International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2024/40 Volume 11, Issue 5, September – October (2024)

SURVEY ARTICLE

# Machine Learning for Internet of Things (IoT) Security: A Comprehensive Survey

Haifa Ali Saeed Ali
Department of Computer Application, CMR Institute of Technology (Affiliated to Visvesvaraya Technological University), Bangalore, India.
✉ shiekhhaifa@gmail.com

Vakula Rani J
Department of Computer Application, CMR Institute of Technology (Affiliated to Visvesvaraya Technological University), Bangalore, India.
vakula.r@cmrit.ac.in

Received: 22 June 2024 / Revised: 05 October 2024 / Accepted: 15 October 2024 / Published: 30 October 2024

**Abstract – The Internet of Things (IoT) represents a network of interconnected gadgets, enabled by technology facilitating seamless communication between gadgets and the cloud. The adoption of IoT and its unique features expose these systems and devices to various intrusions. Traditional security methods are inadequate to secure IoT and requires to reevaluate the existing security protocols. While IoT devices come with built-in security features such as encryption and authentication, they require more advanced techniques to ensure robust system protection. Machine learning has emerged as a vital tool in enhancing IoT security, proving effective in mitigating cybersecurity risks and improving the intelligence of security systems. This survey provides a comprehensive overview of IoT systems, with a focus on their security aspects, including features, architectures, protocols, and associated risks. It also highlights recent algorithmic advancements, emphasizing the pivotal role of ML in strengthening IoT security. Furthermore, it categorizes attacks on IoT systems, offering a systematic understanding of vulnerabilities, and identifies relevant datasets to support future research efforts.**

**Index Terms – IoT Security, Machine Learning (ML), Deep Learning (DL), IoT Applications, Security, Attacks, Datasets, Cyber-Attacks, Challenges, IoT Layers.**

## 1. INTRODUCTION

The Internet of Things (IoT) consists of inter-connected physical objects that communicate through software, sensors, and network connectivity to share and collect data. Its primary objective is to enable autonomous interaction between devices, creating a smart, interconnected environment that profoundly impacts people's lives. IoT is applied in various fields, including intelligent homes, autonomous vehicles, gene therapy, and medical advancements. However, its inherent characteristics also pose significant security and privacy challenges, making IoT systems vulnerable to attacks such as impersonation and intrusion. The enormous amount of data produced by IoT platforms require secure transmission and analysis to prevent privacy breaches. Despite its many benefits, IoT introduces security challenges due to its unsupervised operation, reliance on wireless networks, and inability to support complex security systems. To address these challenges requires comprehensive strategies that account for the unique requirements of IoT environments. Modifications to current security frameworks for information and wireless networks are essential to develop robust IoT security solutions that accommodate the global accessibility, resource limitations, and lossy network characteristics of IoT. Traditional defense mechanisms such as encryption, authentication, access control, network security, and application security face limitations and are often inadequate for IoT systems.

However, these security mechanisms can be enhanced to satisfy the distinct needs of the IoT ecosystem. Advanced techniques, such as ML and DL, can be utilized for data analysis, enabling the identification of normal and abnormal behaviors based on interactions among IoT devices. By leveraging data from IoT components, it becomes possible to detect malicious behavior early by analyzing typical interaction patterns.

The motivation behind this survey is to furnish academicians and researchers with an extensive understanding of how ML DL methodologies can address security challenges in IoT environments, particularly focusing on mitigating attacks. These techniques play a vital role in forecasting new attacks by analyzing patterns from previous ones, thereby aiding in the detection of unknown threats. Furthermore, recent literature lacks a thorough examination of the capabilities of ML and DL in securing IoT systems, especially in handling emerging threats and scaling to real-world applications. This paper aims to fill that gap by systematically reviewing recent advancements, applications, and limitations of ML and DL in IoT security. Figure 1 depicts the crucial significance of ML/DL on the IoT environment.

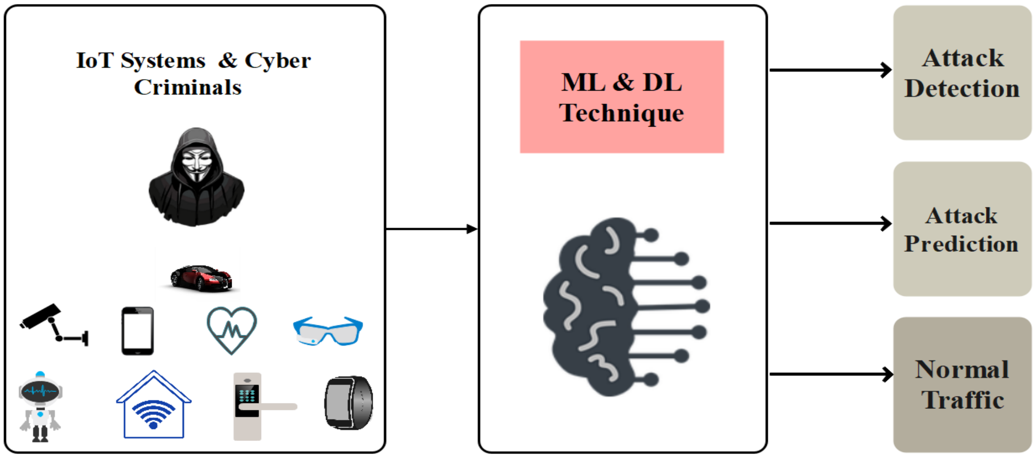


Figure 1 ML/DL Role in IoT System

This research paper aims to furnish researchers and readers with a thorough understanding of IoT and ML methods, specifically their positive impacts on detecting IoT attacks. Since there have been limited comprehensive studies on ML and DL in this area since 2018, a modern literature review covering all articles on IoT security using ML and DL methods is essential. Few studies offer an exhaustive examination of IoT, including its characteristics, protocols, architecture, and layered attacks, in addition to exploring relevant ML and DL techniques and datasets for IoT attacks.

In this paper, we analyzed ML approaches and recent advancements in DL techniques, providing insights into enhancing security protocols for IoT devices. This research also [1], explored various potential threats to IoT systems, including inherent and emerging threats to IoT security. A detailed discussion on ML & DL techniques for IoT security is presented, including their advantages, drawbacks, potential applications, and future research directions.

The study [2] explored security solutions and assault vectors for IoT networks, highlighting the weaknesses that necessitate ML and DL techniques. It offered a detailed discussion of accessible ML and DL strategies for addressing IoT security challenges and explored future research possibilities. Authors [3] conducted an in-depth analysis of IDS for IoT, covering IoT intrusions and ML/DL methodologies for disclosing assaults in IoT networks.

The authors also discussed the security issues encountered by IoT infrastructures and examined advanced ML-based solutions for protecting these systems, emphasizing how ML aids IoT security measures and the difficulties in implementing ML-based security solutions. The authors [4] addressed the major security challenges and unresolved issues faced by IoT infrastructures. It provided a thorough analysis and critique of the most advanced ML-based solutions for protecting such systems, detailing how ML enhances security measures, as well as the security requirements. Authors [5] applied DL, ML, and federated learning (FL) algorithms to IoT security, covering various models and offering overviews, assessments, and summaries of FL- and DL-based IoT security strategies.

Despite these reviews, gaps remain in comprehensively addressing all relevant aspects of IoT security and ML/DL techniques, including insufficient exploration of emerging threats and scalability issues in real-world IoT environments. In this research study, we tackle the constraints identified in previous research and furnish thorough insights for researchers. Additionally, we conducted a focused analysis by addressing the following questions:

- RQ.1: What are the possible vulnerabilities and assaults inherent within the interconnected network of IoT devices?
- RQ.2: The frameworks, algorithms, and structures of IoT security impact the effectiveness of ML and DL methods in strengthening IoT system security?
- RQ.3: How can current security measures, involving ML and DL, be enhanced to better protect IoT architecture against attacks?

The contributions of this research, summarized below, are based on the questions above:

- A thorough discussion on potential characteristics, IoT protocols, architectures, vulnerabilities, applications, and prevalent assaults in the IoT environment.

- A comprehensive study of ML and DL methods for IoT security, covering their advantages, disadvantages, solutions to security challenges, and applications.
- An analysis of current surveys on ML/DL, categorizing research papers from 2018 to 2024.
- An In-depth classification of attacks on IoT layers, including principles, weaknesses, and objectives of each layer.
- An evaluation of diverse datasets in IoT security, providing insights into their benefits and drawbacks.
- A presentation of possible research challenges in ML/DL for IoT security, along with discussion on future trends.

The remainder of the survey is organized as follows: Section 2 provides a brief overview of the IoT system. Section 3 reviews ML and DL methods, while Section 4 analyzes existing surveys on ML and DL by examining studies from 2018 to the present. Section 5 discuses and emphasizes the classification of attacks on IoT layers. Section 6 introduces datasets in the IoT system, and Section 7 discusses research challenges, future trends, and related discussions on ML/DL. Finally, Section 8 concludes the paper.

## 2. OVERVIEW OF THE IOT SYSTEM

This section furnishes an overview of the IoT systems, covering the characteristics, architecture, protocols, and vulnerabilities that raise significant security concerns.

### 2.1. Characteristics of IoT

The following attributes are vital for the efficient design, deployment, and management of IoT systems, as identified in [2], [6]:

Actuating and Sensing: IoT gadgets contain sensors to gather environmental data and may include actuators to carry out actions based on this data, such as adjusting thermostat settings.

Scalability: The ability to handle substantial volumes of data effectively is crucial in IoT systems, enabling insightful analysis and decision-making.

Safety: Concerns about the security of personal data have emerged with the rise of IoT devices, highlighting the need for measures to avert unauthorized access and data breaches.

Interoperability: Given the numerous origins of IoT gadgets and the use of various communication protocols, interoperability is essential to ensure seamless and efficient collaboration between different devices.

Energy Efficiency: Many IoT gadgets depend on batteries or limited energy sources, emphasize the importance of energy-efficient designs to extend device operation without frequent recharging.

Real Time Operations: The capability for processing and responding in real-time is vital for IoT applications, whether for managing autonomous vehicles or monitoring vital infrastructure.

Network Connectivity: As the quantity of IoT gadgets increases, maintaining connectivity becomes more challenging. Solutions such as cloud services and gateways help optimize network performance.

Remote monitoring and Control: A key advantage of IoT is the capacity to remotely monitor and control devices. Users can access and manage IoT devices from any location with an internet access, providing comfort and flexibility.

Cost-Effectiveness: As IoT adoption increases, the cost of IoT gadgets and associated technologies has decreased. Cost-effectiveness is a vital factor in the extensive adoption of IoT across various industries and applications. These characteristics form the foundation for addressing security concerns and designing effective IoT systems.

### 2.2. IoT Architecture and Protocols

IoT architecture indicates to the framework that defines the interactions and relationships between the various components of an IoT system. It includes devices (things), communication protocols, cloud services, and applications that work together to gather, process, and act upon data. Different studies offer various classifications of IoT architecture, with some [7, 8] identifying three essential layers, while others [9], [10, 11] categorize it into three, four [12] or five layers. In this study, we present the three-layer approach: Perception layer, Network layer, and Application layer.

#### 2.2.1. Perception layer

The perception layer handles with the physical connectivity and hardware components of the system [13, 14]. It includes devices, sensors, actuators, and technologies that enable connectivity to the network. The key elements of the physical layer in IoT are shown in Figure 2. This layer also incorporates protocols for performing specific tasks, as illustrated in Figure 3.

#### 2.2.2. Network layer

In an IoT system, the network layer is crucial for facilitating device connectivity and enabling data exchange across networks [15, 16]. It aligns with the OSI (Open Systems Interconnection) model and is responsible for routing packets between devices across different networks. Various protocols in this layer handle transmitting IP datagrams from the source to the target network.

Key protocols include:

- IPv4 (Internet Protocol Version 4): The most widely deployed internet protocol, using a 32-bit address scheme to identify devices in a network.
- IPv6 (Internet Protocol Version 6): The latest version of the internet protocol, which uses a 128-bit address scheme and is the successor to IPv4.
- 6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks): A protocol that allows IPv6 packets to be transmitted over low-power, low-rate wireless networks, commonly used in IoT devices. It is designed to tackle the challenges of connecting devices with limited power, processing capabilities, and memory.
- RPL (Routing Protocol for Low-Power and Lossy Networks): A protocol designed for routing data in low-power IoT networks.
- LoRaWAN (Long Range Wide Area Network): A low-power, long-range protocol designed for wireless battery-operated devices.

Selecting a network layer protocol depends on the particular needs and limitations of the IoT implementation, considering factors like interoperability, security, scalability, and power efficiency.

### 2.2.3. Application Layer

This layer is the top layer, accountable for delivering specific functionality and services to various IoT applications [17]. It enables communication between devices, applications, and services within the IoT ecosystem. Figure 4 demonstrates the three layers and the protocols used in each layer. Various application layer protocols are employed to facilitate interoperability, data sharing, and communication between IoT systems and devices: HTTP (Hypertext Transfer Protocol): Used for web communication. Devices can send and receive data over the internet using HTTP or its secure version, HTTPS. It is commonly used for web-based communication and RESTful APIs.

- CoAP (Constrained Application Protocol): A lightweight protocol designed for networks and devices with constraints. It is often used where a simple and efficient communication protocol is needed.
- WebSocket: A protocol that enables full-duplex communication over a single socket, enabling real-time message exchange between client and server.
- MQTT (Message Queue Telemetry Transport): A lightweight messaging protocol designed for low-bandwidth, high-latency, or unreliable networks. It operates on top of the TCP/IP protocol and is frequently used in IoT for its publish-subscribe model, making it suitable for scenarios with intermittent connectivity.
- XMPP (Extensible Messaging and Presence Protocol) and AMQP (Advanced Message Queuing Protocol): Additional protocols used for message-oriented communication in IoT systems.

These layers and protocols work together to ensure the efficient operation and communication of IoT systems, with each layer addressing specific functional and technical requirements.

### 2.3. Internet of Things Vulnerabilities

IoT gadgets have become more prevalent in every facet of everyday life, providing simplicity and automation [18]. However, they also introduce significant security challenges and vulnerabilities. Below are some common IoT vulnerabilities [19], [20]:

- Inadequate Authentication and Authorization: Numerous IoT gadgets come with default usernames and passwords that are often left unchanged by users, making them vulnerable to unauthorized access. The absence of Two-Factor Authentication (2FA) also makes it easier for hackers to obtain illegal access to IoT gadgets.
- Poorly Implemented Encryption: Some IoT devices transmit data without adequate encryption, making it susceptible to interception and manipulation by attackers. The use of weak encryption methods further increases the risk of compromising sensitive data.
- Outdated Software and Firmware: When manufacturers fail to release regular firmware updates, devices remain be susceptible to known exploits. Additionally, some devices are unable to install updates, leaving them exposed to security vulnerabilities.
- Privacy Concerns: Inadequate privacy protections may result to the exposure of sensitive user information, resulting in data leaks. Moreover, manufacturers may gather and retain more user data than necessary, increasing the risk of privacy breaches due to insufficient user data management.
- Limited User Awareness: Many users are unaware of the hazards related to with IoT gadgets, which can lead to insufficient security practices, such as neglecting to change default settings or failing to apply security measures.
- Inadequate Physical Security: A lack of tamper protection can result in unauthorized physical access to IoT devices, compromising their security. gadgets without proper physical security measures are vulnerable to being manipulated or stolen. These vulnerabilities

emphasise necessity of developing robust security practices and educating users about potential risks in IoT systems.

2.4. Internet of Things Applications

IoT applications span across multiple industries and fields, offering innovative solutions to improve efficiency, connectivity, and automation. Below are some of the prominent IoT applications:

2.4.1. Smart Home Automation

In intelligent homes, appliances like refrigerators, televisions, doors, and heating systems can be automated and remotely controlled [1]. Users can customize door settings, maintain cameras, manage home security systems, and control appliances such as air conditioners and heaters. Energy consumption can also be optimized by automating tasks like lighting and temperature management. Examples include smart thermostats that adjust temperature and humidity based on user preferences and energy-efficient lighting systems that are remotely controlled. Integrated cameras, sensors, and alarms enable remote surveillance and form part of smart security systems.

2.4.2. Smart Cities

Urban areas leverage IoT devices like meters, lights, and sensors to collect and analyze data, which is used to improve public utilities, infrastructure, and services. Smart city technologies aim to simplify daily tasks, enhance efficiency, and address public safety, traffic management, and environmental sustainability issues. Examples include smart meters for effective energy management and connected vehicles [21]. Traffic management systems, such as intelligent traffic lights and parking systems, reduce congestion, while waste management solutions use sensors to optimize collection routes.

2.4.3. Smart Transportation

Smart transportation integrates IoT and other advanced technologies to boost the sustainability, safety, and efficacy of transportation networks. It relies on interconnected sensors and data from mobile gadgets, GPS, accelerometers, and weather sensors to optimize urban traffic and freight scheduling, improve road safety, and reduce delivery times [22].

2.4.4. Smart Vehicles

Smart vehicles, or intelligent cars, are equipped with AI-controlled computer systems that relieve drivers of routine driving tasks. This technology aims to improve highway safety by reducing the driver's decision-making burden. Key features include telematics for data collection and transmission, fleet management for monitoring vehicle operations, and the integration of IoT technologies for autonomous vehicles.

2.4.5. Smart Agriculture

Precision agriculture, or smart agriculture, utilizes IoT sensors to monitor crop health, irrigation, and soil conditions. Wearable technologies and sensors are also used for cattle monitoring, tracking the health and behavior of livestock. These technologies enhance productivity, sustainability, and efficiency in farming [1].

2.4.6. Smart Healthcare

IoT gadgets are widely utilized in healthcare for remote patient monitoring and timely interventions. For instance, sensors can be implanted to observe glucose levels in diabetic patients and send alerts when levels become critical. Wearable devices track health indicators and communicate data to medical professionals. Additionally, smart pill dispensers help monitor drug adherence, and asset tracking systems in hospitals manage medical supplies and equipment.

2.4.7. Smart Environment

Smart environmental technologies use data-driven strategies to monitor and improve both built and natural environments. These innovations address environmental issues, promote sustainability, and enhance quality of life. Air quality sensors measure pollutants, providing real-time data for managing environmental health, while water sensors monitor the condition of natural bodies of water to detect pollution.

2.4.8. Smart Grid

This domain is the next generation of energy infrastructure, enhanced with IoT connectivity and communication technologies to improve resource utilization. It enables more efficient electricity distribution, real-time monitoring, and disaster prevention. Smart grids also detect energy spikes and device malfunctions, helping to enhance reliability and reduce power transmission costs. In Table 1, the applications, principles, and weaknesses of IoT in various domains are summarized.

2.5. Internet of Things Critical Attacks

An IoT assaults indicate to a breach of an IoT system, targeting gadgets, networks, data, or users. Cybercriminals exploit these vulnerabilities to steal data or gain control over automated systems, threatening their functionality. Due to the inherent weaknesses in the IoT environment, it remains constantly exposed to cyberattacks. These assaults can be categorized as either active or passive, and they are still under investigation, as researchers have not yet developed definitive solutions to fully protect IoT systems. This subsection discusses the most critical active and passive assaults in the IoT environment. The objectives and details of each attack are outlined in Tables 2 and 3. Below are the primary types of IoT attacks.

### 2.5.1. Passive Internet of Things Attacks

Passive IoT attacks involve unauthorized monitoring, eavesdropping, or information gathering without actively interfering with the communication or functionality of IoT devices [23]. These attacks are often subtle and aim to collect sensitive information for malicious purposes. Defending against passive IoT attacks requires strong encryption, secure communication protocols, monitoring network traffic for anomalies, and using intrusion detection systems. Below are common types of passive IoT attacks:

- Eavesdropping

Eavesdropping in IoT threats refers to the unauthorized monitoring and interception of communication between an IoT device and a network. In this type of attack, the assailant covertly listens to the data or messages being transmitted to acquire sensitive information, such as credentials or personal data, without actively disrupting communication [24].

- Traffic Analysis Attack

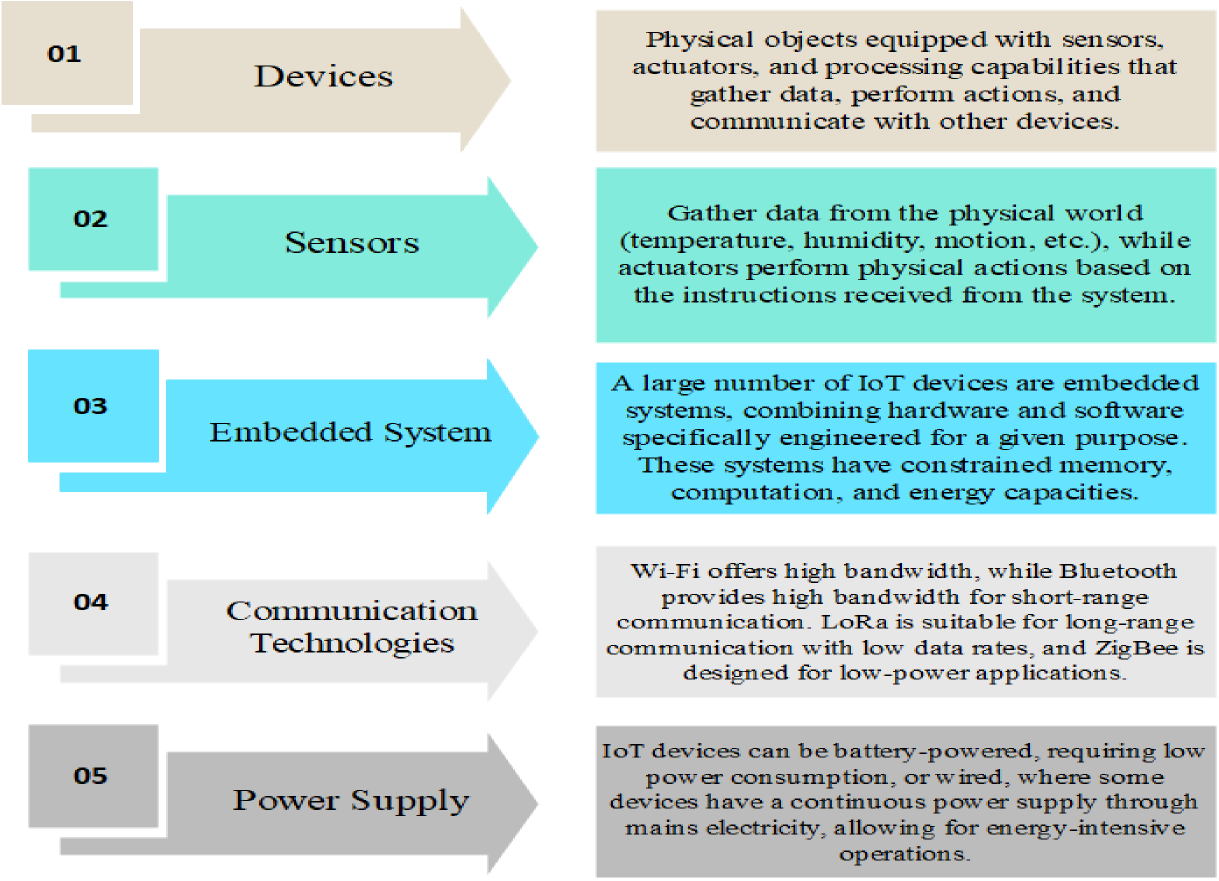
This attack involves the illegal monitoring and analysis of network traffic to gain insights into patterns, behavior, or private data shared between IoT devices. Unlike other attacks that exploit device or network vulnerabilities, traffic analysis focuses on passive observation of data transmission [25].

