Journal of Information Systems Engineering and Management
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Comprehensive Survey on Effective and Diverse Attack Detection Techniques in IoT

Zarinabegam K Mundargi[1,2]*, Azra Nasreen[1]

[1]*Department of Computer Science and Engineering, R.V College of Engineering, Visvesvaraya Technological University, Belagavi, Karnataka. India- 590018*

[2]*Department of Artificial Intelligence and Data science, Vishwakarma Institute of Technology, Pune-411037, Maharashtra, India*

**Corresponding Email: zarin1100@gmail.com*
Co-author Email: azranasreen@rvce.edu.in

ARTICLE INFO

Received: 30 Dec 2024

Revised: 12 Feb 2025

Accepted: 26 Feb 2025

ABSTRACT

Introduction: The rapid proliferation of the Internet of Things (IoT) has introduced significant security susceptibilities, making IoT devices frequent targets for diverse cyberattacks.

Objectives: This survey investigates attack detection techniques in IoT, emphasizing two prominent approaches: machine learning (ML) and deep learning (DL). The ability of traditional machine learning techniques, such as decision trees, support vector machines, and k-nearest neighbors, to detect anomalies and classify attacks is examined, proving its applicability to fundamental IoT security issues.

Methods: In contrast, DL approaches, includes convolutional neural networks (CNNs), recurrent neural networks (RNNs), and autoencoders, are examined for their advanced capability to automatically extract features and recognize complex attack patterns.

Results: This survey compares the strengths and limits of these approaches across diverse IoT attack scenarios, including DDoS, malware, and spoofing attacks. A particular focus is given to evaluating supervised and unsupervised learning methodologies in real-world IoT environments.

Conclusions: In order to create reliable, scalable, and adaptable threat detection systems, the survey synthesizes insights from the body of current research to identify important trends, issues, and future directions in IoT security. The results offer a thorough grasp of how ML and DL may be used to increase IoT networks' resistance to changing cyberthreats.

Keywords: Internet of things, diverse attacks, machine learning, deep learning, cyberattacks.

INTRODUCTION

One of the most important and difficult areas of information technology research is cybersecurity, which demands constant development to handle its growing complexity [1]. The incorporation of new technologies like the IoT, which creates special vulnerabilities, makes the problem even more apparent. IoT, sometimes known as the "internet of devices," is expanding at a rate never seen before; by 2020, there will likely be 50 billion linked gadgets worldwide. IoT usage across a variety of cutting-edge applications, includes smart homes, smart cities, driverless cars, and intelligent industrial systems, is what is causing this exponential growth [2].

These developments pose serious dangers to data availability, privacy, and integrity even as they also hold out the possibility of revolutionary advantages. Malicious actors may take advantage of these hazards in order to compromise systems or abuse private data. As a result, cybersecurity in the IoT ecosystem now encompasses more than just preventing unwanted access to networks and systems; it also includes guaranteeing the availability, confidentiality, and integrity of data while preserving individual privacy. As more and more applications that heavily rely on connected devices continue to develop, the importance of tackling IoT security concerns has increased. The need for strong security measures and creative ways to combat potential threats and vulnerabilities has made protecting these interconnected systems a top priority [3].

As IoT continues to gain prominence, attacks on connected devices have become a significant concern. These devices are susceptible to various threats, including privilege escalation, eavesdropping, and denial-of-service attacks [4]. As a result, safeguarding IoT devices from these attacks is becoming more crucial than ever. Furthermore, because IoT devices are physically dispersed, it is simple for unauthorized individuals to gain access [5]. Furthermore, for real-time communication, some elements in such an integrated system rely on wireless networks, which are vulnerable to eavesdropping. Because of this, the system is susceptible to online attacks like web injection, which might lead to data breach and the release of personal information [6]. IoT devices require enhanced and extremely robust intrusion detection (ID) solutions. When malware or a security breach is detected, DL can swiftly assess enormous volumes of data and enable autonomous security system adjustments with very little computing power [7]. Deep learning-based security solutions operate across devices, their underlying operating systems, and files, without needing a network connection to identify threats [8]. The following figure represents the IDS development in IoT environment.

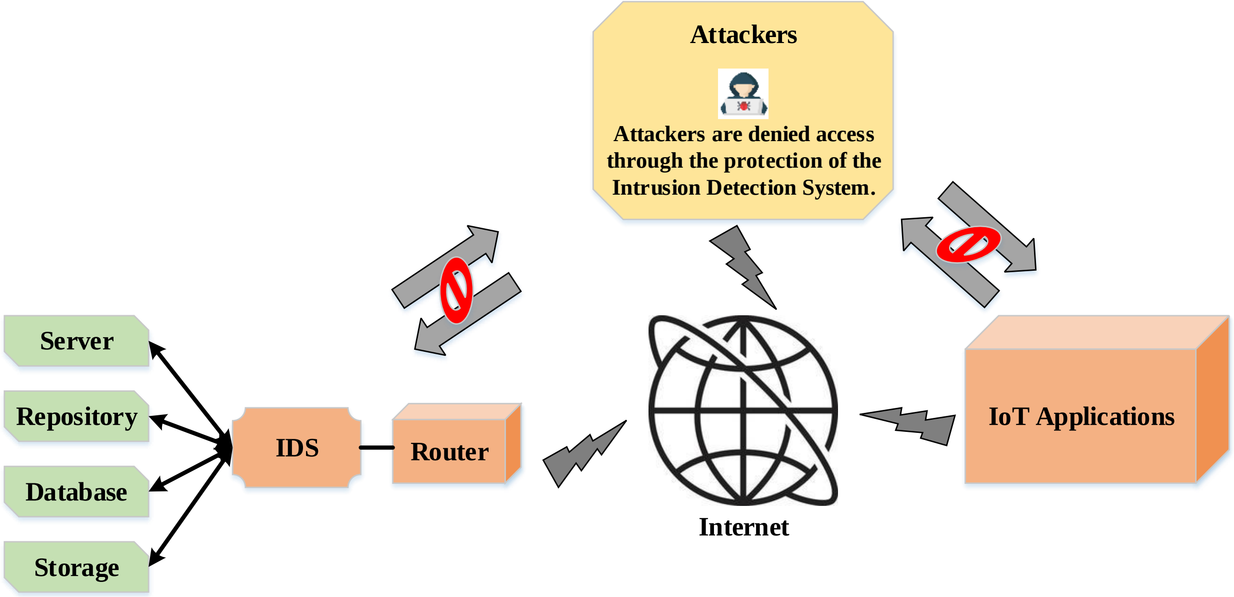
Attackers
Attackers are denied access through the protection of the Intrusion Detection System.
Server
Repository
Database
Storage
IDS
Router
Internet
IoT Applications

Figure 1: An IDS deployment scheme for IoT environment

The IoT widespread adoption has revolutionized a number of sectors by facilitating automation and seamless communication. But because assaults are increasingly targeting IoT devices, their broad usage has also brought about serious security issues [10]. Conventional ID systems (IDS) often find it challenging to adjust to the dynamic and intricate nature of IoT networks, which produce massive volumes of diverse data and are constantly exposed to an ever-changing threat landscape [11].

DLs ability to evaluate massive amounts of data, spot complex patterns, and adjust to novel attack routes has made it a potent tool for IoT threat detection. Using deep learning-based techniques to automate feature extraction and enhance detection accuracy offers reliable, scalable, and effective ways to secure IoT environments. Deep learning's potential to improve IoT security is examined in this study, with particular attention paid to its strengths, weaknesses, and prospects for reducing IoT-based cyber threats [12]. The survey's primary contributions are as follows:

1. This survey offers a detailed examination of both ML and DL techniques for attack detection in IoT networks, highlighting their respective capabilities and limitations.

2. The survey systematically compares conventional ML methods, includes decision trees, support vector machines, and k-nearest neighbors, with advanced DL models, including CNNs, RNNs, and autoencoders, across a variety of IoT attack scenarios such as DDoS, malware, and spoofing.

3. It emphasizes the applicability of supervised and unsupervised learning approaches in real-world IoT environments, providing insights into their performance under practical conditions.

4. By synthesizing insights from existing literature, the survey identifies current trends, challenges, and gaps in IoT attack detection, including the need for scalability, adaptability, and robustness in detection systems.

5. The survey emphasizes the possible of leveraging ML and DL to enhance the resilience of IoT networks against evolving cyber threats, ensuring robust and adaptive security frameworks.

6. The survey is organized into three primary sections. Section 2 offers a widespread overview of the IoT, covering its architecture and categorizing various attacks targeting IoT networks. Section 3 presents an in-depth exploration of ML and DL techniques for detecting IoT-specific attacks, focusing on their strengths, limitations, and practical applications. Section 4 provides a discussion on the findings of the survey. Finally, Section 5 concludes by summarizing the key insights, identifying open research challenges, and suggesting future directions to enhance IoT security using ML and DL approaches.

OVERVIEW OF IOT, IOT ARCHITECTURE, AND IOT ATTACKS:

A McKinsey prediction estimates that by 2023, there will be more than 43 billion IoT devices in use worldwide. From facilitating remote medical monitoring to helping oil companies prevent spills, these billions of gadgets are already transforming our society and will do so even more so in the years to come. The most difficult part, however, is ensuring that such a wide variety of devices work in unison. This is where the layers, systems, and devices within the IoT architecture play a crucial role. It is essential to have a basic grasp of IoT threats before exploring them further. It is crucial to get a thorough grasp of the many technical terms used in the field [13].

Vulnerability: Vulnerabilities are intrinsic flaws in a system or its architecture that let unauthorized users carry out commands, get data without permission, and launch denial-of-service attacks. These vulnerabilities exist in both the software and hardware components of IoT systems. Hardware vulnerabilities are particularly challenging to detect due to their complexity and subtle nature. Compatibility, interoperability, and the significant amount of labour needed for remediation make fixing these vulnerabilities challenging. Operating systems, application software, and control software can all be found to have software vulnerabilities. Errors in software design are caused by both human factors and program complexity. Human weaknesses frequently give birth to technical vulnerabilities, which result in inadequate resources, poor system management, and poor communication. [14].

Exposure: Exposure is the term used to describe a defect or mistake in the system setup that permits an unauthorized individual to take actions to get information. Resilience against physical attacks is one of the main issues facing the IoT. Devices are frequently left unattended and placed in easily accessible areas in the majority of IoT applications, which makes them more susceptible to prospective attackers. Due to this degree of vulnerability, an attacker could potentially take control of the device, alter its code, obtain cryptographic secrets, or replace it with a hostile device that they could control [14].

Threats: A threat is any intentional or unintentional action that exploits weaknesses in a system, leading to harmful consequences. There are two primary types of threats: natural and human. Natural disasters including hurricanes, floods, fires, and earthquakes can seriously damage computer systems. It is difficult to totally prevent natural disasters from occurring, but there are steps that may be taken to lessen their effects. Disaster recovery plans, including backup and contingency strategies, are the most effective means of safeguarding systems against natural disasters. Human hazards are dangers caused by individuals, such as external actors functioning outside of the network and within players having permissioned access. These dangers are distinguished by their malicious purpose, which aims to cause damage and interfere with a system's ability to function [14].

