EASR

Engineering and Applied Science Research

https://www.tci-thaijo.org/index.php/easr/index

Published by the Faculty of Engineering, Khon Kaen University, Thailand

Intrusion detection system and mitigation of threats in IoT networks using AI techniques: A review

Geo Francis E* and S. Sheeja

Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India

Received 8 December 2022
Revised 5 October 2023
Accepted 16 October 2023

Abstract

In recent times, IoT has been used in a wide range of applications for improving the quality of life. Conversely, IoT turns out to be progressively a superlative target for malicious attacks due to its huge range of openness, distributed nature, and objects. However, for maintaining IoT system security, there is a need for an effective Intrusion detection system (IDS), standing as a fundamental tool in the cyber security environment, which implements a detector that uninterruptedly observes the network traffic. Therefore, the network requires an efficient IDS system for detecting various attacks. Various IDS systems have been implemented for detecting intrusion in the IoT network; however, it is required to have a review of recent developments. The present study, therefore, reviews a range of existing IDS models that are employed in IoT networks for detecting intrusion along with recent threats. Various datasets employed in IDS and the challenges faced by IDS are also explored in this study. This study is implemented with a futuristic vision to improve the existing IDSs competent enough to face the latest attacks and threats in IoT Networks.

Keywords: Intrusion detection, Internet of Things, Threats, Prevention of attacks, IDS

1. Introduction

The Internet of Things (IoT) environment plays a significant role in real-life smart approaches such as smart homes, cities, and healthcare. The huge scale and ubiquitous IoT environment have introduced novel security challenges. Moreover, since IoT devices typically function in an unattended background, hackers may physically access these devices with malicious determination [1]. Likewise, as IoT systems are connected generally to wireless networks, eavesdropping can be employed to access private information from the communication channel. Furthermore, IoT devices can't afford advanced security features due to their limited computation resources and restricted energy. Based on interdependent and interconnected IoT settings, new attack planes are being developed very frequently. Hence, the IoT environment is more susceptible compared to conventional computing methods. This necessitates research in particular preventive and detective systems for the IoT environment to protect it from various threats. An intrusion detection system (IDS), therefore, is developed as a defensive mechanism for protecting the IoT environment from various threats as illustrated in Figure 1 [1].

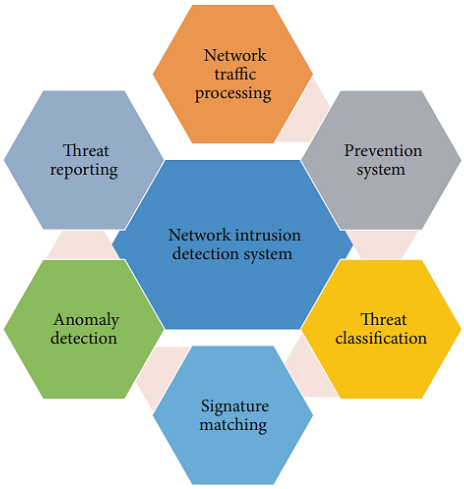

Figure 1 Applications of Intrusion Detection System [2]

*Corresponding author.
Email address: edakulathur@hotmail.com
doi: 10.14456/easr.2023.66

As the growth of IoT technology has grown increasingly high, IoT is used in different applications for different purposes. However, there is no standard defined architecture of work that is strictly adhered to across the board. Nevertheless, 4 layer architecture design is used widely and is the most accepted form in general. Figure 2 shows the different layer architecture of IoT.

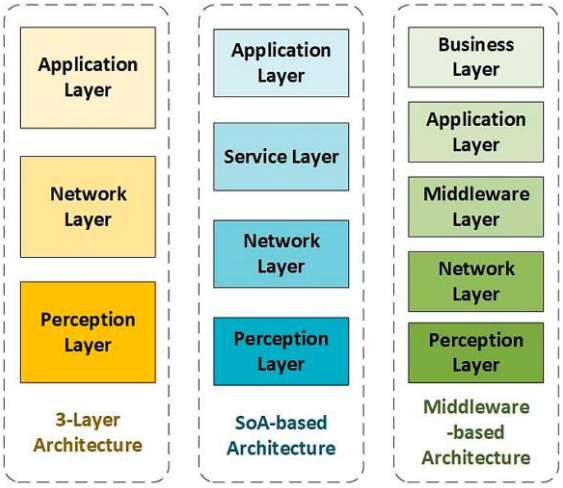

Figure 2 IoT Architecture [3]

Perception layer

The perception layer is the first layer of the IoT system and it consists of things or endpoint devices that serve as the channel between the digital and physical worlds [4]. The perception denotes the physical layer which comprises sensors and actuators which are capable of gathering, accepting and processing the data over the network. Sensors and actuators can be connected either using wired or wireless connections.

Network layer

The network layer of the IoT architecture is primarily responsible for delivering communication and connectivity between the devices in IoT systems [5]. It comprises of technologies and protocols which enable devices to connect and communicate with each other and with the wider internet. The network layer may comprise of gateways and router which acts as the intermediaries between the devices and the wider internet, and may also consist of security features like encryption and authentication to protect against unauthorized access. In addition, the network layer contains DAS (data acquiring system) and internet gateways. A DAS performs aggregation of data and conversion of functions. It is important to transmit and process the data gathered by the sensor devices, which can be attained by using a network layer [6]. This layer permits these devices to connect and communicate with other servers, smart devices and other network devices and aids in better transmission of data for the devices.

Pre-processing layer/Service layer

The processing layer in the IoT architecture refers to the software and hardware components that are responsible for collecting, analyzing and interpreting the data from the IoT devices [7]. This layer is responsible for receiving the raw data from the devices and then processes it by constructing it accessible for further inquiry or action. The data pre-processing layer consist of different tools and technologies which aid in data management system and analytic platforms. Tools are utilized for extracting meaningful insights from the data and make decision based on that data.

Application layer

Application layer serves as the user-facing layer of IoT solutions which includes smartphone app for controlling the IoT devices in the smart homes [8]. Application layer delivers the solutions like analytics, reporting and device control to the end users. Application layer comprises of different software and applications which include web portals, mobile apps and other UI design which are designed to interact with underlying infrastructure of IoT [9]. Further application layer includes data visualization tools and other advanced analytical capabilities.

Like the existing 4 layers, fog layer is also employed in IoT for several purposes. Fog layer comprises of different devices such as gateway, access points, base stations, routers and specific fog servers termed as fog nodes, which offer connectivity and storage services [10]. As attacks can cause various problems such as transmission of information or theft of information present in the network, it is important to detect the attacks and eliminate them. Hence, fog layer has been used for detection of attacks in the cloud server for IoT devices. Fog layer based approach for detecting the malicious nodes in the IoT network is employed on ommnet++ simulator [11].

Anomaly based approaches are used to detect cyberattacks that model the expected character of IoT devices to detect occurrences of attacks. A distributed and lightweight IDS integrating Multi-layer Perceptron (MLP) and autoencoder, are used to provide accurate and efficient intrusion detection. This type of IDS operates on two-layered fog architecture, an attack identification module within cloud and anomaly detector within fog node. It is able to characterize the actual behaviour within fog nodes and identify several attack types with better detection rate [12].

The memory and computational limitations are considered as the emerging vulnerabilities in IoT run environments. The lack of safer architecture in IoT system is the significant barrier in developing security. So, the AI4SAFE-IoT [13] is applied for secure

architecture for IoT edge layer infrastructure. This is developed on AI-powered security at edge layers for securing IoT organization. It tends to interpret attributes of stages of an attack cycle based on Cyber Kill Chain model. Each threat in edge layer is handled by its corresponding security module due to the combination of AI security modules in different layers of AI4SAFE-IoT.

