Vol.4, No.1, Page 1596- 1621, 2026 https://doi.org/10.59628/jast.v4i1.2234 ISSN 2958-9568 JAST

SUN PUBLISHER

مجلة جامعة صنعاء للعلوم التطبيقية والتكنولوجيا

Sana'a University Journal of Applied Sciences and Technology

https://journals.su.edu.ye/index.php/jast/

Survey On Intelligent Anomaly Detection Techniques In IOT Security

Haifa Hamoud Al-Hamadi *, Ibrahim Ahmed Al-Baltah and Nagi Ali Al-shaibany

Department of Information Technology, Faculty of Computer Sciences and IT, Sana'a University, Sana'a, Yemen

*Corresponding author: hifa.alhmadi@su.edu.ye

Abstract

The rapid development of various advanced technologies, including the Internet of Things (IoT), coupled with users' heavy reliance on technology in various aspects of their daily lives, has led to an increase in the number of devices connected to the Internet. As a result of this rapid growth, the amount of data generated will increase significantly, as the Internet of Things covers many areas, from industrial and healthcare sectors to smart cities and smart homes. However, many challenges, attacks, vulnerabilities, and various anomalies related to the security of IoT devices arise, negatively impacting individuals and organizations. Several anomaly detection techniques have emerged, including machine learning and deep learning, which in turn detect anomalies. This enhances the security, integrity, reliability, and effectiveness of IoT systems. This paper provides a comprehensive survey of peer-reviewed articles from 2018 up to the present that focus on machine learning and deep learning in anomaly detection and attacks on various layers of the Internet of Things architecture. The survey results provide potential insights and recommendations for future research endeavors.

Article Info

Keywords:
Anomaly detection, Internet of Things (IOT), Machine learning (ML), Deep learning (DL), IOT Security, IOT layer attacks.

Article History:
Received: 9-September-2025,
Revised: 31-October-2025,
Accepted: 7-November-2025,
Published: 29 January 2026.

1. INTRODUCTION

With increasing development in the field of communications and information technology, significant progress has been made in improving the accuracy and efficiency of business and increasing productivity [1]. Currently, Internet connectivity is crucial in numerous fields, with more than 5.45 billion users globally. [2]. In recent years, there has been a significant transformation in the advancement of various technologies, including the Internet of Things (IoT) and smart-device communications[3]. An extensive and heterogeneous network of devices connected by sensors and actuators via wired and wireless networks constitutes the Internet of Things, allowing different objects and smart devices to communicate with each other over the Internet [3].

IoT networks consist of a group of devices interconnected by various communication protocols, hardware, and operating systems [4]. IoT technologies are important for developing applications in various fields, such as education, agriculture, transportation, healthcare, and home automation [5]. The total number of connected devices worldwide is approximately 17 billion, with 7 billion being Internet of Things devices, excluding laptops, smartphones, and tablets. The number of devices is expected to reach 75.44 billion by the end of 2025 [5]. The number of studies from 2000 to 2019 in IoT was approximately 9589 [6].

In the healthcare sector, IoT applications are expected to contribute an annual growth rate of between $1.1 trillion and $2.5 trillion in 2025, with a global impact estimated between $2.7 trillion and $6.2 trillion [7]. IoT devices are designed to configure themselves independently, allowing them to connect to networks without a manual configuration. This is accomplished using various protocols and technologies. These devices can easily connect to networks, discover services, and adjust their configurations without extensive manual intervention [8]. As IoT becomes more integrated into everyday

©2026 The Author(s). This article is licensed under CC By 4.0

life, the adoption of IoT-based devices is on the rise [7]. Owing to the IoT architecture, problems of latency, device heterogeneity, compatibility, power consumption, power availability, communication, bandwidth, security, privacy, scalability, energy efficiency, and lack of standard protocols, which in turn creates a gap in IoT [6].

