697–48707, 2018.

[69] T. T. H. Le, Y. Kim, and H. Kim, "Network intrusion detection based on novel feature selection model and various recurrent neural networks," *Applied Sciences*, vol. 9, no. 7, p. 1392, 2019.

[70] Y. Yang, K. Zheng, C. Wu, and Y. Yang, "Improving the classification effectiveness of intrusion detection by using improved conditional variational autoencoder and deep neural network," *Sensors*, vol. 19, no. 11, p. 2528, 2019.

[71] C. Tang, N. Luktarhan, and Y. Zhao, "SAAE-DNN: deep learning method on intrusion detection," *Symmetry*, vol. 12, no. 10, p. 1695, 2020.

[72] M. H. Shahriar, N. I. Haque, M. A. Rahman, and M. Alonso, "G-ids: generative adversarial networks assisted intrusion detection system," in *2020 IEEE 44th Annual Computers,*

Software, and Applications Conference (COMPSAC), pp. 376–385, Madrid, Spain, July 2020.

[73] T. Su, H. Sun, J. Zhu, S. Wang, and Y. Li, "BAT: deep learning methods on network intrusion detection using NSL-KDD dataset," *IEEE Access*, vol. 8, pp. 29575–29585, 2020.

[74] C. Ieracitano, A. Adeel, F. C. Morabito, and A. Hussain, "A novel statistical analysis and autoencoder driven intelligent intrusion detection approach," *Neurocomputing*, vol. 387, pp. 51–62, 2020.

[75] G. Andresini, A. Appice, and D. Malerba, "Nearest cluster-based intrusion detection through convolutional neural networks," *Knowledge-Based Systems*, vol. 216, article 106798, 2021.

[76] R. V. Mendonca, A. A. M. Teodoro, R. L. Rosa et al., "Intrusion detection system based on fast hierarchical deep convolutional neural network," *IEEE Access*, vol. 9, pp. 61024–61034, 2021.

[77] S. Al and M. Dener, "STL-HDL: a new hybrid network intrusion detection system for imbalanced dataset on big data environment," *Computers & Security*, vol. 110, article 102435, 2021.

[78] Z. Wang, Y. Zeng, Y. Liu, and D. Li, "Deep belief network integrating improved kernel-based extreme learning machine for network intrusion detection," *IEEE Access*, vol. 9, pp. 16062–16091, 2021.

[79] A. Yazdinejadna, R. M. Parizi, A. Dehghantanha, and M. S. Khan, "A kangaroo-based intrusion detection system on software-defined networks," *Computer Networks*, vol. 184, article 107688, 2021.

[80] A. Verma and V. Ranga, "Statistical analysis of CIDDS-001 dataset for network intrusion detection systems using distance-based machine learning," *Procedia Computer Science*, vol. 125, pp. 709–716, 2018.

[81] V. Kumar, A. K. Das, and D. Sinha, "Statistical analysis of the UNSW-NB15 dataset for intrusion detection," in *Computational Intelligence in Pattern Recognition*, pp. 279–294, Springer, Singapore, 2020.

[82] I. Sharafaldin, A. H. Lashkari, and A. A. Ghorbani, "A detailed analysis of the cicids2017 data set," in *International Conference on Information Systems Security and Privacy*, pp. 172–188, Springer, Cham, 2018.

[83] N. Moustafa, "A new distributed architecture for evaluating AI-based security systems at the edge: network TON_IoT datasets," *Sustainable Cities and Society*, vol. 72, article 102994, 2021.

[84] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, "Network intrusion detection system: a systematic study of machine learning and deep learning approaches," *Transactions on Emerging Telecommunications Technologies*, vol. 32, no. 1, article e4150, 2021.

[85] A. Drewek-Ossowicka, M. Pietrołaj, and J. Rumiński, "A survey of neural networks usage for intrusion detection systems," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 497–514, 2021.

[86] A. Aldweesh, A. Derhab, and A. Z. Emam, "Deep learning approaches for anomaly-based intrusion detection systems: a survey, taxonomy, and open issues," *Knowledge-Based Systems*, vol. 189, article 105124, 2020.

[87] S. U. Jan, S. Ahmed, V. Shakhov, and I. Koo, "Toward a lightweight intrusion detection system for the Internet of Things," *IEEE Access*, vol. 7, pp. 42450–42471, 2019.

[88] M. A. Khan, M. A. Khan, S. U. Jan et al., "A deep learning-based intrusion detection system for mqtt enabled iot," *Sensors*, vol. 21, no. 21, p. 7016, 2021.