1.1 IoT Protocols

The MQTT, which is a widely used publish-subscribe based IoT protocol is applied in communication of sensor data. The DNN in MQTT based protocol is used for intrusion detection in IoT. In MQTT, three abstract level features like Bi-flow, Uni-flow and Packet-flow are involved in protecting IoT nodes against intrusions and attacks. The input layers of DNN considers the features of MQTT protocol based network [14].

The intrusion detection in smart devices for home automation is performed by using a controller which is responsible for action of actuators according to data extracted from sensors. In order to get a representative home automation network, Z-stick Gen5 and Z-Wave USB stick is plugged and thus the controller is able to manage Z-wave actuators and sensors. The Z-wave device is capable of monitoring vibration, humidity, light, temperature, and motion of devices in IoT network. By using z-wave commands, the switches can be turned on or off and energy consumption of electrical outlet is monitored [15].

IDS is a software (or) tool, which may defend (or) secure the network (or) system from intrusions. The purpose of IDS is to detect various attacks and system usages, which can't be determined through firewalls. Often, this is very significant for achieving protection versus action at the high range that compromises the integrity, availability (or) confidentiality of the network [16]. IDS for monitoring the network traffic with an issue and suspicious activities alerts when it detects such activities. Some IDS can perform actions such as blocking the traffic sender if it detects any anomalous traffic like a suspicious IP address. IDS is also classified based on their location such as Network IDS (NIDS) and Host IDS (HIDS). HIDS analyses and monitors the host activities, system calls, application logs, and modifications that occur in system files for identifying the intrusion such as login over un-privileged data. However, the NIDS monitors the network traffic by employing techniques like packet-sniffing for collecting traffic over the network and to detect the attacks like port scans and DoS [17].

There are two kinds of NIDS such as pattern matching IDS and statistical anomaly IDS. IDS is practically classified, further, as anomaly-based IDS and signature-based IDS. To detect zero-day attacks, anomaly-based IDS is used. Effective and efficient IDS design mainly depends on the selection of appropriate approaches such as the deep learning (DL) (or) machine learning (ML) approach along with the feature selection methods in the range of improving the system performance and reducing computation. This paper, therefore, reviews various IDS methods and their limitations for effective improvement.

The main objectives of the proposed study are:

- To explore recent studies that are employed in IDS,
- To examine recent threats and risk factors that affect the IDS security range
- To find the challenges that are faced in the efficient implementation of IDS.

1.2 Paper organization

In section 1, a brief introduction to the present study is given with objectives and in section 2, recent studies in IoT intrusion detection system is discussed. Following this, in section 3, various attacks on the IoT environment are listed and explained and then the cause and risk factors of recent cyber security threats are elaborated in section 4. Various datasets that are employed in IDS are explained in section 5. In section 6, prevention and control techniques employed for intrusion detection are explored. The challenges faced in implementing an effective IDS are deliberated in section 7 and then the paper is concluded with the future direction in section 8.

2. Survey methodology

Survey methodology was accomplished through Google scholar. The terms which were used for fetching the information includes 'Attacks in IoT', 'Threats caused by attacks in IoT network', 'datasets employed in IDS', 'Prevention of attacks in IoT'. In the introductory stages, the studies were opted on the basis of different criteria such as title related to the study. Consequently, screening of abstract was done and when suitable, the general script is also reflected. Further citations of the papers were evaluated and included as required with a total of 66 distinguished studies which matches. Figure 3 shows the survey methodology of the paper.

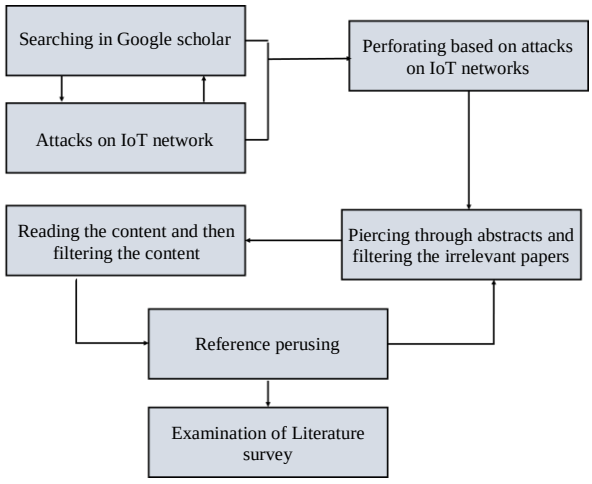

Figure 3 Survey methodology

3. Recent studies in IoT Intrusion Detection System (IDS)

In the recent past, various methods are implemented for detecting intrusion in the IoT environment. The IoT network is built-up with billions of physical devices that are connected to the internet through networks, which perform with less intervention from a human. In this section, therefore, recent studies employed from the year 2021 in IoT intrusion detection systems are reviewed. The detection and blocking of attacks by using IDS in IoT network is depicted in Figure 4.

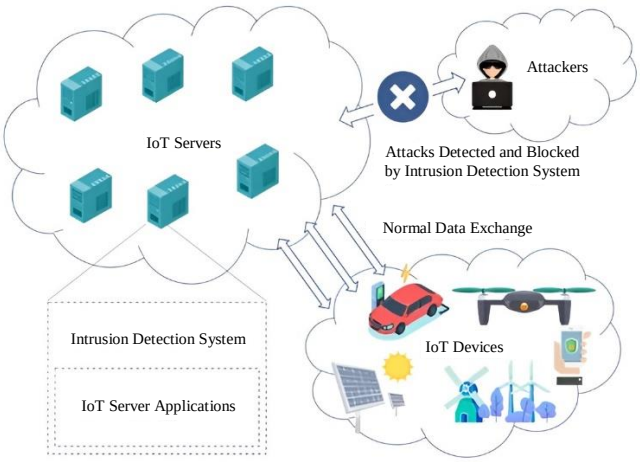

Figure 4 Representation of IDS in IoT Network [18]

The federated learning (FL) based intrusion detection system (IDS) is proposed by Mothukuri et al. [19], which proactively recognizes the intrusion over the IoT environment with the support of decentralized on-device data. Along with this, it uses federated training sequences over GRUs- Gated recurrent units system and maintains the data integral over local IoT networks through sharing merely the learned weights with the FL central server. Ensemble portion of this system groups information from various resources for optimizing the accuracy of the global machine learning (ML) system. Similarly, a novel IDS is instigated with the baptized BotIDS [20] grounded over Deep convolutional neural networks (Deep-CNN). The system is designed, employed, and tested IDS against the well-defined attack named Botnet with a specific dataset entitled Bot-IoT.

In a similar context, an intelligent and novel IDS called the APAE model [21] is employed with the support of an asymmetric parallel auto-encoder and is competent to sense various attacks in IoT systems. APAE's encoder portion possesses a lightweight frame that in parallel comprises two encoders, which individually result in three succeeding convolutional filter layers. The decoder portion of APAE varies from its encoder portion and possesses eight successive convolution layer transpose. The designed APAE has a lightweight and suitable frame for real-time attack recognition and grades very good simplification enactment even after training, utilizing constrained training records. Generally, IoT networks communicated through machine-to-machine protocols like Message Queuing Telemetry Transport (MQTT) [22]. In terms of the IoT heterogeneous structure and the security absence through design methods, the security device in IoT with MQTT intrusion is required and it can be positioned as IDS. In that terms, Deep learning (DL) grounded IDS network is trained with a public dataset that contains MQTT attacks.

At present, inadequate security procedures cause the IoT system as feeblest links for shielding the security attacks and thus stirring objects to various attackers [23]. Thus, a novel IDS approach is employed with powerful DL models. Motivated by the advantages of LSTM- long short term memory, Whale integrated LSTM System (WILS), the system project an enterprise intelligent IDS for detecting the threats in different circumstances over IoT environment [23]. Likewise, IDS based DL approach is designed to expose IoTDDoS Botnet intrusions. The dataset utilized in the system [24] is developed and designed within a real-time network surrounding the Cyber-Range Lab (CRL) of the UNSW Canberra Cyber Centre. Moreover, in the real industrial IoT network, the main factor that affects the DL-based IDS model is data imbalance [25]. Thus, it is explored that the IDS network is based on the data level. Three data-based schemes such as data augmentation over VAE – variational auto-encoder, a data balancing over conditional VAE, and data balancing over random under-sampling and conditional VAE are combined with the DL-based IDS network.