Owing to this scale and heterogeneity, it is difficult to implement security measures on devices, which leads to security vulnerabilities [4]. This attracts malicious actors seeking to exploit the technology [7].The increasing number of devices not only increases the opportunities and attack surface, but also exposes many security vulnerabilities that attackers exploit to gain access to IoT devices and compromise data. Therefore, monitoring system behavior is essential for early detection and prevention of threats and vulnerabilities [9].

Internet-connected devices require resource-intensive security measures such as encryption systems owing to their low power consumption [4]. Maintaining the security of such systems is critical [5]. Symantec reported nearly three billion cyberattacks in 2019, an increase of 300% from the previous year [7]. Attackers can exploit vulnerabilities to breach privacy, alter and destroy data, and gain unauthorized access [5]. The annual cost of cyberattacks is estimated at $10.5 trillion, and this number is expected to increase in the coming years [2].

The rapid growth of the Internet of Things (IoT) has led to the emergence of new security challenges [10]. These challenges raise concerns that must be resolved and addressed to enhance and improve the security of IoT environments [5]. Collaboration with various policymakers, researchers, and stakeholders is essential to develop best practices, policies, regulations, and standards to enhance the security and reliability of IoT [5]. Cybersecurity is an integral part of information management in the IoT environment [10]. The widespread proliferation of IoT devices in homes, smart power grids, and smart cars, along with the significant complexity of communication protocols, poses a variety of threats [10], especially those related to security and privacy, such as device hacking and unauthorized access to data [11].

The Internet of Things aims to connect the physical and digital worlds. The Internet of Things (IoT) has enhanced the quality of users' lives, providing them with convenience, simplicity, and luxury [5].

Research contrition and Scope:

The contribution of this study is that it presents research based on machine learning and deep learning in the field of anomaly detection and attacks in IoT networks. This study aimed to analyze several recent studies. Sixty-nine research papers were selected to review the literature related to machine learning and deep learning for anomaly detection in IoT in different domains and attacks that may affect different layers of the IoT architecture. These papers were collected from various publications, including IEEE, Elsevier, Springer, MDPI, and others, to ensure the inclusion of the latest information. This paper also addresses the challenges and future research paths for applying machine learning and deep learning techniques to anomaly detection in the IoT and various attacks.

This study relied on a methodology of reviewing recent research surveys, where compiling research papers from several peer-reviewed publications, including IEEE, MDPI, Springer, Elsevier, and others, which were published between 2018 and up to present. It focuses on analyzing recent studies on anomaly detection using machine learning and deep learning algorithms and attacks on different layers of the IoT architecture. To maintain the integrity of the research, research papers based on both machine learning and deep learning related to anomaly detection in the IoT and attacks on the layers of the IoT architecture were collected.

Each study was analyzed according to its field, experimental methods, datasets used, advantages and challenges of the proposed frameworks, and the results obtained. This study examined sixty-nine research papers to review the literature related to both machine learning and deep learning techniques and to compare the results of different algorithms and attacks. There is still room for future research in this field. The remainder of this paper is organized as follows. Section 1 provides an introduction to the field. Section 2 presents and reviews related literature. Section 3 provides an overview of the IoT, its architecture and layers. Section 4 explains the security concerns associated with each layer, presents some of its different aspects and discusses its security and vulnerability. Section 5 describes the methodology used in this study. Section 6 presents different IoT Domains. Section 7 discusses the anomaly detection and the algorithms used. Section 8 focuses on the open challenges of IoT security attacks and potential areas. Finally, Section 9 concludes the study conclusion and future research with references.

2. RELATED WORK

Unmanned aerial vehicles (UAVs) are becoming increasingly widespread and are used in various fields, including agriculture, military, and commercial. They have become crucial for individuals and organizations by facilitating and improving the performance of various tasks with greater ease and security. In this study [12], we conducted a comprehensive review of UAV intrusion detection methods, classifying studies according to their objectives, datasets, extracted features, and algorithms, with a focus on machine learning and deep learning approaches. This study also highlights its main limitations. Detecting intrusions in UAVs has recently received significant attention from both academia and industry to address current threats and to develop detection frameworks. Furthermore, this

©2026 The Author(s). This article is licensed under CC By 4.0

study provides background information, presents state-of-the-art methods, proposes a taxonomy of detection techniques, identifies key problems, and anticipates future trends. However, it does not discuss the broader integration of emerging technologies such as generative artificial intelligence and quantum computing to enhance UAV intrusion detection. It also recommends improvements, such as developing shared datasets, enhancing privacy, and improving performance [12]. Subsequent studies have begun to explore these trends, particularly in the broader context of IoT security, in which these techniques are leveraged to enhance model robustness and data protection.

