International Journal of Safety and Security Engineering
Vol. 14, No. 4, August, 2024, pp. 1073-1086
Journal homepage: http://iieta.org/journals/ijsse

A Comprehensive Review of Cyber-Attacks Targeting IoT Systems and Their Security Measures

Maryam Lazim Mutleg*, Ali Majeed Mahmood, Muna Mohammed Jawad Al-Nayar

Control and Systems Engineering Department, University of Technology-Iraq, Baghdad 10066, Iraq

Corresponding Author Email: cse.22.21@grad.uotechnology.edu.iq

Copyright: ©2024 The authors. This article is published by IIETA and is licensed under the CC BY 4.0 license (http://creativecommons.org/licenses/by/4.0/).

https://doi.org/10.18280/ijsse.140406

Received: 2 May 2024
Revised: 20 July 2024
Accepted: 1 August 2024
Available online: 30 August 2024

Keywords:
cyber-attacks, cybersecurity, Internet of Things, Intrusion Detection Systems, IoT layer architecture

ABSTRACT

The Internet of Things (IoT) represents the backbone of current and future technologies. The main objective of IoT is to make human life easier by automating most daily jobs. The endless web of connections entices opponents to utilize the IoT's weaknesses. For that reason, this technological innovation faces a few serious safety and confidentiality problems. These problems are the actual motivation of this research. This paper reviews the latest research and possible types of attacks that can affect IoT systems including the exploration of IoT infrastructure. Various cybersecurity threats, including network, application, and physical attacks, that aim to compromise the IoT are discussed. Moreover, regarding attack types, we performed a statistical analysis using Excel for the percentage of most attacks and found that DDoS is the most common with 21%. In addition, by comparing Deep Learning (DL) accuracy measures with traditional methods, DL methods achieved an accuracy of more than 98%, so they are better and more effective in detecting and classifying the attack types due to their high accuracy. However, rarely do researchers focus on computational complexity. Finally, the paper highlights some statistics using Python language on the negative impact of attacks on network traffic.

1. INTRODUCTION

The Internet of Things has the potential to make numerous advances in global technology because of its ability to interact with most aspects of life [1, 2]. Covering smart cities, modern medical techniques, smart homes, and smart agriculture [3, 4]. IoT refers to a networked embedded computing system that operates in soft real-time [5] and it consists of billions of devices linked together that can transmit information to each other electronically. IoT makes several facilities feasible, including tracking, monitoring, and controlling, which alters how people interact with physical items. IoT uses an extensive range of developed devices, involving laser scanners, gas inductors, and Radio Frequency Identification (RFID) infrared sensors IoT allows for the monitoring and control of many characteristics of items or procedures, including light, sound, chemistry, method, biology, and position. The information in IoT is based on real-time data which is so important [6]. Enabling things to be connected at anytime, anywhere, with anything, and with anybody utilizing any path/network and any service is the aim of the IoT [7]. Due to the variety of device connectivity, IoT devices have numerous vulnerabilities that hackers could exploit to undermine their security [8, 9]. The process of protecting data through attack prevention, detection, and response is known as cybersecurity [10-12]. A safety instrument known as an Intrusion Detection System (IDS) may recognize and block network and computer system access [13, 14]. IDS monitors system and network activity to look for odd trends that might point to a security breach [15-17]. The two primary IDS classes are anomaly identification and signature identification. Signature identification systems evaluate identified attack patterns, or signatures, using system activity and network data., to identify potential threats. alternatively, anomaly identification makes use of Machine Learning (ML) methods to establish a foundation of normal activity and spot deviations that could point to an intrusion [18]. The one with the best performance among them is intrusion detection using DL [19]. This is illustrated by the significant powers of Deep Learning, which include self-adaptation, great generalization, self-learning, and the detection of unusual assault behavior [20, 21].

Figure 1 illustrates four layers that can be distinguished in IoT architecture. This paper introduces a review of IDS for IoT systems concerning the IoT's layer architecture. The paper organization is as follows: Section 2 briefly discusses security attacks in IoT according to layers. In Section 3, a brief explanation of IDS for IoT. In Section 4, prior work evaluation is introduced. Section 5 discusses the outcomes and evaluations of the statistics.

1.1 Perception layer

Several sensors, including infrared, RFID, ZigBee, and QR codes, are used by this layer to gather data. Temperature, humidity, force, vibration, pH level, pressure, speed, and so on can all be considered forms of information. The information is transmitted via the network layer to be obtained in the central information processing unit [22].

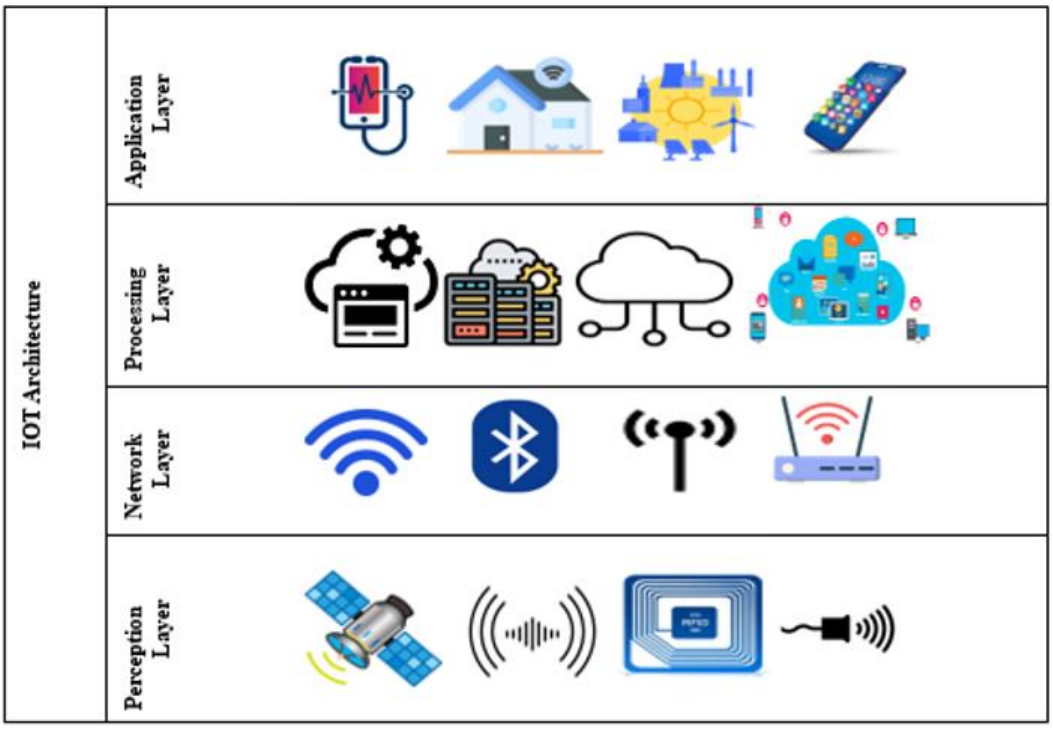


Figure 1. IoT architecture based on layers [22]

1.2 Network layer

The information conveyed at this layer may be communicated via satellite, infrared equipment, Wi-Fi, and other media, depending on the type of sensor and data sensitivity. Consequently, information is safely moved over the network layer from the perception layer to higher layers [22].

1.3 Processing layer

The application and network layers are combined within this stratum. This layer can perform all cloud and cognitive calculations. Supportive base layer capabilities include things like service administration and data storage from lower-level layers to databases. Additionally, this residue can compute, record, and handle statistics on its own as the foundation for astute computing [22].

1.4 Application layer

The application layer reflects the reaction to user requests. The processed statistics of lower layers are used to create offerings that can be useful to the end user. The data offers a foundation for these kinds of applications, which could help the user in a variety of ways, including communication, private healthiness teaching, technology, domestic goods, and transportation. Features like identification and confidentiality should be part of IoT data security. Since IoT could be used in highly important industries, including postal services, smart homes, transportation, and healthcare, its security and privacy must be impeccable. Every security factor should have a targeted solution described [22].

2. METHODOLOGY

A thorough overview of IoT security threats is provided. Different types of IDS for IoT systems are identified. In addition, perform a comprehensive review of existing research related to Intrusion Detection Systems and IoT security attacks.

2.1 Security attacks in IoT

In this section, several security risks on each layer that have emerged recently are briefly addressed. IoT security attacks can be categorized using three broad categories, as shown previously in Figure 2 [23]. Table 1 illustrates a brief comparison between the most common attacks including their negative impact along with the probable method of defense.