Consequently, for enhancing network security, [26] employed an end-to-end system for classification and detection of network attacks with the support of a DL-based recurrent device. The projected system extracts the hidden layer features from the recurrent systems and further utilizes KPCA- kernel-based principal component analysis feature selection methods for evaluating the optimal features. Then, the recurrent model's optimal features are fused along with classification performed with the ensemble meta-classifier. The novel IDS relies upon DL and ML methodologies for identifying the new intrusions, which failed to detect the existing system over the IoT network. The system performed features selection with the ReliefF algorithm. Intrusions and Cyber-attacks have become the main obstacles to the IIoT- Industrial Internet of Things adoption over critical industries [27].

The common problem of the IIoT network is the imbalance of data distribution, which affects the ML-based IDS. Thus, the EvolCostDeep model was introduced with a hybrid of SAE- stacked autoencoders and CNN- convolutional neural networks with a cost in need of loss function. A lightweight IDS-based DL and knowledge graph is introduced in [28]. Initially, the system extracts key features and semantic relationships through statistical analysis and a knowledge graph. Then, IoT system entreaties are transformed into word vectors with multi-view feature alignment and fusion. Finally, an attention-based CNN- Bi-LSTM system is introduced [28] for detecting malicious requests that can arrest long-distance dependency and contextual semantic evidence. Similarly, a lightweight IDS is proposed for improving the efficiency of IDS and reducing the attack detection execution time [29]. In a range of importance, the RF algorithm is used for ranking the features and the data dimension are reduced by selecting the top fifteen significant features. Then, DNN- deep neural network framework is utilized for classifying the anonymous traffic through analyzing TCP/IP packets over the dataset called NSL-KDD i.e., defined as network security laboratory-knowledge discovery. The study [30] introduced an effective IDS model with the support of Competitive Swarm Henry Optimization (CSHO) based Deep Maxout network for finding the attacks

on IoT network. After recent studies in IoT intrusion detection systems, various attacks that are directed toward distributing IoT networks are deliberated.

The effective use of IDS and ML is considered as a key to manage with improving cybersecurity attacks by using efficient and effective process in IoT network. Mostly, the ML enabled IoT systems uses centralised methods in which the IoT devices tends to share the data's to datacenters for further analysis. The FL (Federated Learning) approach enabled IDS for IoT [31] system is used in several sectors such as transportation and healthcare sectors. The FL based IDS technique with multi-class classifier is used in detection of various attacks in IoT.

The IDS system tends to track and examine network traffic from several sources and thus identifies malicious actions. Security has to be developed and incorporated in each layer of IoT system. Based on the detection approaches, the IDS technique in IoT is classified as specified-based, anomaly-based, signature-based and hybrid [32].

4. Various attacks on IoT environment

The dynamic and distributed nature of IoT system produces weak communication channels that are used by hazardous objects in order to exploit and open new threats. The cyber security attacks that cause serious effects on the IoT environment are summarised. The Figure 5, denotes the various security attacks in IoT system and some of the attacks are deliberated in this section.

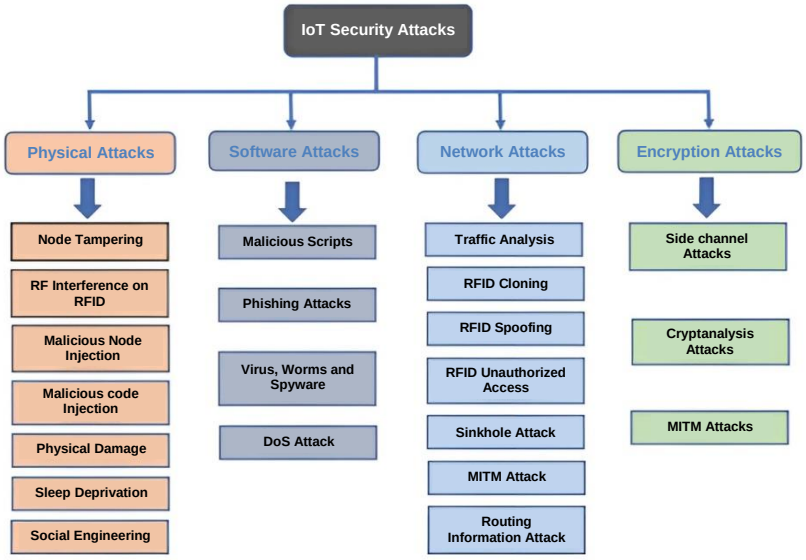

Figure 5 Common Security Attacks in IoT Network [33]

4.1 Physical attacks

Physical Attacks are a kind of cryptanalysis (or) the evolution of system information in the range of discovering the devices' hidden aspects and employing their properties [34]. This attack takes place when the IoT system can be accessed physically. The majority of cyber security attacks take place within the company; therefore, it is necessary to ensure the safety of the area where IoT devices are located, which is not an option always [35]. Cyber security attacks are performed through physical means where an attacker injects a USB drive for spreading malicious code. It is highly important; therefore, to have AI-based security measures for ensuring the protection of data and devices.

4.2 Encryption attacks

If the IoT network is not protected, an attacker may sense it and capture the data for later use. In addition to this, "once critical components such as encryption key are found, attackers could deploy their malicious scripts and take control over the system". For this particular reason, encryption over IoT networks is needed and it is determined to be the part of the cyber security effort.

4.3 Denial of Service (DoS)

DoS is an attack intended to shut down a network (or) machine, setting it inaccessible to envisaged users. This attack is accomplished by flooding the target with traffic (or) sending information that triggers a crash over the network. When a service like a website becomes unavailable, a DoS attack will take place. Through a botnet, a large range of systems targets one system that forces various devices for requesting a service simultaneously. More than aiming at capturing the data, in this scenario, attackers are seriously trying to cause an impact on the business, by making the service unavailable.

4.4 Ransom-ware

Ransomware is a kind of malware, which encrypts the files and locks down file access. Then, the attacker will demand money to provide the file key to recover the data, so that the user can retrieve the file. Generally, this kind of attack causes an effect on day-to-day business, and the encryption key frequently arises at a heavy amount.

4.5 Privilege escalation

In this, hackers will look for an IoT device's weakness and bugs in the range of gaining access to the resources, which are generally protected through user profile (or) with an application. Typically, hackers seek to steal confidential data (or) deploy malware (or) employ their newly gained privileges.

4.6 Firmware hijacking

A firmware attack is a type of malicious code, employed in the network (or) device through a backdoor over the processors' software. Backdoors were the code paths that permit certain individuals to bypass security and enter the system. Therefore, the firmware of the IoT network needs to be kept updated to avoid cyber security risks. Updates also need to be done from safe and reliable sources or else the attackers may take control of the device. The important thing in protecting from third-party attacks is that most hardware manufacturers will not encrypt the embedded firmware cryptographically.

4.7 Botnets

During the botnet attack, the IoT system will be controlled by remote bots. This is referred to as Mirai. Generally, it possesses the ability to utilize smart, connected devices for transferring private data and sensitive data that can be sold to other bidders found on the internet. At present, Mirai continues to be a huge challenge, and millions of IoT systems are affected by this problem.

4.8 Man-in-the-Middle

In a Man-in-the-Middle attack, an attacker breaks communication between two systems and intercepts the communication between them secretly, and the system makes the receiver think that they are receiving legitimate messages. These attacks, generally communicate with both the target parties and hence it is named man-in-the-middle. For example, it may look like an email (or) a message from the bank that requests to log in and give instructions to make an action. Now the fake website of attackers gathers the victim's credentials and thus can cause further destruction.