- Passive Device Fingerprinting

Passive device fingerprinting in IoT refers to identifying and profiling IoT devices on a network without actively engaging with them. This involves observing and analyzing network traffic, characteristics, and patterns generated by devices to create a unique fingerprint or signature. The data can be used for goal such as targeted attacks, reconnaissance, or unauthorized access [26].

- Radio Frequency (RF) Snooping

RF snooping in IoT involves the unauthorized interception and analysis of radio frequency signals emitted by IoT devices. These attacks exploit wireless communication channels used by IoT devices to exchange information, potentially leading to the extraction of sensitive data, device identification, or remote control of targeted devices [27].



Physical objects equipped with sensors, actuators, and processing capabilities that gather data, perform actions, and communicate with other devices.

Gather data from the physical world (temperature, humidity, motion, etc.), while actuators perform physical actions based on the instructions received from the system.

A large number of IoT devices are embedded systems, combining hardware and software specifically engineered for a given purpose. These systems have constrained memory, computation, and energy capacities.

Wi-Fi offers high bandwidth, while Bluetooth provides high bandwidth for short-range communication. LoRa is suitable for long-range communication with low data rates, and ZigBee is designed for low-power applications.

IoT devices can be battery-powered, requiring low power consumption, or wired, where some devices have a continuous power supply through mains electricity, allowing for energy-intensive operations.

Figure 2 Key Components of Physical Layer

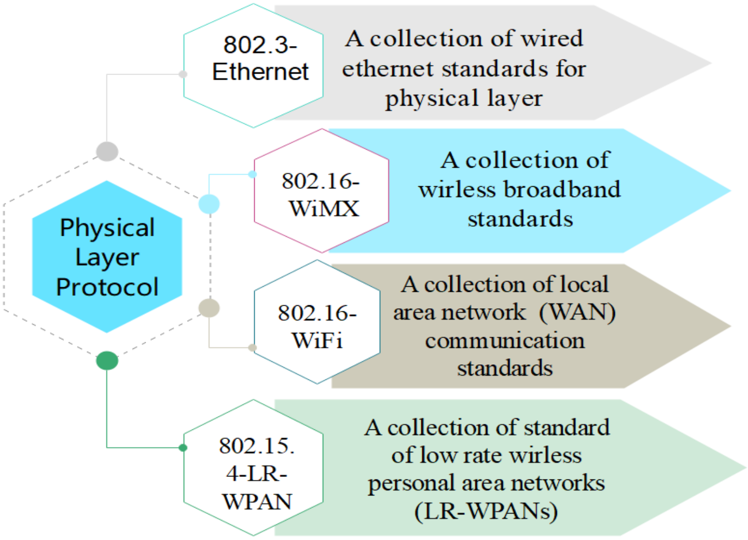

Physical Layer Protocol
802.3- Ethernet
A collection of wired ethernet standards for physical layer
802.16- WiMX
A collection of wirless broadband standards
802.16- WiFi
A collection of local area network (WAN) communication standards
802.15. 4-LR-WPAN
A collection of standard of low rate wirless personal area networks (LR-WPANs)

Figure 3 Physical Layer Protocols

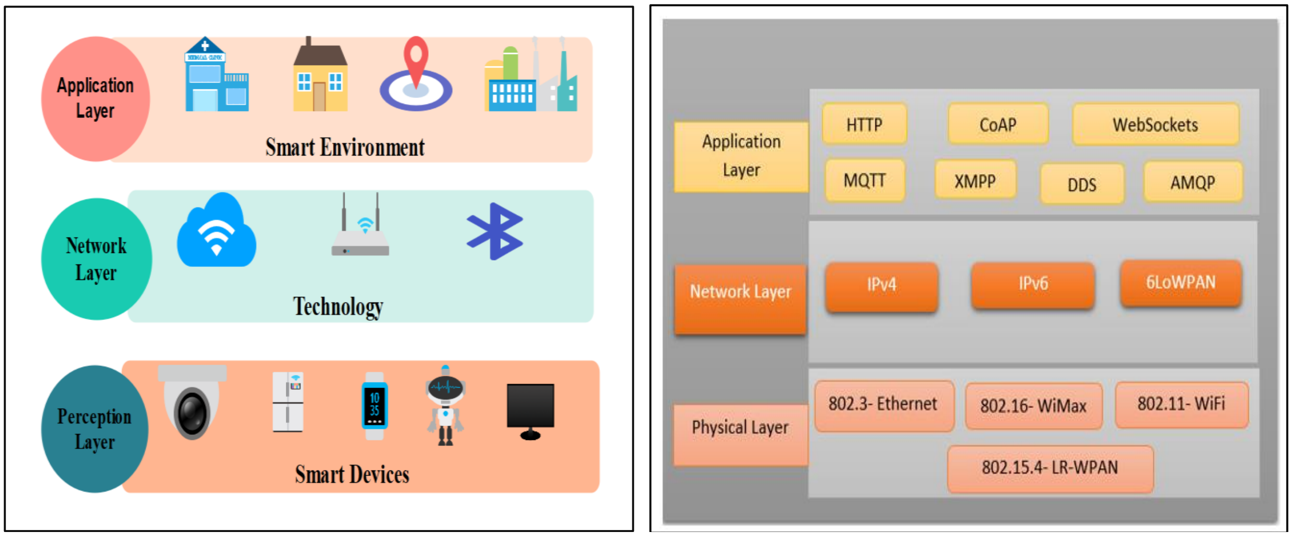


Figure 4 Protocols Based IoT Architecture

Table 1 IoT Application Principles and Weaknesses

| Domain | Principle | Weaknesses |
|---|---|---|
| Smart Home | Upgrading the standard of living Safety, security and convenience in the home. | Lack of physical security.<br>Vulnerabilities in devices.<br>Weak passwords.<br>Inadequate authentication. |
| Smart Cities | Encompasses intelligent homes, intelligent traffic management, intelligent disaster management, intelligent utilities, etc. | Weaknesses in security protocols.<br>Lack of encryption.<br>Lack of standardization and interoperability.<br>High Implementation Costs. |

| | | |
|---|---|---|
| Smart Environment | Encompasses diverse IoT applications like fire disclosure in forests, observing the amount of snow in high altitude areas, avoiding landslides, premature disclosure of earthquakes, pollution observation, etc. | FN and FP may result in disastrous results for such IoT applications.<br>Integrating diverse technologies, protocols, and devices can be complex, leading to challenges in maintaining and managing the system.<br>Privacy breaches. |
| Smart Grids | A bi-directional power network that facilitates the transmission of both electricity and data using digital communications technologies. | Physical and cyber-attacks criticality of data delivery latency.<br>The smart grid may be more vulnerable to cyberattacks, equipment malfunctions, and system failures due to its reliance on digital technologies.<br>Intelligent grids rely heavily on digital communication and data transfer, making them vulnerable to cyber-assaults and hacking. |
| Smart Healthcare | Enhancing the quality of care delivered.<br>Enhancing patient health outcomes.<br>Minimizing healthcare expenses. | Sensitive health data gathering, and storage provide serious security threats.<br>Insufficient cost-effective intelligent and precise medical sensors.<br>Lack of a standard architecture of IoT system.<br>High handling volume data and challenge of interoperability, etc.<br>Require robust privacy measures to ensure that patients' personal health information. |
| Smart Transportation | Decreased traffic congestion leads to improved air quality, less wasted time, and decreased consumption of energy. | The software of the control system could be compromised by hackers.<br>creating issues with data privacy and the possibility of misuse or illegal access.<br>High Implementation cost.<br>Energy Requirements. |
| Smart Vehicles | Analyzes intelligent vision for safe driving, intelligent monitoring of driving that is insecure, intelligent disclosure of automobile power and transmission systems, intelligent vehicle navigation and transportation systems, and intelligent technology that can be assisted by vehicles. | Vulnerability to Hacking.<br>Accomplishing a high level of safety in autonomous vehicles is challenging,<br>High energy consumption.<br>Data Privacy Risks. |
| Smart Agricultural | Managing farms with the utilize of sophisticated information and communication technology to raise product quantity and quality while reducing the amount of human work necessary. | Vulnerable to cyber threats.<br>Farmers' Privacy Concerns.<br>Lack of technical skills.<br>Affected by adverse weather conditions. |

- Bluetooth Sniffing

Bluetooth sniffing involves the unauthorized interception and analysis of Bluetooth communication between devices. This can result in the extraction of confidential information, device identification, or even unauthorized access or control of IoT devices that rely on Bluetooth for communication [28].

- Social Engineering

IoT social engineering attacks trick users into revealing information about IoT devices without authorization by exploiting human weaknesses. Social engineering relies on psychological manipulation to convince people to perform certain actions or disclose sensitive information [29].

- Location Tracking

Location tracking attacks involve the illegal acquisition or alteration of location data from IoT devices. Attackers may exploit vulnerabilities in networks or devices to trace the location of devices or individuals. Techniques such as GPS spoofing, malicious firmware updates, or RFID/NFC skimming may be used to achieve these goals [30].

### 2.5.2. Active Internet of Things Attacks

Active IoT assaults involve direct interference with the normal functioning of IoT gadgets, networks, or systems. These attacks seek to manipulate, disrupt, or gain unauthorized control over the targeted IoT infrastructure. Below are types of active IoT attacks:

- Denial of Service Attack (DoS)

A DoS assaults prevents a system from being accessible by legitimate users, prohibiting them from using the system's resources. This may result to significant financial and time losses for service providers, as users may switch to other services due to security apprehensions. DoS assaults can exhaust network resources, bandwidth, and CPU time, emphasizing the necessity for a complete security strategy that involving technical measures and proactive monitoring [31].

- Distributed Denial of Service (DDoS) Attacks

This assault entails overwhelming a target server or website with a massive amount of fake traffic from multiple sources to slow down or disrupt the service. It differs from a DoS attack in that DDoS utilizes numerous computers and internet connections, often through a botnet, to flood the target. DDoS attacks can cause significant congestion in IoT devices and networks, leading to service interruptions [32].

- Man-In-The-Middle Attack

This assault transpires when an assailant intercepts communication between two parties, such as IoT devices, without their knowledge. The assailant can eavesdrop, alter, or inject false data into the communication, effectively gaining unauthorized access or manipulating the data being transmitted. It transpires when an individual or cybercriminal intervenes in the connection between a system and a user, or between two users, to steal personal information, messages, data, and more.

Users may believe they are connecting normally, but during MiTM assault, the assailant controls all interactions between the two parties or between the user and the system. The attacker can also alter messages while remaining undetected. The primary objective of these assaults is to steal personal information, such as login credentials, card details, transaction data, and other sensitive information [33, 34].

- IoT worms and malware

Attacks involving malware and IoT worms propagate malicious software created to penetrate vulnerabilities in IoT gadgets. These attacks often include self-replicating malware that disseminates through IoT networks, infecting multiple devices and potentially causing significant damage. IoT malware can take various forms, including worms, viruses, and trojans, and can have numerous harmful effects, such as stealing confidential information, impairing device functionality, or even posing physical threats. The risk of IoT malware attacks increases with the number of connected devices [35, 36].

- Jamming Attacks

Jamming is one of the vulnerabilities used to compromise wireless environments. It works by denying service to legitimate users, as authorized traffic is congested by illegitimate high-frequency signals. Jamming assaults interfere existing wireless network connections by transmitting unwanted signals to IoT gadgets, causing issues for users by keeping the network continuously occupied. additionally, these attacks can reduce the functionality of IoT devices by consuming additional energy, bandwidth, memory, and other resources. Attackers employ various techniques to jam radio frequency (RF) signals, preventing IoT devices from sending or receiving data [37, 38].

- Sinkhole Attacks

A sinkhole assault indicates to a malicious activity where an attacker diverts or redirects the traffic of IoT devices to a destination under their control. The term "sinkhole" indicates that the attacker creates a point where the diverted traffic is directed.

Sinkhole attacks can serve various purposes, including eavesdropping on communications, collecting critical information, or disrupting the normal operation of IoT devices. These attacks can be passive or active, depending on how they are executed [39].

- Zero-Day-Attacks

This attack takes advantage a potentially malicious software vulnerability that the vendor or developer may not be aware of, often indicated to as Day Zero. To mitigate risks to software users, developers must act quickly to address vulnerabilities as they are discovered. The assault can encompass malware, adware, spyware, or unauthorized access to user information. In IoT, zero-day assaults exploit weaknesses in devices or systems that are unknown to the vendor or the public. These vulnerabilities are termed "zero-day" because there is no prior protection or awareness at the time of the attack. Zero-day attacks can be both passive and active, depending on their interpretation in relation to cybersecurity [40].

Table 2 Passive Attacks

| Passive Attack | Objectives |
|---|---|
| Eavesdropping | Collect sensitive information, such as credentials or data, without actively disrupting the communication |
| Traffic Analysis | Gain insights about how IoT devices typically operation, identify vulnerabilities, or gather vital information. |
| Passive Device Fingerprinting | Identify software versions, identify particular devices, or obtain information for possible exploitation. |
| Radio Frequency (RF) Snooping | Obtain information about communication patterns or extract data without direct access to the gadget. |
| Bluetooth Sniffing | Extract confidential information or observe the interactions between Bluetooth-enabled IoT devices. |
| Social Engineering | Utilize collected Information for SE schemes like phishing and impersonation. |
| Location Tracking | Monitor the movements of individuals or objects that are linked to IoT gadgets. |

Table 3 Active Attacks

| Active Attack | Objectives |
|---|---|
| DoS | Produce a disturbance in service by rendering devices or systems temporarily or permanently unavailable. |
| DDoS | Increase a DoS attack's impact and make it more challenging to mitigate. |
| MiTM | Eavesdrop on sensitive information, alter data while it's being transmitted, or pretend to be an authorized communicator. |
| IoT worms and malware | Infect an extensive number of devices in order that initiate a botnet, steal information, or carry out coordinated attacks. |
| Jamming Attacks | Disable or degrade connection, leading to service disruption or loss of connectivity. |
| Sinkhole | Compromise the connection and control of IoT appliances for malicious purposes. |
| Zero-Day-Attacks | Exploit security flaws in IoT devices or software for which no security patch or update has been released |

Consequently, it is crucial to understand and mitigate both passive and active attacks to secure IoT ecosystems. Reducing the risks associated with these attacks requires implementing robust encryption, authentication methods, and frequent security assessments. Unfortunately, traditional security defence mechanisms often lack the capabilities to confront these potential attacks. Therefore, modern security measures must be adopted to prevent and detect these threats, which jeopardize vulnerable IoT systems. This paper discusses and presents security measures that can effectively combat IoT attacks. The categorization of IoT critical attacks is illustrated in Figure 5.

### 2.6. Existing Surveys in IoT Security

The IoT environment has provided numerous benefits, facilitating remote device usage and leveraging smart devices powered by artificial intelligence to meet human needs. However, despite these advantages, these devices are often inadequately equipped from a security perspective to protect against cyberattacks. Various studies and reviews have conducted thorough analyses of literature on security threats. In this subsection, we examine significant surveys focused on IoT security. For instance, study [41] addressed primary challenges in the IoT environment, including security communication, issues and unresolved challenges, along with potential solutions.

Study [42] analyzed security issues, unique IoT characteristics, significant security challenges, and solutions in relation to previous surveys. Study [43] discussed IoT security challenges, open issues, and provided a foundation for future research. Study [44] offered a comprehensive classification of security risks within the IoT framework, providing insights to help IoT developers in managing hazards and security flaws for improved protection. It also presented alternative five-layer and seven-layer IoT architectures alongside the current three-layer design. Modern approaches to enhancing IoT device security include leveraging machine learning, edge computing, fog computing, and blockchain technology while also addressing unresolved research issues. Author [45] presented a complete categorization for authentication and access (AA) in IoT networks, evaluating various elements of AA using conventional and ML-driven approaches to assess their potential to enhance IoT ecosystem security and identify research areas. The topic of IoT architecture in the context of AA schemes was also covered, focusing on different risks and attacks at each IoT layer. IoT applications utilizing machine learning algorithms for AA were examined for their requirements and existing challenges.

Study [46] analyzed recently proposed models, protocols, and encryption techniques for securing IoT networks, highlighting the latest security trends. It discussed the classification of IoT attacks and provided an updated analysis of protocols and standards proposed for IoT systems. Study [47] reviewed current IoT security issues related to potential future attacks, identifying concerns associated with IoT integration with cloud and blockchain technologies, changes in cryptography due to quantum computing, and the growth of artificial intelligence. Study [48] compiled information on reported security vulnerabilities, their classification, and remedies proposed to address IoT security challenges.

Study [49] identified major security concerns and anticipated challenges within the IoT ecosystem, guiding authentication methods and addressing various threats. Study [50] provided a concise overview of security issues across different IoT protocol layers, along with preliminary simulation findings. Through our review of these studies, we summarize them in Table 4, focusing on discussions about IoT security and the limitations of these studies.

## 3. REVIEW ON MACHINE LEARNING AND DEEP LEARNING

Traditional security mechanisms have demonstrated inadequate in tackling the security challenges related to IoT. Therefore, researchers and experts must explore more efficient mechanisms to confront the security risks that threaten this technology and, consequently, human lives. For this reason, modern methods related to artificial intelligence (AI) have been investigated and shown to be capable of combating cyberattacks, such as hacking devices and cracking passwords. Due to their distinct problem-solving approaches, learning algorithms have found widespread adoption in various real-world applications. The emergence of low-computation-cost algorithms, combined with the availability of vast datasets and the development of novel methods, has contributed to the current advancements in learning algorithms, commonly referred to as ML and DL.

ML is an area of AI focused on developing systems that learn or enhance their performance based on the data they consume, while DL is a subfield of ML. AI is an umbrella term that indicates to systems or gadgets that simulate human intelligence. ML, DL, and AI are often discussed together, and the terms are sometimes employed interchangeably; however, they do not represent the same concept. It is vital to note that while ML and DL methods are forms of AI, not all AI encompasses ML or DL.

ML enables machines to learn independently without human guidance to perform tasks. It deduces a model for solving future problems by extracting specific patterns from data [51]. This field emerged from scientists' aspirations to create autonomous systems that infer without human intervention, moving beyond the previous reliance on direct commands. In today's world, ML is pervasive in various sectors. Whether we link with banks, shop online, or use social media, ML algorithms play a crucial role in ensuring our experiences are efficient, seamless, and secure.

The technologies surrounding ML are evolving rapidly. Conventional ML methods rely on engineered features, while DL methods represent advancements in learning techniques that utilize multiple non-linear processing layers for feature abstraction and transformation, aiding in pattern analysis. Therefore, the aim of this review of ML and DL is to provide readers with a comprehensive understanding of both. In this section, we will first examine ML techniques from an IoT security perspective, discussing their pros and cons, along with solutions for IoT security. Next, we will review DL algorithms, their advantages and disadvantages, and their applications in addressing IoT security challenges.

### 3.1. Machine Learning (ML) Techniques

In this subsection, we furnish an overview of ML methods that have proven effective in disclosing and mitigating cyber-assaults in IoT-based environments. ML involves training a computer to achieve a performance criterion by using previous or sample data [52]. ML algorithms create a mathematical model that aids in generating predictions or decisions using training data and previous data samples, without the need for explicit programming. ML merges computer science and statistics to develop prediction models, with a fundamental aspect being the development and use of algorithms that derive knowledge from past data. Providing more data generally improves the performance of ML algorithms.

ML techniques are suitable for IoT devices with resource constraints, as they can detect various IoT attacks early by observing network behavior [53]. ML methods can be broadly classified into two categories: Supervised Machine Learning

(SML) and Unsupervised Machine Learning (USML). This subsection addresses common ML techniques, such as PCA, K-means clustering, Decision Trees (DT), Support Vector Machines (SVM), Naive Bayes (NB), k-Nearest Neighbors (KNN), Random Forest (RF), Association Rule (AR), and Ensemble Learning (EL), along with their pros and cons in IoT security.

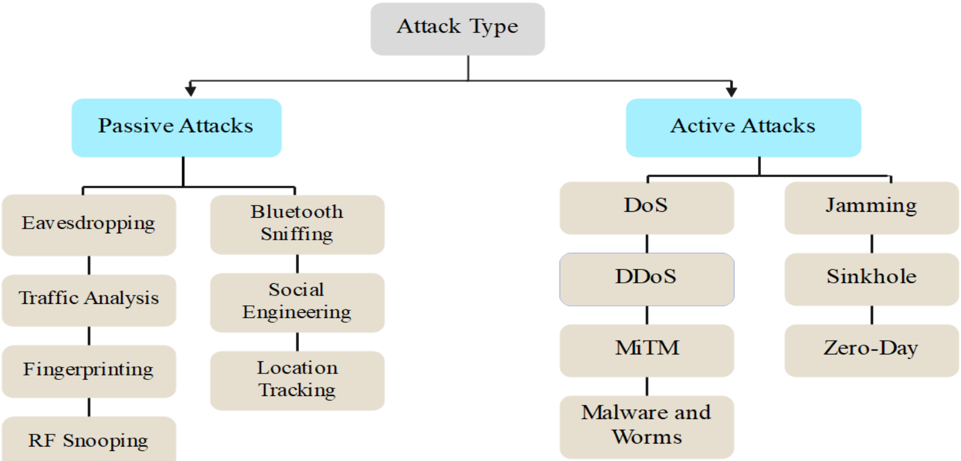


Figure 5 IoT Critical Attacks

3.1.1. Support Vector Machines (SVM)

It is a SML methods which is commonly utilized to tackle classification and regression problems; Nevertheless, it is applied in classification problems. It is composed of three important concepts:

1. Support Vectors: Data points closest to the hyperplane.
2. Hyperplane: A decision boundary that separates diverse classes of data.
3. Margin: The distance between the hyperplane and the nearest data points from diverse classes.