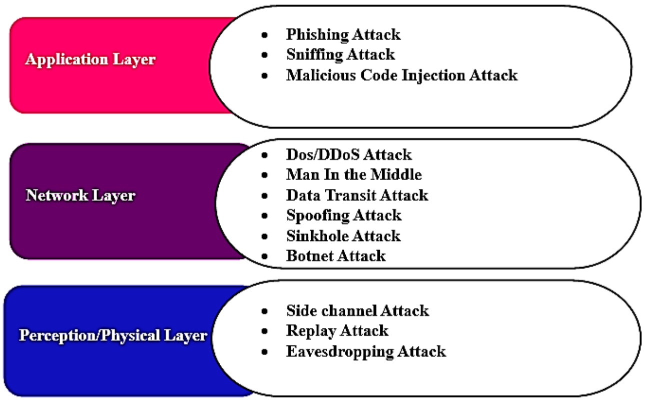


Figure 2. Assaults into IoT networks [24]

2.1.1 Application layer attacks

Software package assaults are the leading reason for insecurity in PC security. Implementation of IoT System gadgets, admission to touchy data, facts access, and denial of service can all be programmed using Trojan horse applications, worms, viruses, adware, and malicious scripting software program assault [23]. A few examples of these attacks can be seen in the next subsections.

a) Phishing attacks

Phishing attacks start when consumers get spoof emails from someone who seems to be authentic. These emails may contain harmful links and encourage the recipient to update their account details. The attacker uses spoof emails, bogus websites, or both in an attempt to trick internet users and obtain their personal information [25].

b) Malicious code injection

Scripts intentionally designed to damage IoT device capabilities are known as malicious scripts. They can be added, altered, or removed from the software [26]. This is a coded assault that directly targets the software's code and damages the network without authorization. The hacker then inserts malicious code into the software, infecting it.

c) Sniffing attacks

By installing a sniffer program on the device, an adversary could compel an assault on the device and gain access to network information that could corrupt the system [26]. Sniffing is a strategy used to alter the content or try to look for the file format. Another name is Multipurpose Internet Mail Extensions (MIME) sniffing or media-type sniffing. Files, that contain deliberate payloads or malicious content, are uploaded by the attacker [27].

2.1.2 Network layer attacks

Networks used by IoT systems are the focus of the offensive. Without going near a network, this offensive can be executed. Some of the most common attacks are as follows:

a) DoS/DDoS

Denial of Service (DoS) is one of the most destructive and rapidly expanding categories of cyberattacks characterized by high damage and significant impact on business operations. An attacker can prevent authorized users from using the service by overloading the capacity or assets of a device or network that is being targeted [28, 29]. DoS assault occurs when an attacker utilizes a single machine to compromise the service. Distributed DoS is an extended DoS assault that multiplies the attack's stress level on the targeted machine or system by starting the attack from numerous compromised devices. The ultimate goal of both of these assaults is to bring down the service by flooding the system with network traffic or by using a significant amount of system resources [30, 31].

b) Man in the Middle

The concept of Man in the Middle (MITM) refers to a hacker's attempt to disrupt communication between two systems. Since the assailant covertly intercepts communications between the two parties and sends them assuming they are talking directly to each other, it can be a dangerous attack. Since they are the ones having the real conversation, the attacker can trick the receiver into thinking they are still getting a valid message [32].

c) Botnet attack

Botnets are a group of devices on the internet that are infected with software, allowing hackers to monitor them. Cybercriminals employ a botnet to launch attacks, such as DDoS attacks, illegal access, data theft, and credential leaks [33]. Numerous unprotected IoT devices, along with the most recent developments in botnet technology, are being used by hackers to turn IoT devices into a botnet army that launches botnet attacks [34]. A hacker using a botnet attack will infect IoT devices with malware, enabling them to receive instructions from a command-and-control server and perform destructive actions [34].

d) Data transit attack

The environment in which data is shared and kept in daily life may represent the primary target of rivals and attackers. Sensitive data is stored on local servers or in cloud storage. However, due to this data being transferred from one server to another, it is more vulnerable to attack. Huge amounts of data are sent between the environment's sensors, cloud, actuators, and other devices. Therefore, the most susceptible attack vector for IoT devices is data transportation [34].

e) Spoofing attack

A type of cloning called spoofing does not physically duplicate an RFID tag. The attackers use specialized devices with enhanced capabilities that may mimic RFID tags given certain data content to achieve spoofing. An attacker impersonates a legitimate RFID tag in this kind of assault to obtain its rights. For this impersonation to work, full access to the same channels of telecommunication as the original tag is required. Knowing the protocols and secrets that will be used for any authentication that occurs is part of this process [35].

f) Sinkhole attack

An attacker can seize control of a node inside a network by using a sinkhole attack against an IoT system to draw all traffic from nearby nodes. These attacks increase network congestion and strength consumption at nodes. Furthermore, discarding all packets in place of transmitting them to their destination can make the IoT open to denial-of-service attacks [36].

g) Sybil attack

This assault allows an attacker to be in two places using an unauthorized node known as the Sybil node to impersonate extra nodes. A Sybil attack can motivate close by Wireless Sensor Network (WSN) nodes to accept faulty records. A Sybil node, for instance, may be capable of voting greater than as soon as in a WSN voting machine, which could provide a fraud result [36].

2.1.3 Perception layer attacks

Hardware-based attacks are the most common ones against the perception layer. Technologies like WSN, RFID, Zigbee, and other sensor types are typically included in the perception layer. The attacker needs to be within the network or very near to the nodes that make up the IoT. A few common attacks on the perception layer are listed below.

a) Replay attacks

In these types of assaults, the message is intercepted by the attacker from the communication medium and then subsequently sent to the same network. Smart devices can be compromised by hackers, who can then transmit data as an authorized node [37].

b) Eavesdropping

When smart devices are infiltrated, attacks like Eavesdropping may happen. The attacker can read the communications between the devices because of the insecure communication connection. The attacker obtains the data from insecure transmission media in this passive attack [37].

c) Side channel attack

Since Side Channel Attack (SCA) operates under the assumption that data leaks constantly, adversaries may be able to take advantage of a smart device's data leakage to identify significant patterns of correlation among activities and connection nodes. As a result, they will have access to certain private, critical information for their malicious purposes [38].

Table 1. A summary of differences, harms, and defense methods for different types of attack

Attack Type	Differences	Harms	Defense Methods
Phishing	Uses social engineering to take advantage of people's trust and conduct	Disclosing financial or personal data harms reputation and trust.	Granting device access with Multi-Factor Authentication (MFA), email and web filtering, and detecting phishing in real-time.
Malicious code injection	It directly changes or manipulates data or the behavior of programs.	Directly alters or manipulates data or software behavior. theft and alteration of data. System vulnerability and management. Identity theft, monetary losses, and reputational harm	Web Application Firewalls (WAF), parameterized queries, reliable coding techniques, and regular updates to reduce injection risks.
Sniffing attacks	Sniffing attacks passively intercept data in transit without changing it	Makes it possible for hackers to access network resources without authorization, jeopardizing network security as a whole.	Encryption, secure protocols, network segmentation, monitoring and IDS/IPS, raise awareness by user education
DoS/DDoS	**DoS:** Makes numerous requests to IoT devices or networks, overloading them to the point where they can't handle legitimate traffic. **DDoS:** Uses multiple compromised devices to flood IoT networks or services, causing a complete shutdown.	IoT devices become inaccessible, disrupting processes or services that depend on them. Uses up device resources (CPU, memory, and bandwidth), which could cause a reboot or device failure.	Traffic filtering and rate limiting, device hardening, and cloud-based protection
Man in the Middle	MitM allows the attacker to take control over a device without the user's knowledge and steal data.	Attackers can alter data packets, resulting in inaccurate actions or judgments based on false information. intercept and misuse sensitive data.	Encryption, authentication, and secure protocols
Botnet attack	From the word robot, the term bot refers to malicious software that is intended to do tasks automatically, typically through the internet.	Network downtime, data theft and privacy breaches, financial losses and reputational damage.	Network monitoring, botnet detection tools, Determine and stop communications from botnets.
Data transit attack	Modification or interception of data while it is being transmitted across networks or between computers.	Privacy violations and data exposure. compromise data integrity Possibility of financial fraud and identity theft.	Encryption, secure communication protocols, network segmentation, monitoring, and access control
Spoofing attack	Manipulate trust mechanisms to trick users or systems.	Unauthorized access and identity theft, fraud and data manipulation, data integrity and availability.	Authentication, packet filtering, network segmentation, real-time monitoring
Sinkhole attack	Change network configurations or routing protocols, to divert traffic.	Intercepting private information, compromising the confidentiality and integrity of the network.	Secure Routing Protocols, Network Monitoring, DNS Security, Management of Vendors
Sybil attack	Rather than directly breaching systems, Sybil attacks take advantage of the construction of numerous identities to trick them.	Falsification of reputation-based systems, Disruption of network functionality, decreased dependability and trust in the impacted systems.	Identity verification, centralized trust authorities, utilize behavior tracking and anomaly detection.
Replay attacks	Concentrate on repurposing intercepted data, instead of taking advantage of holes in hardware or software.	Facilitates access without proper authorization, compromises confidentiality and system integrity, data manipulation and fraudulent transactions	Systems encrypting traffic, using cryptographic authentication, and appending a timestamp to every message segment.
Eavesdropping	Concentrate on observing and interpreting data without changing it while it is in transit.	Compromises the privacy of data, allows financial fraud and identity theft to occur, reveals private business information	Encryption and secure protocols, virtual private networks, network segmentation, physical security, awareness and training.
Side channel attack	Focuses on side channels — unintentional information leaks from hardware or software applications. as opposed to conventional attacks that take use of software flaws.	Leaks confidential data (like cryptographic keys) via visible side channels (such power usage and electromagnetic emissions).	Cryptographic countermeasures, physical security measures, continuous monitoring and detection IDS.