4.9 Eavesdropping

In eavesdropping, an attacker bypasses the network traffic operating in a range to steal sensitive information through a weak connection between the server and IoT device. Generally, it performs through listening to the analog or digital voice communication (or) through sniffed data interception. Again, in this scenario, the attacker escapes with corporate and sensitive data.

4.10 Brute force password attack

In a brute force password attack, various passphrases (or) passwords will be submitted by the hackers, waiting for the luck to get it done and once it is over, it gives to authorize the IoT devices. They even use applications for generating a huge assortment of repeated guesses. Now, hackers will access the IoT devices and install malware (or) steal the data.
Some real world cyber attacks that affected millions of people are shown as follows [36],

- A largest breach since 2009 on RockYou website was due to leak of passwords, which affected nearly 32 million accounts. This was done by making employees and businesses by clicking on documents and links in email.
- One of the most important ransomware attacks was held in 2017 that impacted 200,000 PCs in 150 nations. As it affected several number of industries, a global repair bill of about $6 billion was required.
- Another major attack in the year 2014 occurred, in which the accounts of Yahoo were compromised. Nearly, 500 million accounts were hacked, where basic information and passwords except bank information were stolen during the cyber-attack.
- Adobe cyber-attack compromised personal information of 38 million users, where the users lost their IDs and passwords. Nearly, 2.9 million users even lost credit card information and passwords.

5. Cause and risk factor on recent cyber security threats

At present, the world is highly connected. This connectivity not only plays a vital role in personal lives but is also increasingly prevalent in professional work. Connected machines, processes, and devices perform various crucial functions in industries. This increased connectivity also causes the risk of cyber-attacks. Attackers have proven to adopt the developing techniques and tools, which can exploit the explosion of IIoT and IoT systems. According to the report [37], the cause for recent cyber security threats for companies as well as individuals are listed below.

5.1 Cloud exposure

Various IoT and artificial intelligence (AI) enabled devices and smart ecosystems are heavily reliant on cloud infrastructures for data storage and processing. This can yield a productive ground for cyber attackers. Vulnerabilities relied on this are listed as:

- Sensitive data exposure over the cloud relied on analysis and process,
- Negotiated storage of data may be open for data tampering and theft, and
- High data latency generates added exposure, which doesn't exist on the non-cloud relied structures.

5.2 Insecure IoT devices

Generally, it has been believed that all the professional and personal information stored in IoT system are safe and secure, but they are not. Investigations have resulted that the average IoT system can be surveyed for weakness, several thousand stretches per week. The risk factors are:

- Insufficient security practices over individual device holders and machines or devices, OEMs and operatives.
- Lack of inbuilt security protocols may place an IoT device vulnerable to cyber breaching in the whole device lifespan.

5.3 Interconnected systems

Organizations or industries, which deploy smart machine and system infrastructures generally result in an extremely broad base of customers, suppliers, and partners. Cyber-criminals can do these interconnection approaches for creating attacks that are both deep and broad. Particular risk factors include:

- Inconsistent and insufficient security protocol hardening across multiple devices controlled through multiple units.
- Enlarged dependence over service providers and remote employees, who may be less proficient in appropriate security approaches and procedures.

5.4 Design oversight

In the rush of getting new IoT products to market, manufacturers of the devices may de-prioritize the deployment and design of efficient security components. This issue can be further intensified through the datum that various devices have limited computing power and storage.

6. Dataset employed in intrusion detection

The dataset plays a significant part in the evaluation of IDS methods, specifically assessing the capability of the introduced methods over threat detection. The datasets utilized for the analysis of network packets in commercial products are not easily accessible due to their privacy matters. Moreover, there are few open source datasets like KDD, ADSA-LD, DARAPA, and NSL-KDD that are widely used benchmark datasets. The existing datasets, which are used to build and perform a comparative analysis of IDS are deliberated in this section along with their limitations and features.

6.1 DARPA

The initial exertion for producing an IDS data-set was made in 1998 by Defense Advanced Research Project Agency- DARPA and it resulted in a Knowledge Discovery and Data Mining (KDD) - KDD98 dataset [38]. DARPA introduced a program at the MIT Lincoln-Labs for generating a realistic and comprehensive IDS bench-marking network. Though the data-set was an efficient support for the IDS research, the capability and accuracy in the consideration of real-life circumstances have been extensively criticized. It was composed through numerous computers associated over the internet, by modeling a US Air-force environment. Host log and network packet files were received. The composed network packets were around 4 GB consisting of 49,00,000 records.. Two weeks of test data resulted in two million connection records and each possesses 41 features that are organized as abnormal (or) normal. These datasets were out of data as they don't result in the recent malware attack records.

6.2 KDD 99

The DARPA data1998 was utilized as the basis for deriving the KDD Cup99 data that has been employed in Third International Knowledge Discovery and Data Mining Tools Competition [39]. From 1999, KDD Cup99 was the most widely used dataset for the IDS evaluation. It is built on the data captured from the DARPA 98 dataset. This dataset provides a standard dataset to be audited and that included a wide variety of intrusions simulated in a military network area. The last modification of this dataset was in the year 1999 and therefore, the recent attacks on networks are not available in this dataset [40].

6.3 NSL-KDD

NSL-KDD is one of the benchmark datasets available in public that is developed from the earlier KDD cup99 dataset. The statistical evaluation performed over the cup99 dataset raised serious problems which widely affect the accuracy of IDS and mislead the anomaly-based IDS evaluation. The major problem faced in Cup99 is that it has a huge range of duplicate packets, over 75% and 78% of network packets are duplicates in both the testing and training dataset [41]. Therefore, to solve these existing issues in Cup99, the NSL-KDD dataset is employed. It contains 125,973 train dataset records and 22,544 testing set records. NSL-KDD dataset size is more than sufficient to utilize the whole dataset practically without the need for random sampling. This has produced comparable and consistent outcomes from various research. The NSL-KDD dataset encompasses 22 training imposition attacks and 41 features (attributes). In the NSL-KDD, 21 features are referred to as the association itself, and 19 attributes are described as the connection environment inside the same host.

6.4 CAIDA

DDoS- Distributed Denial of Service attack traces are present in the CAIDA dataset and it was collected in 2007. This kind of DoS tries to interrupt the regular traffic of the directed network (or) computer by overwhelming the target with a network-packet flood, averting regular traffic from accomplishing their legitimate destination computer. The drawback of this dataset is that it doesn't upshoot the diversity of attacks. In addition to this, collected data doesn't provide attributes form the entire network which makes it more problematic for differentiating the normal and abnormal traffic flows [42].

6.5 ISCX 2012

In ISCX 2012 dataset, the traces of real network traffic were evaluated for identifying the normal behavior for computers from real traffic of SMTP, IMAP, FTP, POP3, HTTP, and SSH protocols. This dataset generally relies on the realistic network traffic that is labeled and presents diverse attack scenarios [43].

6.6 GureKddcup

The gureKddcup data is established from MIT University laboratory, over seven weeks of an experiment that resulted in the large database in UCI repository format, and 41 attributes are extracted [44] based on three groups that are already existing in the kddcupp99 dataset [19]. Gurekddcup was developed based on the procedures employed in kddcup99 data formation by another team from the University of Basque Country.

It comprises of no flood attacks with a tcpdump list file and 15 percent of normal connections from the gureKddcup dataset. Most of the flood connections are ignored in gureKddcup and it has a total of 1,78,810 connections, among which 1,74,872 are normal connections and the remaining 2937 are attacks. The total dataset is about 4.3 GB. The dataset also provides the tcpdump list file for the corresponding data, unlike other datasets.