The following categories can be used to group human dangers: (1) People who lack experience and rely on easily accessible hacking tools are the primary source of unstructured threats. (2) Those who are aware of system weaknesses and have the capacity to understand, develop, and use programs and scripts for exploitation are considered structured threats. The advanced persistent threat (APT) phenomena is one example of a structured threat. It is a sophisticated network assault that specifically targets important data in government and commercial organizations, such as manufacturing, banking, and national defence, in order to get data illegally [14].

Attacks: Attacks are intentional actions to damage or disrupt a system by exploiting flaws. They are motivated by self-gratification or restitution, and attack cost measures the effort required to carry out an attack. Attack actors, including hackers, illicit individuals, and governmental entities, pose significant risks to digital technology. Common attack types include close-in assaults, insider exploitation, passive network attacks, which observe communications without protection to decode weakly encrypted information, and active network attacks, which scan unencrypted traffic to uncover sensitive data. Attack cost measures the effort required to carry out an attack, considering factors like skill level, resources, and drive [14].

IoT architecture:

The way devices are arranged and configured to satisfy the individual demands of users is known as IoT architecture. Each of its three to seven levels has a specific function. Interoperability, security, and other issues are brought up by the IoT architecture's lack of standardized protocols. Up to seven levels may be included in the architecture [15].

Perception Layer: The perception layer, also known as the device layer, consists of various components such as sensors, GPS modules, security cameras, RFID scanners, and others. These gadgets can be utilised with industrial equipment including automated guided vehicles (AGVs), industrial robots, and conveyor systems. These gadgets convey raw materials, collect sensory data, monitor the production floor and the surrounding area, and more [15].

Transport Layer/Network Layer: Information is sent to the processing systems at the next tier via the transport/network layer. IoT gateways employ data transfer protocols (DTPs) to transport data to local or cloud data centers after converting analogue input to digital representation. IoT protocols are a set of rules that govern how devices within systems, capable of detecting, collecting, and sharing data in real-time, communicate with each other. Different protocols exist; some are general-purpose, while others are tailored to data transfer, wireless connection, or device management. The smooth operation of IoT systems depends on appropriate protocols, which provide appropriate data connection and exchange. IoT systems operate well when appropriate protocols are used to guarantee correct data connection and exchange.

Edge Layer: In IoT workloads, firmware, embedded operating systems, and physical hardware make up the edge layer. With the growth of IoT networks, latency becomes a major performance issue. This challenge is tackled by edge computing, which is implemented through the edge layer of the IoT system. It facilitates data processing and analysis near the data source, reducing latency and enhancing efficiency. Computing power can be positioned close to sensors to minimize latency and facilitate immediate data sharing. This is essential for some application scenarios, such industrial safety systems and driverless autos. Every IoT edge device broadcasts data packets to nodes so they may be processed further. When anomalies are identified, smart edge devices have the ability to halt target functions or initiate damage control activities. The edge layer has the ability to speed up data processing and offer essential insights.

Processing Layer: Comprising servers and databases, the processing layer also referred to as the middleware layer performs a number of tasks, including making decisions, calculating optimization methods, and storing enormous amounts of data [15]. Platforms for cloud computing that are capable of analyzing and interpreting real-world data make up this layer. It uses vast data modules and cloud services to transform raw sensor data into relevant information. Furthermore, the system can react to inputs and answers instantly acknowledgements to the processing layer. It has the capability to process the data it receives and make decisions. This layer is also responsible for generating predictions and offering insights based on the information collected during the perception stage [16].

Application Layer: IoT infrastructure's application layer analyses data to solve business issues or accomplish aims. It is composed of services and applications that are constructed on top of the processing layer. Software tools convert processing layer data into information that is useful to automated processes or people. The application layer provides users with access to data collected and processed in previous layers through tools like dashboards and mobile applications, allowing them to monitor and analyze network data. Middleware integration with IoT software is achieved through Application Programming Interfaces (APIs).

Business Layer: The business layer is in charge of evaluating application layer data and solutions and directing operational choices to improve customer happiness, cost effectiveness, productivity, and security. It contains many application layer instances and controls models and transactions tied to connected devices. This layer is in charge of managing business logic and putting policies in place to guarantee that the IoT system's business goals are met. It also contains analytics, rules, and business process management [16].

Security Layer: The success of an IoT solution depends on the security layer, which permeates all IoT architectural levels. Sensitive data is often exchanged by an IoT system. The IoT security layer consists of three main parts [16].

- **Device Security:** It begins with devices that have perception-layer hardware and firmware defences. It involves protecting actual IoT endpoints against malware and hijacks. Using cryptographic keys for proper authentication, reinforced exteriors, preventing unauthorized programs from operating on linked devices, and resolving firmware update and security patch issues are all ways to keep your devices safe. [17].
- **Connection Security:** Usually, it uses encryption to protect information that is sent via networks. Transport Layer Security (TLS) is the basic protocol for IoT connection security. End-to-end encryption removes the chance of data being intercepted and abused by unauthorized users [17].
- **Cloud Security:** Encryption is crucial to cloud security because it lessens the possibility that private information may be made public through data breaches. Restricting access to IoT apps requires the deployment of robust authentication and authorization constraints. To protect against malicious devices, devices must be authorized before connecting to the cloud or an IoT system [17].

The IoT uses technologies like computation, sensor networks, Internet protocols, and communication to turn physical things into smart ones. For both business and academics to implement smart city concepts using billions of linked devices, an ideal IoT infrastructure is essential. The IoT paradigm entails linking various systems and objects via various communication protocols. With the help of computing equipment and physical items connected into a communication network, the IoT architecture provides customers with intelligent services. Each level is explained in the subsections that follow.

i) Physical object: Physical sensors that perceive, gather, and analyses data are part of the IoT's physical object level. These sensors, which include motion, acceleration, temperature, and humidity sensors, have a variety of detecting uses. Heterogeneous sensor configuration requires the plug-and-play technique. Because of their limited computing and battery capacity, IoT sensors are resource-constrained [18]. Context-aware IoT systems require an understanding of sensor data. A significant quantity of IoT big data is generated at this level. Big data and the proliferation of IoT devices are closely related. Making better judgements for the IoT's safe rollout can be aided by big data analysis.

ii) Connectivity: The IoT platform aims to deliver intelligent services by enabling collaboration between diverse sensors. However, because of their limited processing and storage capabilities and dependence on battery power, these sensors are resource-constrained. To address these challenges, IoT devices must function efficiently in noisy communication environments while minimizing power consumption. Key challenges include developing low-power communication technologies for sensor data transmission, designing efficient routing protocols that account for sensor memory limitations, and assigning unique IP addresses to billions of Internet-connected devices [19]. To tackle these issues, IoT leverages emerging communication technologies such as Near-Field Communication (NFC), RFID, IEEE 802.15.4, Bluetooth, WiFi, 6LoWPAN, and ultra-wideband (UWB).

iii) Middleware: Developers can concentrate on the issue at the system or hardware level by using middleware, which is software that simulates the intricacies of a system or hardware. Cooperative processing is made possible by the software level it provides between applications, the operating system, and network communication layers. It acts as a bridge between an application and the system software from a computational standpoint. Its primary purposes include facilitating collaboration among diverse IoT objects, ensuring interoperability among IoT devices, facilitating device scalability, and managing the future expansion of IoT devices. Context-aware computing is used to interpret sensor data and provide consumers intelligent services [20]. It also facilitates device discovery and context awareness. Finally, it protects IoT devices' privacy and security because the data they gather is usually about people or businesses. In order to handle security and privacy concerns, middleware must include procedures that enable a secure IoT system.

iv) Big Data Analytics: The IoT generates vast amounts of data that can be used to build intelligent IoT systems for smart services. Big data is produced by physical devices used in IoT applications, and researchers have explored methods to integrate big data analytical methods with IoT design. Big data can be efficiently mined for hidden insights by ML and DL, which can then transform it into actionable information with little human intervention. There are three types of analytical techniques: perspective, predictive, and descriptive analytics. Descriptive analytics describes current or past events, predictive analytics predicts the future based on current patterns, and prescriptive analytics provides recommendations for decision-making. Big data related to IoT system behavior is crucial for building ML/DL to secure IoT systems [21].

v) Applications: There are numerous uses for IoT. Among the well-known uses are smart buildings, smart grids, smart transportation, and smart healthcare. These applications are covered in brief in the subsections that follow.

- **Smart Healthcare:** IoT-enabled medical devices track patient health, notify patients in an emergency, and enable prompt intervention. IoMT is being used by around 60% of the healthcare industry, changing the system from being disorganized to synchronized. It was projected that there will be 20–30 billion IoMT devices worldwide by 2020 [22]. Even with improvements, protecting IoT systems while maintaining adaptable access in an emergency is still a major problem.

- **Smart Transportation:** By combining information from sensors, CCTV, GPS, and weather apps, smart transport systems use the IoT to control traffic in cities. Both user suggestions and real-time traffic analysis are offered by this system. Through data fusion and analytics, it also improves delivery efficiency, cargo timetables, and road safety [23].

- **Smart Governance:** By combining sensor data from many industries, IoT supports governance by empowering decision-makers. Through data correlation, IoT offers knowledge-based solutions that get beyond the drawbacks of conventional monitoring systems. By taking into account many viewpoints from various sources, this guarantees the best possible conclusions.

- **Smart Agriculture:** Real-time monitoring of variables like temperature, moisture content, and humidity is made possible by IoT in agriculture. These insights aid in disease and insect detection, irrigation automation, and water and soil quality monitoring. The system's accurate environmental monitoring increases efficiency and production [24].

- **Smart Grid:** Smart grids driven by IoT enhance electricity management between customers and providers. These grids improve real-time monitoring, safety, and efficiency [25]. IoT analytics let decision-makers adapt the supply of electricity to consumer demands, optimize power transmission, and avert calamities.

- **Smart Homes:** IoT is used by smart home systems to remotely operate appliances like air conditioners, refrigerators, and TVs. They adjust to changes in their surroundings by utilizing face recognition to unlock doors or regulate the temperature. For smooth automation, smart houses combine external systems, such as smart grids, with interior IoT devices [26].

- **Smart Supply Chain:** IoT-enabled sensors, such as RFID and NFC, track products throughout manufacturing and transit, streamlining supply chain operations. These technologies produce data that enhances decision-making and machine uptime. This improves customer service, product delivery, and corporate productivity.

- **Collaboration and Business Objective:** IoT fosters societal and economic progress by integrating data from several levels to fit with company objectives. IoT device big data analysis enhances corporate results and helps with strategic planning [26]. In order to maximize development and decision-making, this level places a strong emphasis on human contact with IoT.

IoT Security Threats:

Intelligent interaction is made possible by the IoT, which links the virtual and physical worlds. IoT devices must, however, adhere to strict security regulations in both their physical and virtual environments. Because these systems are diverse and sophisticated, maintaining security in the face of extensive attack surfaces is difficult. To get the appropriate level of security, holistic considerations are required [27]. IoT devices cannot support complicated security mechanisms because of their low computational and power capabilities, and they are susceptible to physical access and eavesdropping. The IoT system may be vulnerable to passive and active assaults, which might compromise authorization, confidentiality, integrity nonrepudiation, and authentication.