The primary goal of SVM is to partition datasets into categories by obtaining a maximum margin hyperplane [54, 55]. In IoT security, SVM algorithms have made significant strides in detecting, classifying, and mitigating security risks. The application of kernel techniques and non-linear decision boundaries has improved their ability to categorize complex threats in IoT environments. For example, a study [56] combined the TOPSIS and Shannon Entropy methods based on a bijective soft set to verify selected features for identifying malicious traffic in IoT networks using SVM and other ML techniques. This resulted in the development of a feature selection (FS) algorithm named Corrauc, which uses a wrapper technique to precisely refine and select useful features for the chosen ML methods based on the AUC metric. The findings indicated that the suggested method attained an accuracy exceeding 96% utilizing SVM. However, the paper could benefit from providing more details on the process of selecting optimal features to ensure precise detection of malicious traffic in IoT networks. In [57], the authors proposed an intrusion detection system (IDS) using ML to disclose novel assaults with SVM, achieving up to 99.8% accuracy and 100% recall. Nonetheless, limitations in the proposed methods include the need for more training samples for selective forward attacks, as well as improvements required in the Matthews correlation coefficient (MCC) and precision.

3.1.2. Decision Tree (DT)

This algorithm is a form of (SML) that describes the input and associated output in the training data. DTs can be employed for both classification and regression tasks and are represented by a tree-like diagram that results from a series of feature-based splits. A DT starts with a root node and ends with leaf nodes. The root node is where the initial population split occurs, based on various features [58]. The leaf nodes represent the final decisions. DTs are crucial for IoT security because of their high accuracy in identifying intrusions, such as DDoS assaults. Their simplicity and reliability make them an efficient tool for researchers. DTs utilize pruning methods to mitigate overfitting by removing unnecessary branches, which greatly improves performance on large IoT datasets. Boosted decision trees, such as Gradient Boosting, enhance the disclosure of complex assaults. DTs have shown exceptional performance in detecting IoT attacks, establishing them as a key technique in machine learning. For example, a study [59] compared various ML methods, including DT, KNN, ANN, RF, and NB, using the Bot-IoT dataset to analyze HTTP DDoS attacks. The study found that DT, RF, and KNN scored higher compared to other ML methods.

Another study [60] presented and implemented a sequential detection architecture for an ML-based botnet attack detection system, utilizing J48 DT, ANN, and NB, which showed a higher performance score in creating a lightweight, high-performing detection system.

3.1.3. Random Forest (RF)

RF is a (SML) method where multiple DTs are built and combined to form an RF, which creates a robust and accurate prediction model for better overall outcomes. In RF, trees are randomly constructed and trained to select a class by voting. The method's performance improves as the number of trees increases, leading to higher classification accuracy and prediction reliability. RF is widely utilized in IoT security operations, such as anomaly disclosure, due to its exceptional classification capabilities. Recent advancements in RF utilize ensemble methods that combine multiple DTs to enhance classification accuracy and robustness in detecting anomalies in IoT communications. Additionally, feature importance analysis allows RF to identify critical features in high-dimensional IoT data, improving the model's interpretability [61]. For instance, a study [62] employed RF and other ML techniques to disclose and prevent DoS assault traffic arriving from smart home LAN devices. RF achieved 99% accuracy and precision compared to other ML algorithms in the proposed methods. Another study [63] suggested a method to classify Advanced Persistent Threat (APT) malware in IoT networks using SMOTE-RF, which is trained to address imbalanced and multi-classification issues. The suggested method attained an accuracy rate of 80%.

3.1.4. Naive Bayes (NB)

NB is a (SML) algorithm based on Bayes' theorem and is commonly utilized for solving classification problems. NB makes predictions based on the probability of an event occurring given the prior data [64]. In IoT security, the NB is employed to forecast attacks based on historical data and is particularly effective in detecting network layer anomalies. It has benefited from methodologies such as Gaussian Naive Bayes, which allows it to handle continuous data more efficiently in IoT applications. This enhancement makes NB suitable for real-time intrusion detection that requires quick classifications [65]. A study in [66] proposed intrusion detection methods based on Naïve Bayes, noting that the Bayes classifier is particularly well-suited for intrusion detection systems (IDS) due to its high classification speed. Another study [67] presented an IDS model based on a two-layer dimension reduction and a two-tier classification module, built to disclose malicious activities such as User-to-Root (U2R) and Remote-to-Local (R2L) attacks using NB and KNN. The model achieved a DR of 84.82% with a high false alarm rate (FAR) of 5.56%, while the two-tier model attained a DR of 83.24% and FAR of 4.83%.

Table 4 Existing Surveys in IoT Security

| Ref. | IoT Characteristics | IoT Protocols | IoT Architectures | IoT Security Solution | IoT Challenges | Limitations |
|---|---|---|---|---|---|---|
| [41] | ✕ | ✕ | ✓ | ✓ | ✓ | Deficiency to taxonomy ant bit discussion on attacks detection scheme in IoT layers.<br>Deficiency to present security solution mechanism, IoT vulnerabilities are not considered |
| [42] | ✓ | ✕ | ✕ | ✕ | ✓ | IoT security measures are not adequately regarded and focuses on the of IoT features' impact on security and privacy without emphasis regarding IoT security requirements. |
| [43] | ✕ | ✕ | ✕ | ✕ | ✓ | IoT security requirements and mechanisms are disregarded.<br>Deficiency to discuss IoT application. |
| [44] | ✕ | ✓ | ✓ | ✓ | ✓ | Deficiency to discussions on important IoT security requirements. |
| [45] | ✕ | ✕ | ✓ | ✓ | ✓ | Lacks classification and minimal discussion on ML techniques, moreover, IoT Vulnerabilities are not specified. |

| | | | | | | |
|---|---|---|---|---|---|---|
| [46] | ✗ | ✓ | ✓ | ✓ | ✓ | Concentrate on affection protocols in support security solutions without concentrating on IoT security requirements. |
| [47] | ✗ | ✓ | ✓ | ✓ | ✓ | Deficiency to discuss the IoT mechanism. |
| [48] | ✗ | ✗ | ✓ | ✗ | ✓ | Lack to present the solutions to IoT Security. |
| [49] | ✗ | ✗ | ✓ | ✗ | ✓ | Modern Security methods are ignored and minimal debate on the attack detection schemes. |
| [50] | ✗ | ✗ | ✓ | ✗ | ✓ | Modern Security methods are ignored.<br>Deficiency to discuss on the attack detection schemes. |

3.1.5. K-Nearest Neighbor (KNN)

KNN is a simple SMLA that can be utilized to both regression and classification tasks, though it is more commonly utilized for classification. KNN measures the distance between data points using the Euclidean distance as a metric, calculating the average value of the unknown data point based on its k-nearest neighbors. KNN is widely used in IoT security for detecting malware, anomalies, and intrusions. Recent advancements in rapid nearest-neighbor search methods have improved the scalability of KNN, allowing it to handle larger IoT datasets without compromising classification speed. Distance-weighted voting has further improved its predictive accuracy in identifying attacks [68]. In [69], a distributed modular solution utilizing KNN was proposed to disclose IoT malware network activity in large-scale networks, demonstrating the effectiveness of the KNN classifier.

3.1.6. Principal Component Analysis (PCA)

PCA is an USML algorithm used for dimensionality reduction in ML models. PCA reduces the complexity of datasets by minimizing the quantity of features while retaining essential information. This process improves computational efficiency, speeds up calculations, and helps mitigate overfitting in machine learning models. PCA is often integrated with other machine learning techniques to develop more effective security strategies. Recent improvements have combined PCA with feature selection techniques to enhance its ability to identify relevant features for detecting IoT security vulnerabilities, simplifying attack detection models while boosting computational speed. PCA enhances machine learning performance by identifying features linked to IoT attack detection [70]. For example, in [71], a two-level detection strategy was proposed to identify unusual network traffic in IoT networks using PCA algorithms. The experiment, conducted with various datasets and employing a 95% threshold, demonstrated a high true positive rate (TPR).

3.1.7. Association Rule (AR)

Association Rule (AR) is employed to discover hidden relationships between variables in a dataset. It detects frequent patterns or variable combinations, which are often seen in assaults scenarios, and builds models to predict future classifications based on these patterns. Although AR approaches are not widely utilized in IoT contexts, further research is recommended to optimize or integrate them with other strategies to improve IoT security [72].

3.1.8. K-Mean Clustering

K-Means is an (USML) algorithm that groups unlabeled datasets into clusters, with K representing the number of predefined clusters. It is a simple and effective method for identifying categories in unlabeled datasets without requiring prior training. The algorithm iteratively separates data into K clusters by locating the optimal K Centre points and assigning each data point to the nearest Centre. In [73], the author proposed an organized insider assaults model called CPMA, where attackers maliciously manipulate packets that meet specific conditions using K-Means clustering. The experimental findings indicated that the suggested scheme, utilizing K-Means, achieved high disclosure performance and effectively organized malicious nodes' assaults modes with high accuracy. Recent advancements in initialization methods have improved K-Means accuracy in anomaly detection, making it more effective in IoT security applications.

3.1.9. Ensemble Learning (EL)

Ensemble Learning (EL) improves machine learning outcomes by combining multiple models. This strategy typically yields better predictive performance than using a single model. EL has been applied to various complex problems, especially in forecasting and predictive tasks. Techniques like AdaBoost and Gradient Boosting improve detection accuracy by combining weak classifiers into a resilient robust classifier, which addresses the imbalanced nature of IoT security datasets. Various EL methods, such as stacking, boosting, and voting, can be applied in IDS strategies, enhancing their effectiveness [74].

In [75], the authors suggested a new smart ensemble-based IDS designed to be deployed at the IoT gateway. The method applied NB, SVC, and KNN classifiers and achieved high accuracy and performance when combined with EL techniques, exceeding 90% in accuracy compared to methods without EL. While ML techniques are effective in disclosing cyber-attacks in IoT environments, they face challenges related to reliability, accuracy, and efficient labeling of data. These methods must adapt to the diverse data generated by IoT applications, but they also come with limitations.

Table 5 highlights the benefits and drawbacks of diverse ML techniques and their applicability to different types of assaults. Although many studies have proposed ML-based methods to mitigate IoT security concerns, there remain deficiencies in their findings.

Table 6 presents previous work on using ML to detect assaults in IoT environments [76-87].

### 3.2. Deep Learning (DL) Techniques

Recently, the incorporation of DL in IoT systems has gained significant attention as a research area. DL outperforms classical ML techniques, particularly when applied to large datasets, which is one of its primary advantages [88]. DL is the most advanced method for analyzing data to assess both benign and malicious behaviors of IoT components based on the interactions between devices within an IoT environment. By learning from past attacks, DL models can accurately predict future attacks. DL is a branch of ML that employs multiple non-linear processing layers to abstract and transform features in a discriminative or generative manner for pattern analysis. Because DL techniques can capture hierarchical representations in deep architectures, they are often referred to as hierarchical learning techniques [1]. Examples of discriminative DL methods include Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs). Hybrid DL methods include Autoencoders (AEs), Deep Belief Networks (DBNs), Restricted Boltzmann Machines (RBMs), Generative Adversarial Networks (GANs), and Ensembles of DL Networks (EDLNs).

Table 5 Advantages and Disadvantages of ML Techniques

| Technique | Advantages | Disadvantages | Application |
|---|---|---|---|
| SVM | Employ kernel mechanisms and is capable of simulate decision boundaries that are non-linear.<br>SVMs are well-known for their capacity to generalize and for being applicable to data that has a lot of feature attributes but few sample points.<br>Perfect for data with a numerous of feature attributes.<br>Memory and storage are used less.<br>Extremely scalable and task-performing.<br>Suitable to IoT Security due to has a higher classification accuracy. | Unbalanced samples have an impact on conventional SVM performance efficiency.<br>Memory-sensitive and could find it challenging to choose the best kernel when modeling massive data sets. | Use with:<br>Anomaly Detection.<br>IoT-Botnet detection.<br>DoS/DDoS Detection |
| NB | Employ to address practical issues such as text classification and spam detection.<br>High Scalable, Rapid, Robust.<br>Appropriate for carrying out multi-stage classification and needs less data for classification.<br>Handle with high-dimensional data points. | Incapable of extracting valuable information from feature correlations and interactions. | Suitable for Anomaly disclosure in IoT network. |

| | | | |
|---|---|---|---|
| RF | Its applicability to any size data sets and flexibility of implementation are not quite complex.<br>Suitable for simulating real-world situations.<br>High veracity and less prediction time. | Require a long time to train period than other supervised algorithms.<br>Impacted when the quantity of trees surpasses a particular threshold, which causes the algorithm to become sluggish and less efficient for real-time classification tasks. | Suitable for DoS, DDoS, Probe, R2L, U2R attacks, intrusion anomalies, and unauthorized IoT devices. |
| K-NN | Simple to use.<br>Reasonable score to accuracy to detect U2R and R2L attacks. | Unqualified for data with high dimensional and are memory intensive.<br>Not function well with enormous data sets and are highly sensitive to outliers and missing values. | Suitable for U2R, R2L, Flooding attacks, DoS, DDoS.<br>And Intrusion detection and anomalies. |
| K-mean | Simple algorithm and flexible.<br>Functions well with unlabeled data.<br>Utilize for confidential data anonymization in an IoT system. | less effectiveness than techniques in SL. methods, especially in detecting known attacks.<br>Obtained poor cluster formation results, if the clusters are not globular. | Suitable for: Detecting anomalies.<br>Sybil attacks in IoT. |
| DT | Basic, simple to use, and transparent technique. | Demands large storage.<br>Understanding DT-based approaches are simple only if a few DTs are included. | DDoS<br>Network traffic |
| PCA | Reduce data dimensionality and rise the computational speed.<br>Enhances the effectiveness of ML techniques by choosing features related to IoT assault disclosure. | Not resistant to any outliers, which has an impact on its performance.<br>Presupposes a linear connection between two features, making it challenging to assess the correlation between the features. | Used in IoT system real-time detection |
| AR | Effortless usages. | Time Complexity is high. | Intrusion Detection |
| EL | Suitable for complex problem in IoT attacks detection<br>Providing high performance | Long time for training and testing phase. | Used with anomaly detection and botnet disclosure |

Table 6 Previous Studies on IoT Attacks Detection-Based ML Algorithms

| Reference | Algorithm | Attacks | Shortcoming | Observation |
|---|---|---|---|---|
| [76] | DT, NB, RF, SVM | Malicious Bot-net | Inappropriate feature selection lead to misclassify malicious traffic flow. | DT and RF fulfilled high performance, However SVM, and NB were slightly weak. |
| [77] | KNN, DT, XGB, RF | APT malware | Less performance measurement. | RF achieved high performance compare the rest of classifiers. |

| | | | | |
|---|---|---|---|---|
| [78] | SVM, DT, NB, USML | DDoS | FAR is high.<br>Specificity is less. | The classifiers performance evaluation, however, FAR and specificity need to be improved. |
| [79] | NB, C4.5, RF | Anomaly and Intrusion | Time taken to establish the model is high. | The classifiers obtained exceptional performance but the time need to be minimized. |
| [80] | EL, RF, DR, KNN | Botnet | Imbalanced dataset.<br>Binary-class classification model. | The ensemble model achieved high performance, however the time computation is high. |
| [81] | DT, XGB, LR | Botnet | Binary-class classification.<br>Overfitting model.<br>Testing accuracy for balanced data is less. | The model achieved high performance Metric with EL classifier compare to the other two classifiers, but the model needs to get rid of overfitting and increase the test accuracy in balanced dataset. |
| [82] | DT, RF, SVM | Injection attack | Performance classifiers reduces as the quantity of features increases. | Classifiers fulfilled high performance metric except SVM achieved the vilest performance. However, the model requires to adjust the number of selected features. |
| [83] | Voting, stacking | DDoS | Execution time is high. | The models achieved high performance but the time of execution is high specially in stacking. |
| [84] | DT, SVM, NB | Routing Attack | Overfitting in few classes. | The models achieved high performance metric, but the model lack lacks clarification. |
| [85] | NB, LR, DT, KNN, RF | DDoS | Binary- class classification.<br>Overfitting model. | The model contains two experiments, both fulfilled high performance but only in binary classification. |
| [86] | RF, DT, XGB, GB | MiTM, DoS | Binary-class classification. | The classifiers achieved high performance metric to detect MiTM but achieved reasonable performance metric to detect DoS. |
| [87] | ML | Black hole attack | The energy consumption is high. | The energy consumption is increase by increase the quantity of nodes. |

### 3.2.1. Convolutional Neural Network (CNN)

CNNs are a type of DL model frequently employed for image classification and recognition. They analyze input images and classify them into categories such as dogs, cats, lions, and tigers. Unlike other neural networks, CNNs process images as two-dimensional pixel arrays, focusing directly on the images rather than relying on feature extraction. CNNs consist of three layers: the input layer, which supplies inputs to the model (each neuron in this layer corresponds to features in the data); the hidden layers, which can consist of multiple layers; and the output layer, which converts the outputs of the hidden layers into probability scores for each class using a logistic function such as sigmoid or SoftMax. CNNs have been enhanced with sophisticated architectures such as ResNet and DenseNet, which improve their feature extraction capabilities from IoT traffic data. Moreover, CNNs can utilize multi-channel inputs to analyze various characteristics of network data simultaneously, enhancing their ability to detect complex cyber-attacks. Their capacity to process large datasets makes CNNs highly effective in IoT security, leading to improved detection results. For example, a study in [89] presented a technique combining two CNN models (CNN-CNN) to disclose assaults on IoT networks. Using raw network traffic data, the first CNN model identifies key features that assist in disclosing IoT assaults. The second CNN utilizes these features to generate a strong disclosure model that reliably identifies IoT assaults. The suggested approach attained a confusion matrix score of 98%. The ability of CNNs to concurrently learn relevant features and perform classification removes the need for manual feature extraction, producing an end-to-end model that, with optimization algorithms, offers exceptional results for IoT security-based IDS [90].

### 3.2.2. Recurrent Neural Network (RNN)

RNNs, or Artificial Neural Networks (ANNs), are primarily applied in speech recognition and natural language processing (NLP). RNNs are designed to recognize patterns in various data types, comprising text, genomes, handwriting, spoken language, and numerical time-series data. RNNs are used by systems such as Apple's Siri and Google's voice search for processing sequential data. RNNs are especially effective in IoT security because of their ability to analyze sequential data, making them essential for network IDS (NIDS). Long Short-Term Memory (LSTM) networks enhance RNNs by mitigating the vanishing gradient problem and enabling the detection of long-term dependencies, which are crucial for disclosing IoT security vulnerabilities in time-series data. As a result, DL methodologies such as RNNs have become a central focus in NIDS research [91]. In [92], a proposed model integrated DL and metaheuristic techniques by using RNNs within a multi-modal framework to efficiently capture complex correlations in diverse network traffic data. The model used a wavelet-based feature extraction method to improve the discriminative power of the generated features, achieving remarkable performance metrics with a 98% accuracy score and an AUC of 99%.

### 3.2.3. Auto-Encoders (AEs)

AEs are an area of neural network in which the dimensionality of the input and output layers are equal. Since an AE replicates data from the input to the output in an unsupervised manner, it is also referred to as a replicator neural network. The AE network consists of two main components: the encoder function (h = f(x)) and the decoder function responsible for reconstructing the input (r = g(h)) [1].

The encoder takes the input and converts it into an abstract representation named a code, while the decoder uses this code to rebuild the original input. During AE training, the goal is to minimize reconstruction error. Recent advancements in variational autoencoders (VAEs) have improved their ability to learn data distributions and extract features, increasing their efficacy for unsupervised anomaly detection in IoT security. In IoT networks, AEs can proficiently detect various types of IoT assaults. A study [93] developed an architecture based on an asymmetric parallel autoencoder (APAE), with two encoders working simultaneously, each with three successive layers of convolutional filters. This lightweight architecture enhances AE's ability to detect unknown attacks and improve detection rates. Another study [94] proposed the nonsymmetric autoencoder (NAE) model, where the encoder extracts complex hidden representations of network traffic, and the decoder reconstructs the input data with high accuracy, achieving superior detection rates for abnormal attacks.

### 3.2.4. Restricted Boltzmann Machine (RBM)

RBMs are generative and stochastic neural networks that can model probability distributions over input groups. They are used for feature selection and extraction in various applications, including dimensionality reduction, classification, and regression. RBMs consist of two layers: an input (visible) layer and a hidden layer, which serve as the foundational elements of Deep Belief Networks (DBNs). RBMs excel at pattern recognition tasks such as interpreting handwritten text and identifying radar targets in low signal-to-noise ratio conditions. Additionally, RBMs are used in recommendation systems, enhancing user suggestions through filtering algorithms [95]. Improvements in RBMs, such as layer-wise pre-training, allow these models to develop hierarchical features that improve their ability to detect intricate attack patterns in IoT networks. RBMs are crucial for identifying attacks in IoT environments [96]. A previous study [97] proposed an innovative approach for anomaly detection by projecting raw features through a constrained Boltzmann machine. This approach outperformed several modern methods when evaluated on a widely known anomaly detection dataset, demonstrating strong performance metrics.