7. Prevention and control techniques

Various prevention and control measures that are taken in intrusion detection are explained in this section. At present, access control, firewalls, and cryptography are the chief defensive devices positioned in contradiction to the intrusion. These methods function as the first line of defense over any connected network and computer-based system. In a range of ensuring secured communication, cryptography is employed, and for user authentication, access control is utilized. Both the applications of anti-threat contribute to securing the whole system, only results in external security. Thus, it was insufficient for providing internal security for computer networks. A firewall network is either hardware (or) software employed for controlling the outgoing and incoming traffic according to the pre-defined rules. At the entry servers point, a basic firewall is installed to allow (or) divert IPs- Internet protocols and their addresses (IP addresses).

To access openly obtainable services like hypertext transfer protocols and domain label servers, the firewall authorizes the incoming traffic from the global range over the internet. A numeral of OS- operating systems attributes are inbuilt in firewalls. Most firewalls protect the contents and digital devices but traditional firewalls can't block and detect Trojan horses, worms, and viruses. Though both the firewalls and IDS are employed for the security of the network, they have various functions such as firewall exploration for exterior intrusions, whereas IDS guards intrusions that are instigated from within the system. Various firewalls are discussed in [45].

Traditional firewalls can't detect internal attacks like user-to-root-attacks, port-scanning, and flooding attacks, because they sniff out network packages at the network borders. These customary firewalls cannot detect complex attacks such as DDoS and DoS. They also face difficulty, to differentiate the difference between normal traffic and DoS attack traffic over the network. Access control that serves as the defense frontline over intrusion, supports both the integrity and confidentiality parameters.

Followed by these common solutions, various IDS employed for the detection of intrusion are listed below with proposed models and implementation approaches. Recently, the internet transported revolution through the entire world for sharing information at one stand. Since data is considered the most valuable and secure data, organizations and companies are spending a huge amount of money on the security solutions such as antivirus, and firewalls and they intend to protect resources and data from cyber-attacks and un-authorized access such as eavesdropping, hacking, and phishing. Even with these bulk security mechanisms, attackers are still able to exploit the vulnerabilities in the web application for stealing the credentials of users. IDS- intrusion detection system is mainly proposed by the researchers for detecting the network malicious activities to mitigate the cyber-attacks. Various machine learning techniques such as multilayer perceptron, K-nearest neighbor, Naïve Bayes, support vector, and decision tree have been analyzed for IDS implementation for classifying the network connections as malicious (or) normal [46]. Four measures such as sensitivity, accuracy, F-score, and precision have been taken into consideration for assessing the machine learning (ML) ability. Thus it results in decision trees as the best classifier for IDS. Similarly, the system [47] designed an IDS over an IoT network and detected various intrusion attacks based on hybrid CNN techniques. It is designed for a wide range of IoT applications. This design is compared and validated with the conventional ML and DL models. According to experimental evaluation results, the system is more sensitive to intrusion over an IoT network.

Accordingly, for enhancing the security of the IoT network, the system [48] presented a Passban IDS, which can safeguard the IoT devices which are directly connected. The individuality of the model was that it could be installed directly on very cheap IoT gateways, thus gaining full edge computing paradigm advantages for detecting the cyber threats as close as possible to the corresponding data sources. The Passban model is designed in a way of detecting various malicious attacks such as HTTP, SYN flood attacks, Port scanning, and SSH Brute force. The RDTIDS- Rules and decision tree-based IDS model [49] combine various classifier techniques such as decision tree and rule-based methods such as JRiPalgorithm, Forest PA, and REP tree. Particularly, the first and second approaches take the input features from the data set and classify the network traffic as attacks and non-attacks. The system [50] designed a novel UIDS- unified IDS model for securing the IoT environment from four different attacks namely generic, probe, DoS, and exploit. It is also capable of detecting normal network traffic. Focusing on the IoT security problem, the study [51] implements a Levenberg Marquardt - Back Propagation - Neural Network (LM-BP-NN) method. The LM-BP-NN design is introduced in IDS. LM algorithm possesses fast optimization and strong robustness and these specific characteristics are used for optimizing the conventional BP-NN threshold weight.

The system [52] identified five chief design principles, which should be taken in terms of developing DL- Deep Learning based IDS on IoT network. With the identified features [52], designed a TCNN- temporal convolutional neural network as a DL frame for IDS over IoT that combines CNN with causal convolution. However, TCNN is combined with the SMOTE-NC- Synthetic Minority Oversampling technique- Nominal Continuous for handling the unbalanced dataset. Similarly, the system [53] designed an E-GraphSAGE model, the GNN method permits for capturing both graph edge features along with the topological information for network intrusion detection (ID) over an IoT environment. The paper [54] implemented a novel host-based automated architecture for ID. The system combines kernel space and user space information and an ML approach for detecting various types of intrusion over smart devices. The tracing approach is used for the automatic detection of the device's behaviour, and processes this data into a numeric array for training various ML algorithms and shows alerts whenever an intrusion is detected.

In a range of securing data from unusual attempts and misuse, ML techniques are found as the key solution for improving IDS [55]. Ensemble-based IDS is employed for the improved intrusion detection system. The IPv6 emergence and open access public network installation are attracting cybercriminals to compromise the information of users [56]. Thus, RNN-IDS-random neural network-based heuristic IDS is employed for IoT networks. A lightweight ML-based IDS approach is employed in [57] with high performance for the limited IoT networks such as IoTIDS, which is based on the hybrid genetic algorithm (GA) and grey wolf optimized labelled as GA-

GWO. The main objective of the system is to reduce the huge wireless network traffic dimension with the intelligent selection of the most informative traffic features. Table 1 shows the various IDS methods, the dataset employed in this system, and the attacks that are detected in the system.

Table 1 Various IDS methods, their dataset, and attacks.

Reference	Dataset	Methods	Attacks
[1]	KDDCup, NSL-KDD, BoT-IoT, and CICIDS-2017	DL and enhanced Transient search optimization.	DDoS, FTP-patator, portscan, SSH-Patator, U2R, Probe, DoS.
[6]	UNSW-NB-15, KDDCupp 2017, CICIDS 2017	Lightweight APAE	DoS, U2R, Worms,Fuzzers
[7]	Public dataset containing MQTT attacks.	DL based IDS	MQTT
[8]	CIDDS-001,KDD, UNSWND-15	WILS-TRS	DoS, Bottnets, MIM, data probing, and spying
[9]	UNSW Canberra Cyber	DL	DoS, bottnets
[17]	ToN_IoT	ReliefF based IDS	DDOS, DoS, injection, XSS, password, scanning, mitm.
[20]	Bot-IoT	DeepCNN	DDoS
[24]	ISCX-2012	EFSAGOA	Network attacks
[30]	BoT-IoT and CICIDS-2017	Decision tree and rule-based models	DoS, port scan, Brute-force, web attack.
[31]	NSL-KDD-99	UIDS	DoS, probe, generic, and exploit
[32]	KDDCup 99	LM-BP neural network	DoS, R2L, and U2L
[33]	BoT-IoT	TCNN	DoS, DDoS, information theft.
[34]	ToN-IoT, BoT-IoT , NF-ToT-IoT and NF-BoT-IoT	E-GraphSAGE	DDoS, DoS, information theft.
[36]	CICIDS-2017	Ensemble-based IDS	DoS, web attack.
[37]	NSL-KDD99	RNN-IDS	DoS attack
[38]	AWID	GA-GWO	Various attacks
[39]	BoT-IoT	Multi-level DDoS mitigation	DDoS

8. Critical analysis

An analysis of different IDS approaches in IoT network is performed and analysis of these studies is described in the form of graphical representation. Figure 6 shows datasets reviewed in the paper.