Security Properties for IoT Systems:

i) **Confidentiality**: Protects sensitive IoT data against unwanted access, including personal, medical, and industrial data. Location confidentiality is one of the difficulties as hackers may still identify and follow IoT devices even when data and communication are encrypted.

ii) **Integrity**: Prevents unwanted changes to IoT data while it is being sent wirelessly. In applications like medical implants where mistakes might save lives, maintaining data integrity is essential to preventing malicious inputs like SQL injections and ensuring dependable device operations.

iii) **Authentication**: Before allowing access to the system, entity IDs are established. Trade-offs are necessary for IoT devices, particularly in safety-critical industries like healthcare, where authentication techniques must strike a compromise between security and system limitations like battery life or flexibility.

iv) **Authorization**: Restricts access to IoT systems so that only devices or people with permission may communicate with sensors or data. Managing access privileges in settings with a broad user base and preserving data security during sensing and transmission are two challenges.

v) Availability: Ensures that authorized entities may always access IoT services. Continuous service delivery is a crucial area of study for IoT security since threats like DoS attacks and active jamming can interfere with availability.

vi) **Non-repudiation**: Prevents users or devices from disputing their operations by providing verifiable logs of activity. Ensuring responsibility for transactions is crucial in situations like payment systems, even if it is less important in many IoT systems.

Threats in IoT

This section offers a thorough summary of the physical and cyber dangers that affect the IoT ecosystem, along with possible attack points such network services, cloud services, and physical devices.

Cyber Threats:

i) Passive Threats: Eavesdropping on networks or communication channels in order to follow sensor bearers, collect data from sensors, or both is known as passive threat. In addition to violating privacy, such attacks may lead to the collection of sensitive health information, which is highly valued on the black market. Personal health information, for example, can be worth $50, whereas credit card information and social security numbers are only worth $1.50 and $3, respectively. Additionally, when a communication channel is within range, attackers can use it to track the position of IoT device holders. There are serious privacy issues as a result.

ii) Active Threats: Eavesdropping and altering IoT systems to change settings, regulate communications, or refuse services are examples of active threats. Active attacks include DoS, malicious inputs, data manipulation, and impersonation. Malicious input attacks include inserting malicious software into IoT systems, which may result in code execution and system interruption, whereas impersonation attacks try to imitate an authorized user or IoT device. Unauthorized modifications to sent or stored data are known as data tampering, and they can affect IoT system functions like changing billing rates in IoT-based smart grids. Distributed DoS (DDoS) and other DoS attacks use bandwidth or resource depletion to interfere with services. Advanced botnets, such as Mirai, have launched widespread DDoS assaults by taking use of IoT devices.

Physical Threats:

Physical Destruction: Deliberately destroying IoT components or inadvertently causing harm due to natural catastrophes like earthquakes or floods, as well as man-made calamities like wars, are examples of physical hazards. These dangers cause service disruptions by targeting easily accessible IoT devices like sensors and cameras. IoT devices are more susceptible to these kinds of assaults due to their ubiquitous physical presence, especially since many of these components are simple to access and destroy.

IoT Attack Surfaces:

i) Physical Device Surface: IoT systems heavily rely on physical components like sensor nodes and RFID tags. RFID technology bridges the gap between virtual and physical interactions and enables real-time object tracking. However, because of their limited resources and sensitive data, these devices frequently have security problems that leave them vulnerable to DoS attacks, spoofing, counterfeiting, and eavesdropping. These gadgets' physical accessibility makes them much more vulnerable.

ii) Network Service Surface: Physical components like sensors and actuators that are connected via wired and wireless technologies make up IoT systems. Although sensor networks are essential to IoT systems, they have the same security vulnerabilities as conventional networks, particularly when combined with IoT. To get network information like IP and MAC addresses, attackers may target open ports or take advantage of flaws in routing protocols. The increased mobility and connection of IoT raises the possibility of assaults like man-in-the-middle, DoS, and hacking. Furthermore, threats like viruses, infiltration, and identity theft are introduced by the usage of standard Internet protocols (TCP/IP) to link billions of IoT devices.

iii) Cloud Service Surface: Cloud computing and IoT system integration has several advantages, like increased computational and energy efficiency, but it also raises serious security issues. Data security vulnerabilities may be exploited by attackers using techniques includes SQL injection, cross-site request forgery, and cross-site scripting (XSS). It is also possible for attackers to escalate privileges and obtain unauthorized access due to vulnerabilities in virtual servers. Sensitive information, including that from home sensors or medical records, is also made public, raising privacy issues. Cloud computing's multi-tenancy characteristic increases the likelihood of data leaks, underscoring the necessity of strong privacy safeguards for IoT-cloud connections. The following figure 2 shows the classifications of cybersecurity in IoT system.

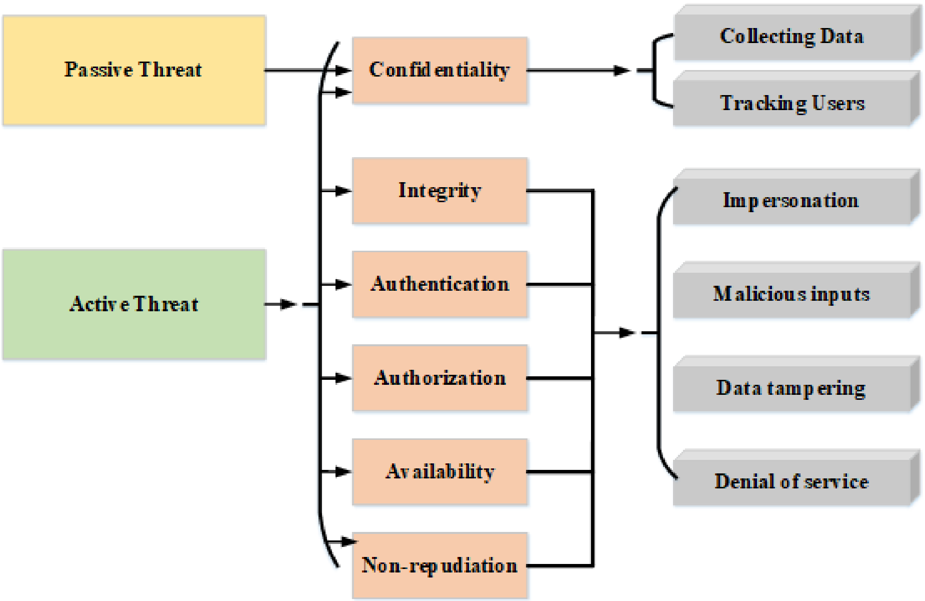

Figure 2: Classification of Cybersecurity Threats in IoT Systems

Intrusion Detection in the IoT

A crucial component of protecting IoT networks is ID. These networks are intrinsically insecure because of their dispersed architecture, resource-constrained devices, and dependence on wireless communication. The following figure 3 represents the classifications of ID in IoT.

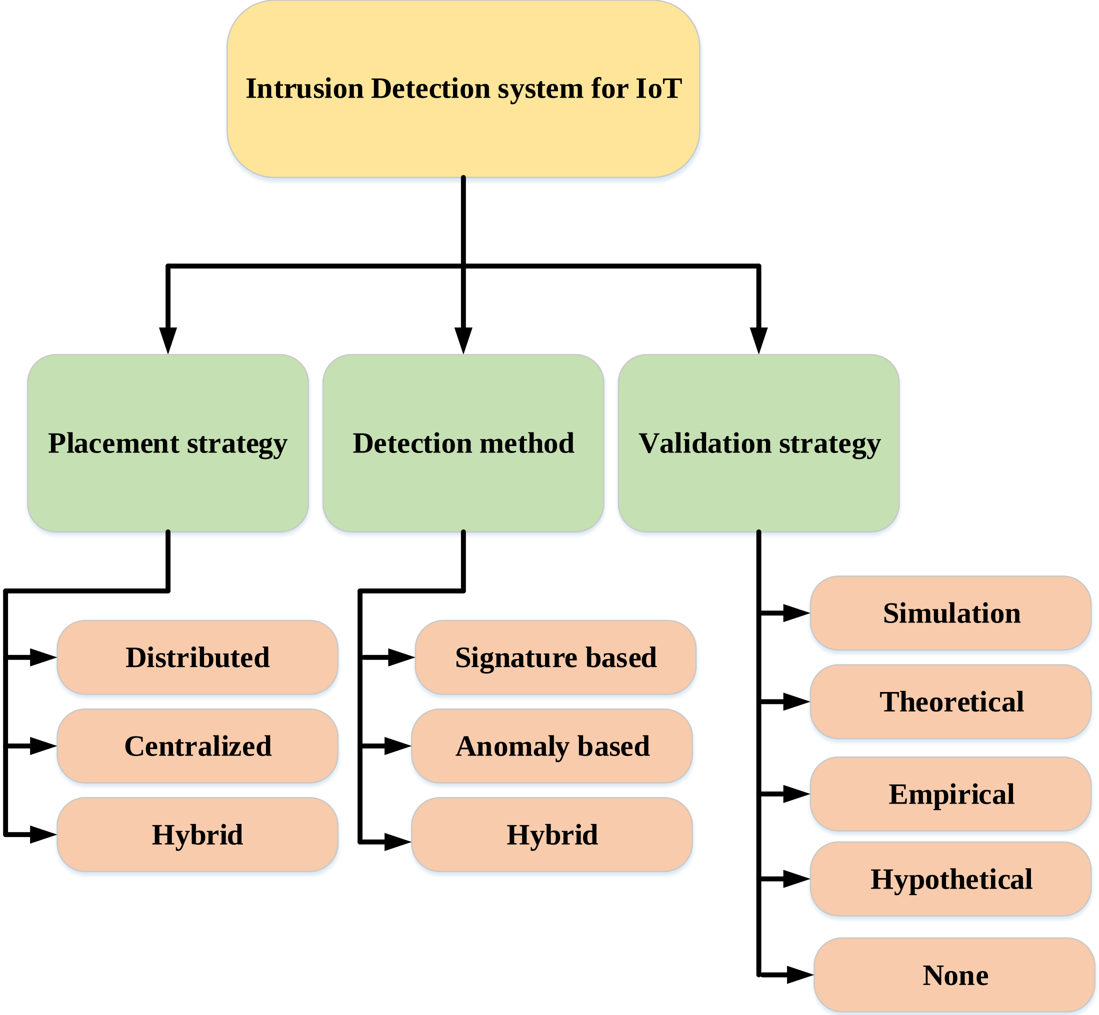

Figure 3: Classifications of Intrusion detection in IoT

Unauthorized acts or activities that damage the IoT ecosystem are referred to as IoT intrusions. Stated differently, an intrusion occurs when an attack jeopardises the availability, confidentiality, or integrity of data in an Internet of Things context. An incursion is, for instance, when an attack interferes with computer services, making them inaccessible to authorized users. An intrusion detection system (IDS) is a piece of hardware or software that keeps systems safe by spotting hostile activity on computers [28]. The main objective of an IDS is to identify unauthorized system access and detect malicious network traffic, tasks that go beyond the capabilities of traditional firewalls. By doing so, IDS enhances the security of computer systems, protecting them from malicious actions that threaten their availability, integrity, or confidentiality.