This study [3] focuses on surveying advanced studies on intrusion detection and prevention systems (IDS/IPS) in the Internet of Things (IoT). It primarily examined machine learning and deep learning approaches used in IDS and IPS, offering analyses and comparisons based on feasibility, challenges, compatibility, and related issues. The study also included a questionnaire summarizing the advantages and disadvantages of various approaches, and discussed the foundations of intrusion detection systems across different categories, locations, functions, and architectures.

Mapping techniques were employed along with mitigation methods to analyze the risk factors, and several research issues and proposed solutions were identified. Furthermore, this study introduced a hybrid framework that integrates mapping-based risk analysis for effective security modeling in intrusion detection and prevention. In addition, it did not extensively discuss performance metrics beyond accuracy, such as detection time and resource consumption, or the potential integration of emerging technologies, such as blockchain and generative artificial intelligence [3]. Subsequent research has begun to explore these dimensions to enhance the operational efficiency and adaptability within IoT security systems.

In [5], the authors reviewed and compared recent research papers based on machine learning and deep learning to enhance Internet of Things (IoT) security. This study aimed to identify the major security challenges and threats affecting IoT applications and to examine the vulnerabilities inherent in IoT systems. It emphasizes the important role of machine learning and deep learning in addressing these risks, including cyberattacks and data breaches. However, this study did not include a comparative evaluation of traditional or hybrid security approaches. It also highlights several research challenges and potential future directions for using machine learning and deep learning methods in IoT security [5]. Subsequent studies have expanded on this work by analyzing the integration of traditional, hybrid, machine learning, and deep learning-based techniques to better understand their advantages and practical applicability.

In [7], researchers provided a detailed review of deep-learning-based intrusion detection systems (IDSs) for identifying botnets in the Internet of Things (IoT). This study examined several architectures, including convolutional neural networks (CNNs), recurrent neural networks (RNNs), and generative adversarial networks (GANs), highlighting their ability to improve the detection accuracy, identify abnormal behavior patterns, and extract high-level features. Some studies reviewed in this study used datasets such as CICIDS2017 and CSE-CIC-IDS2018 to evaluate models such as BoostedEnsML, which combines different network traffic sources and simulates diverse attack scenarios to assess IDS performance. The review also emphasized efforts to improve comparability and robustness in IDS research and encourage collaboration within the community.

While the study mainly focused on traditional botnet attacks, it paid limited attention to emerging threats, such as AI-driven or adversarial attacks that directly target ML/DL-based systems [7]. Later studies started to examine these evolving attack types and their implications for developing more resilient IoT security frameworks.

A smart grid is a modern energy grid that integrates advanced communication technologies and the Internet of Things (IoT) to provide sustainable and reliable electricity. However, this integration also increases exposure to cyber threats, which can have severe operational and financial impacts. In [13], the authors reviewed machine-learning-based feature selection methods for detecting cyberattacks in smart grids, providing a comprehensive analysis of the system's most significant vulnerabilities. The study also discussed several approaches to intrusion detection, including signature-based, machine learning, anomaly detection, and rule-based methods. While providing valuable insights into these approaches, little attention has been paid to the legal and policy aspects necessary to enhance cybersecurity in smart grids, such as compliance standards and government regulations. This paper also highlights emerging research directions that incorporate artificial intelligence and blockchain technologies to enhance the resilience of smart grid infrastructures [13].