### 3.2.5. Deep Belief Network (DBN)

A DBN is a type of generative neural network that uses an unsupervised learning model. DBNs are often referred to as "Boltzmann Machines" and consist of multiple layers of neural networks. They have enhanced their ability to predict complex patterns in IoT traffic for threat detection through unsupervised pre-training followed by supervised fine-tuning. DBNs have emerged as a critical technique for detecting malicious activities in IoT security [98]. While researchers have not yet thoroughly analysed every aspect of DBN-based intrusion detection model, further research is expected to present these techniques in greater detail, as DBNs are ideal for feature extraction and are particularly robust for classification tasks.

### 3.2.6. Generative Adversarial Network (GAN)

GANs are ML models that contains two neural networks competing against each other to improve their prediction accuracy. GANs typically operate in an unsupervised manner within a cooperative zero-sum game framework. To use GANs effectively, the first step is to identify the desired outcome and collect an initial training dataset based on these parameters. GANs have advanced significantly through the use of conditional GANs and semi-supervised learning methods, enhancing their ability to create realistic attack scenarios. This strengthens model robustness and prepares systems to defend against unknown attacks. In IoT security, GANs can proficiently protect systems from unknown intrusions [99]. GANs are also capable of securing the IoT physical layer [100]. A previous study [101] introduced a technique for detecting human activity using generative adversarial micro-aggregation, which improved data privacy while generating realistic samples based on the estimated distribution of the original data. This method showed superior efficacy in securing IoT systems. Despite the benefits of using DL to combat IoT assaults, some challenges remain. Table 7 illustrates the benefits and drawbacks of DL methods and their applicability in assault detection. Table 8 outlines various DL algorithms from previous studies that discuss researchers' efforts to address IoT security challenges referred to in [102-115]. Table 9 summarizes the key hardware and resource requirements for applying ML and DL in low-power IoT devices, which is crucial for optimizing model performance while maintaining energy efficiency and practical operation.

Table 7 Advantages and Disadvantages of DL Techniques

| Technique | Advantages | Disadvantages | Applications |
|---|---|---|---|
| CNN | Ideal for rapid and extremely efficient feature extraction.<br>Require less preprocessing Compared to other methods that are ideal for rapid and highly effective feature extraction.<br>It may employ raw network security data to automatically learn behavior. | Needs high computational power.<br>Highly challenge when using on resource-constrained IoT devices. | Malware attacks<br>Anomaly attacks |
| RNN | Can automatically learn new information and predict sequences based on historical data.<br>Suitable to IoT Security due to IoT environment creates sequential data in some circumstances.<br>high prediction capability. | Addressing the problem of gradients that vanish or extend, which poses difficulties while learning long data sequences.<br>Training Slow and complex tasks. | Malware attacks |
| AEs | Used in dimensionality reduction and extract the features. | Required high computational.<br>Since the training dataset is not typical of the testing dataset, the outcomes could not be what was expected. | Botnet attacks |
| RBM | RMBMs' feedback function enables the elicit of vital features, that are then utilize to log IoT traffic behavior. | Require a lot of computational capacity.<br>Features cannot be represented by a single RBM. | R2L, DoS, U2R and Probe |
| DBN | Exceptionally accurate and reliable.<br>It is suitable for significant feature extraction because it has been trained on unlabeled data. | Demand a large computational cost. | R2L, DoS, U2R |
| GAN | Suitable for Zero-day attack. | Training is challenging and provides erratic outcomes. | Mirai, Bashlite, Scanning, MiTM |

Table 8 Previous Studies IoT Attacks Detection-Based DL Algorithms

| Reference | Algorithm | Attacks | Shortcoming | Observation |
|---|---|---|---|---|
| [102] | DNN | DDoS | Binary-class classification<br>Imbalanced dataset. | The model achieved high performance metric and high AUC Roc Curve, however, the model was limited to binary classification, and if the model was applied to multi-class classification, the performance and detection veracity would differ. |
| [103] | CNN, LSTM | Phishing, DDoS | FPR is high. | LSTM model obtained higher performance evaluation compare to CNN, however, FPR require to be reduced. |
| [104] | AE | DOS, probe, R2L, U2L | Low accuracy.<br>Imbalanced dataset. | The accuracy for the statics and adaptive IDS based attacks is low. |
| [105] | FDL, DNN | Zero-day botnet attack | High training time.<br>BoT-IoT dataset has overfitting. | FDL model outperform high veracity compared to the other models. |
| [106] | DBN | Security breach | Performance metric for unknown attacks is less. | The model fulfilled high performance evaluation, however, the unknown attacks achieved the vilest score. |
| [107] | GAN | Botnet attacks, adversarial evasion attacks | Imbalanced dataset.<br>Performance evaluation slightly low. | GAN obtained high veracity, however the other performance metric achieved low score. |
| [108] | RBM | Anomaly | Performance evaluation need to be increased. | A novel approach has reasonable performance evaluation with 20, and 38 features. However, the more features, the less performance. |
| [109] | DNN, GAN | Anomaly | Some attack class obtained less performance. | GAN model obtained higher performance metric compared to DNN, however, still multi-class classification attacks detection is challenge. |
| [110] | CNN, LSTM | Botnet | The dataset has overfilling. | LSTM achieved high accuracy and performance metric, and less FA, however, with overfitting, the classifiers may misclassify in prediction. |
| [111] | RNN, DNN | DoS, Probe, R2L, U2R | High error rate.<br>The performance metric for each attack not mentioned. | The proposed achieved high-performance evaluation, however, the author mentioned the classifier's average result not each class's performance results. |
| [112] | FFNN, LSTM | Malicious traffic | Binary-class classification. | FFNN achieved better performance metric than LSTM, however, the |

| | | | | |
|---|---|---|---|---|
| | | | | author did not determine type of malicious traffic in the datasets used. |
| [113] | MLP | DDoS | High false positive.<br>Binary-class classification. | The proposed achieved high veracity and true positive, however, the dataset is imbalanced. |
| [114] | DL | Normal, Flooding, Blackhole, and Selective Forwarding | Imbalance dataset.<br>Attacks classes findings not mentioned. | The suggested approach acquired high performance evaluation. However, the dataset is imbalanced and that would affect on the prediction results. |
| [115] | RNN | Botnet | FPR and FNR are high. | The proposed achieved exceptional results. However, the false rate is very high. |

Table 9 Hardware and Resource Considerations for ML and DL in Low-Power IoT Devices

| Aspect | Description |
|---|---|
| Processing Capabilities | Microcontrollers (MCUs): Low-power IoT devices frequently depend on MCUs with constrained processing capabilities relative to conventional CPUs or GPUs. Consequently, ML and DL models must be optimized for efficient performance on these systems. Lightweight algorithms, such as decision trees or linear regression, are better suited for low-complexity problems, but complex models require adaptations to adjust to hardware constraints.<br>Application-Specific Integrated Circuits (ASICs): designed for certain functions can substantially enhance performance and efficiency in ML and DL applications. Hardware accelerators such as Google’s Edge TPU and NVIDIA's Jetson series are designed to execute neural network models with optimal power and speed efficiency. |
| Memory Constraints | RAM and Storage: IoT devices frequently possess constrained RAM and storage space. Models must be sufficiently compact to adhere to these limitations, requiring approaches such as model pruning, which eliminates less significant weights, and quantization, which diminishes weight precision (e.g., from 32-bit to 8-bit), hence decreasing memory consumption.<br>Feature Selection: Employing techniques like PCA to reduce the number of features helps optimize memory utilization and enhance processing efficiency. This is especially significant in IoT environment, where data may be high-dimensional. |
| Energy Efficiency | Low-Power Consumption: Given that numerous IoT devices rely on batteries, reducing energy usage is essential. Optimized algorithms that necessitate reduced computations and diminished data transmission will enhance battery longevity. Methods like as low-power modes and dynamic voltage and frequency scaling (DVFS) can optimize performance and energy consumption.<br>Edge Computing (EC): Performing computations near the data source EC diminishes the necessity for data transmission to centralized computers., hence reducing energy expenses linked to data transfer. This facilitates expedited decision-making and diminishes the total workload on the device. |
| Hardware Accelerators and Frameworks | Dedicated Hardware Accelerators: Devices such as FPGAs (Field-Programmable Gate Arrays) can be configured to execute particular machine learning algorithms effectively, offering a balance between adaptability and performance in IoT applications. |

## 4. EXISTING SURVEYS ON ML AND DL TECHNIQUES

This article presents and discusses previous studies on ML and DL, comparing them with the survey we present. Since 2018, many studies on IoT security have been conducted, with a particular focus on ML and DL applications for IoT security. Our survey addresses the shortcomings in previous discussions of these two techniques, as well as inadequate allocation of attention to their capabilities. For instance, the author in [116] provided a comprehensive review and analysis of diverse ML methodologies, highlighting issues with different ML approaches for detecting invasive activities. The research in [117] analyzed the possibilities and challenges of utilizing data in ML solutions for IoT privacy by exploring various data sources, analyzing them, and examining ML-based solutions currently in development, designed to preserve IoT privacy. In [118], the threats to IoT security were reviewed, along with a systematic analysis of those threats from both the training and testing/inference perspectives. The author categorized current ML-based defensive techniques into four groups.

The research in [119] focused on studies related to intrusion detection (ID) for computer network security and ML techniques for IoT. In [120], the Cisco IoT reference model architecture was used to classify well-known security concerns, allowing the study to focus on IoT security threats and vulnerabilities. Additionally, an analysis of previous studies on DL-based IDS in IoT security was included. In [121], the IoT design was presented after an in-depth literature analysis of ML techniques and the essential role of IoT security concerning various attack vectors.

In [122], the IoT network security needs, assault vectors, and available security solutions were analyzed. The author also highlighted the weaknesses in existing security solutions that require ML and DL techniques and detailed the various ML and DL technologies currently available to tackle security concerns in IoT networks. The study in [123] evaluated current approaches for categorizing IoT security risks and challenges in IoT networks, with a focus on network intrusion detection systems (NIDS). A thorough analysis of NIDS using various IoT learning strategies was also provided.

In [124], the notion of malware and botnets causing DDoS assaults in IoT was outlined and contrasted, along with the different DDoS defense strategies. In [125], a detailed investigation of IoT malware disclosure and static analysis methods was presented, covering key techniques, along with the pros and cons of current static IoT malware disclosure frameworks.

In [126], assaults were classified into groups based on the most pertinent security threats, countermeasures, and real-world assaults across the generalized IoT/IIoT architecture. The study also discussed how blockchain can be applied to efficiently address these issues. The study in [127] provided fundamental information on security threats and safeguards in IoT networks, covering topics such as the IoT market, security architecture, and procedures for security managers and IoT developers. The author in [128] discussed primary security and forensic issues in the IoT domain and presented papers addressing these topics.

In [129], DNN topologies and the potential benefits of deep learning were discussed, along with a detailed analysis of IoT use cases powered by DL. In [130], a comprehensive overview of current IoT security solutions and developments was presented, focusing on IoT security threats. The survey in [131] provided a recent overview of various ML techniques for IoT applications, covering supervised and unsupervised models that support IoT frameworks and the importance of ML models in relation to IoT.

In [132], a classification system for IoT attacks was provided, along with an examination of IoT security weaknesses at different levels. The study also presented an analysis of recent security systems by evaluating the effectiveness of new solutions. The study in [133] reviewed IoT security protection and concluded that AI methods such as ML and DL can offer novel abilities to meet IoT security requirements. In [134], a brief description of ML and DL-based IDS was provided, discussing different types of assaults and anomalies and how these systems disclose them.

In [135], a detailed account of cutting-edge approaches to IoT data challenges was provided, while in [136], a systematic literature review (SLR) examined the utilize of DL approaches for anomaly-based IDS in IoT environments. The study extracted data from sources like IEEE Xplore, Scopus, WoS, Elsevier, and MDPI. In [137], a summary of DL techniques in cybersecurity applications was provided, including explanations of GANs, RNNs, restricted Boltzmann machines, and deep autoencoders (AEs), followed by how these DL methods apply to various types of assaults such as network intrusions, malware, spam, insider threats, and more.

In [138], a review of the pros and cons of ML algorithms in IoT security was presented, with a concentrate on the application of DL and Federated Learning (FL) in IoT security. FL models enable systems to share information while protecting data privacy. In [139], the specifics of ML security attacks in cyber-physical systems were outlined, along with defense strategies, threat models, and a comparative analysis of ML model performance under diverse assault scenarios. The study in [140] reviewed privacy and security concerns related to DL algorithms, categorized various assault types, and examined protection strategies, including privacy-preserving techniques like Homomorphic Encryption (HE) and hash functions.

The study in [141] discussed the major security problems and challenges that IoT infrastructures face, providing a thorough examination of ML-based solutions for IoT security. Additionally, the limitations of common ML-based security techniques for IoT were discussed. In [142], a tutorial-style analysis of advanced DL architectures for cybersecurity applications was provided, along with an evaluation of recent contributions and challenges.

In [143], the latest findings on ML/DL-based scheduling strategies were examined, covering the trade-offs between accuracy and execution time, as well as the security and privacy of learning-based algorithms in real-time IoT systems. The study in [144] aimed to enhance IoT device security by reviewing ML systems and the latest advances in DL techniques, identifying future IoT device threats and protection concerns. The study also evaluated DL/ML strategies for IoT security, discussing their potential and limitations.

Lastly, in [145], a comprehensive overview of IoT security intelligence based on DL/ML technologies was presented, highlighting research topics and future directions. Prior studies have substantially enhanced our comprehension of IoT security, although it is impossible to cover every aspect in one study. We analyzed these studies along with additional studies [146-150], classified their contributions from 2018 to the present in a sequential and descending order based on the years of publishing, and compared them with our survey, as summarized in Table 10.

### 4.1. Research Papers Methodology

In this survey, a collection of research articles was compiled from various sources, including Elsevier, IEEE, Springer, MDPI, ACM, Hindawi, and others, published between 2018 and 2024. These articles focus on ML and DL survey papers and models. Each study was analyzed based on the problem statement it attempted to tackle, the domain in which it was executed, the types of attacks it aimed to detect, the methods used to address the problem, and the outcomes obtained. A total of 200 papers were gathered for the literature review on ML and DL methods.

Figure 6 illustrates the number of papers published in the journals mentioned in this survey, showing an increase in publications from Elsevier and IEEE compared to other sources. Additionally, Figure 7 highlights the number of papers published between 2018 and 2024.

Table 10 Analyzing and Classifying the Previous Studies Between 2018-2024

| Reference | Year | ML | DL | Dataset | Domain | Attacks/Threats | Countermeasures | Challenges/Issues |
|---|---|---|---|---|---|---|---|---|
| [116] | 2018 | ✔ | ✖ | ✖ | ✖ | ✔ | ✔ | ✔ |
| [118] | 2018 | ✔ | ✖ | ✖ | ✖ | ✔ | ✔ | ✔ |
| [128] | 2018 | ✖ | ✖ | ✖ | ✖ | ✖ | ✖ | ✔ |
| [119] | 2019 | ✔ | ✖ | ✔ | ✖ | ✖ | ✖ | ✔ |
| [122] | 2019 | ✔ | ✔ | ✖ | ✖ | ✔ | ✔ | ✔ |
| [123] | 2019 | ✖ | ✖ | ✔ | ✖ | ✔ | ✔ | ✔ |
| [124] | 2019 | ✔ | ✖ | ✖ | ✖ | ✔ | ✔ | ✔ |
| [126] | 2019 | ✖ | ✖ | ✖ | ✔ | ✔ | ✔ | ✔ |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [1] | 2020 | ✓ | ✓ | ✗ | ✓ | ✓ | ✗ | ✓ |
| [117] | 2020 | ✓ | ✗ | ✗ | ✗ | ✗ | ✗ | ✓ |
| [120] | 2020 | ✗ | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ |
| [121] | 2020 | ✓ | ✗ | ✓ | ✗ | ✓ | ✓ | ✓ |
| [125] | 2020 | ✗ | ✗ | ✓ | ✗ | ✓ | ✓ | ✗ |
| [127] | 2020 | ✗ | ✗ | ✗ | ✗ | ✓ | ✓ | ✗ |
| [129] | 2020 | ✗ | ✓ | ✓ | ✓ | ✗ | ✓ | ✗ |
| [133] | 2020 | ✓ | ✗ | ✗ | ✗ | ✓ | ✓ | ✗ |
| [134] | 2021 | ✓ | ✓ | ✗ | ✗ | ✓ | ✗ | ✓ |
| [135] | 2021 | ✓ | ✓ | ✓ | ✗ | ✗ | ✗ | ✓ |
| [136] | 2021 | ✗ | ✓ | ✓ | ✗ | ✓ | ✗ | ✓ |
| [137] | 2021 | ✗ | ✓ | ✓ | ✗ | ✓ | ✓ | ✗ |
| [140] | 2022 | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ | ✗ |
| [143] | 2022 | ✓ | ✓ | ✗ | ✗ | ✗ | ✓ | ✗ |
| [144] | 2022 | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ | ✗ |
| [150] | 2022 | ✓ | ✗ | ✗ | ✗ | ✓ | ✓ | ✓ |
| [138] | 2023 | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ | ✗ |
| [142] | 2023 | ✗ | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| [145] | 2023 | ✓ | ✓ | ✗ | ✗ | ✗ | ✗ | ✓ |
| [146] | 2023 | ✓ | ✗ | ✓ | ✗ | ✓ | ✗ | ✗ |
| [147] | 2024 | ✓ | ✓ | ✗ | ✗ | ✓ | ✓ | ✗ |
| [148] | 2024 | ✓ | ✗ | ✗ | ✓ | ✗ | ✓ | ✗ |
| [149] | 2024 | ✓ | ✓ | ✗ | ✓ | ✓ | ✓ | ✗ |
| Our Survey | 2024 | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |

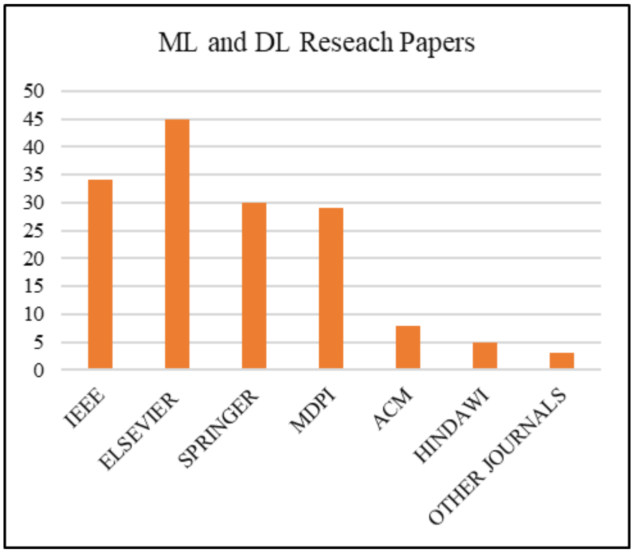


Figure 6 Number of Papers Published in the Journals

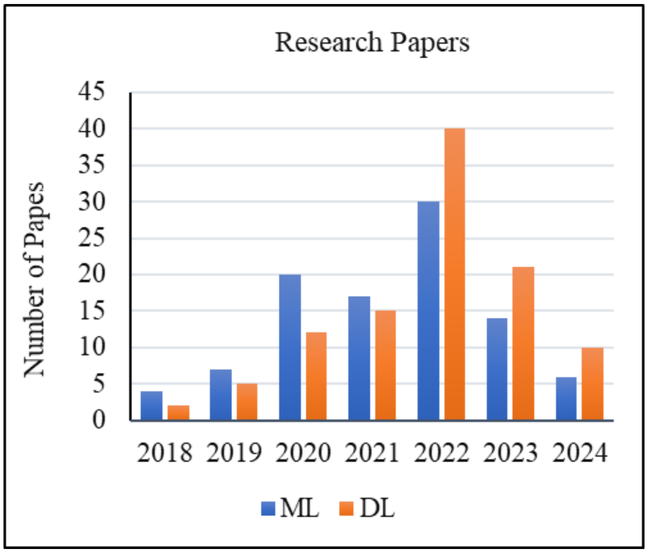


Figure 7 Papers Published Between 2018-2024

## 5. CLASSIFICATIONS OF IOT LAYERS ATTACKS

As mentioned in Section 2, the IoT architecture contain of three key tiers: the perception layer, network layer, [151], and application layer, as demonstrated in Figure 4. The perception layer is made up of sensors and controllers that collect data. The network layer's primary role is to establish connections between networks, using protocols and various connections. Finally, the application layer responds to the user and software programs, allowing users to access and retrieve data.

The goal of this section is to understand the risks of attacks at each layer and provide an overview of the solutions offered by researchers, along with the benefits of each study. This section discusses the types of assaults at each layer and the solutions presented by researchers.

### 5.1. Perception Layer Attacks

This layer in IoT is accountable for gathering information via actuators, Zigbee, and RFID. It faces a variety of attacks aimed at damaging or destroying its devices. Attackers may penetrate and modify devices through social engineering, launching large-scale attacks such as device destruction, eavesdropping, or other assaults. Physical assaults, such as manipulating energy sources or disrupting communication mechanisms, may require the attacker to be in close proximity to the target. For example, physical attacks like jamming, eavesdropping, interference, and traffic analysis can disrupt the physical layer. Robust approaches, including ML/DL technologies, are required to detect and secure this layer. Several researchers have addressed physical layer attacks, particularly jamming attacks using radio frequency (RF). One technique compared SVM and K-NN methods in multi-track and single-route scenarios. The RF technique, combined with AdaBoost, achieved superior findings compared to other methods. Additionally, RF showed better accuracy and lower false alarms compared to other techniques. In [152], the author proposed P4NIS, a network invulnerable schema with three layers of protection to identify and prevent eavesdropping attempts. The findings showed that, compared to contemporary techniques, P4NIS reduced encryption costs by 69.85%–81.24% and minimized false alarms. In [153], a ML model using SVM was presented to classify spoofing assaults on signals received by unmanned aerial vehicles (UAVs). K-fold examinations were conducted to improve the learning pattern, which was termed K-learning. The model, using GPS features, achieved high levels of accuracy, precision, recall, and F-score (99%, 98%, 99%, and 98%) when compared to earlier research. Additionally, Table 11 summarizes a few studies, [154], [155], [156], [157] detailing the contribution of each study, the type of assault tackled, and the outcomes obtained.