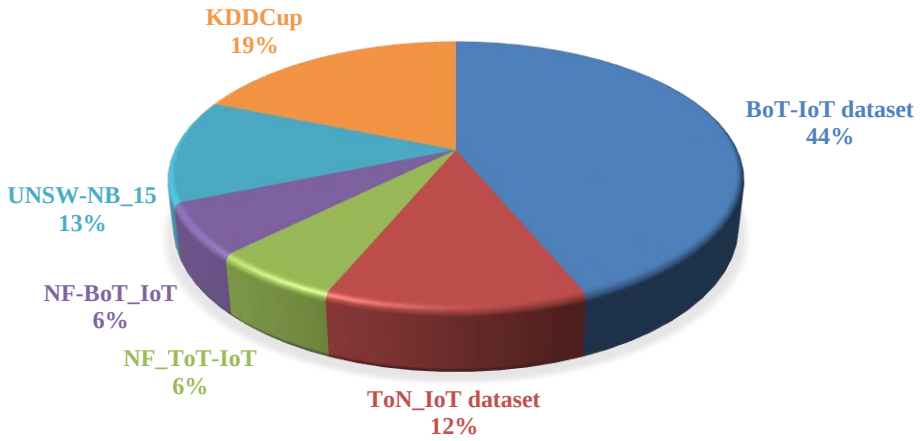

Figure 6 Dataset Count

Figure 6 shows that BoT-IoT datasets have been used in different existing studies. The Figure 7 shows the year-wise distribution of studies considered in the study.

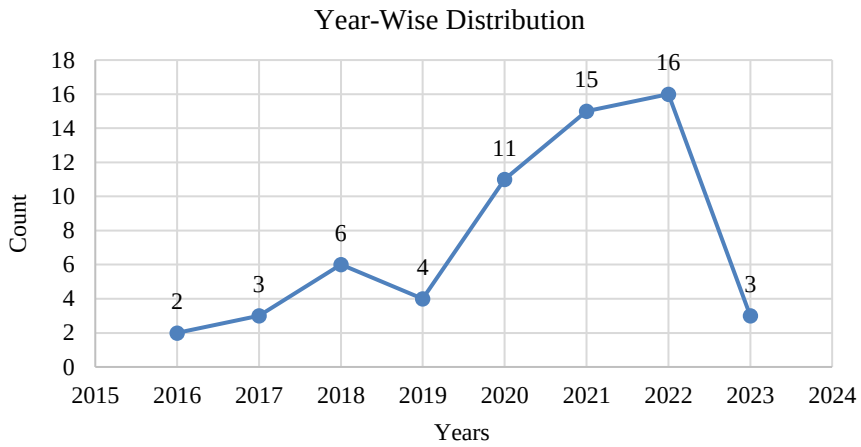

Figure 7 Year-Wise Analysis of Studies Used in the Study

From the analysis, it is inferred that maximum studies based on IDS in IoT network are taken from the years 2020, 2021 and 2022. From the overall analysis, it has been concluded that these attacks have gained significant attention from the critical analysis during the years 2020, 2021, 2022. However, there are possibilities that these attacks can be increased in the upcoming years as well. Therefore, effective measures should be considered in order to prevent attacks from the IoT network.

9. Challenges in detecting intrusion over IoT

This part of the review presents the security challenges over IoT, which are particularly prevalent for ensuring data security such as integrity, availability, and confidentiality. Generally, the attack over the data is classified as passive (or) active, where the active attacks are apprehensive about the data subversion (or) destruction within the grid, and passive attacks are concerned with the privacy subversion (or) data theft. Numerous inherent characteristics of the IoT environment cause problems in security to be diverse and widespread from the conservative security concerns. These mainly stem from the perception layer due to their reserved nature. In the view of [58], all the security problems can be due to the power limit extension of the devices, that somewhat that conservative security solutions do not suffer due to their non-mobile nature.

As an unconstrained energy source can support huge processing and memory, the cryptographic principles are the base for the requirement of security information such as various processes and memory for the chief processing, and storage need to be done effectively. Moreover, implementation and technology-related challenges are not the only areas that cause IoT networks to be insecure. Profit-driven Novel and profit-driven business, the competitive sector results from manufacturing the device need to consider security as an addition [59]. Due to the pre-dominate devices sensing nature, data theft is termed out as a huge risk. The data is frequently perceived as too inconsequential for apprehension. It inclines to be remote from the truth; as an illustration, privacy betrayal can be done in smart meters and even physical security breaches by data leakage [60]. A deeper concern is with smart cities, where the data privacy challenges may cause "an unequal society" by refinement.

Generally, the application layer of IoT technologies includes those convoluted within the service, frequently placed around message passing, and thus travels the complete network zone from the perception-layer sensors to the back-end support approach. The outcome produces various "SMART" solutions like smart cities [61]. Thus, this layer will span a device's multitude. Accordingly, security solutions will be necessary to reflect this accordingly. As with the transport layer, cryptography is effortlessly positioned over the back-end (or) end-user devices but is less supportive over the observation method with IDS [62]. Thus, the safeguarding at this layer determination preferably requires to span the entire network layer where inter-operability among them is cited as a chief security issue in IoT [59, 63, 64].

Emerging a real-time and online abnormality-based IDS model for IoT networks is very perplexing. It is as IDS needs to absorb the normal performance initially for detecting malicious (or) abnormal activities. The culture division adopts that there is no attack (or) noise throughout this epoch that cannot be assured. IDS might produce false alarms if these problems are not properly lectured.

It could be stimulating for developing a trained model for specific devices. These models could be employed for IDS in organizations utilizing similar device types. It would assist other systems that can deploy this system and hence saves time, which could be necessary for collecting the data and IDS training. It also supports detecting the malicious IoT network that is previously negotiated because its characteristics vary from normal performance captured through trained models. However, implementing such models is a challenging portion.

Dimensionality reduction and feature selection approach employed for the IDS are suitable for working over a particular normal traffic type and for detecting a specific kind of attack that may not work once the normal environment (or) the sequences of attacks change a bit, specifically during a fast-changing IoT environment semi-supervised learning approach, reinforcement learning (RL) and transfer learning (TL) are static not explored well. Therefore, the experiments designed for IDS in the context of IoT security need to obtain more significant objectives such as fast training, real-time application, and a unified system for intrusion detection over IoT.

ML and DL-based algorithms and techniques are widely used for model training over a huge dataset. It is facilitating efficient cyber-attack handling. Moreover, regarding the ML and DL algorithm use over the intrusion detection in the IoT environment, the challenges that need to be focused are the resource constraints with the IoT system, and the ML/DL algorithm [64] usage for safeguarding the IoT networks. Other challenges with the usage of ML/DL techniques in distributed and large networks like IoT environments face are scalability problems, as an illustration in the context of several choices and scenarios of IDS deployment. Therefore, to overcome the individual ML/DL algorithm limitations, the author [65] uses ensemble DL/ML algorithms which perform better in comparison to individual ML algorithms; likewise, such algorithms are computationally affluent, and thus, network fallouts in latency problems that cannot be given in a precarious model comprising risk for human-lives such as autonomous and health (or) IoVs- internet of vehicles-systems.

Recent attacks faced on IoT networks are stated as follows. More than one billion IoT attacks are found in the year 2021 [66]. The fact that 50% of micro and home business networks faced suspicious network traffic (or) attacks in 2021, including brute force attacks, DPI policy-based attacks, DDoS, and phishing attacks. In addition to this, it is found the active rise in both Mozi and Mirai malware families. The most surprising consequence is that the IoT devices are the most vulnerable to attacks. According to the analysis, 46% of the attacks were on routers.