2.2 Intrusion Detection System for IoT

Intrusion Detection System (IDS) makes a high effort to compromise the accessibility, privacy, or truth of reserves [39]. IDS is a hardware or software instrument that collects and analyzes data from different computers or network components to identify security vulnerabilities, including misuse and penetration. Diverse IDS "flavors" identify questionable activity in different ways [39]. In IoT, several types of IDSs, including host, network, protocol-based, application protocol-based, and hybrid IDS. Figure 3 shows the five types of IDS. Table 2 demonstrates a comparison between the key IDSs in terms of the advantages and challenges with the application scenarios.

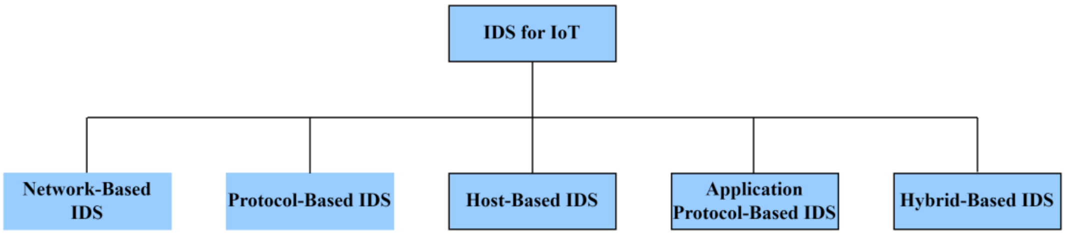


Figure 3. Types of Intrusion Detection Systems for the Internet of Things

Table 2. Comparison between Intrusion Detection Systems

IDSs	Advantages	Challenges	Application Scenarios
Application Protocol-based IDS	1) APIDS is an expert in deciphering and analyzing application-level protocol behaviors. Because of its specificity, it can identify attacks that aim to exploit weaknesses unique to certain protocols. 2) Compared to conventional Network-Based Intrusion Detection Systems, contextual analysis is deeper with APIDS. It can distinguish between typical and anomalous protocol behaviors at the application layer. 3) When compared to generic IDS techniques, APIDS typically has lower false positive rates since it can more precisely distinguish between malicious and authorized activity because it is aware of the expected behavior of particular application protocols.	1) Deep protocol analysis can increase resource usage and latency, particularly in environments that need real-time processing or have a high transaction volume. 2) Analysis of various and intricate application protocols necessitates certain expertise and tools. Creating precise detection methods for every protocol can be difficult and resource-consuming. 3) The efficiency of APIDS depends on rapid updates and modifications in response to changing attack methods and application protocols. Vulnerabilities could be exploited before detection mechanisms can be updated as a result of delayed updates.	1) Monitoring and evaluating HTTP/HTTPS protocols to defend online apps against typical attacks like SQL injection, Cross-Site Scripting (XSS), and command injection. 2) Secure database environments by constantly monitoring SQL protocols for anomalous database requests, SQL injection attacks, and unauthorized access attempts. 3) Improve security in IoT networks by monitoring unique application protocols for IoT devices, including CoAP for IoT communications and MQTT for IoT messaging.
Hybrid IDS	1) Combines various detection methods (e.g., host-based, anomaly-based, network-based, and signature-based) to identify a variety of known and unidentified threats. 2) Hybrid IDS can lower the number of false positives. 3) Provide a better contextual awareness of threats and deeper insights into security issues by connecting events across host and network environments. 4) Able to use various detection techniques and update detection rules and algorithms in response to new and emerging threats, allowing it to adapt and change	1) Increased setup and maintenance costs because of the necessity for constant upgrades and monitoring as well as the integration of numerous IDS technologies. 2) Demands a lot of resources to design, implement, and maintain. These resources include computational power for data IDS technologies. correlation and analysis as well as knowledge of several 3) It can be difficult to integrate several IDS systems and guarantee smooth data correlation and communication between host-based and network components.	1) Protecting extensive corporate networks with a variety of IT systems and applications, where thorough threat detection and reaction capabilities are crucial. 2) Mixing standard network and host-based IDS technology with cloud-specific IDS solutions to improve security in cloud environments. 3) Defending sensors, Industrial Control Systems (ICS) components, and IoT devices from cyberattacks by combining specialist IoT IDS solutions with conventional IDS technologies.
Network IDS	1) Real-time network traffic monitoring makes it possible to quickly identify and respond to insecure activities or possible intrusions. 2) Efficiently identifies threats and external attackers as well as internet-based attacks coming from outside the company's network boundary. 3) Centrally monitors and analyzes network traffic for all systems and devices inside the network perimeter.	1) Limits the ability to detect dangers hidden in encrypted communications since it is unable to decrypt encrypted traffic (HTTPS, TLS, etc.). 2) Tendency to cause false alarms as a result of typical fluctuations in network traffic patterns or normal actions that are misinterpreted for attack activity.	1) Installed in sizable business networks with the purpose of monitoring and safeguarding servers, apps, and vital assets from outside threats and illegal access attempts. 2) Equipped with sensors built into cloud infrastructure to track network traffic between Virtual Machines (VMs) and identify irregularities that could be signs of illegal access or malicious activity. 3) Used to protect Supervisory Control and Data Acquisition (SCADA) systems and Operational Technology (OT) networks against cyber threats in critical infrastructure sectors (such as manufacturing and energy).
Host IDS	1) HIDS offers comprehensive insight into file system modifications, process activity, and user interactions. 2) Efficient in identifying malicious activity and insider threats coming from the network perimeter of the company.	1) Utilize system resources, such as CPU, memory, and disk input/output, to track and examine host activity, which may have an effect on responsiveness and performance. 2) Restricts protection to the host or endpoint where HIDS is installed; hence,	1) Installed to monitor and defend against outside intrusions, malware infections, and insider threats on vital workstations, servers, and endpoints. 2) Designed to be integrated into cloud instances and Virtual Machines (VMs) in order to track host-level activity and

	3) Enables the creation of unique security rules and policies that are adapted to particular host environments, applications, or legal requirements. 4) It is useful in situations with sporadic or restricted network connectivity since it functions independently of network traffic.	for complete coverage, deployment on each individual system is required. 3) Needs constant maintenance, configuration upgrades, and administration to guarantee that HIDS rules and signatures are up to date and effective against changing threats.	identify irregularities that could point to compromised Virtual Machines or illegal access. 3) Deployed on embedded systems and IoT devices to guard against attacks unique to the IoT, identify illegal modifications, and monitor firmware integrity.
Protocol-based IDS	1) Focus on monitoring and analyzing application-specific protocols (such as HTTP, FTP, and SMTP), PIDS offers targeted detection of attacks and vulnerabilities unique to these protocols. 2) Determines whether unusual data payloads or unapproved protocol instructions are signs of an impending attack or other deviations from the typical behaviors of the protocol. 3) Appropriate for systems like web servers, email servers, and database servers where protecting certain application protocols is essential.	1) Restricted efficacy in identifying dangers concealed in encrypted communications (HTTPS, TLS), since PIDS is unable to examine the contents of encrypted payloads. 2) Prone to attacks or evasion strategies that take use of flaws in particular protocol implementations or variances across various applications. 3) Prone to raising false alerts as a result of innocuous actions that mimic harmful patterns or deviations in proper protocol behaviors.	1) Used to scan HTTP/HTTPS traffic for flaws and threats aimed at web applications on web servers and application gateways. 2) Configured to monitor SMTP, POP3, or IMAP protocols for questionable activity, spam attempts, or malicious attachments within email servers or gateways. 3) Used on SFTP or FTP servers to track file transfer protocols and identify attempts to access file systems or upload or download files without authorization.

2.2.1 Application Protocol-Based Intrusion Detection System

An employee or organization may refer to an Application Protocol-Based Intrusion Detection System (APIDS) usually exists in an information middle cluster. Identifies intrusions with the aid of tracking and reading the transmission of application-accurate protocols. For instance, due to the fact the middleware communicates with the Internet server's database, this will apprehend the SQL protocol within the middleware [39].

2.2.2 Hybrid Intrusion Detection System

Combining two or greater intrusion detection methods results in a hybrid packaging detection device. In the context of the hybridized IDS, the mixture of network intelligence and host agent or device data yields a comprehensive view of the network apparatus. When evaluating IDS, it is more practical to use a hybrid detection system [39].

2.2.3 Network Intrusion Detection System

To examine traffic coming from several network devices, Network Intrusion Detection System (NIDS) is put inside the network at a predefined location. Each packet that travels across the network is looked at and it contrasts with a database of known assaults. The administrator will receive a warning if any suspicious activity or intrusion is found. An example of the NIDS places one on a subnet with a firewall installed to check for firewall breach attempts [40].