IDS systems are broadly categorized into two main types:

i) Signature-based Intrusion Detection Systems (SIDS): Detect known attack patterns by matching them with predefined signatures.

ii) Anomaly-based Intrusion Detection Systems (AIDS): Recognize departures from typical conduct to identify possible dangers, such as unidentified assaults.

SURVEY OF MACHINE LEARNING AND DEEP LEARNING APPLICATION ON DIVERSE ATTACK DETECTION IN IOT

The IoT has revolutionized the digital landscape by connecting devices, systems, and services across various domains. However, this growth has also introduced security challenges, such as denial of service, data tampering, impersonation, and unauthorized access. These attacks compromise core security requirements of IoT systems. ML and DL techniques have emerged as powerful tools for detecting and mitigating diverse attacks in IoT environments. These techniques analyze complex patterns, recognize anomalies, and predict threats in real-time, enabling proactive and efficient security solutions. The paper examines how ML and DL approaches are applied in IoT attack detection, emphasizing how they might strengthen IoT systems' resistance to changing cyberthreats. It emphasizes the importance of developing robust, scalable, and lightweight algorithms tailored to IoT networks' unique characteristics and constraints.

Survey of Machine Learning Techniques for Diverse Attack Detection in IoT:

The rapid growth of IoT has made it a prime target for various cyberattacks, necessitating the usage of advanced ML techniques for attack detection. ML offers intelligent solutions for identifying anomalies, patterns, and threats in IoT environments. These methods enhance detection accuracy, minimize false alarms, and adapt to evolving attack strategies. This section discovers the application of ML techniques in addressing diverse IoT security challenges.

Churcher et.al [29] Attacks became more likely due to the growing number of IoT devices and the data they contained. Since traditional IDS were unable to handle these threats, ML techniques like logistic regression (LR), k-nearest neighbor (KNN), support vector machines (SVM), decision trees (DT), naïve Bayes (NB), random forests (RF), and artificial neural networks (ANN) proved to be more successful. The Bot-IoT dataset was utilized in this study to compare ML methods for binary and multi-class classification. However, the performance of the models, particularly in multi-class classification, could be impacted by the imbalance of attack types in the dataset, potentially leading to less accurate detection for underrepresented attack categories.

Hasan et.al [30] This study observed the impact of various threats and attacks on the IoT. The research compared the performance of several ML models, includes LR, SVM, Decision Tree (DT), RF, and ANN, in detecting attacks and anomalies in IoT systems. The evaluation metrics used included area under the ROC Curve, F1 score, recall, accuracy, and precision. The results showed that the test accuracy for ANN, RF, and DT was 99.4%, with RF slightly outperforming the others. However, ML models, especially ANN and Random Forest, proved to be computationally expensive and did not scale well to large IoT networks with limited resources, potentially leading to higher latency and decreased system performance in real-world deployments.

Rashid et.al [31] Smart city development has been greatly influenced by the IoT, which has improved service quality and operational efficiency. However, because IoT devices linked to sensors on massive cloud servers are susceptible to malevolent assaults, this expansion also increases cybersecurity risks. Using ML algorithms, including ensemble techniques like bagging, boosting, and stacking, this research investigates an attack and anomaly detection strategy. Additionally, the study takes into account multi-class classification, cross-validation, and feature selection. However, it can also lead to overfitting, especially when the underlying models have high complexity, making the detection system less adaptable to new, unseen attack patterns or anomalies.

Sarker et al. [32] investigated how ML approaches assisted in addressing the growing concerns in cybersecurity over cyber anomalies and threats. The study highlighted that security features and data characteristics determined the effectiveness of learning-based security models. A thorough empirical analysis of the effectiveness of several models was also provided, along with Cyber Learning, an ML-based cybersecurity model with correlated-feature selection. It utilized a security framework based on ANN with multiple hidden layers, as well as established ML classification techniques. The study aimed to provide a reference point for data-driven security modelling in cybersecurity. However, it noted that incorporating complex models like ANN and ensemble techniques could lead to overfitting, particularly when datasets did not sufficiently simulate real-world scenarios or contained noisy data.

Alissa et.al [33] IoT transitions were hampered by the increase in cyberattacks and security threats, such as botnets, brought on by the proliferation of IoT devices. In the context of the Internet of Things, recent studies proposed using ML and DL techniques to detect and classify botnet assaults. This work proposed machine learning techniques for binary class categorization using the publicly accessible UNSW-NB15 dataset. To solve the issue of class imbalance, the SMOTE-Over Sampling approach was used. The proposal included preprocessing and exploratory data analysis as part of a comprehensive ML workflow. The process involved six basic stages, including logistic regression, XGBoost, and decision trees. The decision tree achieved a 94% test accuracy, outperforming expectations and demonstrating the potential of ML to address these challenges. However, the study did not address the scalability of the proposed pipeline in large-scale IoT networks, where high data volumes and diverse attack types were prevalent.

Gaber et.al [34] Wireless sensors are essential for connecting components and integrating IoT and 5G technologies in smart cities, an IoT application that is expanding quickly. However, manufacturers' negligence in addressing security concerns with IoT devices continues to pose security and privacy risks. One way to lessen these dangers is through ID. Using two feature selection strategies and ML classifiers (SVM, RF, DT), this study suggests an ID approach for identifying injection assaults in IoT applications. However, the focus on injection attacks does not address other critical IoT threats, such as DDoS, malware, or zero-day attacks, limiting the comprehensive applicability of the IDS.

Karthikeyan et al. [35] linked IoT and WSN as systems that processed and shared data to improve decision-making. Protective measures were needed to secure these systems to guarantee dependability and safety. The study utilized the Firefly Algorithm and ML to enhance IoT and WSN security. By improving ID accuracy in the WSN-IoT environment, the proposed FAML approach added a new level of complexity to security optimization strategies. The FAML approach classified data using the Grey Wolf Optimizer algorithm and a support vector machine model. However, it resulted in significant computational overhead, particularly in large-scale IoT and WSN environments.

Al-Sarem et.al [36] A major concern was the rise in attacks on IoT networks, particularly botnet attacks. The limited battery life and computing capacity of IoT systems made it challenging to optimize the effectiveness of IDS designed to detect these threats. This study suggested a feature selection strategy based on aggregated mutual information and ML techniques to improve the detection of IoT botnet assaults. The N-BaIoT benchmark dataset was utilized to detect different types of botnet assaults using actual traffic data from nine commercial IoT devices. Using a range of evaluation metrics, the proposed method outperformed alternative approaches, demonstrating its efficacy and efficiency. However, the study lacked a detailed analysis of specific botnet attack types or network anomalies, highlighting the need for more granular insights.

Bhayo et.al [37] The IoT was found to be highly susceptible to Distributed Denial of Service (DDoS) attacks due to its complex network structure and vulnerable sensors and devices. The integration of IoT with Software Defined Networking (SDN) showed potential for enhancing security. However, DDoS attacks remained a significant threat to IoT networks. To address this issue, a ML -based method was proposed to identify DDoS attacks in an SDN-WISE IoT controller. The suggested framework classified SDN-IoT network packets using NB, DT, and SVM algorithms. The results established the framework's effectiveness in detecting DDoS attacks, indicating its potential to enhance IoT network security and mitigate such threats. However, the study lacked comprehensiveness in addressing other IoT security challenges, such as data breaches, ransomware, and advanced persistent threats.

Panda et.al [38] Network attacks, particularly botnets, increasingly targeted smart digital devices and IoT systems. As a countermeasure, effective ML and DL techniques combined with appropriate feature engineering were proposed to identify and protect networks against such vulnerabilities. This study utilized the UNSW-NB15 dataset, an unbalanced and noisy IoT-Botnet dataset, to categorize cyberattacks. K-Medoid sampling and scatter search-based feature engineering techniques were used to create a representative dataset with the best feature subsets. The suggested approaches were validated using two DL techniques (DMLP and CNN) and three ML techniques. Among these, the scatter search-based DMLP classifier outperformed competing models in terms of detection rate, accuracy, precision, recall, and F1-score, while also demonstrating lower computational cost.

Tyagi et.al [39] The IoT was described as a network of interconnected devices that continuously shared information and made decisions. Due to the appeal of this interconnected architecture to cybercriminals, it became essential to develop a system capable of reliably and automatically detecting anomalies and attacks in IoT networks. This research presented an IDS designed to swiftly and accurately differentiate between malicious and benign traffic. The system was based on a unique feature set synthesized from the BoT-IoT dataset. The study showed how well seven lightweight characteristics might distinguish between four different kinds of assaults: information theft, reconnaissance, DoS, and DDoS. Additionally, it highlighted the suitability and efficiency of supervised ML algorithms for enhancing IoT security. However, the research raised concerns about the potential for overfitting to the dataset, which might affect performance when applied to unseen or dynamic data.

Soe et.al [40] The majority of cyberattacks were found to be botnet-based, and their frequency had increased due to the rapid development and widespread adoption of IoT devices. These devices often lacked the memory and processing power required for robust security features, making it easier for attackers to bypass existing rule-based detection systems. Three distinct machine learning algorithms—ANN, J48, and NB—were used in a study to attain overall detection performance in a sequential detection architecture ML-based botnet attack detection framework. The proposed architecture could be extended with sub-engines for detecting additional attack types and was shown to be effective in detecting botnet-based assaults. However, its scalability to larger IoT networks with diverse devices and traffic patterns was not evaluated.

Tuan et.al [41] Network traffic is seriously threatened by botnets, which are made up of numerous PCs under the direction of botmasters. They are in charge of a number of online assaults, such as malware, spam, and DDoS. This study used the UNBS-NB 15 and KDD99 datasets to experimentally analyses these techniques for Botnet DDoS attack identification. The KDD99 dataset outperformed the UNBS-NB 15 dataset, according to the results, suggesting that ML may be used to identify botnet DDoS assaults. However, it can overfit, potentially causing inflated performance metrics in controlled environments but poor generalization in real-world scenarios.

Gad et.al [42] The IoT is an expanding network infrastructure-based collection of physical objects that exchange data and interact. IoT networks, however, are becoming more and more susceptible to security lapses, especially cyberattacks. Many scholars are concentrating on ML techniques as IDSs to improve security. In order to identify IoT threats and prevent harmful events, this paper suggests a novel machine learning-based distributed detection system. The ToN-IoT dataset, which was produced from a large, diverse IoT network, was used for training and testing. The first model, which is based on data collected from every layer of the same IoT system, is the one that is suggested. The XGBoost approach performed better than other ML techniques for each node in the suggested model.

Saheed et.al [43] The increasing number of internet-connected devices, collectively known as the IoT, brought new security and privacy challenges. As IoT devices proliferated, more resources were allocated to research aimed at enhancing ID. IoT adoption accelerated across various sectors, including healthcare, yet security and privacy concerns remained significant obstacles. To address these issues, this study suggested a ML-IDS for identifying attacks on IoT networks. The approach utilized Principal Component Analysis for dimensionality reduction, the Minimum-Maximum concept for feature scaling, and six ML models for detection. However, the solution introduced substantial computational overhead, posing challenges for real-time ID in resource-constrained IoT environments.