10. Conclusion and future direction

In the last decade, the IoT environment usage has increased drastically in day-to-day life owing to their converting object capacity from various application sectors into internet hosts. In parallel, there are user security and privacy issues faced due to IoT security vulnerabilities. That stimulates a need for developing more robust security solutions for the IoT environment. In such a situation, IDS is found as a crucial technique for enhancing IoT security. In this study, a survey on IDS over the IoT network is deliberated. Various IoT attacks, causes and risk factors, and data set employed for IDS have been discussed. Then, this study reviews recent trends in IoT systems and the prevention and control measures that are taken for improving IDS systems, and then the challenges faced in detecting intrusion are discussed in detail. This study aims at providing the scholars with a summarized but wide-ranging and beneficial insight over several security challenges confronted at present by IDS. Various IDS have been implemented; they still need to focus on the recent threats which are being increased in recent days. In the future, the escalating activity of Mozi and Mirai needs to be focused on. Also, the computational and dynamic efficiency of the system for feature selection can be designed as working under all kinds of attacks and normal traffic. However, it would be a stimulating exploration of employing RL in combination with DL, because their combination can benefit the IoT environment by involving huge data dimensionality and non-stationary environments.

11. Reference

[1] Fatani A, Abd Elaziz M, Dahou A, Al-Qaness MAA, Lu S. IoT intrusion detection system using deep learning and enhanced transient search optimization. IEEE Access. 2021;9:123448-64.

[2] Wang Y, Ma J, Sharma A, Singh PK, Gaba GS, Masud M, et al. An exhaustive research on the application of intrusion detection technology in computer network security in sensor networks. J Sens. 2021;2021:1-11.

[3] Lombardi M, Pascale F, Santaniello D. Internet of Things: a general overview between architectures, protocols and applications. Information. 2021;12(2):87.

[4] Ali SR. IoT: the revolutionary tech and its challenges in the modern technological landscape [thesis]. United States: Governors State University; 2022.

[5] Firouzi F, Farahani B, Weinberger M, DePace G, Aliee FS. Iot fundamentals: definitions, architectures, challenges, and promises. In: Firouzi F, Chakrabarty K, Nassif S, editors. Intelligent Internet of Things. Cham: Springer; 2020. p. 3-50.

[6] Krishnamurthi R, Kumar A, Gopinathan D, Nayyar A, Qureshi B. An overview of IoT sensor data processing, fusion, and analysis techniques. Sensors. 2020;20(21):6076.

[7] Skouteli E. Cybersecurity and the Internet of Things [thesis]. Greece: The International Hellenic University (IHU); 2023.

[8] Rastogi A. A study of the architectures, protocols, and applications of the Internet of Things (IoT). Int J Food Nutr Sci. 2022;11(6):1016-23.

[9] Thakral M, Singh RR, Kalghatgi BV. Cybersecurity and ethics for IoT system: a massive analysis. In: Saxena S, Pradhan AK, editors. Internet of Things. Transactions on Computer Systems and Networks. Singapore: Springer; 2022. p. 209-33.

[10] Tran-Dang H, Kim DS. Fog computing: fundamental concepts and recent advances in architectures and technologies. Cooperative and Distributed Intelligent Computation in Fog Computing. Cham: Spromger; 2023. p. 1-18.

[11] Gaurav A, Gupta BB, Hsu CH, Yamaguchi S, Chui KT. Fog layer-based DDoS attack detection approach for internet-of-things (IoTs) devices. IEEE International Conference on Consumer Electronics (ICCE); 2021 Jan 10-12; Las Vegas, USA. USA: IEEE; 2021. p. 1-5.

[12] Labiod Y, Amara Korba A, Ghoualmi N. Fog computing-based intrusion detection architecture to protect iot networks. Wireless Pers Commun. 2022;125(1):231-59.

[13] HaddadPajouh H, Khayami R, Dehghantanha A, Choo KKR, Parizi RM. AI4SAFE-IoT: an AI-powered secure architecture for edge layer of Internet of Things. Neural Comput Applic. 2020;32:16119-33.

[14] Khan MA, Khan MA, Jan SU, Ahmad J, Jamal SS, Shah AA, et al. A deep learning-based intrusion detection system for MQTT enabled IoT. Sensors. 2021;21(21):7016.

[15] Gassais R, Ezzati-Jivan N, Fernandez JM, Aloise D, Dagenais MR. Multi-level host-based intrusion detection system for Internet of Things. J Cloud Comp. 2020;9:1-16.

[16] Lin F, Zhou Y, An X, You I, Choo KKR. Fair resource allocation in an intrusion-detection system for edge computing: ensuring the security of Internet of Things devices. IEEE Consum Electron Mag. 2018;7(6):45-50.

[17] Mohamed RH, Mosa FA, Sadek RA. Efficient intrusion detection system for IoT environment. Int J Adv Comput Sci Appl. 2022;13(4):572-578.

[18] Zhong M, Zhou Y, Chen G. Sequential model based intrusion detection system for IoT servers using deep learning methods. Sensors. 2021;21(4):1113.

[19] Mothukuri V, Khare P, Parizi RM, Pouriyeh S, Dehghantanha A, Srivastava G. Federated-Learning-Based anomaly detection for IoT security attacks. IEEE Internet Things J. 2022;9(4):2545-54.

[20] Idrissi I, Boukabous M, Azizi M, Moussaoui O, El Fadili H. Toward a deep learning-based intrusion detection system for IoT against botnet attacks. IAES Int J Artif Intell. 2021;10(1):110-20.

[21] Basati A, Faghih MM. APAE: an IoT intrusion detection system using asymmetric parallel auto-encoder. Neural Comput Applic. 2023:35:4813-33.

[22] Mosaiyebzadeh F, Rodriguez LGA, Batista DM, Hirata R. A network intrusion detection system using deep learning against mqtt attacks in IoT. IEEE Latin-American Conference on Communications (LATINCOM); 2021 Nov 17-19; Santo Domingo, Dominican Republic. USa: IEEE; 2021. p. 1-6.

[23] Jothi B, Pushpalatha M. WILS-TRS—a novel optimized deep learning based intrusion detection framework for IoT networks. Pers Ubiquit Comput. 2023;27:1285-301.