2.2.4 Host Intrusion Detection System

Operations are conducted on separate hosts for communal appliances. A Host Intrusion Detection System (HIDS) efficiently checks all incoming and outgoing packages from the device and alerts the system administrator upon identifying any suspicious or malicious activity. It takes a shot from documents on the machine right now and compares it with the earlier snapshot. Should the analytical device records be updated or removed, the administrator receives an alert to investigate [40].

2.2.5 Protocol-Based Intrusion Detection System

By accepting the related HTTP protocol and regularly managing the HTTPS protocol stream, the Protocol-Based Intrusion Detection System (PIDS) makes an effort to safeguard the web server. This device has to reside on this interface before right away having access to the internet representation layer to utilize HTTPS as it is not encrypted [40].

2.3 Prior work evaluation

With the increasing need for IoT systems in life, the number of researchers in this field has also increased due to their suffering from the weaknesses of these systems, resulting an increase in attacks.

Many research studies of IDSs are discussed with their challenges in detecting IoT attacks. In 2016, Hodo et al. [41] centered on identifying threats and typical trends within an IoT. The ANN process is tested on a mock IoT. The experimental findings showed that multiple DDoS/DoS attacks may be detected with 99.4% accuracy.

Zarpelão et al. [42] outlined a study of IDS research activities for the Internet of Things and categorized IDSs that have been proposed in the literature based on the following characteristics: validation strategy, security threat, detection mechanism, and IDS installation plan. Several options for each attribute were also covered, along with details of studies that either offer attack detection algorithms for IoT threats that may be included in IDSs or suggest particular IDS schemes for IoT.

In 2017, Chawla [43] developed a unique IDS that looked for security irregularities in IoT networks using Machine Learning techniques. This detection platform facilitated compatibility between several network communication protocols used in IoT and offered security as a service.

In 2019, Jan et al. [44] developed a lightweight attack detection strategy utilizing a supervised Machine Learning-based Support Vector Machine (SVM) to detect an adversary attempting to inject unnecessary data into IoT infrastructure. The simulation effects display that the proposed SVM-based classifier, aided by a combination of three complex capabilities, can perform satisfactorily in phrases of classification accuracy and detection time.

In 2020, Smys et al. [45] proposed an IDS for the IoT community and originated across unique styles of attacks based totally on a hybrid convolutional neural network version. The proposed model is suitable for a wide range of IoT applications. The work was validated and compared with conventional Machine Learning and Deep Learning models. Experimental results demonstrate that the proposed hybrid model is more sensitive to attacks in IoT networks.

Keserwani et al. [46] proposed an IDS to identify various attacks for IoT. A combination of Grey Wolf Optimization (GWO) and Particle Swarm Optimization (PSO) is used to extract relevant IoT network features. The extracted features are fed to a Random Forest (RF) classifier to achieve high attack detection accuracy. The experiments are conducted in the Python programming environment to evaluate the proposed model on KDDCup99, NSL-KDD, and CICIDS-2017 datasets. The proposed GWO-PSO-RF NIDS model achieved an average accuracy of 99.66% for multiclass classification. In 2022, Aldhyani and Alkahtani [47] evaluated an improved EDoS attack detection and mitigation system based on SVM, KNN, RF tree algorithms, and DL, namely CNN and LSTM.

In 2023, Kerrakchou et al. [48] established a framework for botnet classification on networks designed for IoT. Table 3 presents an in-depth analysis of every relevant work. The review provides an overview of each study concerning the layer, attack type, and dataset types.

Table 3. List of dataset types along with attack's type with its corresponding layer in IoT-based DL

Ref.	Type of Dataset	Attack Type	Layer
[45]	UNSW-NB15	Different types of attacks	Network layer
[46]	KDDCup99, NSL–KDD, CICIDS-2017	Identify various attacks	Various layers
[47]	UNSW -NB	EDoS	Cloud computing
[48]	BoT-IoT	Botnet	Network layer
[49]	Cyber-physical subsystem, KDD	Distinguish malicious acts from non-malicious ones	Application and network layer
[50]	CICIDS2017, NSL-KDD	DDoS	Network layer
[51]	CIC-IDS-2017	DoS, DDoS, port scan, brute force, web-attack, botnet, infiltration, heartbleed	Application and network layer
[52]	Collected from Kaggle	Probe, DoS, R2L, U2R	Network layer
[53]	KDD Cup, LAN, Cloud	DDoS	Network layer
[54]	NSL-KDD	Cyber-attacks	Network layer
[55]	Real car-hacking data	Attack messages sent on a Controller Area Network (CAN) bus	Network layer
[56]	ToN_IoT, UNSW NB-15	Data poisoning	Application layer
[57]	CSE-CIC-IDS2018	DoS, Bot, Web, brute force	Application and network layer
[58]	UNSW-NB 15	Predict and detect attacks in cyberspace	Network layer
[59]	KDD99	Different attacks	Various layers
[60]	CSE-CIC IDS-2018, UNSW-NB15, ISCX-2012, NSL-KDD, CIDDS-001	Detect attack traffic	Network layer
[61]	ToN-IoT	Detect various attacks	Various layers
[62]	UNSW-NB15, BoT-IoT	DoS, DDoS, worms	Application and network layer
[63]	ToN-IoT	DDoS, ransomware, password	Application and network layer
[64]	SWaT	Detect anomalous behaviors	Application layer
[65]	ToN-IoT, Edge-IIoT, UNSW2015	Malware	Application layer
[66]	ToN-IoT, BoT-IoT	DDoS	Network layer
[67]	ToN-IoT	DoS, DDoS, MITM, information theft, and gateways attacks	Network layer
[68]	ToN-IoT, SWaT, CICIDS2017	Detect attacks in IoT environments	All layer
[69]	IoTID20, IoT23, N-BaIoT	Securing IoT edge computing	Network layer
[70]	X-IIoTID	Adversarial attacks	Network layer
[71]	BoT-IoT, ToN-IoT	MITM, password, injection, backdoor, ransomware, DoS, DDoS, Scanning, reconnaissance, XSS, and theft attack	Application and network layer
[72]	Data Kaspersky	Blackhole	Network layer
[73]	UNSW-NB15	Detect cyberattacks effectively at the edge of the IoT network	Application and network layer
[74]	IDS2017	Monitor network traffic and identify suspicious or malicious activities	Network layer
[75]	NSL-KDD, AWID, BoT-IoT	Identify and mitigate cyber-attacks and malicious events	Application and network layer
[76]	CICIDS2017, MQTT-IDS-2020	Predict and prevent network attacks in real-time before they cause any more damage to the system under attack	Application and network layer
[77]	Edge_IIoT	Identify the patterns in collected data, and detect the malicious traffic corresponding to attacks	Application layer
[78]	NSL-KDD, real-world	Detection of the minority malicious actions	Application layer
[79]	Fraud detection	DDoS	Network layer
[80]	CICIDS2017, NSL-KDD, KDDCup99, UNSW-NB15, BoT-IoT	Classify the intrusion from IoT data	Application layer
[81]	CICIDSS2017	DDoS	Network layer
[82]	NSL-KDD, KDD CUP 99, CICIDS 2017	To protect the data privacy of the agents	Application layer
[83]	ToN-IoT, BoT-IoT	DoS, DDoS, reconnaissance, information theft	Network layer
[84]	NSL-KDD, UNSW-NB15	Malware and ransomware	Application layer

Figure 4 summarizes the studies of the most attack types. Table 4 provides a thorough analysis of methods concerning feature selection methodology and the classifier type. Since there are numerous efficient classifier algorithms, one can select the optimal classification method based on factors such as low latency and high accuracy.

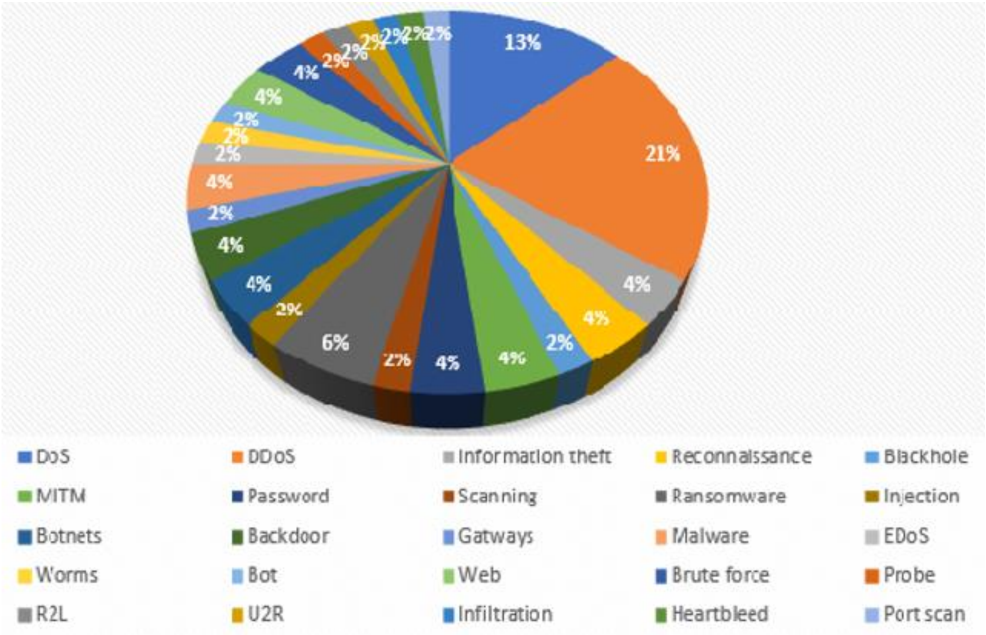


Figure 4. The ratio of most attack types

Table 4. A summary of achieved accuracy along with the applied feature selection approach