Sadhwani et.al [44] This research presented a lightweight ID solution for IoT networks, which were vulnerable to virus propagation and DDoS attacks. To safeguard critical infrastructure, ensure business continuity, and enhance user experience, the model analyzed network traffic patterns and identified irregularities. The study focused on the growing concerns surrounding IoT devices and DDoS assaults, aiming to improve the security of critical network systems. The system balanced attack classes across the TON-IOT and BOT-IOT datasets by employing ML classifiers and a novel data preprocessing method. It utilized various classifier types, including LR, RF, NB, ANN, and KNN algorithms, to develop a lightweight intrusion detection system capable of defending against DDoS attacks in IoT networks effectively. However, the research did not assess the impact of increasing network size or traffic volume, which could influence the model's scalability and performance.

Campos et al. [45] highlighted the growing significance of IoT while addressing its vulnerability to cyberattacks. Using side-channel approaches that tracked device power consumption, the study proposed a method to analyze IoT networks and detect assaults. Without altering device behavior, the researchers demonstrated that a ML -powered monitoring system could identify intrusions. Tests conducted under various conditions, including real-time detection, novel threats, and customized datasets, yielded positive results. Portability, repeatability, and simplicity were identified as key advantages of the proposed system. It could be installed on numerous devices without requiring extensive resources. Based on IoT network architecture and device power limitations, the study suggested several deployment strategies. However, choosing the best attributes for categorization presented difficulties and may affect the IDS's overall efficacy and accuracy.

Gaur et.al [46] DDoS attacks overloaded target networks with malicious traffic from multiple domains, endangering network security. Using feature selection techniques to detect these attacks was a challenging task. For the early detection of DDoS attacks on IoT devices, a hybrid methodology utilizing chi-square, Extra Tree, and ANOVA techniques on ML classifiers, including RF, DT, KNN, and XGBoost, was presented. The proposed hybrid technique proved useful for early DDoS attack detection on IoT devices, as demonstrated by its 82.5% feature reduction ratio and 98.34% accuracy with ANOVA for XGBoost. Combining multiple feature selection methods and classifiers added complexity to the system, which could impact deployment and real-time execution in resource-constrained IoT environments.

ANOH et al. [47] emphasized the need for preventive measures due to the rise in assaults on connected devices caused by the IoT in communication networks. IDS were employed to analyze network data and identify anomalous activities. The study aimed to develop an IDS using ML models and the UNSW-NB15 dataset. After data cleaning and feature engineering in the preprocessing stage, models such as LR, SVM classifier, DT, RF, and XGBoost were used to predict attacks. Based on experiments conducted utilizing the UNSW-NB15 dataset, the random forest model was identified as the best performer, clearly outperforming the other models in detecting rare abnormal behaviors.

Buiya et.al [48] Smart homes, wearable technology, industrial systems, and healthcare applications are just a few of the areas of human existence that are being revolutionized by the IoT. The goal of this project is to create, select, assess, and implement cutting-edge ML models for identifying cyberattacks on IoT network traffic. A dataset simulating IoT network traffic, including DDOS, MITM, and botnet assaults, was employed in the study. It was discovered that Random Forest outperformed LR in attack detection, exhibiting remarkable accuracy and fewer false negatives. However, it but faces computational challenges, particularly with large datasets, potentially impacting real-time applications. The following table 1 represents the ML techniques for diverse attack detection in IoT

Table 1: ML techniques for diverse attack detection in IoT

Ref.No	Method	Dataset	Objective	Advantages	Limitation/Future scope
[29]	LR, KNN, SVM, DT, NB, RF, ANN	Bot-IoT Dataset	Compare ML methods for binary and multi-class classification for attack detection	KNN achieved 99% accuracy in multi-class classification; RF outperformed others in binary classification	Imbalance in attack types may reduce accuracy for underrepresented attacks
[30]	Logistic Regression, SVM, Decision Tree, RF, ANN	IoT Attack Dataset	Evaluate performance of ML models in detecting attacks	ANN, Random Forest, and Decision Tree achieved 99.4% accuracy	High computational cost; models may not scale well in large IoT networks
[31]	Ensemble Techniques (Bagging, Boosting, Stacking)	IoT Attack Dataset	Investigate ML -based attack and anomaly detection in IoT	Stacking ensemble model performed better in performance metrics	Risk of overfitting with complex underlying models; less adaptability to unseen attack patterns
[32]	ANN, Multi-class and Binary Classification	Cyber Learning Framework	Examine the efficacy of ML in cybersecurity anomaly detection	High effectiveness for cyber anomaly detection using correlated-feature selection	Overfitting risk with ANN and ensemble models, especially with noisy datasets
[33]	Logistic Regression,	UNSW-NB15 Dataset	Address botnet attacks in IoT through ML	Decision Tree achieved 94% test accuracy	Limited scalability in large-scale IoT

	XGBoost, Decision Trees				networks with diverse attack types
[34]	SVM, Random Forest, Decision Tree	Wireless Sensor Networks (IoT) Dataset	ID for identifying injection attacks in IoT applications	Effective at identifying injection attacks	Limited to injection attacks, ignoring other IoT threats like DDoS and malware
[35]	Firefly Algorithm, Grey Wolf Optimizer (GWO), SVM	WSN-IoT Environment Dataset	Enhance ID accuracy in WSN-IoT environments	Improved classification accuracy and introduced complexity in security optimization	Significant computational overhead in large-scale IoT and WSN environments
[36]	Feature Selection (Mutual Information, PCA, ANOVA), ML Techniques	N-BaIoT Dataset	Enhance detection of IoT botnet attacks	Effective feature selection and detection method	Lacks analysis of specific botnet types and network anomalies
[37]	NB, DT, SVM	SDN-WISE IoT Controller	Detect DDoS attacks in SDN-based IoT networks	Effective in identifying DDoS attacks	Focused solely on DDoS attacks, ignoring other IoT security issues like ransomware
[38]	Scatter Search, K-Medoid Sampling, DL (DMLP, CNN), ML Techniques	UNSW-NB15 Dataset	Identify cyberattacks, particularly botnets in IoT	DMLP classifier outperformed others in accuracy and recall	Noise and unbalanced dataset; limited scalability to large networks
[39]	SVM, ANN, NB, DT, Unsupervised Learning (USML)	UNBS-NB15 and KDD99 Datasets	Identify Botnet DDoS attacks using ML techniques	Identified Botnet DDoS attacks with ML techniques	Overfitting risk in controlled environments; poor generalization in real-world scenarios
[40]	XGBoost, ML-based IDS	ToN-IoT Dataset	Distributed detection system for IoT security	First model based on data from all IoT layers; high performance	Requires further validation for larger IoT networks
[43]	Principal Component Analysis (PCA), Minimum-Maximum scaling, ML Models	IoT Network Dataset	Develop a machine-learning-based IDS for IoT attacks	High performance with several metrics (accuracy, F1-score)	Computational overhead limits real-time detection in resource-constrained environments
[44]	Lightweight IDS for IoT networks	IoT Security Dataset	Protect IoT networks from viruses and DDoS attacks	Lightweight solution for IoT	Lacks scalability for diverse IoT systems

[45]	Side-Channel Analysis, ML	Custom IoT Network Dataset	Analyze IoT networks and detect intrusions through device power consumption tracking	Portability, repeatability, and simplicity; effective in real-time detection and novel threats	Feature selection challenges could affect classification accuracy and system efficiency
[46]	Random Forest, Gradient Boosting Machines (GBM), SVM	IoT Attack Dataset	Improve detection of advanced persistent threats (APT) in IoT networks	GBM and Random Forest offered high detection accuracy	Limited adaptability to evolving APT strategies
[47]	LR, SVM, DT, RF, XGBoost	UNSW-NB15 Dataset	Develop an IDS to detect anomalies in IoT communication networks	Random Forest performed best, effectively detecting rare abnormal behaviors	Limited to the UNSW-NB15 dataset; potential need for real-time adaptation and scalability
[48]	Ensemble Learning, Hybrid Classifier	IoT Botnet Dataset	Enhance IoT botnet detection and classification	Hybrid models increased robustness against false positives	Needs additional evaluation on different attack types and network conditions

Summary

The reviewed studies highlight the growing cybersecurity challenges in IoT environments, driven by the proliferation of devices and diverse attack vectors such as DDoS, botnets, and malware. ML and DL techniques, including SVM, ANN, DT, RF, and ensemble methods, have proven effective in ID and attack classification, often leveraging datasets like Bot-IoT, UNSW-NB15, and KDD99. While models like RF and KNN excel in binary and multi-class classification, challenges such as class imbalance, computational overhead, scalability, and overfitting remain prevalent. Advanced approaches, including feature selection, ensemble techniques, and hybrid optimization algorithms, enhance detection accuracy but often struggle with adaptability to dynamic and large-scale IoT networks. Despite these advancements, the studies emphasize the need for lightweight, scalable, and generalized IDS to address IoT's evolving security landscape effectively.

Survey of deep Learning Techniques for Diverse Attack Detection in IoT

The IoT has transformed many businesses, the growing complexity of cyberattacks poses security risks. Complex assaults may be difficult to detect with conventional security measures like firewalls and signature-based IDS. CNNs, RNNs, LSTM networks, autoencoders, and reinforcement learning are examples of DL approaches that have shown potential in identifying threats in IoT settings. But there are also issues including unbalanced datasets, high processing costs, a lack of labelled data, and real-time assault detection. DL technology should be the main focus of future research to improve IoT security.

Abu Al-Haija et al. [49] noted that the IoT's high-speed communication capabilities had made it a standard for low-power lossy networks. However, due to limitations in processing, storage, and communication power, IoT infrastructures were found to be susceptible to cyberattacks. The study introduced IoT-IDCS, a novel intelligent and self-governing DL-based cyberattack detection and classification system for IoT communication networks. The system utilized Intel CPUs, Nvidia GPUs, and high-performance computing. It comprised three subsystems: traffic classification, learning, and feature engineering. However, the system struggled to generalize to unseen attack types or real-world scenarios, particularly as the attack landscape evolved.

Brindha Devi et al. [50] observed that DDOS assaults were highly likely due to the large number of IoT devices and inadequate security, which could impact the accessibility of a particular node or the entire network. The paper presented a DL-focused method for identifying and thwarting such assaults. It introduced an improved Recursive Feature Elimination (RFE), higher-order statistical features, enhanced second-order technical indicator-based features, and data normalization as part of a novel four-stage attack detection method for the IoT. Classifiers such as Recurrent Neural Networks (RNNs), bidirectional gated recurrent units (BI-GRUs), and bidirectional long short-term memory (BI-LSTM) were used, with their outputs averaged to assess the presence of assaults. Upon detecting an event, the proposed BAIT targeted mitigation was implemented to remove offending nodes from the networks. However, the system could struggle with poor generalization when encountering new, unseen attack patterns or varying network conditions.

Manimurugan et al. [51] highlighted that while the IoT had become an essential tool for building smart environments, security and privacy concerns remained significant problems. To address these issues, a Deep Belief Network (DBN) algorithm model based on DL was suggested as an IDS. The outcomes were compared with those of different classifiers. However, the approach often dealt with large volumes of data, and training DL models on massive datasets proved to be computationally expensive and time-consuming, especially in environments with limited resources.