Table 11 Attack Detection in Physical Layer

| Reference | Contribution | Attacks | Algorithm | Results |
|---|---|---|---|---|
| [154] | The study provided a wireless fingerprinting-based PHY-layer continuous authentication and spoofing disclosure method for a real WSN in which diverse nodes connect to a central sink node. | Spoofing | DT | ACC: 95.43 |
| [155] | The author used DL with LSTM to provide confidentiality and privacy in physical layer. | DDoS | LSTM | ACC: 0.99<br>AUC: 0.99<br>R: 0.98<br>P: 0.95 |
| [156] | Proposed a CDAE model that decreases feature dimensions, removes noise, and extracts key vectors. | Malicious | AE | ACC: 0.98<br>AUC: 0.99 |
| [157] | Provided the advanced hybridized optimization technique AHGFFA to avoid attacks issues using USML in the MANET-IoT sensors system. | Malicious | UML | DR: 0.98<br>EC: 5 |

### 5.2. Network Layer Attacks

This layer is accountable for transmitting data from the perception layer to the application layer for processing [158]. This layer faces several threats, including eavesdropping, man-in-the-middle (MITM) assault, Sybil assault, routing information threats, and DDoS. When compromised, IoT devices may become botnets, enabling hackers to hinder communication paths between source and destination. Hackers can also launch Sybil attacks by exploiting compromised or fake nodes, tampering with security keys and routing tables, which can affect higher levels of the IoT system. Because the network layer sits between the physical and application layers, it plays a vital role in IoT security. Numerous efforts have been made to secure this layer, with many studies achieving exceptional results in disclosing IoT assaults at the network layer. Table 12 analyzes studies [159-164] related to IoT assaults at the network layer.

### 5.3. Application Layer Attacks

This layer handles several data transactions and is responsible for establishing a user interface between end users and endpoints. Securing the application layer poses significant challenges. Many of the vulnerabilities found here are based on sophisticated user inputs that are difficult to disclose with IDS. Additionally, this layer is vulnerable to software-based assaults such as malware, viruses, worms, etc., and is publicly accessible and visible to everyone. One notable example of an application layer attack is SQL injection, which was responsible for significant data breaches in 2014. SQL injection ranks third in frequency of attacks after DDoS and malware. Other common vulnerabilities in this layer include security misconfiguration, which allows hackers to alter program details and access confidential information without being detected by network security measures. In Table 13, we present recent studies [165-170] that address IoT attack detection at the application layer. Additionally, Figure 8 illustrates the taxonomy of IoT attack layers.

In Section 2, we discussed the prominent assaults in the IoT environment, which are considered the most critical threats impacting general IoT security. In this section, we have outlined the attacks that occur in each tier, focusing on the primary challenges in each layer. This helps researchers identify issues specific to each layer and gain comprehensive knowledge of the challenges within each IoT layer. Table 14 provides detailed information, and Table 15 outlines the key principles of attacks on IoT layers [171-185].

Table 12 Attack Detection in Network Layer

| Reference | Contribution | Attacks | Algorithm | Results |
|---|---|---|---|---|
| [159] | Presented a DL model named DeepAK-IoT to disclose cyber-assaults in IoT networks. | Botnet | DeepAK base DL | ACC: 90.57<br>F1: 88.87<br>P: 89.59 |
| [160] | Used DL to present a new anomaly-based IDs method for IoT networks. In particular, a DNN model with filter-based FS that eliminates highly linked features has been introduced. Additionally, the model is fine-tuned utilizing a range of parameters and hyperparameters. | DoS | DNN, GAN-DNN | ACC:<br>DNN: 84.4<br>GAN-DNN: 90.9 |
| [161] | The author provided a new technique using the RF classifier to get over the attacks. This method utilizes EL to combine many DRs in order to generate precise and efficient forecasts for the quick identification of hazards in IoT networks. | DDoS | RF | ACC: 99.53<br>P: 0.99<br>F1: 0.98<br>AUC: 0.99 |
| [162] | The author designs a model using ensemble approaches on the KDD Cup 99 dataset after doing a survey of the literature on the most recent studies utilizing deep learning techniques. | Anomaly | AE, GAN | AE = ACC: 97.96<br>P: 90.68<br>GAN =<br>ACC: 90.26<br>P: 91.27 |
| [163] | Provided an IDS defensive system that applies anomaly disclosure and ML to enhance the security of IoT networks against DoS assault. They also used two several features selection algorithms, the GA and the Correlation-based Feature Selection (CFS) algorithm, and evaluated how well they performed. | DoS | DT, RF, SVM, KNN | ACC, P, R, F1 are 0.99 for all classifiers |
| [164] | This paper provided a novel ID method IoT devices based on DL. To identify malicious traffic that could start an assault on linked IoT gadgets, this intelligent system employs a four-layer deep Fully linked (FC) network architecture. Based on the experimental performance analysis, the suggested system demonstrated reliable performance for both simulated and real invasions. | Blackhole<br>Sinkhole<br>Workhole<br>DDoS | DNN | ACC: 93.74<br>P: 93.73<br>R: 93.82<br>F1: 93.47<br>DT: 93.21 |

Table 13 Attack Detection in Application Layer

| Reference | Contribution | Attacks | Algorithm | Results |
|---|---|---|---|---|
| [165] | This research, which focused on communication and environmental dynamics in industrial settings, proposed a novel method for detecting jamming in IoT. It focused on gathering QoS, and connection parameters during normal communication and | Jamming | Stack LSTM | ACC: 99.5<br>P: 99.4<br>R: 99.26 |

| | | | | |
|---|---|---|---|---|
| | jamming assaults in production lines equipped with wireless IoT gadgets with server-client architecture in order to better examine the communication conditions and jamming in the industrial production environment. | | | S: 99.66<br>F1:99.34 |
| [166] | The study presented FMDADM, a framework for SDN-enabled IoT networks that applied ML for DDoS disclosure and mitigation. Three disclosure modules and a mitigation module make up the suggested framework. | DDoS | RF, SVM, KNN, GNB, DT | ACC: 99.79<br>P: 99.43<br>F1: 99.77<br>R: 99.79<br>S: 99.59<br>FPR:0.91<br>FNR:0.23 |
| [167] | This paper offered a ML model to detect DDoS against CoAP | DDoS | DT, RF, LSVC, NB | ACC=<br>RF, DT: 0.98<br>P, R, F1=<br>RF, DT: 0.92 |
| [168] | Introduced an IoT micro-security extension that is integrated into the device. This extension utilizes a CNN model to identify and prevent URL-based assaults targeted at a client's IoT gadgets. An LSTM model is deployed on the backend servers to identify botnet assaults on IoT gadgets. | Phishing, DDoS | CNN, LSTM | CNN=<br>ACC: 0.94<br>AUC: 0.92<br>LSTM=<br>ACC: 0.97<br>AUC: 0.99 |
| [169] | Proposed an AD method utilizing the DNN for the IoT network layers to taxonomy traffic as normal and abnormal. | Theft, DoS, DDoS, | DNN | ACC: 0.99 |
| [170] | This work presented a novel IDS using ML in the application and transport layers, the author used BoT-IoT dataset | DDoS, DoS | DL, ML | ACC; 0.99<br>CM: 0.99 |

Table 14 IoT Architecture

| Layer | Attack | Major Purpose | Challenges |
|---|---|---|---|
| Perception Layer | Reverse Engineering.<br>Jamming.<br>Social Engineering.<br>Tampering.<br>Spoofing.<br>DoS.<br>RF Interference.<br>Signal Manipulation. | Collected Information | IoT is unreliable and susceptible to hackers.<br>Destroying perception gadgets and falsifying data collected.<br>The devices are resource constrained.<br>Data confidentiality.<br>Power consumption.<br>Reliability. |

| | | | |
|---|---|---|---|
| Network Layer | MiTM.<br>DDoS.<br>DoS.<br>Spoofing.<br>Routing attacks<br>Sinkhole attacks<br>RFID clone.<br>Sybil attack.<br>Eavesdropping.<br>Traffic analysis.<br>Ransomware. | Deliver the collected data | TCP and IP protocol.<br>Energy effectiveness.<br>Network congestion due to high volume of data on network.<br>Dynamic Network Structure.<br>Heterogeneity.<br>Confidentiality. |
| Application Layer | Malicious and Code.<br>Injection attacks.<br>XSS.<br>DNS spoofing and phishing.<br>SQL injection.<br>Manipulation of data.<br>Software Tampering.<br>API abuse. | User-requested assistance | User Interaction and Experience.<br>Performance and Scalability.<br>High volume data lead to massive issue in IoT security.<br>Leak of data due to attacks against software.<br>Resilience and Reliability. |

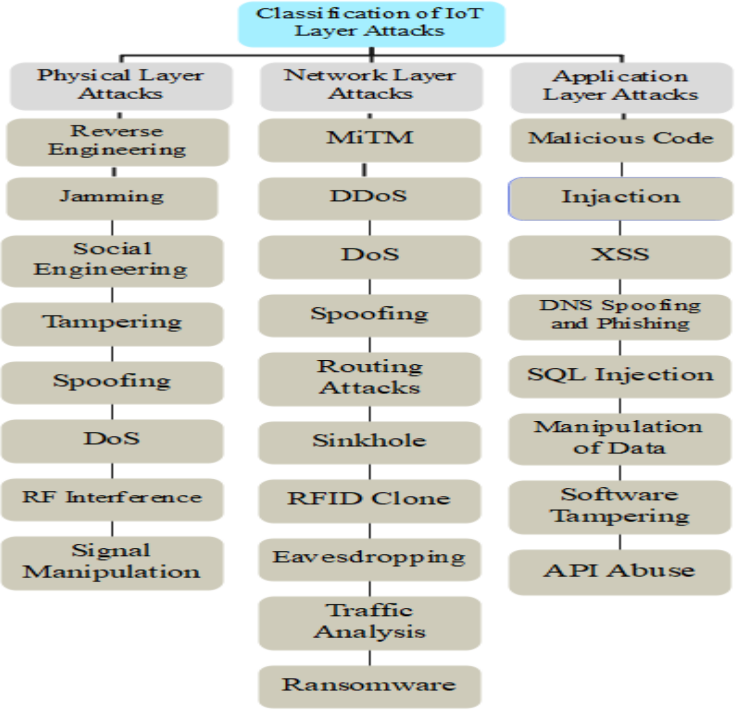


Figure 8 IoT Attacks Layer Classification

Table 15 The Principle of Attacks in IoT Layers

| Attacks | Description |
|---|---|
| Tampering Attack [171] | A form of physical assault when the attacker aims to breach security, alters memory, and gains further information by reacting with a malfunctioning device |
| Spoofing Attack [172] | Hackers pose as authorized users or devices in order to distribute malware, steal data, and get around access control measures. |
| Reverse Engineering [173] | A person-to-person assault where the criminal makes direct connect with the target in an attempt to get them to furnish crucial information. |
| Physical damage [174] | Carrey out in a situation where the hacker is approaching the device. A malicious user has the capability to take control a computer or communication system, harm property, and jeopardize lives. |
| RFID Cloning [175] | Signifies the process of duplicating the data from an RFID electronic tag or intelligent card to a cloned tag that will resemble the original tag and possibly replace it. |
| RF interface [176] | Target devices that employ radio, Wi-Fi, Bluetooth, and Bluetooth Low Energy (BLE) as communication means |
| Code and malicious [177] | Malicious software, sometimes known as malware, that has the ability to rapidly or gradually damage client PCs, databases, networks, and even server clusters. |
| Injection attacks [178] | A malicious code injected into the network which retrieves all the data from the database to the hacker. |
| DNS Spoofing and Phishing. [179] | Attackers may spoof DNS responses or launch phishing attacks aiming IoT applications to disclosing private data including login passwords or bank account information |
| SQL injection [180] | SQL injection assault exploit weaknesses in IoT apps that store and retrieve data from databases. Attackers can extract sensitive data, alter database contents, or run unauthorized instructions on the underlying database server by adding malicious SQL queries in the input fields or API parameters. |
| XSS [181] | Cross-site Scripting attacks penetrate websites visited by other users with malicious scripts, aimed targeting web-based Internet of Things applications. Attackers can alter web interfaces, take illicit actions on behalf of authorized users, and steal session cookies by taking advantage of XSS vulnerabilities. |
| Software Tampering [182] | On IoT devices, hackers may tamper with the firmware or software to add backdoors, vulnerabilities, or malicious features. Firmware-altering assaults pose a vital risk to the security, reliability, and integrity of IoT gadgets by allowing data to be exfiltrated, causing malfunctions or unauthorized access. |
| Sybil attacks [183] | A group of nodes that broadcast fake data from a random network by pretending to be several peer identities in order to compromise an IoT ecosystem. |
| API abused | Assailants misuse Application Programming Interfaces (APIs) made available by IoT applications to carry out illicit operations, obtain private information, or alter device settings. Attacks using API abuse can take advantage of poorly constructed APIs, weak access restrictions, or insufficient input validation systems. |
| Manipulation of data | In order to trick consumers, set off false alarms, or bring about disruptive events, attackers alter or corrupt data that is transferred between IoT gadgets and applications. Attacks that modify data might jeopardize the integrity and reliability of IoT systems, resulting in incorrect judgments or actions taken in responding to misrepresented data. |

| | |
|---|---|
| Routing attacks [184] | Routing attacks aim to modify or interfere with device-to-device communication by targeting the routing protocols and techniques utilized in IoT networks. Attackers might, for instance, create routing loops, reroute traffic to hostile nodes, or insert erroneous routing information, all of which could cause network congestion or fragmentation. |
| Ransomware [185] | Attacks using ransomware encrypt or prevent users from accessing files, systems, or devices and demand a ransom to be paid by the target in order to unlock the device. Ransomware can harm an organization's brand in addition to causing large financial losses and operational problems. |

## 6. INTERNET OF THINGS SECURITY DATASETS

In this paper, we discuss the datasets commonly used to construct IoT security models. We focus on the typical and popular datasets that help researchers gain insights into the types of datasets they will use to develop models for identifying IoT attacks. Additionally, we discuss the pros and cons of each dataset, along with research papers that have utilized these datasets.

### 6.1. BoT-IoT Dataset

This dataset is an extensive dataset for IoT botnet research, containing both malicious and benign traffic gathered from various IoT gadgets. It simulates real-world IoT network conditions by incorporating traffic data from multiple IoT devices. The dataset contains five distinct attack scenarios, each with several assault variations, and was created at UNSW Canberra's Cyber Range Lab. The source files are available in multiple formats, including CSV files, Argus files, and original pcap files. The dataset includes attacks such as DDoS, DoS, OS and service scanning, keylogging, and data exfiltration, with DDoS and DoS assaults further classified based on the protocol used [186]. The dataset serves as a reference for assessing the performance of ML and IDS IDS in identifying IoT botnet activity.

### 6.2. UNSW-NB15 Dataset

The dataset an extensively used network traffic dataset for assessing IDS. The UNSW-NB 15 dataset was generated in the UNSW Canberra Cyber Range Lab using the IXIA PerfectStorm tool to build a blend of real-world modern-day activities and artificial modern-day assault behaviors. It comprises of about two million records totaling 49 features that were obtained with the aid of Argustools, Bro-IDS, and a few specially developed algorithms. The labeled dataset UNSW-NB15 includes network traffic information gathered under controlled environment [187].

### 6.3. ToN-IoT Dataset

This dataset is one of the recent IoT and IIoT datasets, designed to assess the accuracy and effectiveness of various AI-based cybersecurity technologies. It includes data from IoT and IIoT sensor telemetry datasets, Windows 7 and 10 operating system datasets, and TLS and network traffic statistics from Ubuntu 14 and 18. The dataset was gathered from a large-scale, realistic network at the Australian Defense Force Academy (ADFA), School of Engineering and Information Technology (SEIT), UNSW Canberra, and the IoT Lab of UNSW Canberra Cyber [188].

### 6.4. IoT-23 Dataset

The dataset comprises network traffic data from 23 distinct IoT gadgets across different categories, addressing various IoT applications such as industrial control systems, wearable technologies, intelligent home devices, and healthcare equipment. The dataset includes traffic from devices like fitness trackers, IP cameras, smart doorbells, smart thermostats, and industrial sensors. The IoT-23 dataset aims to support IoT security research and development, particularly in traffic analysis, anomaly detection, and IDS. Researchers can employ this dataset to evaluate the effectiveness of security algorithms and processes in protecting IoT networks and devices [189].

### 6.5. MQTT-IoT-IDS2020 Dataset

In machine-to-machine (IoT) communication, one of the most utilized protocols is the Message Queuing Telemetry Transport (MQTT) protocol. It is the initial dataset that mimics a network based on MQTT. 12 sensors, a broker, a phony camera, and an assailant make up the network. A dataset concentrates on IoT security, specifically to identifying security risks in IoT networks utilizing the MQTT protocol. IDS for IoT networks can be trained and assessed using the labeled data in the dataset, which includes both normal and assault traffic [190].

### 6.6. CICIDS 2017 dataset

This dataset is a labeled network traffic dataset collected in a controlled environment. It was generated as a result of research conducted by the Canadian Institute for Cybersecurity (CIC). The dataset's primary objective is to promote cybersecurity research and development, especially in IDS.

It provides a standard benchmark for assessing the effectiveness of IDS methods and algorithms. The dataset captures network protocol traffic, such as TCP, UDP, and ICMP, along with traffic from various services and applications, offering a broad range of network behaviors for analysis [191].

### 6.7. CTU-13 Dataset

The CTU-13 dataset, generated by the Czech Technical University (CTU) in Prague, is a popular benchmark dataset in cybersecurity, particularly for NIDS. It contains of labeled network traffic data generated in a lab setting that simulates various types of cyberattacks [192].

### 6.8. NetFlow BoT-IoT Dataset

The BoT-IoT dataset was employed to build the NF-BoT-IoT v1 dataset, an IoT NetFlow-based dataset. The features were extracted from publicly available pcap data, and the flows were labeled with the appropriate attack types. There are 600,100 data flows in total, of which 13,859 (2.31%) are benign, and 586,241 (97.69%) are assault samples.

The dataset includes four distinct assault categories. The distribution of all flows in this dataset is demonstrated in the table below [193]. The dataset has two versions: version one (discussed here) and version two, which also uses features extracted from pcap data and labeled flows.

In version two, out of 37,763,497 total data flows, 37,628,460 (99.64%) are assault samples, and 135,037 (0.36%) are benign. The dataset contains four distinct assault categories.

### 6.9. NetFlow ToN-IoT dataset

The NF-ToN-IoT v1 dataset was created utilizing the publicly accessible pcap files from the ToN-IoT dataset to generate its NetFlow records. This resulted in the NF-ToN-IoT NetFlow-based IoT network dataset. Of the total 1,379,274 data flows, 270,279 (19.6%) are benign samples, and 1,108,995 (80.4%) are attack samples. The NF-ToN-IoT v2 dataset was similarly produced utilizing publicly available pcap files, resulting in 16,940,496 total data flows, of which 10,841,027 (63.99%) are assault samples, and 6,099,469 (36.01%) are benign. Both NetFlow datasets, NF-BoT-IoT v1 and v2, as well as NF-ToN-IoT v1 and v2, were created by Mohanad Sarhan [193].

### 6.10. N-BaIoT Dataset

The dataset tackled the scarcity of botnet databases, particularly in the IoT domain. It contains authentic traffic data collected from nine commercial IoT gadgets confirmed to be infected with the BASHLITE and Mirai botnets [194]. Furthermore, there are several other IoT datasets that are less prevalent. For more details and further knowledge, refer to [195].

In this section, we provided an overview of key IoT security datasets, along with references to assist researchers in easily locating them. Each dataset has its advantages and disadvantages, which we will outline in Table 16. Additionally, Table 17 presents some studies [196-205] that have utilized these IoT security datasets.