Classifier Type	Accuracy	Feature Selection Approach
CNN [45]	98.6%	No
GWO–PSO–RF [46]	99.66%	Grey Wolf Optimization (GWO) and Particle Swarm Optimization (PSO)
SVM, KNN, RF, CNN, LSTM [47]	99% for binary classification 98.27% for multi-classification	Correlation algorithms, with a threshold value of 50%
RF, GB, DT, ANN, naïve bayes, LR [48]	99.99%	No
GRNN, PNN, RBNN, FFNN, ENN and pattern recognition networks [49]	99.8% for binary classification, 44.4% for multi-classification	No
AE+DNN [50]	98.92%	No
PCA, isolation forest, one-class SVM, auto-encoder [51]	100%	No
XGBoost [52]	99%	PCA algorithm
DT, KNN, naive bayes and DNN [53]	-	No
IoT-IDCS-CNN [54]	99.3%	No
Unsupervised Korhonen Self-Organizing Map (SOM) network [55]	-	No
GBM, RF, naive bayes, feed-forward DNN [56]	-	No
DFFM, SRBMM, GRUM, LSTMM [57]	100%	No
DT [58]	98%	No
LSTM [59]	99.49%	Principal Component Analysis (PCA) and Mutual Information (MI)
DT, KNN, SVM [60]	100% for DT, 99.6% for KNN, 99.8% for SVM	No
ResNet, EfficientNet [61]	-	No
LBDMIDS [62]	99.9%	No
XGBoost [63]	99% for binary classification 98.3% for multi-classification	Chi2 technique
Hybrid anomaly detection [64]	-	No
DenseNet, inception time [65]	100%	No
LR, RF, naïve bayes, ANN, KNN [66]	100%	Extra tree classifier
RF, ET, KNN, SVC stacking method [67]	98.63%	Mutual Information (MI), Pearson Coefficient Correlation (PCC), K-Best feature
DIS-IoT [68]	99.6% for binary classification 99.7% for multi-classification	No
DNN, CNN, LSTM [69]	99%	No
Robust Layered Defense (ROLDEF) [70]	-	No
CNN [71]	99.8%	Kernel Principal Component Analysis (KPCA)

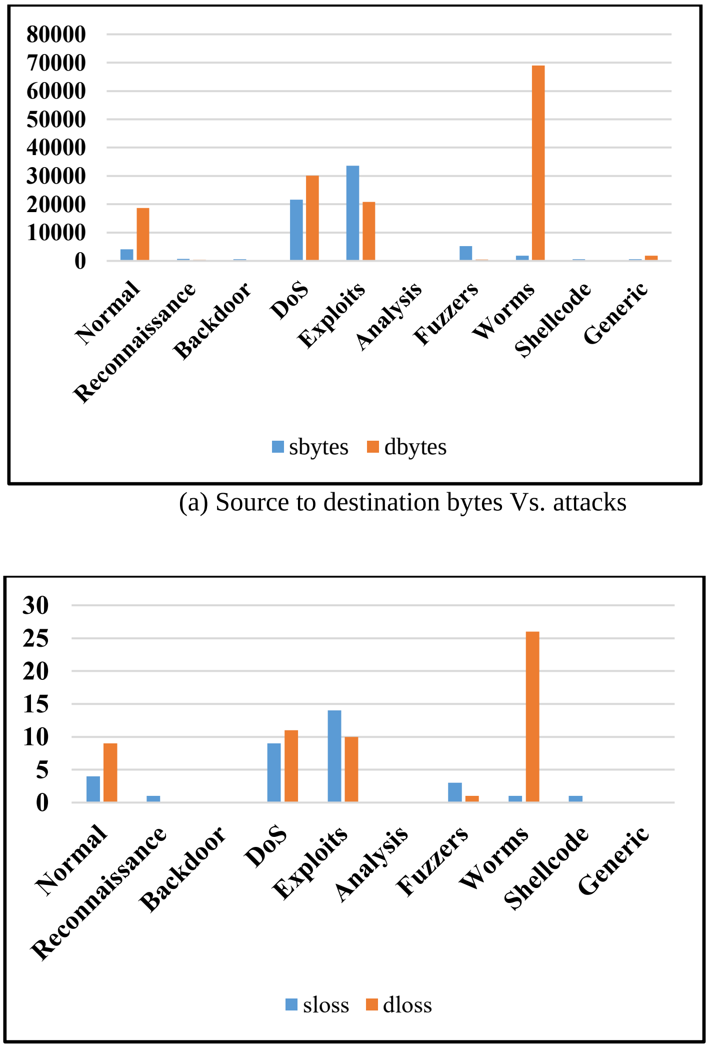
Classifier Type	Accuracy	Feature Selection Approach
Deep Learning ResNet50 [72]	99%	No
RF, LightGBM, ANN, DT, KNN, XGBoost [73]	-	ANOVA and embedded feature selection techniques
CNN [74]	-	PCA, autoencoder, and Random Forest techniques
FCM-SWA [75]	98.82%	Maximum Correntropy Criterion (MCC)
EARLYCNN, EARLYRNN [76]	89%	No
DTL and GA [77]	100%	No
CNN-GRU [78]	-	No
SVM, RF, KNN [79]	99.85%	No
KNN, AR-PDTN [80]	99.8%	No
CNN, GRU [81]	99.7%	No
EFedID [82]	97.3%	No
CNN [83]	99%	No
Cascaded long-short-term memory [84]	98.96%	Recursive feature elimination, information gain

3. RESULT AND DISCUSSION

Ensuring an entirely secure IoT is still a challenging issue that may impede the full integration of IoT applications into everyday life. There are many unresolved problems and obstacles are impending to a more secure IoT, which offers excellent research opportunities. The literature's top accuracy claims were made by a few studies [51, 57, 65, 66, 77]. We notice that the network layer of an IoT system is considered to be certainly one of its most susceptible layers. Figure 5 illustrates the impact of attacks on the performance of network traffic. The statistic was achieved on the UNSW_NB15 dataset [85], which includes the most parameters that affect the network traffic [86]. We can calculate the average value of all values of each metric for a certain attack category using the following procedure. Let M represents a set of metrics, C represents a set of attack categories, the mean is the average of the values for an element from M for a given attack category from C which can be calculated in the following expression.

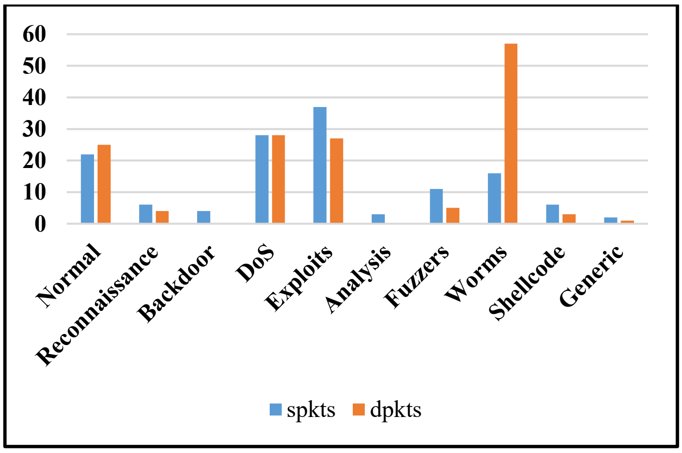
$$mean_{mc} = \frac{1}{N_{mc}} \sum_{i=1}^{N_{mc}} x_{imc} \;\; \forall\, m \in M, c \in C \tag{1}$$

where, N_{mc} = number of elements in the series of m-th metric and c-th attack, x_{imc} = i-th element in the series of m-th metric and c-th attack.



(a) Source to destination bytes Vs. attacks

(b) Loss of network data Vs. attacks



(c) Packet count Vs. attacks

Figure 5. The impact of attacks on the network traffic

In Figure 5, it can be noticed the most important metrics are to be monitored when analyzing network intrusion detection datasets by considering them along with the attack categories' expected behaviors. First, it has to define categories to estimate the possible behavior, as shown in Table 5.

Table 5. Types of attack for UNSW-NB15 dataset

Attack Type	Description
Normal	Natural transaction data.
Fuzzers	Providing randomly generated data to a program or network in an attempt to cause it to be suspended.
Analysis	It includes several port-scan, spam, and HTML file penetration attacks.
Backdoors	A method of secretly getting around a system security measure to access a computer or its contents.
DoS	A deliberate attempt to prevent unauthorized individuals from accessing a server or network resource, usually by momentarily stopping or disrupting the operations of a host that is connected to the Internet.
Exploits	When an operating device or piece of software has a safety flaw, the attacker takes advantage of that information using taking gain of the vulnerability.
Generic	A method is effective against all block ciphers (with a specified block and key size) regardless of the block cipher's structure.
Reconnaissance	Includes every strike that can be used to mimic information-gathering strikes.
Shellcode	A short code segment that is the payload for software vulnerability exploitation.
Worms	The attacker multiplies itself so that it can infect further systems. It frequently spreads over a computer network, taking advantage of holes in the target computer's security to gain access.