Dutta et al. [52] introduced an ensemble approach to network anomaly detection that utilized meta-classifiers and deep models such as DNN and LSTM, based on the stacking generalization principle. The technique pre-processed the data in two steps, using a stacking ensemble learning approach for classification and a Deep Sparse AutoEncoder (DSAE) for feature engineering. The findings of the evaluation were examined, statistical significance was assessed, and the results were compared with the most advanced methods for detecting network anomalies. The research emphasized the significance of DL methods for identifying and categorizing network abnormalities at both the host and network levels. However, imbalanced training datasets for anomaly detection could bias the model toward normal traffic classification, potentially leading to poor detection of rare or novel attacks.

Saba et al. [53] noted that while the IoT had completely transformed the way we use gadgets and apps, security risks remained a major problem. ML and DL emerged as modern techniques for securing IoT devices, capable of identifying patterns when conventional approaches were ineffective. The study introduced a CNN-based method for anomaly-based IDS that effectively analyzed traffic across the IoT by harnessing its potential. However, its ability to detect emerging attacks remained uncertain due to the need for retraining in dynamic IoT environments.

Abbas et al. [54] highlighted that the network architecture of IoT, a vital tool for tackling social problems, was becoming increasingly susceptible to cyberattacks. Businesses were at serious risk from these attacks, which could disrupt internet operations and limit access to data. ML and DL were being explored for their potential in preventing cyberattacks, as they could be used to identify patterns from annotated datasets. DL techniques could help in detecting cyberattacks by extracting patterns and identifying intrusions early through network data detection and segregation. DL models such as RNNs, CNN), and DNNs were employed to identify attacks on network traffic streams. The suggested strategy was tested utilizing the CICDIoT2023 dataset. However, its high computational resource requirements made it potentially infeasible for deployment in resource-constrained IoT devices.

Popoola et al. [55] recognized that while DL is a useful technique for identifying botnet assaults, its high memory requirements and the large volume of network traffic data make it unsuitable for IoT devices with limited memory. The research proposed a hybrid DL approach that utilized the LSTM Autoencoder (LAE) to reduce the feature dimensionality of large-scale IoT network traffic data. To accurately categorize network traffic samples, the technique was further examined using deep Bi-LSTM. Tests conducted on the BoT-IoT dataset confirmed that the hybrid DL approach was effective. The results presented that LAE outperformed the most advanced feature dimensionality reduction techniques, significantly reducing memory space for storing large amounts of network traffic data. However, the approach could struggle to scale to large, diverse IoT networks due to the overwhelming amount of data and the potential for performance degradation.

Susilo et al. [56] noted that as more and more gadgets were connected to the internet. However, despite the growing ubiquity of IoT devices, security concerns with the technology were aggregate. The study suggested that ML could be employed to enhance IoT security. It covered standard datasets and machine-learning and deep-learning techniques aimed at improving IoT security performance. By improving accuracy, the deep-learning model had the potential to enhance the effectiveness of IoT network mitigation. However, it faced the risk of overfitting to training data, which could result in high performance on training data but poor performance on unseen or real-world data, thereby reducing its effectiveness in practical applications.

Ahmad et al. [57] highlighted that the creation of zero-day hacks had made the IoT a significant security concern. For IoT networks, a NIDS could offer an effective security solution; however, newer versions often exhibited a high false alarm rate (FAR) when identifying abnormalities. The study suggested an effective anomaly detection method for IoT networks that utilized mutual information (MI) and DNN. The DNN-based NIDS model showed a reduction in FAR by 0.23-7.98% and an improvement in accuracy by 0.57-2.6% compared to other DL models. When only the top 16-35 numerical features were used with MI, the model's complexity decreased, but its performance also suffered. Overall, the accuracy of the deep learning-based models increased by 0.99 to 3.45%. However, the selected features failed to capture critical aspects of the data, which could adversely affect detection accuracy.

Maseer et al. [58] noted that the proliferation of internet services, including cloud computing and IoT devices, had made cyberattack security more challenging due to the massive dimensionality of network traffic data. Existing DL algorithms struggled to distinguish between abnormal and normal behavior in line connections because of excessive dynamics and imbalanced data. The paper proposed using the hybrid weighted deep belief network (HW-DBN) approach to build an efficient and reliable IDS model, called DeepIoT.IDS, capable of detecting both recent and emerging cyberattacks. However, the approach could struggle to scale efficiently due to the increasing data dimensionality and dynamic network traffic, potentially leading to delayed detection or degraded performance.

Chakraborty et al. [59] identified a significant challenge for cyber specialists and academics in detecting new assaults. Attackers were using complex strategies like polymorphism to alter attack patterns, making it difficult to identify them. Current signature-based detection techniques were inefficient, with a year-long undetected rate. To address this issue, the study proposed a rule-based deep neural network method. The suggested approach significantly improved results on the CICIDS 2017 dataset and other benchmark datasets. With an accuracy of over 99% for novel assaults, the model effectively balanced attack detection, false positive rates, and false negative rates. The approach also managed privacy and security concerns during automated communication between network devices (IoT), recognizing and categorizing various hazard levels. However, the system might face challenges in scaling efficiently to accommodate the vast and diverse nature of IoT devices and network traffic.

Ahmim et al. [60] discussed how the proliferation of connected devices due to the IoT had made individuals more vulnerable to cyberattacks, particularly DDoS attacks. Conventional ML techniques often failed to detect DDoS assaults. To address this, the study suggested IDS based on deep learning, which could be implemented at the cloud or fog level in an IoT environment. The model combined various DL techniques, including CNNs, LSTMs, Deep Autoencoders, and DNNs. It consisted of two primary layers. The model outperformed other ML and DL models in terms of accuracy, false alarm rate, average accuracy, average detection rate, and true positive rate. However, it may struggle with efficient scaling due to the growing and diverse nature of IoT devices and network traffic.

Sivasakthi et al. [61] emphasized the security risks posed by the IoT, particularly in identifying hybrid assaults. To improve detection accuracy and resistance to evolving hybrid attack patterns, the study proposed HybridRobustNet (HRN), a robust learning system that combines deep neural networks, ML algorithms, and ensemble approaches. HRN incorporated real-time adaptive learning algorithms to reduce false positives and identify complex interactions between attack components. Experiments conducted on an IoT testbed demonstrated that HRN outperformed state-of-the-art methods in terms of attack detection accuracy, resilience to evasion tactics, and low false positive rates. However, integrating HRN into IoT infrastructures could be challenging due to the heterogeneity of devices and communication protocols, requiring careful planning and implementation.

Madhu et al. [62] explored the growing interest in the IoT due to its intelligent decision-making, communication mechanisms, and connectivity. To enhance comfort and convenience, IoT incorporated artificial intelligence techniques. The study introduced the Device-based Intrusion Detection System (DIDS), a DL model designed to manage computational overhead in large networks while improving throughput as well as maintaining low false alarm rates. Compared to conventional methods, the DIDS model detected attacks earlier, required less computational time, and was effective in identifying threats. However, it faced challenges in inspecting encrypted network traffic, as it could not analyze the contents of encrypted packets without decryption.

Awajan et al. [63] highlighted the explosive expansion of the IoT, which has made it a prime target for hackers. The increasing frequency of cyberattacks on IoT devices and communication media can lead to significant service disruptions, financial losses, and risks to identity protection. To address these concerns, the study suggested an innovative IDS based on DL to ensure the reliability, security, and profitability of IoT-enabled systems. The system used a four-layer deep fully connected network architecture to identify malicious traffic that could trigger attacks on connected IoT devices. It effectively detected Blackhole, DDoS, Opportunistic Service, Sinkhole, and Workhole attacks, with an average accuracy of 93.74%. However, the system might have developed a bias towards the majority class, which could result in lower detection rates for less common attacks.

Shurman et al. [64] proposed two methods for identifying Distributed Reflection Denial of Service (DrDoS) attacks in the IoT. The first method uses a hybrid IDS to detect IoT-DoS attacks, while the second employs DL models based on LSTM networks to identify DrDoS attacks. Experimental results showed that these techniques could effectively detect malicious activity, helping to protect IoT networks from DoS and DDoS attacks. However, the approach may be vulnerable to adversarial attacks due to subtle data perturbations, which could allow attackers to evade detection and undermine the reliability of the IDS.

Morshedi et al. [65] presented an advanced method for detecting intrusions in IoT networks using raw data and DL algorithms. The model, trained and tested on various attack scenarios like DDoS attacks, port scanning, and botnet activities, utilized the CICIDS2017 dataset. It employed an LSTM architecture with thick transition layers to capture both temporal and spatial relationships within the data. Its performance was validated by comparing it with other ML models. However, the growing expansion of IoT networks leads to an increase in data volume, creating challenges for scaling IDS to process large-scale data while ensuring real-time detection capabilities.

Nazir et al. [66] proposed a robust IoT threat detection system to address the growing cybersecurity risks in the expanding IoT ecosystem. The researchers developed a Hybrid CNN-LSTM architecture to enhance IoT security. The model attained impressive accuracy rates of 95% on the IoT-23 dataset and 99% on both the N-BaIoT and CICIDS2017 datasets. Additionally, Principal Component Analysis (PCA) was utilized for data processing optimization. However, the model may be prone to overfitting, especially when trained on datasets that do not fully capture the diversity of real-world IoT network traffic, which could hinder its generalization to unseen attack patterns.

Abbas et al. [67] suggested an ID method for IoT networks that utilizes DL models, includes RNNs, CNNs, and DNNs, to address the limitations of traditional security solutions against evolving attack strategies. The study tested three iterations of each model, with RNN1 achieving the best performance, yielding 98.61% accuracy, 98.55% precision, 98.61% recall, and 98.57% F1-score. This approach enhances ID and encourages further research to improve the robustness of IoT security systems. However, the study acknowledges that the increased sensitivity of the model may lead to unnecessary alerts, which could overwhelm security personnel and reduce detection accuracy.

Yaras et al. [68] addressed the challenge of detecting cyberattacks, particularly DDoS attacks, in IoT networks with numerous sensor nodes. Traditional methods for analyzing network traffic are ineffective due to the large-scale nature of IoT networks. The study suggests a hybrid DL system combining one-dimensional CNN and LSTM to analyze network traffic data in a big data environment. However, the feature reduction method could inadvertently eliminate non-linearly related features, potentially impacting the model's performance. The following table 2 represents the diverse attack detection in IoT using DL.