Table 16 IoT Datasets

| Dataset | Attack type | Advantages | Disadvantages |
|---|---|---|---|
| BoT-IoT | DDoS, DoS, OS and Service Scan, Keylogging and Data exfiltration attacks. | Real-Word Network Traffic.<br>Include a wide variety of IoT gadgets and assault scenarios.<br>Labeled Data.<br>New generated Features.<br>Accessibility Dataset. | Imbalanced Dataset.<br>Accurately labeling network traffic data can be challenging.<br>Has overfitting.<br>Privacy Issues. |
| UNSW-NB15 | Fuzzers, Analysis, Backdoors, DoS, Exploits, Generic, Reconnaissance, Shellcode and Worms. | Realistic Dataset.<br>Offers CSV files and network traffic (PCAP).<br>Labeled Dataset.<br>Diversity Dataset.<br>A collection of a wide array of features derived from network traffic. | Developed with a synthetic environment for producing assault activities.<br>Imbalanced Dataset.<br>Deficiency of update. |

| | | | |
|---|---|---|---|
| ToN-IoT | DoS, DDoS and Ransomware. | Include heterogeneous data sources.<br>Realistic traffic.<br>Cove various attacks. | Launched exclusively on IIoT Network computer systems, IoT gateways, and web applications.<br>Restricted acceptance and validation in the field of cybersecurity research |
| IoT-23 | Malware | An extensive dataset.<br>Labeled dataset.<br>Contain various of protocol which assist researchers to evaluate various IoT device and protocol interactions and vulnerabilities.<br>Benefield for security research. | Imbalanced dataset.<br>Limited to attacks type.<br>Contain Biases which leads to influence the outcomes.<br>Contain sensitive information due to its real-word dataset. |
| MQTT-IoT-IDS2020 | SSH-Brute Force, MQTT brute-force attack, aggressive scan, UDP Scan | Real word traffic data.<br>Includes an extensive amount of network traffic data<br>Contain divers type of attacks. | Dependence on particular protocol.<br>Captures of static network traffic. |
| CICIDS 2017 | Brute Force FTP, Brute Force SSH, DoS, Heartbleed, Web Attack, Infiltration, Botnet and DDoS. | Real-word traffic network.<br>Labeled dataset.<br>Accessibility dataset. | Imbalanced dataset.<br>Contain limited attacks.<br>Need preprocessing for optimization which cause computational cost. |
| CTU-13 | Botnet, Malware | Real-word dataset.<br>Scalability dataset.<br>Labeled dataset. | Limited attack type. |
| NF- BoT-IoT v1, v2 | Benign, DoS, DDoS, theft, Reconnaissance | Real-word data traffic.<br>Applied to disclose Botnet attacks.<br>Used in IoT security researches. | Data quality issues.<br>Analytical complexity.<br>Imbalanced dataset.<br>Contain noise. |
| NF-ToN-IoT v1, v2 | Benign, Backdoor, MiTM, Password, XSS, Scanning, DoS, DDoS, Injection, Ransomware. | Real-word dataset.<br>Contain data different IoT devices.<br>Used in Anomaly detection. | Contain Biases.<br>Contain Noise.<br>Focus only on traffic data.<br>Imbalanced Dataset. |
| N-BaIoT | Mirai, Bashlite | Real Data collected for 9 IoT devices.<br>Used in Anomaly detection. | Imbalanced and Biases dataset.<br>Limited volume of network traffic. |

Table 17 Studies Related to IoT Datasets Using ML and DL Techniques

| Refences | Dataset | Attack | Method used | Findings |
|---|---|---|---|---|
| [196] | UNSW-NB15 | Intrusion | ANN | ACC: 0.84 |
| [197] | BoT-IoT | DoS | ML (SVM, RF), DL (CNN) | ACC:0.90 |
| [198] | MQTT dataset | Brute force, DoS, Flood, Legitimate, Malformed | NN, RF, NB, DT, GB MPL | ACC: 0.98<br>Time: 30s. |
| [199] | CSE-CIC-IDS2018, ToN-IoT, UNSW-NB15 | DDOS, DOS, Backdoor, Injection, MITM, Ransomware, Scanning, Password, XSS | ML (LR, DT, NB), DL (DFF, RNN, CNN) | DT: 0.99 |
| [200] | NF-BoT-IoT<br>NF-ToN-IoT<br>NF-CSE-CIC-IDS2018-v2<br>NF-UNSW-NB15-v2 | Botnet | XGB | ACC: 0.97<br>AUC: 0.99<br>Recall: 0.98<br>Precision: 0.99 |
| [201] | CTU-13 | Botnet | EL, DT, KNN, RF | ACC: 99.07<br>CM: 0.1<br>Time: 12.99s<br>RTime: 0.0004s |
| [202] | IoT-23 | DDoS, botnets like Mirai, Okiruk | KNN, RF | ACC: 0.89<br>Precision: 0.1<br>Recall: 0.81 |
| [203] | N-BaIoT | Mirai and BASHLITE | Supervised and Unsupervised ML | ACC: 99.92 |
| [204] | CIC-IDS2017 | DDoS, Probe, Web attacks, DoS | Hybrid DL | ACC: 99.32 |
| [205] | UNSW-NB15 | Norma, Generic, Exploits, Fizzers, DoS, Reconnaissance, Analysis, Backdoor, Shell code, and Worms | ANN, CNN, LSTM, RNN | ACC: 95.97<br>Training Timing: 6043.32s |

## 7. CHALLENGES, FUTURE TREND, AND DISCUSSION

ML and DL are essential components in ensuring the security of IoT systems; however, they face diverse challenges in IoT security. This section presents the challenges linked to ML and DL in relation to IoT security. Furthermore, it provides a discussion on the roles, future trend, and the limitations of ML and DL methods.

### 7.1. Machine Learning challenges

This section concentrates on the challenges of ML in the IoT environment, summarizing essential obstacles to help researchers build a comprehensive understanding of ML algorithms.

#### 7.1.1. Quantity and Quality of Data

Data is considerable for training ML models. The data generated by several IoT gadgets may be noisy, incomplete, or inconsistent, making it difficult to ensure data quality. Additionally, having enough labeled data for training robust models is a significant challenge.

#### 7.1.2. Scalability and Heterogeneity

IoT gadgets vary widely in design, protocols, and communication standards. Developing ML models that can handle this heterogeneity accurately and scale to support large IoT deployments is challenging.

#### 7.1.3. Insufficient Training Data

Training data is crucial for achieving accurate results in ML. Insufficient data can lead to biased or erroneous predictions. Research indicates that when algorithms are trained with limited data, the accuracy can fluctuate as the data increases, highlighting the need for appropriate training data.

#### 7.1.4. Selection the proper ML techniques

Choosing the correct ML classifier is vital for producing accurate results. Using an inappropriate algorithm can lead to inaccurate outputs, inefficiencies, and reduced effectiveness.

#### 7.1.5. Privacy Concern

IoT systems often collect sensitive information about individuals or organizations. ML models trained on this data can pose privacy concerns if not adequately secured. Enhancing privacy-preserving ML algorithms that can function on encrypted or anonymized data without sacrificing performance is a complex task.

#### 7.1.6. Resource Constraints

IoT appliances often have constrained memory, computational power, and energy resources. Designing lightweight ML algorithms that maintain security and perform well on such devices is challenging.

#### 7.1.7. Dark Web Risks

The dark web is composed of anonymous networks and websites with hidden IP addresses. ML models used in IoT security may be vulnerable to dark web assaults, where malicious actors leverage input data to deceive the model. Designing ML models resilient to such assaults remains a challenge.

#### 7.1.8. Interpretability of the Model

Understanding and analysing ML model decisions is crucial for establishing trust in IoT security systems. However, many sophisticated ML models lack interpretability, making it complex to comprehend their decision-making processes.

#### 7.1.9. False Positive Rate in ML

Many IoT security studies have aimed to reduce the false positive rate (FPR), but only a few have successfully lowered the false alarm rate (FAR) to an Optimal level. This problem persists, and researches are continually working to mitigate it.

Addressing these challenges requires multidisciplinary efforts that combine domain-specific knowledge, ML, cybersecurity, and IoT expertise. Ongoing research and collaboration are vital to developing innovative solutions that boost the security of IoT ecosystems.

### 7.2. Deep Learning Challenges

While DL presents promising solutions for IoT security, it also faces several challenges.

#### 7.2.1. Adversarial Attacks Risks

This assault involves altering input data to manipulate the model’s predictions or decisions. These attacks could be used in IoT security to bypass security measures or trigger false alarms.

#### 7.2.2. Interpretability and Explainability

DL models are often seen as "black boxes" that make decisions through complex internal computations. This lack of transparency can hinder understanding the rationale behind a decision, which is problematic in security applications where understanding the justification is important.

#### 7.2.3. Effectiveness

The constraint resources available on IoT gadgets (memory, bandwidth, and time) can hinder the deployment of DL models. Although DL models can be trained offline, implementing them on devices with limited resources remains challenging. Additionally, applying DL to large datasets is powerful, but DL models rely on raw data processed through multiple layers of neurons, posing ongoing challenges in minimizing storage and computational demands for resource-constrained devices.

#### 7.2.4. Robustness

IoT environments are dynamic, with varying network conditions, device settings, and environmental factors. DL models trained on static datasets may perform poorly in these dynamic conditions, making them more insecure to security breaches.

### 7.2.5. Privacy of Data

DL models require large amounts of data, which often include sensitive information from IoT devices. Ensuring data privacy while collecting enough data to train effective models is a key challenge.

Addressing DL challenges requires innovative algorithms development, optimization strategies, and system-level design tailored to IoT security applications. Collaboration between deep learning and IoT security researchers is necessary to create solutions that balance security, performance, and resource constraints.

### 7.3. Discussion

DL, and ML mitigate some of these limitations by automatically extracting complex features from large, unsupervised IoT datasets, making it particularly effective at identifying advanced security threats. In IoT security, DL has been used to detect attacks and network anomalies by analyzing real-time data from smart home systems and other interconnected appliances.

However, despite the potential of ML and DL, challenges remain, including scalability, energy efficiency, and accuracy. Over classification and misclassification can lead to significant errors in attack detection, resulting in false positives and negatives. Future trends aim to enhance model robustness through techniques like adversarial learning and self-learning systems that adapt to emerging threats in real time.

The development of energy-efficient algorithms and federated learning will improve privacy and reliability for resource-constrained IoT gadgets. Further research is required to tackle these constrains fully and improve the accuracy of assaults disclosure in IoT security systems.

## 8. CONCLUSION

IoT is increasingly integrated into our everyday lives because of the growth of the internet and the vast number of gadgets linked to it. Because IoT networks are dynamic, securing them can be challenging and presents a number of issues for standard security solutions. Securing IoT is complex and traditional security solutions face a several of challenges due to the nature and the characteristics of IoT networks. ML and DL have facilitated the enhancement of a several of sophisticated analytical approaches that may be utilized to enhance IoT security. Moreover, ML techniques can address IoT security issues and challenges caused by the risk of attacks and affected by leaving holed. In this survey, the characteristics, IoT architecture, protocols, and IoT vulnerabilities of IoT systems are highlighted. we discuss IoT applications and present a table that summarizes the pros and cons of each application. Then, we discuss the potential IoT attacks in term of passive attack and active attacks and enhance that with the primary objective for each attack. An existing survey related to IoT security has been presented. ML/DL methods have been discussed with the strength and weakness of each. Furthermore, we discuss the previous studies with respect of them. analyzing and classifying of the existing researches between 2018 up to this date have been discussed. After that, we present the taxonomy of IoT layer attacks and discussed each attack type in detail, providing recent studies that propose solutions using ML/DL methods to address these attacks. Additionally, we summarized the datasets related to IoT security, highlighting their advantages and disadvantages, as well as current research that has applied these datasets. We also discussed the challenges, and the future trends related to ML/DL in the context of IoT security.

The purpose of this survey is to provide a helpful guide for academic researchers, offering comprehensive knowledge of IoT, IoT security, DL/ML techniques, and common IoT attacks at various network layers. By outlining the challenges faced by ML and DL in this domain, we aim to equip researchers with a clear understanding, enabling them to select the most appropriate techniques for disclosing and mitigating IoT attacks.

## REFERENCES

[1] M. A. Al-Garadi et al., “A survey of machine and deep learning methods for internet of things (IOT) security,” IEEE Communications Surveys &amp; Tutorials, vol. 22, no. 3, pp. 1646–1685, 2020. doi:10.1109/comst.2020.2988293.

[2] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, “Machine learning in IOT security: Current solutions and future challenges,” IEEE Communications Surveys &amp; Tutorials, vol. 22, no. 3, pp. 1686–1721, 2020. doi:10.1109/comst.2020.2986444.

[3] A. Thakkar and R. Lohiya, “A review on machine learning and Deep Learning Perspectives of ids for IOT: Recent updates, security issues, and challenges,” Archives of Computational Methods in Engineering, vol. 28, no. 4, pp. 3211–3243, Oct. 2020. doi:10.1007/s11831-020-09496-0.

[4] U. Farooq, N. Tariq, M. Asim, T. Baker, and A. Al-Shamma’a, “Machine learning and the internet of things security: Solutions and open challenges,” Journal of Parallel and Distributed Computing, vol. 162, pp. 89–104, Apr. 2022. doi:10.1016/j.jpdc.2022.01.015.

[5] V. Gugueoth, S. Safavat, and S. Shetty, “Security of internet of things (IOT) using Federated Learning and deep learning — recent advancements, issues and prospects,” ICT Express, vol. 9, no. 5, pp. 941–960, Oct. 2023. doi:10.1016/j.icte.2023.03.006.

[6] B. Patel, J. Vasa, and P. Shah, “IOT concepts, characteristics, enabling technologies, applications and protocol stack: Issues and Imperatives,” International Journal of Wireless and Mobile Computing, vol. 25, no. 4, pp. 397–406, 2023. doi:10.1504/ijwmc.2023.135404.

[7] X. Liang and Y. Kim, “A survey on security attacks and solutions in the IOT Network,” 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), Jan. 2021. doi:10.1109/ccwc51732.2021.9376174.

[8] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, “A survey of IOT security based on a layered architecture of sensing and data analysis,” Sensors, vol. 20, no. 13, p. 3625, Jun. 2020. doi:10.3390/s20133625.

[9] N. Verma, S. Singh, and D. Prasad, “A review on existing IOT architecture and communication protocols used in Healthcare Monitoring System,” Journal of The Institution of Engineers (India): Series B, vol. 103, no. 1, pp. 245–257, Jun. 2021. doi:10.1007/s40031-021-00632-3.

[10] A. Thakkar and R. Lohiya, “A review on machine learning and Deep Learning Perspectives of ids for IOT: Recent updates, security issues, and challenges,” Archives of Computational Methods in Engineering, vol. 28, no. 4, pp. 3211–3243, Oct. 2020. doi:10.1007/s11831-020-09496-0.

[11] V. Hassija et al., “A survey on IOT security: Application areas, security threats, and solution architectures,” IEEE Access, vol. 7, pp. 82721–82743, 2019. doi:10.1109/access.2019.2924045.

[12] D. Swessi and H. Idoudi, “A survey on internet-of-things security: Threats and emerging countermeasures,” Wireless Personal Communications, vol. 124, no. 2, pp. 1557–1592, Jan. 2022. doi:10.1007/s11277-021-09420-0.

[13] B. B. Gupta and M. Quamara, “An overview of internet of things (IOT): Architectural aspects, challenges, and protocols,” Concurrency and Computation: Practice and Experience, vol. 32, no. 21, Sep. 2018. doi:10.1002/cpe.4946.

[14] A. H. Mohd Aman, E. Yadegaridehkordi, Z. S. Attarbashi, R. Hassan, and Y.-J. Park, “A survey on trend and classification of internet of things reviews,” IEEE Access, vol. 8, pp. 111763–111782, 2020. doi:10.1109/access.2020.3002932.

[15] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, “IOT privacy and security: Challenges and solutions,” Applied Sciences, vol. 10, no. 12, p. 4102, Jun. 2020. doi:10.3390/app10124102.

[16] T. M. Ghazal et al., “IOT for Smart Cities: Machine Learning Approaches in smart healthcare—A Review,” Future Internet, vol. 13, no. 8, p. 218, Aug. 2021. doi:10.3390/fi13080218.

[17] J. Asharf et al., “A review of intrusion detection systems using machine and deep learning in internet of things: Challenges, solutions and future directions,” Electronics, vol. 9, no. 7, p. 1177, Jul. 2020. doi:10.3390/electronics9071177.

[18] P. Malhotra et al., “Internet of things: Evolution, concerns and security challenges,” Sensors, vol. 21, no. 5, p. 1809, Mar. 2021. doi:10.3390/s21051809.

[19] M. Yu, J. Zhuge, M. Cao, Z. Shi, and L. Jiang, “A survey of security vulnerability analysis, discovery, detection, and mitigation on IOT devices,” Future Internet, vol. 12, no. 2, p. 27, Feb. 2020. doi:10.3390/fi12020027.

[20] B. I. Mukhtar, M. S. Elsayed, A. D. Jurcut, and M. A. Azer, “IOT vulnerabilities and attacks: Silex malware case study,” Symmetry, vol. 15, no. 11, p. 1978, Oct. 2023. doi:10.3390/sym15111978.

[21] J. Sengupta, S. Ruj, and S. Das Bit, “A comprehensive survey on attacks, security issues and blockchain solutions for IOT and Iiot,” Journal of Network and Computer Applications, vol. 149, p. 102481, Jan. 2020. doi:10.1016/j.jnca.2019.102481.

[22] T. J. Saleem and M. A. Chishti, “Deep learning for the internet of things: Potential benefits and use-cases,” Digital Communications and Networks, vol. 7, no. 4, pp. 526–542, Nov. 2021. doi:10.1016/j.dcan.2020.12.002.

[23] S. Khanam, I. B. Ahmedy, M. Y. Idna Idris, M. H. Jaward, and A. Q. Bin Md Sabri, “A survey of security challenges, attacks taxonomy and advanced countermeasures in the internet of things,” IEEE Access, vol. 8, pp. 219709–219743, 2020. doi:10.1109/access.2020.3037359.

[24] N. Abosata, S. Al-Rubaye, G. Inalhan, and C. Emmanouilidis, “Internet of things for system integrity: A comprehensive survey on security, attacks and countermeasures for Industrial Applications,” Sensors, vol. 21, no. 11, p. 3654, May 2021. doi:10.3390/s21113654.

[25] F. B. H.J. and S. S., “A survey on IOT security: Attacks, challenges and countermeasures,” Webology, vol. 19, no. 1, pp. 3741–3763, Jan. 2022. doi:10.14704/web/v19i1/web19246.

[26] R. R. Chowdhury and P. E. Abas, “A survey on device fingerprinting approach for Resource-constraint IOT devices: Comparative study and research challenges,” Internet of Things, vol. 20, p. 100632, Nov. 2022. doi:10.1016/j.iot.2022.100632.

[27] A. Maatallaoui, H. Touil, and L. Setti, “The impact of radio frequency (RF) attacks on Security and Privacy: A Comprehensive Review,” Proceedings of the 6th International Conference on Networking, Intelligent Systems &amp; Security, May 2023. doi:10.1145/3607720.3607771.

[28] A. Barua, M. A. Al Alamin, Md. S. Hossain, and E. Hossain, “Security and privacy threats for Bluetooth Low Energy in IOT and wearable devices: A comprehensive survey,” IEEE Open Journal of the Communications Society, vol. 3, pp. 251–281, 2022. doi:10.1109/ojcoms.2022.3149732.

[29] K. Chetioui, B. Bah, A. O. Alami, and A. Bahnasse, “Overview of social engineering attacks on social networks,” Procedia Computer Science, vol. 198, pp. 656–661, 2022. doi:10.1016/j.procs.2021.12.302.

[30] N. Ahmed et al., “A survey on location privacy attacks and prevention deployed with IOT in Vehicular Networks,” Wireless Communications and Mobile Computing, vol. 2022, pp. 1–15, Apr. 2022. doi:10.1155/2022/6503299.

[31] M. R. Kadri, A. Abdelli, J. Ben Othman, and L. Mokdad, “Survey and classification of Dos and DDOS attack detection and validation approaches for IOT Environments,” Internet of Things, vol. 25, p. 101021, Apr. 2024. doi:10.1016/j.iot.2023.101021.

[32] P. Kumari and A. K. Jain, “A comprehensive study of ddos attacks over IOT network and their countermeasures,” Computers &amp; Security, vol. 127, p. 103096, Apr. 2023. doi:10.1016/j.cose.2023.103096.

[33] P. Vennam, S. K. Mouleeswaran, S. Shamila, and S. R. Kasarla, “A comprehensive analysis of fog layer and man in the middle attacks in IOT Networks,” 2022 IEEE 2nd Mysore Sub Section International Conference (MysuruCon), vol. 9, pp. 1–5, Oct. 2022. doi:10.1109/mysurucon55714.2022.9972612.

[34] D. Panda, B. Kishore Mishra, and K. Sharma, “A taxonomy on man-in-the-middle attack in IOT Network,” 2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N), vol. 7, pp. 1907–1912, Dec. 2022. doi:10.1109/icac3n56670.2022.10074170.

[35] P. Victor et al., “IOT malware: An attribute-based taxonomy, detection mechanisms and challenges,” Peer-to-Peer Networking and Applications, vol. 16, no. 3, pp. 1380–1431, May 2023. doi:10.1007/s12083-023-01478-w.

[36] C. S. Yadav et al., “Malware analysis in IOT & Android systems with Defensive Mechanism,” Electronics, vol. 11, no. 15, p. 2354, Jul. 2022. doi:10.3390/electronics11152354.

[37] H. Pirayesh and H. Zeng, “Jamming attacks and anti-jamming strategies in wireless networks: A comprehensive survey,” IEEE Communications Surveys &amp; Tutorials, vol. 24, no. 2, pp. 767–809, 2022. doi:10.1109/comst.2022.3159185.

[38] F. Alrefaei, A. Alzahrani, H. Song, and S. Alrefaei, “A survey on the jamming and spoofing attacks on the Unmanned Aerial Vehicle Networks,” 2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), Jun. 2022. doi:10.1109/iemtronics55184.2022.9795809.

[39] A. A. Al-chikh Omar, B. Soudan, and Ala’ Altaweel, “A comprehensive survey on detection of sinkhole attack in routing over low power and lossy network for internet of things,” Internet of Things, vol. 22, p. 100750, Jul. 2023. doi:10.1016/j.iot.2023.100750.

[40] R. Ahmad, I. Alsmadi, W. Alhamdani, and L. Tawalbeh, “Zero-Day attack detection: A systematic literature review,” Artificial Intelligence Review, vol. 56, no. 10, pp. 10733–10811, Feb. 2023. doi:10.1007/s10462-023-10437-z.

[41] R. Patnaik, N. Padhy, and K. Srujan Raju, “A systematic survey on IOT security issues, vulnerability and open challenges,” Advances in Intelligent Systems and Computing, pp. 723–730, Aug. 2020. doi:10.1007/978-981-15-5400-1_68.

[42] K. Shaukat et al., “A review on security challenges in internet of things (IOT),” 2021 26th International Conference on Automation and Computing (ICAC), Sep. 2021. doi:10.23919/icac50006.2021.9594183.

[43] K. M. Sadique, R. Rahmani, and P. Johannesson, “Towards security on internet of things: Applications and challenges in Technology,”

Procedia Computer Science, vol. 141, pp. 199–206, 2018. doi:10.1016/j.procs.2018.10.168.

[44] R. R. Krishna et al., "State-of-the-art review on IOT threats and attacks: Taxonomy, challenges and solutions," Sustainability, vol. 13, no. 16, p. 9463, Aug. 2021. doi:10.3390/su13169463.

[45] V. N and P. T. V. Bhuavneswari, "ADBIS: Anomaly detection to bolster IOT security using machine learning," 2023 IEEE 3rd International Conference on Applied Electromagnetics, Signal Processing, &amp; Communication (AESPC), pp. 1–6, Nov. 2023. doi:10.1109/aespc59761.2023.10390100.

[46] Rachit, S. Bhatt, and P. R. Ragiri, "Security trends in internet of things: A survey," SN Applied Sciences, vol. 3, no. 1, Jan. 2021. doi:10.1007/s42452-021-04156-9.

[47] S. Balogh, O. Gallo, R. Ploszek, P. Špaček, and P. Zajac, "IOT security challenges: Cloud and blockchain, Postquantum cryptography, and evolutionary techniques," Electronics, vol. 10, no. 21, p. 2647, Oct. 2021. doi:10.3390/electronics10212647.

[48] R. F. Ali, A. Muneer, P. D. Dominic, S. M. Taib, and E. A. Ghaleb, "Internet of things (IOT) security challenges and solutions: A systematic literature review," Communications in Computer and Information Science, pp. 128–154, 2021. doi:10.1007/978-981-16-8059-5_9.