Table 6 illustrates a brief definition of the basic features that are utilized in this statistic.

Table 6. Definition of basic features

Name	Description
sbytes	Source to destination bytes
dbytes	Destination to source bytes
sloss	Source packets retransmitted or dropped
dloss	Destination packets retransmitted or dropped
spkts	Source to destination packet count
dpkts	Destination to source packet count

It is worth stating that the following assumption is considered for all plots, the sender will be the client (in case of normal activity) or attacker (in case of abnormal, suspicious, malicious activities) and the destination will be the server (web, application, database, domain, SMS, etc.) or any targeted device.

Thus, for Figure 5(a), the normal activity will include the usual number of bytes required for requesting, data entry, query, etc., and responding. Reconnaissance usually does not require a big exchange. Backdoor attacks are used usually by hardware manufacturers or by application developers and may not require any exchange bytes because of previous knowledge. DoS requires sending a lot of bytes to consume the resources of the server when responding. Exploiting needs bytes to detect vulnerabilities in software applications installed on the server. Analysis attacks usually attack is conducted to gather rough information about the victim device, while the Fuzzer requires more bytes to figure out the vulnerabilities but fewer bytes as a return just to spoil device functionalities. Worm code itself doesn't need to be big but its response needs. shell code is lightweight in both directions. genetic attacks may involve many unclassified types of attacks and there is no specific rule determining their behavior, but there are several factors that specify their exchange amount like the server's main purpose, and territory.

For Figure 5(b), both the sloss and the dloss represent packet loss at the sender and the destination sides, respectively, so at normal activities, these metrics stay in a reasonable range. While in inspection, there will be little loss in both directions because of the original little exchange. The same is true for the backdoor. More For both Dos and Exploits because of their exchange. Lack of loss for analysis due to its required exchange quantity. As expected, the same is true for Fuzzer, exchange also determines the loss ratio. Shellcode, generics, and worms are not exceptions. The last two plots in Figure 5(c), which represent outline packet counts between sender and receiver, can be respected as a scaled representation of the first two plots because of their packet nature, which is a container for several bytes, including network protocol headers.

4. CONCLUSION

IoT has become an important topic in recent years. The IoT has numerous challenges, including significant security and privacy issues, much like other cutting-edge technologies. The operation of the Internet of Things' four layers — perception, network, processing, and application layers are investigated. In summary, it can be concluded that the DDoS attack type is the most common attack, as well as the network layer of an IoT system, can be considered one of its most susceptible layers according to Table 3. From Table 4, it can be noticed that the accuracy of Deep Learning algorithms exceeds 98% compared with traditional methods, so it can be observed that DL algorithms are effective in detecting and classifying the attack types due to their high accuracy and ability to identify complex patterns in IoT data. However, rarely do researchers focus on computational complexity the applied algorithms. Future direction includes proposing a hybrid deep-learning model to classify attacks in real-time IoT systems with high accuracy, less processing time, and minimizing computational complexity. An overview of IDSs for IoT contexts has been provided in this review. Other upsides have included suggestions for creating a reliable and lightweight Intrusion Detection System.

REFERENCES

[1] Al Hasan, R.A., Hamza, E.K. (2023). An improved intrusion detection system using machine learning with singular value decomposition and principal component analysis. International Journal of Intelligent Engineering & Systems, 16(4): 25-38. https://doi.org/10.22266/ijies2023.0831.03

[2] Oudah, M.S., Maolood, A.T. (2022). New pseudo-random key generator for IoT-security model based on a novel 3D coupled map lattice. International Journal of Intelligent Engineering & Systems, 15(5): 139-150. https://doi.org/10.22266/ijies2022.1031.13

[3] Tyagi, H., Kumar, R., Pandey, S.K. (2023). A detailed study on trust management techniques for security and privacy in IoT: Challenges, trends, and research directions. High-Confidence Computing, 3(2): 100127. https://doi.org/10.1016/j.hcc.2023.100127

[4] Mohammed, R.A., Khodher, M.A.A.A., Alabaichi, A. (2023). Image encryption in IoT using hyper-chaotic system. International Journal of Intelligent Engineering & Systems, 16(6): 101-112. https://doi.org/10.22266/ijies2023.1231.09

[5] Zhilenkov, A.A., Gilyazov, D.D., Matveev, I.I., Krishtal, Y.V. (2017). Power line communication in IoT-systems. In 2017 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), St. Petersburg and Moscow, Russia, pp. 242-245. https://doi.org/10.1109/EIConRus.2017.7910538

[6] Hussein, A.Y., Falcarin, P., Sadiq, A.T. (2021). Enhancement performance of random forest algorithm via one hot encoding for IoT IDS. Periodicals of Engineering and Natural Sciences, 9(3): 579-591. https://doi.org/10.21533/pen.v9i3.2204

[7] Patel, K.K., Patel, S.M., Scholar, P. (2016). Internet of Things-IOT: Definition, characteristics, architecture, enabling technologies, application & future challenges. International Journal of Engineering Science and Computing, 6(5): 6122-6131. https://doi.org/10.4010/2016.1482

[8] Alsumaidaie, M.S.I., Alheeti, K.M.A., Al-Aloosy, A.K. (2023). Intelligent detection system for a Distributed Denial-of-Service (DDoS) attack based on time series. In 2023 15th International Conference on Developments in eSystems Engineering (DeSE), Baghdad & Anbar, Iraq, pp. 445-450. https://doi.org/10.1109/DeSE58274.2023.10100180

[9] Hussein, M.A., Hamza, E.K. (2022). Secure mechanism applied to big data for IIoT by using security event and information management system (SIEM). International Journal of Intelligent Engineering & Systems, 15(6): 667-681. https://doi.org/10.22266/ijies2022.1231.59

[10] Cains, M.G., Flora, L., Taber, D., King, Z., Henshel, D.S. (2022). Defining cyber security and cyber security risk within a multidisciplinary context using expert elicitation. Risk Analysis, 42(8): 1643-1669. https://doi.org/10.1111/risa.13687

[11] Fadhil, M.S., Farhan, A.K., Fadhil, M.N. (2021). A lightweight AES algorithm implementation for secure IoT environment. Iraqi Journal of Science, 62(8): 2759-2770. https://doi.org/10.24996/ijs.2021.62.8.29

[12] Naser, S.M., Ali, Y.H., Obe, D.A.J. (2022). Hybrid cyber-security model for attacks detection based on deep and machine learning. International Journal of Online & Biomedical Engineering, 18(11): 17-30. https://doi.org/10.3991/ijoe.v18i11.33563

[13] Mohammed, M.A., Abdul Wahab, H.B. (2023). Decentralized IoT system based on blockchain and homomorphic technologies. Iraqi Journal of Computers, Communications, Control and Systems Engineering, 23(3): 26-38. https://doi.org/10.33103/uot.ijccce.23.3.3

[14] Jassim, S.A., Farhan, A.K. (2022). Designing a new lightweight AES algorithm to improve the security of the IoT environment. Iraqi Journal of Computers, Communications, Control and Systems Engineering, 22(2): 96-108. https://doi.org/10.33103/uot.ijccce.22.2.9

[15] Hussein, A.Y., Sadiq, A.T. (2022). Meerkat clan-based feature selection in random forest algorithm for IoT intrusion detection. Iraqi Journal of Computers, Communications, Control and Systems Engineering, 22(3): 15-24. https://doi.org/10.33103/uot.ijccce.22.3.2

[16] Mhawi, D.N., Hashem, S.H. (2022). Proposed hybrid ensemble learning algorithms for an efficient intrusion detection system. Iraqi Journal of Computers, Communications, Control and Systems Engineering, 22(2): 73-84. https://doi.org/10.33103/uot.ijccce.22.2.7

[17] Hashem, S.H. (2014). Proposed integrated wire/wireless network intrusion detection system. Iraqi Journal of Computers, Communications, Control and Systems Engineering, 14(2): 9-24.

[18] Shewale, Y., Kumar, S., Banait, S. (2023). Machine learning based intrusion detection in IoT network using MLP and LSTM. International Journal of Intelligent Systems and Applications in Engineering, 11(7s): 210-223.