Table 2: Overview of diverse attack detection in IoT using DL

Ref.No	Method	Dataset	Objective	Advantages	Limitation/Future scope
[49]	IoT-IDCS (Intelligent DL-	IoT communication networks	To detect and classify cyberattacks in IoT	High-speed communication capabilities for	Struggles to generalize to unseen

	based Cyberattack Detection)		networks using deep learning.	low-power lossy networks.	attacks and real-world scenarios.
[50]	Recursive Feature Elimination (RFE), RNN, BI-GRU, BI-LSTM	IoT-23, BoT-IoT, and other IoT datasets	Detect and mitigate DDoS attacks in IoT networks using a multi-stage detection and mitigation method.	Improved attack detection through feature engineering and classification.	Poor generalization to new attack patterns and varying network conditions.
[51]	Deep Belief Network (DBN)	CICIDS 2017 dataset	Develop an IDS for IoT networks using a DBN model for attack detection.	Superior results in accuracy, recall, precision, F1-score, and detection rate.	Computationally expensive and time-consuming for large datasets, especially in resource-constrained environments.
[52]	Ensemble Approach (Meta-classifiers, DNN, LSTM)	IoT-23, LITNET-2020, NetML-2020	Detect network anomalies and classify attack types using ensemble learning and feature engineering.	Utilizes DL models for effective network anomaly detection.	Imbalanced datasets may lead to poor detection of rare or novel attacks.
[53]	CNN-based IDS	NID, BoT-IoT datasets	Detect anomalies in IoT networks using CNN for ID.	Achieved high accuracy (99.51% on NID dataset) in anomaly detection.	Detection of emerging attacks is uncertain; requires retraining in dynamic environments.
[54]	DNN, RNN, CNN for NIDS	CICDIoT2023 dataset	Detect cyberattacks on IoT networks through a DL-IDS (NIDS).	DL models can detect attacks early by extracting patterns from network traffic data.	High computational resource requirements; not suitable for deployment in resource-constrained IoT devices.
[55]	Hybrid DL (LSTM Autoencoder, BLSTM)	BoT-IoT dataset	Reduce feature dimensionality in IoT networks and detect attacks using hybrid DL models.	Effective for large-scale IoT traffic and memory-efficient.	Struggles to scale to large, diverse IoT networks; potential performance degradation.
[56]	DL for DoS detection	Standard datasets for DoS attacks	Enhance DoS attack detection in IoT using ML and DL approaches.	High accuracy in DoS attack detection; potential for improving IoT security.	Risk of overfitting to training data; may lead to poor generalization on unseen data.
[57]	Mutual Information and DNN	IoT datasets	Reduce false alarm rates and improve accuracy for	Reduced FAR by 0.23-7.98%; improved	Selected features may miss critical data aspects, affecting detection accuracy.

			anomaly detection in IoT networks.	accuracy by 0.57-2.6%.	
[58]	Hybrid Weighted Deep Belief Network (HW-DBN)	IoT network traffic data	Build an efficient IDS for detecting recent and emerging cyberattacks in IoT networks.	Efficient and reliable detection of cyberattacks using DL models.	Struggles to scale efficiently with increasing data dimensionality and dynamic traffic.
[59]	Rule-based Deep Neural Network	CICIDS 2017, benchmark datasets	Detect polymorphic and new attacks in IoT networks using a rule-based DNN.	Significant improvement in accuracy for novel attacks (over 99%).	Potential scaling issues for diverse IoT traffic; biased towards common attack types.
[60]	DL (CNN, LSTM, Autoencoders, DNN)	IoT datasets	Detect and mitigate DDoS attacks in IoT networks.	Outperforms other DL models in accuracy, detection rate, and true positive rate.	May struggle to scale due to increasing and diverse IoT network traffic.
[61]	HybridRobustNet (HRN)	IoT testbed datasets	Improve detection accuracy for hybrid attacks in IoT networks using DL and ensemble methods.	Improved resilience to evolving attack patterns and reduced false positive rates.	Integration into IoT infrastructures may be challenging due to device and protocol heterogeneity.
[62]	Device-based IDS (DIDS)	Large-scale IoT networks	Manage computational overhead in large IoT networks while improving throughput and attack detection.	Efficient and effective at detecting attacks with lower computational time.	Struggles with encrypted network traffic; unable to analyze encrypted packet contents without decryption.
[63]	DL-based IDS for IoT	IoT networks	Ensure IoT security through a four-layer DL architecture for attack detection.	Successful detection of multiple attack types (Blackhole, DDoS, Sinkhole, etc.).	Potential bias toward majority class, leading to reduced detection rates for less frequent attacks.
[64]	Hybrid IDS, LSTM Networks for DrDoS detection	IoT networks	Detect DrDoS attacks in IoT using hybrid IDS and LSTM networks.	Effective detection of DoS and DDoS attacks.	Vulnerable to adversarial attacks that could lead to evasion.
[65]	DL for Intrusion Detection	Raw IoT data	Detect intrusions in IoT networks using raw data and DL algorithms.	Advanced detection capabilities with DL algorithms.	Struggles with data dimensionality and network traffic dynamics; delayed detection potential.

[66]	Deep Recurrent Neural Network (DRNN)	Bot-IoT, UNSW-NB15 datasets	Detect and classify cyberattacks in IoT networks using DRNN for sequential data analysis.	able to identify patterns and temporal relationships in network traffic.	Struggles with highly imbalanced datasets and may not generalize well for evolving attack strategies.
[67]	Transformer-based IDS	IoT-23, BoT-IoT, and real IoT network traffic	Detect IoT network anomalies using a Transformer-based model to capture complex attack patterns.	Efficient at handling sequential data with long-term dependencies. High accuracy for complex attack types.	High computational overhead and slower performance in real-time detection scenarios.
[68]	Hybrid Neural Network (HNN) with LSTM	CSE-CICIDS 2018, UNSW-NB15, and Bot-IoT datasets	Improve IoT security by detecting anomalies and attacks using a hybrid model combining HNN and LSTM.	Improved capacity to categorize uncommon attack patterns, lower false positive rates, and high detection accuracy.	May require extensive training data and time, and might underperform with previously unseen attacks or rapidly changing network traffic.

Summary:

The studies explore various DL methodologies for enhancing the detection and classification of cyberattacks in IoT networks. One approach introduces a DRNN to detect cyberattacks by leveraging sequential data from IoT datasets. This method captures temporal dependencies in network traffic, enabling effective recognition of attack patterns over time. However, it struggles with imbalanced datasets and may not generalize well to evolving attack strategies. Another study proposes a Transformer-based IDS, focusing on capturing complex attack patterns from IoT datasets. The model offers high accuracy for complex attack types but suffers from high computational overhead, which can hinder real-time detection performance. A third approach presents a HNN combined with LSTM for anomaly detection in IoT networks. This method performs well across multiple datasets, achieving high accuracy and reducing false positives. However, its performance may be compromised by insufficient training data or the presence of previously unseen attacks. Overall, these studies highlight the effectiveness of advanced DL models in improving IoT security, but they also face challenges such as high computational costs, dependency on large datasets, and limited adaptability to novel attack scenarios.

DISCUSSION

The survey paper provides a complete investigation of existing ML and DL approaches for IDS in IoT, highlighting their objectives, advantages, and limitations. It covers a wide range of techniques, from traditional ML models like LR, KNN, SVM, Decision Trees, and Random Forest, to advanced approaches including DNN, LSTM, and ensemble models. Various datasets were used to evaluate these methods. The findings emphasize that models like KNN, ANN, Random Forest, and hybrid approaches demonstrate high accuracy, precision, and F1-scores in detecting cyberattacks like DDoS, botnets, and anomalies. However, limitations such as computational overhead, overfitting, scalability issues in large networks, and poor generalization to unseen attacks persist. The survey suggests future research directions, including addressing imbalanced datasets, enhancing scalability and adaptability, and incorporating lightweight IDS solutions for resource-constrained IoT environments. Overall, it underscores the need for robust, efficient, and generalizable IDS frameworks to secure the growing IoT ecosystem.

CONCLUSION

In conclusion, the prompt advancement of IoT technologies has expanded the attack surface, making IoT devices highly vulnerable to diverse cyber threats. This survey highlights the critical role of ML and DL in addressing these security challenges. Traditional ML techniques offer simplicity and effectiveness in detecting basic anomalies and classifying attacks, making them suitable for less complex IoT environments. However, as the complexity of IoT systems and attack vectors grows, DL approaches demonstrate superior capabilities, particularly in automatically extracting high-level features and identifying intricate attack patterns. By evaluating various ML and DL methods across a range of IoT attack scenarios, this survey highlights the strengths and limitations of these techniques, emphasizing the need for hybrid approaches that combine the efficiency of ML with the sophistication of DL. Furthermore, the insights gathered from supervised and unsupervised learning methods provide a clear direction for developing adaptive and scalable solutions tailored to real-world IoT environments. Finally, this survey emphasizes the importance of leveraging the complementary strengths of ML and DL to design robust, future-ready attack detection systems that can efficiently address the dynamic and evolving security challenges faced by IoT networks.

REFERENCES

[1] Zhang, J.; Pan, L.; Han, Q.-L.; Chen, C.; Wen, S.; Xiang, Y. Deep learning-based attack detection for cyber-physical system cybersecurity: A survey. IEEE/CAA J. Autom. Sin. 2021, 9, 377–391.

[2] Almiani, M.; AbuGhazleh, A.; Al-Rahayfeh, A.; Atiewi, S.; Razaque, A. Deep recurrent neural network for IoT intrusion detection system. Simul. Model. Pract. Theory 2020, 101, 102031.

[3] Thakkar, A.; Lohiya, R. A review on machine learning and deep learning perspectives of IDS for IoT: Recent updates, security issues, and challenges. Arch. Comput. Methods Eng. 2021, 28, 3211–3243.

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

[5] Alladi, T.; Chamola, V.; Sikdar, B.; Choo, K.-K.R. Consumer IoT: Security vulnerability case studies and solutions. IEEE Consum. Electron. Mag. 2020, 9, 17–25.

[6] Abu Al-Haija, Q.; Al-Dala'ien, M.A. ELBA-IoT: An Ensemble Learning Model for Botnet Attack Detection in IoT Networks. J. Sens. Actuator Netw. 2022, 11, 18.

[7] Khan, T.; Sarkar, R.; Mollah, A.F. Deep learning approaches to scene text detection: A comprehensive review. Artif. Intell. Rev.2021, 54, 3239–3298.

[8] Aversano, L.; Bernardi, M.L.; Cimitile, M.; Pecori, R. A systematic review on Deep Learning approaches for IoT security. Comput.Sci. Rev. 2021, 40, 100389.

[9] Uzoka, A., Cadet, E., & Ojukwu, P. U. (2024). The role of telecommunications in enabling Internet of Things (IoT) connectivity and applications. Comprehensive Research and Reviews in Science and Technology, 2(02), 055-073.

[10] Isong, B., Kgote, O., & Abu-Mahfouz, A. (2024). Insights into Modern Intrusion Detection Strategies for Internet of Things Ecosystems. Electronics, 13(12), 2370.

[11] Lingala Thirupathi, D. T. N. R. B., & Kaashipaka, V. Advancements in intrusion detection systems: exploring concepts, innovations, metrics, benchmarks, trends, directions, applications and challenges.

[12] Omolara, A. E., Alabdulatif, A., Abiodun, O. I., Alawida, M., Alabdulatif, A., & Arshad, H. (2022). The internet of things security: A survey encompassing unexplored areas and new insights. Computers & Security, 112, 102494.

[13] A. Simmons, Internet of Things (IoT) architecture: Layers explained, November 2022, [06-04-2023]. https://dgtlinfra.com/internet-of-things-iot-architecture

[14] M. Abomhara, G.M. Køien, Cyber security and the Internet of Things: Vulnerabilities, threats, intruders and attacks, Journal of Cyber Security and Mobility 4 (1) (2015) 65–88.

[15] J. Sengupta, S. Ruj, S. Das Bit, A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT, Journal of Network and Computer Applications 149 (C) (2020) 102481.

[16] S. Shock, the 5 layers of IoT architecture that give it super powers, January 2023, [06-04-2023]. https://novotech.com/learn/m2m-blog/blog/2023/01/03/ the-5-layers-of-iot-architecture-that-give-it-super-power/.