[49] M. Azrour, J. Mabrouki, A. Guezzaz, and A. Kanwal, "Internet of things security: Challenges and key issues," Security and Communication Networks, vol. 2021, pp. 1–11, Sep. 2021. doi:10.1155/2021/5533843.

[50] B. Yedle, G. Shrivastava, A. Kumar, A. K. Mishra, and T. K. Mishra, "A survey: Security issues and challenges in internet of things," Lecture Notes in Networks and Systems, pp. 75–86, Jun. 2020. doi:10.1007/978-981-15-4218-3_8.

[51] S. Chesney, K. Roy, and S. Khorsandroo, "Machine learning algorithms for preventing IOT cybersecurity attacks," Advances in Intelligent Systems and Computing, pp. 679–686, Aug. 2020. doi:10.1007/978-3-030-55190-2_53.

[52] M. Bagaa, T. Taleb, J. B. Bernabe, and A. Skarmeta, "A Machine Learning Security Framework for IOT systems," IEEE Access, vol. 8, pp. 114066–114077, 2020. doi:10.1109/access.2020.2996214.

[53] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of internet of things (IOT): A survey," Journal of Network and Computer Applications, vol. 161, p. 102630, Jul. 2020. doi:10.1016/j.jnca.2020.102630.

[54] A. S. Ahmed and H. A. Salah, "Development a software defined network (SDN) with internet of things (IOT) security for medical issues," Journal of Al-Qadisiyah for Computer Science and Mathematics, vol. 15, no. 3, Sep. 2023. doi:10.29304/jqcm.2023.15.3.1268.

[55] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, "Privacy-preserving support vector machine training over blockchain-based encrypted IOT data in Smart Cities," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 7702–7712, Oct. 2019. doi:10.1109/jiot.2019.2901840.

[56] M. Shafiq, Z. Tian, A. K. Bashir, X. Du, and M. Guizani, "CORRAUC: A malicious bot-IOT traffic detection method in IOT network using machine-learning techniques," IEEE Internet of Things Journal, vol. 8, no. 5, pp. 3242–3254, Mar. 2021. doi:10.1109/jiot.2020.3002255.

[57] C. Ioannou and V. Vassiliou, "Experimentation with local intrusion detection in IOT networks using supervised learning," 2020 16th International Conference on Distributed Computing in Sensor Systems (DCOSS), May 2020. doi:10.1109/dcoss49796.2020.00073.

[58] D. Puthal et al., "Decision tree based user-centric security solution for critical IOT infrastructure," Computers and Electrical Engineering, vol. 99, p. 107754, Apr. 2022. doi:10.1016/j.compeleceng.2022.107754.

[59] A. Churcher et al., "An experimental analysis of attack classification using machine learning in IOT Networks," Sensors, vol. 21, no. 2, p. 446, Jan. 2021. doi:10.3390/s21020446.

[60] Y. N. Soe, Y. Feng, P. I. Santosa, R. Hartanto, and K. Sakurai, "Machine learning-based IOT-botnet attack detection with sequential architecture," Sensors, vol. 20, no. 16, p. 4372, Aug. 2020. doi:10.3390/s20164372.

[61] S. Nakhodchi, A. Upadhyay, and A. Dehghantanha, "A comparison between different machine learning models for IOT malware detection," Security of Cyber-Physical Systems, pp. 195–202, 2020. doi:10.1007/978-3-030-45541-5_10.

[62] R. Doshi, N. Apthorpe, and N. Feamster, "Machine learning ddos detection for consumer internet of things devices," 2018 IEEE Security and Privacy Workshops (SPW), May 2018. doi:10.1109/spw.2018.00013.

[63] S. Li, Q. Zhang, X. Wu, W. Han, and Z. Tian, "Attribution classification method of APT Malware in IOT using machine learning techniques," Security and Communication Networks, vol. 2021, pp. 1–12, Sep. 2021. doi:10.1155/2021/9396141.

[64] I. S. Thaseen, V. Mohanraj, S. Ramachandran, K. Sanapala, and S.-S. Yeo, "A Hadoop based framework integrating machine learning classifiers for anomaly detection in the internet of things," Electronics, vol. 10, no. 16, p. 1955, Aug. 2021. doi:10.3390/electronics10161955.

[65] S. M. Tahsien, H. Karimipour, and P. Spachos, "Machine learning based solutions for security of internet of things (IOT): A survey," Journal of Network and Computer Applications, vol. 161, p. 102630, Jul. 2020. doi:10.1016/j.jnca.2020.102630.

[66] B. Zhang, Z. Liu, Y. Jia, J. Ren, and X. Zhao, "Network intrusion detection method based on PCA and Bayes algorithm," Security and Communication Networks, vol. 2018, pp. 1–11, Nov. 2018. doi:10.1155/2018/1914980.

[67] H. H. Pajouh, R. Javidan, R. Khayami, A. Dehghantanha, and K.-K. R. Choo, "A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IOT backbone networks," IEEE Transactions on Emerging Topics in Computing, vol. 7, no. 2, pp. 314–323, Apr. 2019. doi:10.1109/tetc.2016.2633228.

[68] Z. H. Abdaljabar, O. N. Ucan, and K. M. Ali Alheeti, "An intrusion detection system for IOT using KNN and decision-tree based classification," 2021 International Conference of Modern Trends in Information and Communication Technology Industry (MTICTI), Dec. 2021. doi:10.1109/mticti53925.2021.9664772.

[69] A. Kumar and T. J. Lim, "Edima: Early detection of IOT malware network activity using Machine Learning Techniques," 2019 IEEE 5th World Forum on Internet of Things (WF-IoT), Apr. 2019. doi:10.1109/wf-iot.2019.8767194.

[70] Sharipuddin et al., "Features extraction on IOT intrusion detection system using Principal Components Analysis (PCA)," 2020 7th International Conference on Electrical Engineering, Computer Sciences and Informatics (EECSI), vol. 8491, pp. 114–118, Oct. 2020. doi:10.23919/eecsi50503.2020.9251292.

[71] S. K. Dash et al., "Enhancing ddos attack detection in IOT using PCA," Egyptian Informatics Journal, vol. 25, p. 100450, Mar. 2024. doi:10.1016/j.eij.2024.100450 G. Abbas, A. Mehmood, M. Carsten, G. Epiphaniou, and J. Lloret, "Safety, security and privacy in machine learning based internet of things," Journal of Sensor and Actuator Networks, vol. 11, no. 3, p. 38, Jul. 2022. doi:10.3390/jsan11030038.

[72] L. Liu, X. Xu, Y. Liu, Z. Ma, and J. Peng, "A detection framework against CPMA attack based on trust evaluation and Machine Learning in IOT network," IEEE Internet of Things Journal, vol. 8, no. 20, pp. 15249–15258, Oct. 2021. doi:10.1109/jiot.2020.3047642.

[73] Y. Alotaibi and M. Ilyas, "Ensemble-Learning Framework for intrusion detection to enhance internet of things' devices security," Sensors, vol. 23, no. 12, p. 5568, Jun. 2023. doi:10.3390/s23125568.

[74] P. K. Danso et al., "Ensemble-based intrusion detection for internet of things devices," 2022 IEEE 19th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET), vol. 30, pp. 034–039, Dec. 2022. doi:10.1109/honet56683.2022.10019140.

[75] H. Li, K. Ota, and M. Dong, “Learning IOT in edge: Deep learning for the internet of things with Edge Computing,” IEEE Network, vol. 32, no. 1, pp. 96–101, Jan. 2018. doi:10.1109/mnet.2018.1700202.

[76] S. Li, Q. Zhang, X. Wu, W. Han, and Z. Tian, “Attribution classification method of APT Malware in IOT using machine learning techniques,” Security and Communication Networks, vol. 2021, pp. 1–12, Sep. 2021. doi:10.1155/2021/9396141.

[77] T. A. Tuan et al., “Performance evaluation of botnet ddos attack detection using machine learning,” Evolutionary Intelligence, vol. 13, no. 2, pp. 283–294, Nov. 2019. doi:10.1007/s12065-019-00310-w.

[78] M. Shafiq, Z. Tian, Y. Sun, X. Du, and M. Guizani, “Selection of effective machine learning algorithm and bot-IOT attacks traffic identification for internet of things in Smart City,” Future Generation Computer Systems, vol. 107, pp. 433–442, Jun. 2020. doi:10.1016/j.future.2020.02.017.

[79] A. Arshad et al., “A novel ensemble method for enhancing internet of things device security against botnet attacks,” Decision Analytics Journal, vol. 8, p. 100307, Sep. 2023. doi:10.1016/j.dajour.2023.100307.

[80] K. Alissa et al., “Botnet attack detection in IOT using machine learning,” Computational Intelligence and Neuroscience, vol. 2022, pp. 1–14, Oct. 2022. doi:10.1155/2022/4515642.

[81] T. Gaber, A. El-Ghamry, and A. E. Hassanien, “Injection attack detection using machine learning for smart IOT Applications,” Physical Communication, vol. 52, p. 101685, Jun. 2022. doi:10.1016/j.phycom.2022.101685.

[82] V. Tomer and S. Sharma, “Detecting IOT attacks using an ensemble machine learning model,” Future Internet, vol. 14, no. 4, p. 102, Mar. 2022. doi:10.3390/fi14040102.

[83] S. Rabhi, T. Abbes, and F. Zarai, “IOT routing attacks detection using machine learning algorithms,” Wireless Personal Communications, vol. 128, no. 3, pp. 1839–1857, Sep. 2022. doi:10.1007/s11277-022-10022-7.

[84] H. Gebrye, Y. Wang, and F. Li, “Traffic data extraction and labeling for machine learning based attack detection in IOT networks,” International Journal of Machine Learning and Cybernetics, vol. 14, no. 7, pp. 2317–2332, Jan. 2023. doi:10.1007/s13042-022-01765-7.

[85] S. A. Al-Juboori, F. Hazzaa, Z. S. Jabbar, S. Salih, and H. M. Gheni, “Man-in-the-middle and denial of service attacks detection using machine learning algorithms,” Bulletin of Electrical Engineering and Informatics, vol. 12, no. 1, pp. 418–426, Feb. 2023. doi:10.11591/eei.v12i1.4555.

[86] H. M. Saleh, H. Marouane, and A. Fakhfakh, “Stochastic gradient descent intrusions detection for wireless sensor network attack detection system using machine learning,” IEEE Access, vol. 12, pp. 3825–3836, 2024. doi:10.1109/access.2023.3349248.

[87] J. P, J. Shareena, A. Ramdas, and H. A P, “Intrusion detection system for IOT botnet attacks using Deep Learning,” SN Computer Science, vol. 2, no. 3, Apr. 2021. doi:10.1007/s42979-021-00516-9.

[88] B. Alabsi, M. Anbar, and S. Rihan, “CNN-CNN: Dual Convolutional Neural Network Approach for feature selection and attack detection on internet of things networks,” Sensors, vol. 23, no. 14, p. 6507, Jul. 2023. doi:10.3390/s23146507.

[89] A. Dahou et al., “Intrusion detection system for IOT based on Deep Learning and modified reptile search algorithm,” Computational Intelligence and Neuroscience, vol. 2022, pp. 1–15, Jun. 2022. doi:10.1155/2022/6473507.

[90] I. Ullah and Q. H. Mahmoud, “Design and development of RNN Anomaly Detection Model for IOT Networks,” IEEE Access, vol. 10, pp. 62722–62750, 2022. doi:10.1109/access.2022.3176317.

[91] P. Sanju, “Enhancing intrusion detection in IOT systems: A hybrid metaheuristics-deep learning approach with ensemble of Recurrent Neural Networks,” Journal of Engineering Research, vol. 11, no. 4, pp. 356–361, Dec. 2023. doi:10.1016/j.jer.2023.100122.

[92] A. Basati and M. M. Faghih, “APAE: An IOT intrusion detection system using asymmetric parallel auto-encoder,” Neural Computing and Applications, vol. 35, no. 7, pp. 4813–4833, Apr. 2021. doi:10.1007/s00521-021-06011-9.

[93] Y. Hou et al., “Hybrid intrusion detection model based on a designed autoencoder,” Journal of Ambient Intelligence and Humanized Computing, vol. 14, no. 8, pp. 10799–10809, Sep. 2022. doi:10.1007/s12652-022-04350-6.

[94] Q. E. Ul Haq, M. Imran, K. Saleem, T. Zia, and J. Al Muhtadi, “Review on variants of restricted boltzmann machines and autoencoders for Cyber-Physical Systems,” Internet of Things Security and Privacy, pp. 188–207, Oct. 2023. doi:10.1201/9781003199410-8.

[95] V. S. Desanamukula et al., “A comprehensive analysis of machine learning and deep learning approaches towards IOT Security,” 2023 4th International Conference on Electronics and Sustainable Communication Systems (ICESC), vol. 29, pp. 1165–1168, Jul. 2023. doi:10.1109/icesc57686.2023.10193209.

[96] G. H. Rosa, M. Roder, D. F. Santos, and K. A. Costa, “Enhancing anomaly detection through restricted Boltzmann machine features projection,” International Journal of Information Technology, vol. 13, no. 1, pp. 49–57, Oct. 2020. doi:10.1007/s41870-020-00535-4.

[97] I. Sohn, “Deep belief network based Intrusion Detection Techniques: A Survey,” Expert Systems with Applications, vol. 167, p. 114170, Apr. 2021. doi:10.1016/j.eswa.2020.114170.

[98] T. K. Boppana and P. Bagade, “Gan-ae: An unsupervised intrusion detection system for MQTT Networks,” Engineering Applications of Artificial Intelligence, vol. 119, p. 105805, Mar. 2023. doi:10.1016/j.engappai.2022.105805.

[99] R. Lin et al., “Physical-layer security enhancement in energy-harvesting-based cognitive internet of things: A gan-powered deep reinforcement learning approach,” IEEE Internet of Things Journal, vol. 11, no. 3, pp. 4899–4913, Feb. 2024. doi:10.1109/jiot.2023.3300770.

[100] A. Aleroud, M. Shariah, R. Malkawi, S. Y. Khamaiseh, and A. Al-Alaj, “A privacy-enhanced human activity recognition using Gan & entropy ranking of Microaggregated Data,” Cluster Computing, vol. 27, no. 2, pp. 2117–2132, Jun. 2023. doi:10.1007/s10586-023-04063-1.

[101] M. Alshamkhany et al., “Botnet attack detection using machine learning,” 2020 14th International Conference on Innovations in Information Technology (IIT), Nov. 2020. doi:10.1109/iit50501.2020.9299061.

[102] G. De La Torre Parra, P. Rad, K.-K. R. Choo, and N. Beebe, “Detecting internet of things attacks using distributed deep learning,” Journal of Network and Computer Applications, vol. 163, p. 102662, Aug. 2020. doi:10.1016/j.jnca.2020.102662.

[103] D. Papamartzivanos, F. Gomez Marmol, and G. Kambourakis, “Introducing deep learning self-adaptive misuse network intrusion detection systems,” IEEE Access, vol. 7, pp. 13546–13560, 2019. doi:10.1109/access.2019.2893871.

[104] S. I. Popoola et al., “Federated deep learning for Zero-Day botnet attack detection in IOT-edge devices,” IEEE Internet of Things Journal, vol. 9, no. 5, pp. 3930–3944, Mar. 2022. doi:10.1109/jiot.2021.3100755.

[105] N. Balakrishnan, A. Rajendran, D. Pelusi, and V. Ponnusamy, “Deep belief network enhanced intrusion detection system to prevent security breach in the internet of things,” Internet of Things, vol. 14, p. 100112, Jun. 2021. doi:10.1016/j.iot.2019.100112.

[106] R. H. Randhawa, N. Aslam, M. Alauthman, H. Rafiq, and F. Comeau, “Security hardening of botnet detectors using generative adversarial networks,” IEEE Access, vol. 9, pp. 78276–78292, 2021. doi:10.1109/access.2021.3083421.

[107] G. H. Rosa, M. Roder, D. F. Santos, and K. A. Costa, “Enhancing anomaly detection through restricted Boltzmann machine features projection,” International Journal of Information Technology, vol. 13, no. 1, pp. 49–57, Oct. 2020. doi:10.1007/s41870-020-00535-4.

[108] J. Kumar and G. Ranganathan, “Malware attack detection in large scale networks using the ensemble deep restricted Boltzmann machine,” Engineering, Technology &amp; Applied Science Research, vol. 13, no. 5, pp. 11773–11778, Oct. 2023. doi:10.48084/etasr.6204.

[109] B. Sharma, L. Sharma, C. Lal, and S. Roy, “Anomaly based network intrusion detection for IOT attacks using Deep Learning Technique,” Computers and Electrical Engineering, vol. 107, p. 108626, Apr. 2023. doi:10.1016/j.compeleceng.2023.108626.

[110] A. M. Banaamah and I. Ahmad, “Intrusion detection in IOT using Deep Learning,” Sensors, vol. 22, no. 21, p. 8417, Nov. 2022. doi:10.3390/s22218417.

[111] J. Simon, N. Kapileswar, P. K. Polasi, and M. A. Elaveini, “Hybrid intrusion detection system for wireless IOT networks using Deep Learning algorithm,” Computers and Electrical Engineering, vol. 102, p. 108190, Sep. 2022. doi:10.1016/j.compeleceng.2022.108190.

[112] O. Jullian et al., “Deep-learning based detection for cyber-attacks in IOT Networks: A distributed attack detection framework,” Journal of Network and Systems Management, vol. 31, no. 2, Feb. 2023. doi:10.1007/s10922-023-09722-7.

[113] S. Ahmed et al., “Effective and efficient ddos attack detection using deep learning algorithm, Multi-Layer Perceptron,” Future Internet, vol. 15, no. 2, p. 76, Feb. 2023. doi:10.3390/fi15020076.

[114] V. Shakya, J. Choudhary, and D. P. Singh, “Irada: Integrated Reinforcement Learning and deep learning algorithm for attack detection in wireless sensor networks,” Multimedia Tools and Applications, vol. 83, no. 28, pp. 71559–71578, Feb. 2024. doi:10.1007/s11042-024-18289-7.

[115] N. Sakthipriya, V. Govindasamy, and V. Akila, “Security-aware IOT botnet attack detection framework using dilated and cascaded deep learning mechanism with conditional adversarial autoencoder-based features,” Peer-to-Peer Networking and Applications, vol. 17, no. 3, pp. 1467–1485, Feb. 2024. doi:10.1007/s12083-024-01657-3.

[116] P. Mishra, V. Varadharajan, U. Tupakula, and E. S. Pilli, “A detailed investigation and analysis of using machine learning techniques for intrusion detection,” IEEE Communications Surveys &amp; Tutorials, vol. 21, no. 1, pp. 686–728, 2019. doi:10.1109/comst.2018.2847722.

[117] M. Amiri-Zarandi, R. A. Dara, and E. Fraser, “A survey of machine learning-based solutions to protect privacy in the internet of things,” Computers &amp; Security, vol. 96, p. 101921, Sep. 2020. doi:10.1016/j.cose.2020.101921.

[118] Q. Liu et al., “A survey on security threats and defensive techniques of Machine Learning: A data driven view,” IEEE Access, vol. 6, pp. 12103–12117, 2018. doi:10.1109/access.2018.2805680.

[119] K. A. P. da Costa, J. P. Papa, C. O. Lisboa, R. Munoz, and V. H. de Albuquerque, “Internet of things: A survey on machine learning-based intrusion detection approaches,” Computer Networks, vol. 151, pp. 147–157, Mar. 2019. doi:10.1016/j.comnet.2019.01.023.

[120] I. Idrissi, M. Azizi, and O. Moussaoui, “IOT security with deep learning-based intrusion detection systems: A systematic literature review,” 2020 Fourth International Conference On Intelligent Computing in Data Sciences (ICDS), vol. 2019 july, pp. 1–10, Oct. 2020. doi:10.1109/icds50568.2020.9268713.

[121] S. M. Tahsien, H. Karimipour, and P. Spachos, “Machine learning based solutions for security of internet of things (IOT): A survey,” Journal of Network and Computer Applications, vol. 161, p. 102630, Jul. 2020. doi:10.1016/j.jnca.2020.102630.

[122] Z. Ahmad, A. Shahid Khan, C. Wai Shiang, J. Abdullah, and F. Ahmad, “Network intrusion detection system: A systematic study of machine learning and Deep Learning Approaches,” Transactions on Emerging Telecommunications Technologies, vol. 32, no. 1, Oct. 2020. doi:10.1002/ett.4150.

[123] N. Chaabouni, M. Mosbah, A. Zemmari, C. Sauvignac, and P. Faruki, “Network intrusion detection for IOT security based on Learning Techniques,” IEEE Communications Surveys &amp; Tutorials, vol. 21, no. 3, pp. 2671–2701, 2019. doi:10.1109/comst.2019.2896380.

[124] R. Vishwakarma and A. K. Jain, “A survey of ddos attacking techniques and defence mechanisms in the IOT network,” Telecommunication Systems, vol. 73, no. 1, pp. 3–25, Jul. 2019. doi:10.1007/s11235-019-00599-z.

[125] Q.-D. Ngo, H.-T. Nguyen, V.-H. Le, and D.-H. Nguyen, “A survey of IOT malware and detection methods based on static features,” ICT Express, vol. 6, no. 4, pp. 280–286, Dec. 2020. doi:10.1016/j.icte.2020.04.005.

[126] J. Sengupta, S. Ruj, and S. Das Bit, “A comprehensive survey on attacks, security issues and blockchain solutions for IOT and Iiot,” Journal of Network and Computer Applications, vol. 149, p. 102481, Jan. 2020. doi:10.1016/j.jnca.2019.102481.

[127] P. Williams, I. Dutta, H. Daoud, and M. Bayoumi, “Security aspects of internet of things – A survey,” 2020 IEEE 6th World Forum on Internet of Things (WF-IoT), vol. 5, pp. 1–6, Jun. 2020. doi:10.1109/wf-iot48130.2020.9221429.

[128] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, “Internet of things security and forensics: Challenges and opportunities,” Future Generation Computer Systems, vol. 78, pp. 544–546, Jan. 2018. doi:10.1016/j.future.2017.07.060 .