[19] Zhang, Y., Li, P., Wang, X. (2019). Intrusion detection for IoT based on improved genetic algorithm and deep belief network. IEEE Access, 7: 31711-31722. https://doi.org/10.1109/ACCESS.2019.2903723

[20] Nasser, A.R., Mahmood, A.M. (2021). Cloud-based Parkinson's disease diagnosis using machine learning. Mathematical Modelling of Engineering Problems, 8(6): 915-922. https://doi.org/10.18280/mmep.080610

[21] Nasser, A.R., Hasan, A.M., Humaidi, A.J. (2024). DL-AMDet: Deep learning-based malware detector for android. Intelligent Systems with Applications, 21: 200318. https://doi.org/10.1016/j.iswa.2023.200318

[22] Ahemd, M.M., Shah, M.A., Wahid, A. (2017). IoT security: A layered approach for attacks & defenses. In 2017 International Conference on Communication Technologies (ComTech), Rawalpindi, Pakistan, pp. 104-110. https://doi.org/10.1109/COMTECH.2017.8065757

[23] Sengupta, J., Ruj, S., Bit, S.D. (2020). A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT. Journal of Network and Computer Applications, 149: 102481. https://doi.org/10.1016/j.jnca.2019.102481

[24] Falayi, A., Wang, Q., Liao, W., Yu, W. (2023). Survey of distributed and decentralized IoT securities: Approaches using deep learning and blockchain technology. Future Internet, 15(5): 178. https://doi.org/10.3390/fi15050178

[25] Tewari, A., Jain, A.K., Gupta, B.B. (2016). Recent survey of various defense mechanisms against phishing attacks. Journal of Information Privacy and Security, 12(1): 3-13. https://doi.org/10.1080/15536548.2016.1139423

[26] Bairagi, V.K., Joshi, S.L., Barshikar, S.H. (2018). A survey on Internet of Things. International Journal of Computer Sciences and Engineering, 6(12): 492-496. https://doi.org/10.26438/ijcse/v6i12.492496

[27] Thakur, B.S., Chaudhary, S. (2013). Content sniffing attack detection in client and server side: A survey. International Journal of Advanced Computer Research, 3(10): 7-10. https://www.proquest.com/scholarly-journals/content-sniffing-attack-detection-client-server/docview/1444152627/se-2.

[28] Yaseen, H.S., Al-Saadi, A. (2023). Q-learning based distributed denial of service detection. International Journal of Electrical and Computer Engineering, 13(1): 972-986. https://doi.org/10.11591/ijece.v13i1.pp972-986

[29] Khudhur, D.D., Croock, M.S. (2021). Developed security and privacy algorithms for cyber physical system. International Journal of Electrical and Computer Engineering, 11(6): 5379-5389. https://doi.org/10.11591/ijece.v11i6.pp5379-5389

[30] Yihunie, F., Abdelfattah, E., Odeh, A. (2018). Analysis of ping of death DoS and DDoS attacks. In 2018 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, USA, pp. 1-4. https://doi.org/10.1109/LISAT.2018.8378010

[31] Hammood, B.A.K., Sadiq, A.T. (2023). Ensemble machine learning approach for IoT intrusion detection systems. Iraqi Journal for Computers and Informatics, 49(2): 93-99. http://doi.org/10.25195/ijci.v49i2.458

[32] Perwej, Y., Parwej, F., Hassan, M.M.M., Akhtar, N. (2019). The Internet-of-Things (IoT) security: A technological perspective and review. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 5(1): 462-482.

[33] Ali, I., Ahmed, A.I.A., Almogren, A., Raza, M.A., Shah, S.A., Khan, A., Gani, A. (2020). Systematic literature review on IoT-based botnet attack. IEEE Access, 8: 212220-212232. https://doi.org/10.1109/ACCESS.2020.3039985

[34] Muin, Y., Khairan, A. (2023). Improved accuracy for forensic investigation using SIFT-based copy-move forgery detection. JATISI (Jurnal Teknik Informatika dan Sistem Informasi), 10(4). https://doi.org/10.35957/jatisi.v10i4.6509

[35] Mitrokotsa, A., Rieback, M.R., Tanenbaum, A.S. (2010). Classifying RFID attacks and defenses. Information Systems Frontiers, 12: 491-505. https://doi.org/10.1007/s10796-009-9210-z

[36] Islam, M.R., Aktheruzzaman, K.M. (2020). An analysis of cybersecurity attacks against Internet of Things and security solutions. Journal of Computer and Communications, 8(4): 11-25. https://doi.org/10.4236/jcc.2020.84002

[37] Alkhamisi, K. (2023). An analysis of security attacks on IoT applications. International Journal of Information Systems and Computer Technologies, 2(1): 44-49. https://doi.org/10.58325/ijisct.002.01.0053

[38] Abrishamchi, M.A.N., Abdullah, A.H., Cheok, A.D., Bielawski, K.S. (2017). Side channel attacks on smart home systems: A short overview. In IECON 2017 – 43rd Annual Conference of the IEEE Industrial Electronics Society, Beijing, China, pp. 8144-8149. https://doi.org/10.1109/IECON.2017.8217429

[39] Swarnkar, M., Rajput, S.S. (2023). Artificial Intelligence for Intrusion Detection Systems. CRC Press, Boca Raton, Florida. https://doi.org/10.1201/9781003346340

[40] Sunagar, P.C., Kanavalli, A. (2022). Intrusion detection system using deep learning. In: Deep Learning Applications for Cyber-Physical Systems. IGI Global, Hershey, Pennsylvania, pp. 160-181. https://doi.org/10.4018/978-1-7998-8161-2.ch009

[41] Hodo, E., Bellekens, X., Hamilton, A., Dubouilh, P.L., Iorkyase, E., Tachtatzis, C., Atkinson, R. (2016). Threat analysis of IoT networks using artificial neural network intrusion detection system. In 2016 International Symposium on Networks, Computers and Communications (ISNCC), Yasmine Hammamet, Tunisia, pp. 1-6. https://doi.org/10.1109/ISNCC.2016.7746067

[42] Zarpelão, B.B., Miani, R.S., Kawakani, C.T., De Alvarenga, S.C. (2017). A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications, 84: 25-37. https://doi.org/10.1016/j.jnca.2017.02.009

[43] Chawla, S. (2017). Deep learning based intrusion detection system for Internet of Things. Ph.D. dissertation. University of Washington, Seattle, WA. http://hdl.handle.net/1773/39829.

[44] Jan, S.U., Ahmed, S., Shakhov, V., Koo, I. (2019). Toward a lightweight intrusion detection system for the Internet of Things. IEEE Access, 7: 42450-42471. https://doi.org/10.1109/ACCESS.2019.2907965

[45] Smys, S., Basar, A., Wang, H. (2020). Hybrid intrusion detection system for Internet of Things (IoT). Journal of ISMAC, 2(4): 190-199. https://doi.org/10.36548/jismac.2020.4.002

[46] Keserwani, P.K., Govil, M.C., Pilli, E.S., Govil, P. (2021). A smart anomaly-based intrusion detection system for the Internet of Things (IoT) network using GWO–PSO–RF model. Journal of Reliable Intelligent Environments, 7(1): 3-21. https://doi.org/10.1007/s40860-020-00126-x

[47] Aldhyani, T.H., Alkahtani, H. (2022). Artificial intelligence algorithm-based economic denial of sustainability attack detection systems: Cloud computing environments. Sensors, 22(13): 4685. https://doi.org/10.3390/s22134685

[48] Kerrakchou, I., Abou El Hassan, A., Chadli, S., Emharraf, M., Saber, M. (2023). Selection of efficient machine learning algorithm on Bot-IoT dataset for intrusion detection in Internet of Things networks. Indonesian Journal of Electrical Engineering and Computer Science, 31(3): 1784-1793. https://doi.org/10.11591/ijeecs.v31.i3.pp1784-1793

[49] Albahar, M.A., Al-Falluji, R.A., Binsawad, M. (2020). An empirical comparison on malicious activity detection using different neural network-based models. IEEE Access, 8: 61549-61564. https://doi.org/10.1109/ACCESS.2020.2984157

[50] Bhardwaj, A., Mangat, V., Vig, R. (2020). Hyperband tuned deep neural network with well posed stacked sparse autoencoder for detection of DDoS attacks in cloud. IEEE Access, 8: 181916-181929. https://doi.org/10.1109/ACCESS.2020.3028690

[51] Verkerken, M., D'hooge, L., Wauters, T., Volckaert, B., De Turck, F. (2020). Unsupervised machine learning techniques for network intrusion detection on modern data. In 2020 4th Cyber Security in Networking Conference (CSNet), Lausanne, Switzerland, pp. 1-8. https://doi.org/10.1109/CSNet50428.2020.9265461

[52] Bhattacharya, S., Maddikunta, P.K.R., Kaluri, R., Singh, S., Gadekallu, T.R., Alazab, M., Tariq, U. (2020). A novel PCA-firefly based XGBoost classification model for intrusion detection in networks using GPU. Electronics, 9(2): 219. https://doi.org/10.3390/electronics9020219

[53] Virupakshar, K.B., Asundi, M., Channal, K., Shettar, P., Patil, S., Narayan, D.G. (2020). Distributed denial of service (DDoS) attacks detection system for OpenStack-based private cloud. Procedia Computer Science, 167: 2297-2307. https://doi.org/10.1016/j.procs.2020.03.282

[54] Abu Al-Haija, Q., Zein-Sabatto, S. (2020). An efficient deep-learning-based detection and classification system for cyber-attacks in IoT communication networks. Electronics, 9(12): 2152. https://doi.org/10.3390/electronics9122152