[24] Jithu P, Shareena J, Ramdas A, Haripriya AP. Intrusion detection system for iot botnet attacks using deep learning. SN Comput Sc. 2021;2(3):1-8.
[25] Liu C, Antypenko R, Sushko I, Zakharchenko O. Intrusion detection system after data augmentation schemes based on the VAE and CVAE. IEEE Trans Reliab. 2022;71(2):1000-10.
[26] Ravi V, Chaganti R, Alazab M. Recurrent deep learning-based feature fusion ensemble meta-classifier approach for intelligent network intrusion detection system. Comput Electr Eng. 2022;102:108156.
[27] Telikani A, Shen J, Yang J, Wang P. Industrial IoT intrusion detection via evolutionary cost-sensitive learning and fog computing. IEEE Internet Things J. 2022;9(22):23260-71.
[28] Yang X, Peng G, Zhang D, Lv Y. An enhanced intrusion detection system for IoT networks based on deep learning and knowledge graph. Secur Commun Netw. 2022;2022:1-21.
[29] Ahmad UB, Akram MA, Mian AN. Low-latency intrusion detection using a deep neural network. IT Prof. 2022;24(3):67-72.
[30] Boopathi M. Henry MaxNet: tversky index based feature selection and competitive swarm henry gas solubility optimization integrated Deep Maxout network for intrusion detection in IoT. Int J Intell Robot Appl. 2022;6(2):365-83.
[31] Campos EM, Saura PF, González-Vidal A, Hernández-Ramos JL, Bernabé JB, Baldini G, et al. Evaluating federated learning for intrusion detection in Internet of Things: review and challenges. Comput Netw. 2022;203:108661.
[32] Heidari A, Jabraeil Jamali MA. Internet of Things intrusion detection systems: a comprehensive review and future directions. Cluster Comput. 2023;26:3753-80.
[33] Atlam HF, Wills GB. IoT security, privacy, safety and ethics. In: Farsi M, Daneshkhah A, Hosseinian-Far A, Jahankhani H, editors. Digital twin technologies and smart cities. Cham: Springer; 2020. p. 123-49.
[34] Chang CH, Guajardo J, Holcomb D, Regazzoni F, Rührmair U. ASHES 2018-Workshop on Attacks and Solutions in Hardware Security. Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security; 2018 Oct 15-19; Toronto, Canada. New York: ACM; 2018. p. 2168-70.
[35] Micro.ai. 10 Types of cyber security attacks in IoT [Internet]. 2019 [cited 2019 Nov 12]. Available from: https://micro.ai/blog/10-types-of-cyber-security-attacks-in-the-iot.
[36] Zara S. Real-World examples of cyber attacks and their impact [Internet]. 2023 [cited 2023 Jul 25]. Available from: https://kahedu.edu.in/real-world-examples-of-cyber-attacks-and-their-impact/#:~:text=Yahoo%20was%20hacked%20online%3A%20One,but%20bank%20information%20was%20not.
[37] MicroAI. Cyber-Security-Top Threats for 2022 [Internet]. 2022 [cited 2022 Jun 17]. Available from: https://micro.ai/blog/cyber-security-top-threats-for-2022.
[38] Lincoln Laboratory, MIT. DARPA intrusion detection evaluation dataset [Internet]. 1998 [cited 2022 Jun 17]. Available from: https://www.ll.mit.edu/r-d/datasets/1998-darpa-intrusion-detection-evaluation-dataset.
[39] The UCI KDD Archive, Information and Computer Science University of California. KDD Cup 1999 Data [Internet]. 1999 [cited 2022 Jun 17]. Available from: https://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html.
[40] The UCI KDD Archive, Information and Computer Science University of California. Intrusion detector learning [Internet]. 1999 [cited 2022 Jun 17]. Available from: https://kdd.ics.uci.edu/databases/kddcup99/task.html.
[41] Tavallaee M, Bagheri E, Lu W, Ghorbani AA. A detailed analysis of the KDD CUP 99 data set. IEEE symposium on computational intelligence for security and defense applications; 2009 Jul 8-10; Ottawa, Canada. USA: IEEE; 2009. p. 1-6.
[42] Sekhar C, Rao KV, Prasad MK. Classification of the DDoS Attack over flash crowd with DNN using world cup 1998 and CAIDA 2007 Datasets. i-Manager's J Softw Eng. 2021;15(3):29-36.
[43] Dwivedi S, Vardhan M, Tripathi S, Shukla AK. Implementation of adaptive scheme in evolutionary technique for anomaly-based intrusion detection. Evol Intel. 2020;13(1):103-17.
[44] ALDAPA group. gureKddcup and gureKddcup6percent dataset. Spain: Computer Architecture And Technology Department, University of basque Country; 2019.
[45] Sequeira D. Intrusion prevention systems-security's silver bullet? [Internet]. 2002 [cited 2016 Sep 9]. Available from: https://www.sans.org/white-papers/366/?show366.php&cat=detection.
[46] Manhas J, Kotwal S. Implementation of intrusion detection system for Internet of Things using machine learning techniques. In: Giri KJ, Parah SA, Bashir R, Muhammad K, editors. Multimedia Security. Algorithms for Intelligent Systems. Singapore: Springer; 2021. p. 217-37.
[47] Smys S, Basar A, Wang H. Hybrid intrusion detection system for Internet of Things (IoT). J ISMAC. 2020;2(4):190-9.
[48] Eskandari M, Janjua ZH, Vecchio M, Antonelli F. Passban IDS: an intelligent anomaly-based intrusion detection system for IoT edge devices. IEEE Internet Things J. 2020;7(8):6882-97.
[49] Ferrag MA, Maglaras L, Ahmim A, Derdour M, Janicke H. Rdtids: rules and decision tree-based intrusion detection system for internet-of-things networks. Future internet. 2020;12(3):44.
[50] Kumar V, Das AK, Sinha D. UIDS: a unified intrusion detection system for IoT environment. Evol Intel. 2021;14(1):47-59.
[51] Yang A, Zhuansun Y, Liu C, Li J, Zhang C. Design of intrusion detection system for Internet of Things based on improved BP neural network. IEEE Access. 2019;7:106043-52.
[52] Derhab A, Aldweesh A, Emam AZ, Khan FA. Intrusion detection system for Internet of Things based on temporal convolution neural network and efficient feature engineering. Wireless Communications and Mobile Computing. 2020;2020:1-16.
[53] Lo WW, Layeghy S, Sarhan M, Gallagher M, Portmann M. E-GraphSAGE: a graph neural network based intrusion detection system for IoT. NOMS 2022-2022 IEEE/IFIP Network Operations and Management Symposium; 2022 Apr 25-29; Budapest, Hungary. USA: IEEE; 2022. p. 1-9.
[54] Gassais R, Ezzati-Jivan N, Fernandez JM, Aloise D, Dagenais MR. Multi-level host-based intrusion detection system for Internet of Things. J Cloud Comp. 2020;9(1):1-16.
[55] Abbas A, Khan MA, Latif S, Ajaz M, Shah AA, Ahmad J. A new ensemble-based intrusion detection system for Internet of Things. Arab J Sci Eng. 2022;47(2):1805-19.
[56] Qureshi AuH, Larijani H, Ahmad J, Mtetwa N. A heuristic intrusion detection system for Internet-of-Things (IoT). In: Arai K, Bhatia R, Kapoor S, editors. Intelligent Computing. CompCom 2019. Advances in Intelligent Systems and Computing vol. 997. Cham: Springer; 2019. p. 86-98.
[57] Davahli A, Shamsi M, Abaei G. Hybridizing genetic algorithm and grey wolf optimizer to advance an intelligent and lightweight intrusion detection system for IoT wireless networks. J Ambient Intell Human Comput. 2020;11(11):5581-609.

[58] Yan Q, Huang W, Luo X, Gong Q, Yu FR. A multi-level DDoS mitigation framework for the industrial Internet of Things. IEEE Commun Mag. 2018;56(2):30-6.
[59] Frustaci M, Pace P, Aloi G, Fortino G. Evaluating critical security issues of the IoT world: present and future challenges. IEEE Internet Things J. 2018;5(4):2483-95.
[60] Asghar MR, Dán G, Miorandi D, Chlamtac I. Smart meter data privacy: a survey. IEEE Commun Surv Tutor. 2017;19(4):2820-35.
[61] Eckhoff D, Wagner I. Privacy in the smart city—applications, technologies, challenges, and solutions. IEEE Commun Surv Tutor. 2018;20(1):489-516.
[62] Xin Y, Kong L, Liu Z, Chen Y, Li Y, Zhu H, et al. Machine learning and deep learning methods for cybersecurity. IEEE Access. 2018;6:35365-81.
[63] Soursos S, Žarko IP, Zwickl P, Gojmerac I, Bianchi G, Carrozzo G. Towards the cross-domain interoperability of IoT platforms. European conference on networks and communications (EuCNC); 2016 Jun 27-30; Athens, Greece. USA: IEEE; 2016. p. 398-402.
[64] Cerullo G, Mazzeo G, Papale G, Ragucci B, Sgaglione L. Chapter 4 - IoT and sensor networks security. In: Ficco M, Palmieri F, editors. Security and Resilience in Intelligent Data-Centric Systems and Communication Networks. United States: Academic press; 2018. p. 77-101.
[65] Xiao L, Wan X, Lu X, Zhang Y, Wu D. IoT security techniques based on machine learning: How do IoT devices use AI to enhance security? IEEE Signal Process Mag. 2018;35(5):41-9.
[66] Venturebeat. Report: More than 1B IoT attacks in 2021 [Internet]. 2022 [cited 2022 Jun 17]. Available from: https://venturebeat.com/2022/04/25/report-more-than-1b-iot-attacks-in-2021/.