[17] R. Agar, IoT architecture guide: Major and additional layers of IoT system, November 2022, [06-04-2023]. https://www.helpwire.app/blog/iot-architecture/

[18] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys & Tutorials, vol. 17, no. 4, pp. 2347-2376, 2015.

[19] P. Sethi and S. R. Sarangi, "Internet of things: architectures, protocols, and applications," Journal of Electrical and Computer Engineering, vol. 2017, 2017.

[20] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for internet of things: a survey," IEEE Internet of Things Journal, vol. 3, no. 1, pp. 70-95, 2016.

[21] E. Ahmed et al., "The role of big data analytics in Internet of Things," Computer Networks, vol. 129, pp. 459-471, 2017.

[22] "Internet of Medical Things, Forecast to 2021 [Online]: https://store.frost.com/internet-of-medical-things-forecastto-2021.html," 06-Jun-2017.

[23] G. Dimitrakopoulos, "Intelligent transportation systems based on internet-connected vehicles: Fundamental research areas and challenges," in ITS Telecommunications (ITST), 2011 11th International Conference on, 2011, pp. 145-151: IEEE.

[24] T. Baranwal and P. K. Pateriya, "Development of IoT based smart security and monitoring devices for agriculture," in Cloud System and Big Data Engineering (Confluence), 2016 6th International Conference, 2016, pp. 597-602: IEEE.

[25] M. Marjani et al., "Big IoT data analytics: Architecture, opportunities, and open research challenges," IEEE Access, vol. 5, pp. 5247-5261, 2017.

[26] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1933-1954, 2014.

[27] N. Komninos, E. Philippou, and A. Pitsillides, "Survey in smart grid and smart home security: Issues, challenges and countermeasures," IEEE Communications Surveys & Tutorials, vol. 16, no. 4, pp. 1933-1954, 2014

[28] Zarpelão, B. B., Miani, R. S., Kawakani, C. T., & De Alvarenga, S. C. (2017). A survey of intrusion detection in Internet of Things. Journal of Network and Computer Applications, 84, 25-37.

[29] Churcher, A., Ullah, R., Ahmad, J., Ur Rehman, S., Masood, F., Gogate, M., ... & Buchanan, W. J. (2021). An experimental analysis of attack classification using machine learning in IoT networks. Sensors, 21(2), 446.

[30] Hasan, M., Islam, M. M., Zarif, M. I. I., & Hashem, M. M. A. (2019). Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. Internet of Things, 7, 100059.

[31] Rashid, M. M., Kamruzzaman, J., Hassan, M. M., Imam, T., & Gordon, S. (2020). Cyberattacks detection in iot-based smart city applications using machine learning techniques. International Journal of environmental research and public health, 17(24), 9347.

[32] Sarker, I. H. (2021). CyberLearning: Effectiveness analysis of machine learning security modeling to detect cyber-anomalies and multi-attacks. Internet of Things, 14, 100393.

[33] Alissa, K., Alyas, T., Zafar, K., Abbas, Q., Tabassum, N., & Sakib, S. (2022). Botnet attack detection in iot using machine learning. Computational Intelligence and Neuroscience, 2022(1), 4515642.

[34] Gaber, T., El-Ghamry, A., & Hassanien, A. E. (2022). Injection attack detection using machine learning for smart IoT applications. Physical Communication, 52, 101685.

[35] Karthikeyan, M., Manimegalai, D., & RajaGopal, K. (2024). Firefly algorithm based WSN-IoT security enhancement with machine learning for intrusion detection. Scientific Reports, 14(1), 231.

[36] Al-Sarem, M., Saeed, F., Alkhammash, E. H., & Alghamdi, N. S. (2021). An aggregated mutual information based feature selection with machine learning methods for enhancing IoT botnet attack detection. Sensors, 22(1), 185.

[37] Bhayo, J., Shah, S. A., Hameed, S., Ahmed, A., Nasir, J., & Draheim, D. (2023). Towards a machine learning-based framework for DDOS attack detection in software-defined IoT (SD-IoT) networks. Engineering Applications of Artificial Intelligence, 123, 106432.

[38] Panda, M., Abd Allah, A. M., & Hassanien, A. E. (2021). Developing an efficient feature engineering and machine learning model for detecting IoT-botnet cyber attacks. IEEE Access, 9, 91038-91052.

[39] Tyagi, H., & Kumar, R. (2021). Attack and anomaly detection in IoT networks using supervised machine learning approaches. Revue d'Intelligence Artificielle, 35(1).

[40] Soe, Y. N., Feng, Y., Santosa, P. I., Hartanto, R., & Sakurai, K. (2020). Machine learning-based IoT-botnet attack detection with sequential architecture. Sensors, 20(16), 4372.

[41] Tuan, T. A., Long, H. V., Son, L. H., Kumar, R., Priyadarshini, I., & Son, N. T. K. (2020). Performance evaluation of Botnet DDoS attack detection using machine learning. Evolutionary Intelligence, 13(2), 283-294.

[42] Gad, A. R., Haggag, M., Nashat, A. A., & Barakat, T. M. (2022). A distributed intrusion detection system using machine learning for IoT based on ToN-IoT dataset. International Journal of Advanced Computer Science and Applications, 13(6).

[43] Saheed, Y. K., Abiodun, A. I., Misra, S., Holone, M. K., & Colomo-Palacios, R. (2022). A machine learning-based intrusion detection for detecting internet of things network attacks. Alexandria Engineering Journal, 61(12), 9395-9409.

[44] Sadhwani, S., Manibalan, B., Muthalagu, R., & Pawar, P. (2023). A lightweight model for DDoS attack detection using machine learning techniques. Applied Sciences, 13(17), 9937.

[45] Campos, A. D., Lemus-Prieto, F., González-Sánchez, J. L., & Lindo, A. C. (2024). Intrusion detection on IoT environments through side-channel and Machine Learning techniques. IEEE Access.

[46] Gaur, V., & Kumar, R. (2022). Analysis of machine learning classifiers for early detection of DDoS attacks on IoT devices. Arabian Journal for Science and Engineering, 47(2), 1353-1374.

[47] ANOH, N. G., KONE, T., ADEPO, J. C., M'MOH, J. F., & BABRI, M. (2024). IoT Intrusion Detection System based on Machine Learning Algorithms using the UNSW-NB15 dataset.

[48] Buiya, M. R., Laskar, A. N., Islam, M. R., Sawalmeh, S. K. S., Roy, M. S. R. C., Roy, R. E. R. S., & Sumsuzoha, M. (2024). Detecting IoT cyberattacks: advanced machine learning models for enhanced security in network traffic. Journal of Computer Science and Technology Studies, 6(4), 142-152.

[49] Abu Al-Haija, Q., & Zein-Sabatto, S. (2020). An efficient deep-learning-based detection and classification system for cyber-attacks in IoT communication networks. Electronics, 9(12), 2152.

[50] Brindha Devi, V., Ranjan, N. M., & Sharma, H. (2024). IoT attack detection and mitigation with optimized deep learning techniques. Cybernetics and Systems, 55(7), 1702-1728.

[51] Manimurugan, S., Al-Mutairi, S., Aborokbah, M. M., Chilamkurti, N., Ganesan, S., & Patan, R. (2020). Effective attack detection in internet of medical things smart environment using a deep belief neural network. IEEE Access, 8, 77396-77404.

[52] Dutta, V., Choraś, M., Pawlicki, M., & Kozik, R. (2020). A deep learning ensemble for network anomaly and cyber-attack detection. Sensors, 20(16), 4583.

[53] Saba, T., Rehman, A., Sadad, T., Kolivand, H., & Bahaj, S. A. (2022). Anomaly-based intrusion detection system for IoT networks through deep learning model. Computers and Electrical Engineering, 99, 107810.

[54] Abbas, S., Bouazzi, I., Ojo, S., Al Hejaili, A., Sampedro, G. A., Almadhor, A., & Gregus, M. (2024). Evaluating deep learning variants for cyber-attacks detection and multi-class classification in IoT networks. PeerJ Computer Science, 10, e1793.

[55] Popoola, S. I., Adebisi, B., Hammoudeh, M., Gui, G., & Gacanin, H. (2020). Hybrid deep learning for botnet attack detection in the internet-of-things networks. IEEE Internet of Things Journal, 8(6), 4944-4956.

[56] Susilo, B., & Sari, R. F. (2020). Intrusion detection in IoT networks using deep learning algorithm. Information, 11(5), 279.

[57] Ahmad, Z., Shahid Khan, A., Nisar, K., Haider, I., Hassan, R., Haque, M. R., ... & Rodrigues, J. J. (2021). Anomaly detection using deep neural network for IoT architecture. Applied Sciences, 11(15), 7050.

[58] Maseer, Z. K., Yusof, R., Mostafa, S. A., Bahaman, N., Musa, O., & Al-Rimy, B. A. S. (2021). DeepIoT. IDS: Hybrid deep learning for enhancing IoT network intrusion detection. Computers, Materials and Continua, 69(3), 3946-3967.

[59] Chakraborty, S., Pandey, S. K., Maity, S., & Dey, L. (2024). Detection and classification of novel attacks and anomaly in IoT network using rule based deep learning model. SN Computer Science, 5(8), 1056.

[60] Ahmim, A., Maazouzi, F., Ahmim, M., Namane, S., & Dhaou, I. B. (2023). Distributed denial of service attack detection for the Internet of Things using hybrid deep learning model. IEEE Access, 11, 119862-119875.

[61] Sivasakthi, D. A., Sathiyaraj, A., & Devendiran, R. (2024). HybridRobustNet: enhancing detection of hybrid attacks in IoT networks through advanced learning approach. Cluster Computing, 1-15.

[62] Madhu, B., Chari, M. V. G., Vankdothu, R., Silivery, A. K., & Aerranagula, V. (2023). Intrusion detection models for IOT networks via deep learning approaches. Measurement: Sensors, 25, 100641.

[63] Awajan, A. (2023). A novel deep learning-based intrusion detection system for IOT networks. Computers, 12(2), 34.

[64] Shurman, M., Khrais, R., & Yateem, A. (2020). DoS and DDoS attack detection using deep learning and IDS. Int. Arab J. Inf. Technol, 17(4A), 655-661.

[65] Morshedi, R., Matinkhah, S. M., & Sadeghi, M. T. (2024). Intrusion Detection for IoT Network Security with Deep learning. Journal of AI and Data Mining, 12(1), 37-55.

[66] Nazir, A., He, J., Zhu, N., Qureshi, S. S., Qureshi, S. U., Ullah, F., ... & Pathan, M. S. (2024). A deep learning-based novel hybrid CNN-LSTM architecture for efficient detection of threats in the IoT ecosystem. Ain Shams Engineering Journal, 15(7), 102777.

[67] Abbas, S., Alsubai, S., Ojo, S., Sampedro, G. A., Almadhor, A., Hejaili, A. A., & Bouazzi, I. (2024). An efficient deep recurrent neural network for detection of cyberattacks in realistic IoT environment. The Journal of Supercomputing, 1-19.

[68] Yaras, S., & Dener, M. (2024). IoT-Based Intrusion Detection System Using New Hybrid Deep Learning Algorithm. Electronics, 13(6), 1053.