[129] T. J. Saleem and M. A. Chishti, “Deep learning for the internet of things: Potential benefits and use-cases,” Digital Communications and Networks, vol. 7, no. 4, pp. 526–542, Nov. 2021. doi:10.1016/j.dcan.2020.12.002 .

[130] X. Liang and Y. Kim, “A survey on security attacks and solutions in the IOT Network,” 2021 IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), Jan. 2021. doi:10.1109/ccwc51732.2021.9376174.

[131] V. Porkodi et al., “A survey on various machine learning models in IOT Applications,” 2020 International Conference on Computing and Information Technology (ICCIT-1441), vol. 44, pp. 1–4, Sep. 2020. doi:10.1109/iccit-144147971.2020.9213819.

[132] Y. Harbi, Z. Aliouat, A. Refoufi, and S. Harous, “Recent security trends in internet of things: A comprehensive survey,” IEEE Access, vol. 9, pp. 113292–113314, 2021. doi:10.1109/access.2021.3103725.

[133] H. Wu, H. Han, X. Wang, and S. Sun, “Research on artificial intelligence enhancing internet of things security: A survey,” IEEE Access, vol. 8, pp. 153826–153848, 2020. doi:10.1109/access.2020.3018170.

[134] P. Malhotra et al., “Internet of things: Evolution, concerns and security challenges,” Sensors, vol. 21, no. 5, p. 1809, Mar. 2021. doi:10.3390/s21051809 .

[135] R. Al-amri et al., “A review of machine learning and deep learning techniques for anomaly detection in IOT Data,” Applied Sciences, vol. 11, no. 12, p. 5320, Jun. 2021. doi:10.3390/app11125320.

[136] M. A. Alsoufi et al., “Anomaly-based intrusion detection systems in IOT using Deep Learning: A Systematic Literature Review,” Applied Sciences, vol. 11, no. 18, p. 8383, Sep. 2021. doi:10.3390/app11188383.

[137] D. S. Berman, A. L. Buczak, J. S. Chavis, and C. L. Corbett, “A survey of Deep Learning Methods for Cyber Security,” Information, vol. 10, no. 4, p. 122, Apr. 2019. doi:10.3390/info10040122.

[138] V. Gugueoth, S. Safavat, and S. Shetty, “Security of internet of things (IOT) using Federated Learning and deep learning — recent advancements, issues and prospects,” ICT Express, vol. 9, no. 5, pp. 941–960, Oct. 2023. doi:10.1016/j.icte.2023.03.006.

[139] J. Singh, M. Wazid, A. K. Das, V. Chamola, and M. Guizani, “Machine learning security attacks and defense approaches for emerging cyber physical applications: A comprehensive survey,” Computer Communications, vol. 192, pp. 316–331, Aug. 2022. doi:10.1016/j.comcom.2022.06.012.

[140] M. Tayyab et al., “A comprehensive review on Deep Learning Algorithms: Security and privacy issues,” Computers &amp; Security, vol. 131, p. 103297, Aug. 2023. doi:10.1016/j.cose.2023.103297.

[141] U. Farooq, N. Tariq, M. Asim, T. Baker, and A. Al-Shamma’a, “Machine learning and the internet of things security: Solutions and open challenges,” Journal of Parallel and Distributed Computing, vol. 162, pp. 89–104, Apr. 2022. doi:10.1016/j.jpdc.2022.01.015.

[142] vinayakumar R et al., Deep Learning for Cyber Security Applications: A comprehensive survey, Oct. 2021. doi:10.36227/techrxiv.16748161.v1.

[143] J. Bian et al., “Machine learning in real-time internet of things (IOT) systems: A survey,” IEEE Internet of Things Journal, vol. 9, no. 11, pp. 8364–8386, Jun. 2022. doi:10.1109/jiot.2022.3161050.

[144] S. Bharati and P. Podder, “Machine and deep learning for IOT security and privacy: Applications, challenges, and Future Directions,” Security and Communication Networks, vol. 2022, pp. 1–41, Aug. 2022. doi:10.1155/2022/8951961.

[145] I. H. Sarker, A. I. Khan, Y. B. Abushark, and F. Alsolami, “Internet of things (IOT) security intelligence: A comprehensive overview, machine learning solutions and research directions,” Mobile Networks and Applications, vol. 28, no. 1, pp. 296–312, Mar. 2022. doi:10.1007/s11036-022-01937-3.

[146] C. Alex, G. Creado, W. Almobaideen, O. A. Alghanam, and M. Saadeh, “A comprehensive survey for IOT security datasets taxonomy, classification and Machine Learning Mechanisms,” Computers &amp; Security, vol. 132, p. 103283, Sep. 2023. doi:10.1016/j.cose.2023.103283.

[147] Z. T. Pritee et al., “Machine learning and deep learning for user authentication and authorization in cybersecurity: A state-of-the-art review,” Computers &amp; Security, vol. 140, p. 103747, May 2024. doi:10.1016/j.cose.2024.103747.

[148] R. Priyadarshi, “Exploring machine learning solutions for overcoming challenges in IOT-based Wireless Sensor Network Routing: A comprehensive review,” Wireless Networks, vol. 30, no. 4, pp. 2647–2673, Feb. 2024. doi:10.1007/s11276-024-03697-2.

[149] S Fharis, “Securing the Dynamic Realm: A comprehensive review of ML algorithms in IOT-based home automation systems and beyond,” International Journal of Emerging Trends in Engineering Research, vol. 12, no. 1, pp. 1–7, Jan. 2024. doi:10.30534/ijeter/2024/011212024.

[150] S. A. Haifa Ali and J. Vakula Rani, “Attack detection in IOT using machine learning—A survey,” Engineering Cyber-Physical Systems and Critical Infrastructures, pp. 211–228, 2023. doi:10.1007/978-3-031-18497-0_16.

[151] B. Upadhyaya, S. Sun, and B. Sikdar, “Machine learning-based jamming detection in wireless IOT Networks,” 2019 IEEE VTS Asia Pacific Wireless Communications Symposium (APWCS), Aug. 2019. doi:10.1109/vts-apwcs.2019.8851633.

[152] G. Liu et al., “Softwarized IOT network immunity against eavesdropping with programmable data planes,” IEEE Internet of Things Journal, vol. 8, no. 8, pp. 6578–6590, Apr. 2021. doi:10.1109/jiot.2020.3048842.

[153] A. Shafique, A. Mehmood, and M. Elhadef, “Detecting signal spoofing attack in uavs using machine learning models,” IEEE Access, vol. 9, pp. 93803–93815, 2021. doi:10.1109/access.2021.3089847.

[154] D. Marabissi, L. Mucchi, and A. Stomaci, “IOT nodes authentication and ID spoofing detection based on joint use of Physical Layer Security and machine learning,” Future Internet, vol. 14, no. 2, p. 61, Feb. 2022. doi:10.3390/fi14020061.

[155] A. Sharma et al., “An efficient hybrid deep learning model for denial of service detection in Cyber Physical Systems,” IEEE Transactions on Network Science and Engineering, vol. 10, no. 5, pp. 2419–2428, Sep. 2023. doi:10.1109/tnse.2023.3273301.

[156] Y. Chen et al., “Physical layer authentication for industrial control based on convolutional denoising autoencoder,” IEEE Internet of Things Journal, vol. 11, no. 9, pp. 15633–15641, May 2024. doi:10.1109/jiot.2023.3347603.

[157] S. Alangari, “An unsupervised machine learning algorithm for attack and anomaly detection in IOT Sensors,” Wireless Personal Communications, Feb. 2024. doi:10.1007/s11277-023-10811-8.

[158] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, “A survey of IOT security based on a layered architecture of sensing and data analysis,” Sensors, vol. 20, no. 13, p. 3625, Jun. 2020. doi:10.3390/s20133625.

[159] W. Ding, M. Abdel-Basset, and R. Mohamed, “Deepak-IOT: An effective deep learning model for cyberattack detection in IOT networks,” Information Sciences, vol. 634, pp. 157–171, Jul. 2023. doi:10.1016/j.ins.2023.03.052.

[160] B. Sharma, L. Sharma, C. Lal, and S. Roy, “Anomaly based network intrusion detection for IOT attacks using Deep Learning Technique,” Computers and Electrical Engineering, vol. 107, p. 108626, Apr. 2023. doi:10.1016/j.compeleceng.2023.108626.

[161] T. S. Chu, W. Si, S. Simoff, and Q. V. Nguyen, “A machine learning classification model using random forest for detecting ddos attacks,” 2022 International Symposium on Networks, Computers and Communications (ISNCC), vol. 18, pp. 1–7, Jul. 2022. doi:10.1109/isncc55209.2022.9851797.

[162] M. Liu and L. Yang, “IOT network traffic analysis with Deep Learning,” 2024 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops), vol. 23, pp. 184–189, Mar. 2024. doi:10.1109/percomworkshops59983.2024.10502498.

[163] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, “Anomaly detection ids for detecting DOS attacks in IOT networks based on machine learning algorithms,” Sensors, vol. 24, no. 2, p. 713, Jan. 2024. doi:10.3390/s24020713.

[164] A. Awajan, “A novel deep learning-based Intrusion Detection System for IOT Networks,” Computers, vol. 12, no. 2, p. 34, Feb. 2023. doi:10.3390/computers12020034.

[165] F. T. Zahra, Y. S. Bostanci, and M. Soyturk, “LSTM-based jamming detection and forecasting model using transport and application layer parameters in Wi-Fi based IOT Systems,” IEEE Access, vol. 12, pp. 32944–32958, 2024. doi:10.1109/access.2024.3371673.

[166] W. I. Khedr, A. E. Gouda, and E. R. Mohamed, “FMDADM: A multi-layer ddos attack detection and mitigation framework using Machine Learning for stateful SDN-based IOT Networks,” IEEE Access, vol. 11, pp. 28934–28954, 2023. doi:10.1109/access.2023.3260256.

[167] S. M. Almeghlef, A. A.-M. AL-Ghamdi, M. S. Ramzan, and M. Ragab, “Application layer-based denial-of-service attacks detection against IOT-Coap,” Electronics, vol. 12, no. 12, p. 2563, Jun. 2023. doi:10.3390/electronics12122563.

[168] G. De La Torre Parra, P. Rad, K.-K. R. Choo, and N. Beebe, “Detecting internet of things attacks using distributed deep learning,” Journal of Network and Computer Applications, vol. 163, p. 102662, Aug. 2020. doi:10.1016/j.jnca.2020.102662.

[169] Z. Ahmad et al., “Anomaly detection using Deep Neural Network for IOT Architecture,” Applied Sciences, vol. 11, no. 15, p. 7050, Jul. 2021. doi:10.3390/app11157050.

[170] J. G. Almaraz-Rivera, J. A. Perez-Diaz, and J. A. Cantoral-Ceballos, “Transport and application layer ddos attacks detection to IOT devices by using machine learning and Deep Learning Models,” Sensors, vol. 22, no. 9, p. 3367, Apr. 2022. doi:10.3390/s22093367.

[171] A. K. Pathak, S. Saguna, K. Mitra, and C. Ahlund, “Anomaly detection using machine learning to discover sensor tampering in IOT Systems,” ICC 2021 - IEEE International Conference on Communications, vol. 20, pp. 1–6, Jun. 2021. doi:10.1109/icc42927.2021.9500825.

[172] D. Marabissi, L. Mucchi, and A. Stomaci, “IOT nodes authentication and ID spoofing detection based on joint use of Physical Layer Security and machine learning,” Future Internet, vol. 14, no. 2, p. 61, Feb. 2022. doi:10.3390/fi14020061.

[173] B. Urooj, M. A. Shah, C. Maple, M. K. Abbasi, and S. Riasat, “Malware detection: A framework for reverse engineered Android applications through Machine Learning Algorithms,” IEEE Access, vol. 10, pp. 89031–89050, 2022. doi:10.1109/access.2022.3149053.

[174] J. Sakhnini, H. Karimipour, A. Dehghantanha, and R. M. Parizi, “Physical layer attack identification and localization in cyber–physical grid: An ensemble deep learning based approach,” Physical Communication, vol. 47, p. 101394, Aug. 2021. doi:10.1016/j.phycom.2021.101394.

[175] M. Piva, G. Maselli, and F. Restuccia, “The tags are Alright,” Proceedings of the Twenty-second International Symposium on Theory, Algorithmic Foundations, and Protocol Design for Mobile Networks and Mobile Computing, Jul. 2021. doi:10.1145/3466772.3467033.

[176] M. Jacovic, X. R. Rey, G. Mainland, and K. R. Dandekar, “Mitigating RF jamming attacks at the physical layer with machine learning,” IET Communications, vol. 17, no. 1, pp. 12–28, Oct. 2022. doi:10.1049/cmu2.12461.

[177] M. S. Akhtar and T. Feng, “Detection of malware by Deep Learning as CNN-LSTM machine learning techniques in Real time,” Symmetry, vol. 14, no. 11, p. 2308, Nov. 2022. doi:10.3390/sym14112308.

[178] T. Gaber, A. El-Ghamry, and A. E. Hassanien, “Injection attack detection using machine learning for smart IOT Applications,” Physical Communication, vol. 52, p. 101685, Jun. 2022. doi:10.1016/j.phycom.2022.101685.

[179] Q. Abu Al-Haija, M. Alohaly, and A. Odeh, “A lightweight double-stage scheme to identify malicious DNS over HTTPS traffic using a hybrid learning approach,” Sensors, vol. 23, no. 7, p. 3489, Mar. 2023. doi:10.3390/s23073489.

[180] G. M and P. H B, “Semantic Query-featured Ensemble learning model for SQL-injection attack detection in IOT-ecosystems,” IEEE Transactions on Reliability, vol. 71, no. 2, pp. 1057–1074, Jun. 2022. doi:10.1109/tr.2021.3124331.

[181] P. Chaudhary, B. B. Gupta, and A. K. Singh, “Securing heterogeneous embedded devices against XSS attack in intelligent IOT System,” Computers &amp; Security, vol. 118, p. 102710, Jul. 2022. doi:10.1016/j.cose.2022.102710.

[182] J. Wang and J. Liu, “Deep learning for securing software-defined industrial internet of things: Attacks and countermeasures,” IEEE Internet of Things Journal, vol. 9, no. 13, pp. 11179–11189, Jul. 2022. doi:10.1109/jiot.2021.3126633.

[183] H. B. ul Haq and M. Saqlain, “An implementation of effective machine learning approaches to perform sybil attack detection (SAD) in IOT Network,” Theoretical and Applied Computational Intelligence, vol. 1, no. 1, pp. 1–14, Oct. 2023. doi:10.31181/taci1120232.

[184] M. Albishari, M. Li, R. Zhang, and E. Almosharea, “Deep learning-based early stage detection (DL-ESD) for routing attacks in internet of things networks,” The Journal of Supercomputing, vol. 79, no. 3, pp. 2626–2653, Aug. 2022. doi:10.1007/s11227-022-04753-4.

[185] F. Mofidi, S. G. Hounsinou, and G. Bloom, “L-ids: A multi-layered approach to ransomware detection in IOT,” 2024 IEEE 14th Annual Computing and Communication Workshop and Conference (CCWC), vol. 13291, pp. 0387–0396, Jan. 2024. doi:10.1109/ccwc60891.2024.10427870.

[186] N. Koroniotis, N. Moustafa, E. Sitnikova, and B. Turnbull, “Towards the development of realistic botnet dataset in the internet of things for network forensic analytics: Bot-IOT dataset,” Future Generation Computer Systems, vol. 100, pp. 779–796, Nov. 2019. doi:10.1016/j.future.2019.05.041.

[187] N. Moustafa and J. Slay, “UNSW-NB15: A comprehensive data set for network intrusion detection systems (UNSW-NB15 Network Data Set),” 2015 Military Communications and Information Systems Conference (MilCIS), Nov. 2015. doi:10.1109/milcis.2015.7348942.

[188] N. Moustafa, “A new distributed architecture for evaluating AI-based security systems at the edge: Network ton_iot datasets,” Sustainable Cities and Society, vol. 72, p. 102994, Sep. 2021. doi:10.1016/j.scs.2021.102994.

[189] F. Jeelani, D. S. Rai, A. Maithani, and S. Gupta, “The detection of IOT botnet using machine learning on IOT-23 Dataset,” 2022 2nd International Conference on Innovative Practices in Technology and Management (ICIPTM), Feb. 2022. doi:10.1109/iciptm54933.2022.9754187.

[190] H. Hindy et al., “Machine learning based IOT intrusion detection system: An MQTT case study (MQTT-IOT-IDS2020 dataset),” Lecture Notes in Networks and Systems, pp. 73–84, 2021. doi:10.1007/978-3-030-64758-2_6.

[191] I. Sharafaldin, A. Habibi Lashkari, and A. A. Ghorbani, “Toward generating a new intrusion detection dataset and intrusion traffic characterization,” Proceedings of the 4th International Conference on Information Systems Security and Privacy, 2018. doi:10.5220/0006639801080116.

[192] S. García, M. Grill, J. Stiborek, and A. Zunino, “An empirical comparison of botnet detection methods,” Computers &amp; Security, vol. 45, pp. 100–123, Sep. 2014. doi:10.1016/j.cose.2014.05.011.

[193] M. Sarhan, S. Layeghy, N. Moustafa, and M. Portmann, “NetFlow datasets for Machine Learning-based network intrusion detection systems,” Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, pp. 117–135, 2021. doi:10.1007/978-3-030-72802-1_9.

[194] Y. Meidan et al., “N-Baiot—network-based detection of IOT botnet attacks using deep autoencoders,” IEEE Pervasive Computing, vol. 17, no. 3, pp. 12–22, Jul. 2018. doi:10.1109/mprv.2018.03367731.

[195] F. De Keersmaeker, Y. Cao, G. K. Ndonda, and R. Sadre, “A survey of public IOT datasets for Network Security Research,” IEEE Communications Surveys &amp; Tutorials, vol. 25, no. 3, pp. 1808–1840, 2023. doi:10.1109/comst.2023.3288942.

[196] S. Hanif, T. Ilyas, and M. Zeeshan, “Intrusion detection in IOT using artificial neural networks on UNSW-15 dataset,” 2019 IEEE 16th International Conference on Smart Cities: Improving Quality of Life Using ICT &amp; IoT and AI (HONET-ICT), Oct. 2019. doi:10.1109/honet.2019.8908122.

[197] B. Susilo and R. F. Sari, “Intrusion detection in IOT networks using Deep Learning algorithm,” Information, vol. 11, no. 5, p. 279, May 2020. doi:10.3390/info11050279.

[198] I. Vaccari, G. Chiola, M. Aiello, M. Mongelli, and E. Cambiaso, “MQTTset, a new dataset for machine learning techniques on Mqtt,” Sensors, vol. 20, no. 22, p. 6578, Nov. 2020. doi:10.3390/s20226578.

[199] M. Sarhan, S. Layeghy, N. Moustafa, M. Gallagher, and M. Portmann, “Feature extraction for machine learning-based intrusion detection in IOT networks,” Digital Communications and Networks, vol. 10, no. 1, pp. 205–216, Feb. 2024. doi:10.1016/j.dcan.2022.08.012.

[200] H. Nguyen and R. Kashef, “TS-ids: Traffic-aware self-supervised learning for IOT network intrusion detection,” Knowledge-Based Systems, vol. 279, p. 110966, Nov. 2023. doi:10.1016/j.knosys.2023.110966.

[201] A. Arshad et al., “A novel ensemble method for enhancing internet of things device security against botnet attacks,” Decision Analytics Journal, vol. 8, p. 100307, Sep. 2023. doi:10.1016/j.dajour.2023.100307.

[202] N. Abdalgawad, A. Sajun, Y. Kaddoura, I. A. Zualkernan, and F. Aloul, “Generative deep learning to detect cyberattacks for the IOT-23 dataset,” IEEE Access, vol. 10, pp. 6430–6441, 2022. doi:10.1109/access.2021.3140015.

[203] C. Okur, A. Orman, and M. Dener, “DDOS intrusion detection with machine learning models: N-Baiot Data Set,” Engineering Cyber-Physical Systems and Critical Infrastructures, pp. 607–619, 2023. doi:10.1007/978-3-031-31956-3_51.

[204] Z. K. Maseer et al., “DeepIoT.IDS: Hybrid deep learning for enhancing IOT network intrusion detection,” Computers, Materials &amp; Continua, vol. 69, no. 3, pp. 3945–3966, 2021. doi:10.32604/cmc.2021.016074.

[205] M. Ali et al., “Hybrid machine learning model for efficient botnet attack detection in IOT environment,” IEEE Access, vol. 12, pp. 40682–40699, 2024. doi:10.1109/access.2024.3376400.

Authors

**Haifa Ali Saeed Ali** received the Engineering of Batcheler of Information Technology degree from the Engineering College, University of Aden, Yemen, in 2007, and MCA degree in Computer Application from Visvesvaraya Technological University (VTU), Belagavi, Karnataka, India, in 2017. She is currently a Ph.D. Research Scholar with the Department of Computer Application, CMR. Institute of Technology (affiliated to VTU), Bengaluru, India. She also working in Cyber Security, and IoT. Her area of interests includes Machine Learning, Deep Learning, Internet of Things (IoT), Cyber Security.

SURVEY ARTICLE

**Dr. Vakula Rani J** is a Professor and President of the Institution Innovation Council at CMR Institute of Technology, Bangalore. With over 26 years of teaching and research experience, she specializes in Artificial Intelligence, Computer Vision, Machine Learning, Deep Learning, and Cloud Computing. Dr. Vakula has authored more than 20 research papers published in reputed international journals and conferences. She holds two Australian patents, two Indian design patents, and has filed & published eight Indian patents. A reviewer for renowned Q1 and Q2 journals, she is also certified as an Innovation Ambassador by the Ministry of Education, India. She severed as a member of the Board of Studies and Board of Examiner at various Universities. She is a recognized guide under VTU and guiding four Ph.D., research scholars. She is a Life member in leading National Professional Societies ISC and ISTE.

**How to cite this article:**

Haifa Ali Saeed Ali, Vakula Rani J, “Machine Learning for Internet of Things (IoT) Security: A Comprehensive Survey”, International Journal of Computer Networks and Applications (IJCNA), 11(5), PP: 617-659, 2024, DOI: 10.22247/ijcna/2024/40.