[55] Barletta, V.S., Caivano, D., Nannavecchia, A., Scalera, M. (2020). Intrusion detection for in-vehicle communication networks: An unsupervised Kohonen SOM approach. Future Internet, 12(7): 119. https://doi.org/10.3390/fi12070119

[56] Dunn, C., Moustafa, N., Turnbull, B. (2020). Robustness evaluations of sustainable machine learning models against data poisoning attacks in the Internet of Things. Sustainability, 12(16): 6434. https://doi.org/10.3390/SU12166434

[57] Atefinia, R., Ahmadi, M. (2021). Network intrusion detection using multi-architectural modular deep neural network. The Journal of Supercomputing, 77(4): 3571-3593. https://doi.org/10.1007/s11227-020-03410-y

[58] Al-Omari, M., Rawashdeh, M., Qutaishat, F., Alshira'H, M., Ababneh, N. (2021). An intelligent tree-based intrusion detection model for cyber security. Journal of Network and Systems Management, 29(2): 20. https://doi.org/10.1007/s10922-021-09591-y

[59] Laghrissi, F., Douzi, S., Douzi, K., Hssina, B. (2021). Intrusion detection systems using long short-term memory (LSTM). Journal of Big Data, 8(1): 65. https://doi.org/10.1186/s40537-021-00448-4

[60] Kilincer, I.F., Ertam, F., Sengur, A. (2021). Machine learning methods for cyber security intrusion detection: Datasets and comparative study. Computer Networks, 188: 107840. https://doi.org/10.1016/j.comnet.2021.107840

[61] Kodyš, M., Lu, Z., Fok, K.W., Thing, V.L. (2021). Intrusion detection in Internet of Things using convolutional neural networks. In 2021 18th International Conference on Privacy, Security and Trust (PST), Auckland, New Zealand, pp. 1-10. https://doi.org/10.1109/PST52912.2021.9647828

[62] Saurabh, K., Sood, S., Kumar, P.A., Singh, U., Vyas, R., Vyas, O.P., Khondoker, R. (2022). LBDMIDS: LSTM based deep learning model for intrusion detection systems for IOT networks. In 2022 IEEE World AI IoT Congress (AIIoT), Seattle, WA, USA, pp. 753-759. https://doi.org/10.1109/AIIoT54504.2022.9817245

[63] Gad, A.R., Haggag, M., Nashat, A.A., Barakat, T.M. (2022). A distributed intrusion detection system using machine learning for IoT based on ToN-IoT dataset. International Journal of Advanced Computer Science and Applications, 13(6): 548-563. https://doi.org/10.14569/IJACSA.2022.0130667

[64] Kwon, H.Y., Kim, T., Lee, M.K. (2022). Advanced intrusion detection combining signature-based and behavior-based detection methods. Electronics, 11(6): 867. https://doi.org/10.3390/electronics11060867

[65] Tareq, I., Elbagoury, B.M., El-Regaily, S., El-Horbaty, E.S.M. (2022). Analysis of ToN-IoT, UNW-NB15, and edge-IIoT datasets using DL in cybersecurity for IoT. Applied Sciences, 12(19): 9572. https://doi.org/10.3390/app12199572

[66] Sadhwani, S., Manibalan, B., Muthalagu, R., Pawar, P. (2023). A lightweight model for DDoS attack detection using machine learning techniques. Applied Sciences, 13(17): 9937. https://doi.org/10.3390/app13179937

[67] Alotaibi, Y., Ilyas, M. (2023). Ensemble-learning framework for intrusion detection to enhance Internet of Things' devices security. Sensors, 23(12): 5568. https://doi.org/10.3390/s23125568

[68] Lazzarini, R., Tianfield, H., Charissis, V. (2023). A stacking ensemble of deep learning models for IoT intrusion detection. Knowledge-Based Systems, 279: 110941. https://doi.org/10.1016/j.knosys.2023.110941

[69] Fenanir, S., Semchedine, F. (2023). Smart intrusion detection in IoT edge computing using federated learning. Revue d'Intelligence Artificielle, 37(5): 1133-1145. https://doi.org/ 10.18280/ria.370505

[70] Gungor, O., Rosing, T., Aksanli, B. (2024). ROLDEF: RObust layered DEFense for intrusion detection against adversarial attacks. In 2024 Design, Automation & Test in Europe Conference & Exhibition (DATE), Valencia, Spain, pp. 1-6. https://doi.org/10.23919/DATE58400.2024.10546886

[71] Gaber, T., Awotunde, J.B., Torky, M., Ajagbe, S.A., Hammoudeh, M., Li, W. (2023). Metaverse-IDS: Deep learning-based intrusion detection system for Metaverse-IoT networks. Internet of Things, 24: 100977. https://doi.org/10.1016/j.iot.2023.100977

[72] Salama, R., Alghamdi, W., Yadav, S., Pallathadka, H., Manoharmayum, D.D., Tiwari, M. (2023). Exploring machine learning methods for IoT network intrusion detection systems. Journal of Advanced Zoology, 44(S5): 1045-1053. https://doi.org/10.17762/jaz.v44is-5.1089

[73] Li, D., Majd, N.E. (2023). Intrusion detection in IoT

leveraged by multi-access edge computing using machine learning. In 2023 IEEE International Performance, Computing, and Communications Conference (IPCCC), Anaheim, CA, USA, pp. 441-446. https://doi.org/10.1109/IPCCC59175.2023.10253831

[74] Zou, Y., Liu, C. (2023). A light-weight object detection method based on knowledge distillation and model pruning for seam tracking system. Measurement, 220: 113438. https://doi.org/10.1016/j.measurement.2023.113438

[75] Elsedimy, E.I., AboHashish, S.M.M. (2023). FCM-SWA: Hybrid intelligent approach combining fuzzy C-means and sperm whales algorithm for cyber-attack detection in IoT networks. Available at Research Square. https://doi.org/10.21203/rs.3.rs-3515647/v1

[76] Ahmad, T., Truscan, D., Vain, J. (2023). EARLY: A tool for real-time security attack detection. In: Sadovykh, A., Truscan, D., Mallouli, W., Cavalli, A.R., Seceleanu, C., Bagnato, A. (eds) CyberSecurity in a DevOps Environment. Springer, Cham, pp. 225-251. https://doi.org/10.1007/978-3-031-42212-6_8

[77] Latif, S., Boulila, W., Koubaa, A., Zou, Z., Ahmad, J. (2024). DTL-IDS: An optimized intrusion detection framework using deep transfer learning and genetic algorithm. Journal of Network and Computer Applications, 221: 103784. https://doi.org/10.1016/j.jnca.2023.103784

[78] Chen, Y., Al-Rubaye, S., Tsourdos, A., Baker, L., Gillingham, C. (2023). Differentially-private federated intrusion detection via knowledge distillation in third-party IoT systems of smart airports. In ICC 2023 – IEEE International Conference on Communications, Rome, Italy, pp. 603-608. https://doi.org/10.1109/ICC45041.2023.10279722

[79] Mohammed, B.H., Sallehudin, H., Safie, N., Satar, M., Murhg, H.D., Mohamed, S.A. (2023). Anomaly detection of distributed denial of service (DDoS) in IoT network using machine learning, pp. 1-27. Available at Research Square. https://doi.org/10.21203/rs.3.rs-3496063/v1

[80] VemulapallI, L., Sekhar, P.C. (2023). An intelligent cybersecurity model for IoT networks using adversarially regularized parallel deep transfer network. Journal of Theoretical and Applied Information Technology, 101(20): 6444-6459. https://www.jatit.org/volumes/Vol101No20/19Vol101No20.pdf.

[81] Diaba, S.Y., Elmusrati, M. (2023). Proposed algorithm for smart grid DDoS detection based on deep learning. Neural Networks, 159: 175-184. https://doi.org/10.1016/j.neunet.2022.12.011

[82] He, N.X., Zhang, Z.H., Wang, X.T., Gao, T.G. (2023). Efficient privacy-preserving federated deep learning for network intrusion of industrial IoT. International Journal of Intelligent Systems, 2023(1): 2956990. https://doi.org/10.1155/2023/2956990

[83] Varshney, S., Shikha, Singhi, S., Sharma, B. (2021). Intelligent intrusion detection system using deep learning models. In 2021 5th International Conference on Trends in Electronics and Informatics (ICOEI), Tirunelveli, India, pp. 787-793. https://doi.org/10.1109/ICOEI51242.2021.9452880

[84] Sundaram, K., Natarajan, Y., Perumalsamy, A., Yusuf Ali, A.A. (2024). A novel hybrid feature selection with cascaded LSTM: Enhancing security in IoT networks. Wireless Communications and Mobile Computing, 2024(1): 5522431. https://doi.org/10.1155/2024/5522431

[85] https://github.com/ushukkla/nospammers/blob/master/UNSW_NB15_training-set.csv.

[86] Moustafa, N., Slay, J. (2015). UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 network data set). In 2015 Military Communications and Information Systems Conference (MilCIS), Canberra, ACT, Australia, pp. 1-6. https://doi.org/10.1109/MilCIS.2015.7348942