The authors presented [14] a review of AI techniques, including machine learning and deep learning approaches, in the context of the Industrial Internet of Things (IIoT). The study discussed key IIoT applications, such as real-time manufacturing, agriculture, and transportation, and proposed an IIoT architecture that integrates key components, such as smart sensors, industrial sites, decision-making processes, and control centers, to enhance operational efficiency. This review also covers a range of algorithms, including machine learning models such as k-nearest neighbors (kNN), Support Vector Machines (SVM), Naive Bayes (NB), Decision Trees (DT), Random Forests (RF), Artificial Neural Networks (ANN), and Federated Learning (FL), as well as deep learning models such as autoencoders (AE),

©2026 The Author(s). This article is licensed under CC By 4.0

Convolutional Neural Networks (CNN), Recurrent Neural Networks (RNN), Restricted Boltzmann Machines (RBM), Generative Adversarial Networks (GAN), Deep Reinforcement Learning (DRL), Transformers, and Large Language Models (LLM). Although the study mentioned some security challenges, it paid little attention to a detailed discussion of modern data protection techniques applied in IIoT environments, such as advanced encryption methods, access control mechanisms, or blockchain-based frameworks [14]. Subsequent research has begun to explore these aspects to enhance the reliability and security of IIoT infrastructure.

Using IoT devices and machine-learning algorithms in [15], the authors proposed a methodology for mapping anomaly detection in industrial machinery. This study also reviewed 84 research papers published between 2016 and 2023, providing an overview of anomaly detection research and summarizing recent trends in the field, ensuring that it remains up-to-date and consistent with the latest developments. Although this study primarily focused on detection techniques, it paid limited attention to data security issues in IoT systems and did not include a comparison of existing anomaly detection tools or platforms [15]. Subsequent work has begun to examine these aspects more closely, exploring the relative strengths and applicability of different anomaly detection solutions in IIoT environments.

The authors of [16] provided an overview of the Medical Internet of Things (MIoT) and covered the main privacy and security issues, such as the function of IoT devices and machine learning, as well as the monitoring layers of perception, network, application, and cloud. The study also examined a number of cyberattack risks to MIoT, such as those pertaining to Bluetooth, ZigBee, Wi-Fi 6, and the new 5G technology known as Narrowband Internet of Things (NB-IoT). Robust authentication methods are necessary to secure the MIoT environment, and machine-learning and deep-learning approaches are essential in this respect. The study did not provide actual case studies from hospitals or healthcare systems; instead, it relied on theoretical examples and simulation-based models such as COOJA. Real-world case studies from hospitals or healthcare systems. Additionally, the study covers cybersecurity issues in IoMT from the perspective of the European Union Agency for Cybersecurity (ENISA), referring to the 2030 cybersecurity threat landscape [16].

The authors of [17] examined cybersecurity concerns at the network, application, perception, and support layers of the Internet of Things (IoT). This study addressed the types of DDoS attacks, their impact, and mitigation techniques. To mitigate these effects, this study also compared different models for detecting and preventing intrusions, focusing on detection systems. The study presented a dataset-based classification of anomaly detection methods as well as machine learning and deep learning methods for malware detection and data processing. Although the study addressed security in general, it did not address specific issues such as protecting physical devices from theft or tampering or how to protect data privacy in sensitive applications such as smart health [17].

The authors of [18] examined several Internet of Things (IoT) security risks and vulnerabilities, providing a comprehensive analysis of the application of machine learning and deep learning methods in IoT security. This study categorized these methods into a data-driven list, comparing their advantages, disadvantages, and uses in relation to the Internet of Things (IoT). It also covers how blockchain technology can be combined with deep learning and machine learning to improve IoT security. This study highlighted various IoT security issues, including learning methods and security breaches in networked environments. It also recommends future research avenues for enhancing IoT security by using state-of-the-art technologies. Although the review provides a comprehensive theoretical analysis, it omits case studies and experimental results from actual IoT systems, which could have provided useful information on how machine learning and deep learning techniques can be applied to IoT security [18].

In [19], the authors reviewed the literature on anomaly detection using machine learning and deep learning techniques in the IoT infrastructure, focusing on anomaly and intrusion detection in IoT systems. This study presents a series of recent studies on the use of machine learning and deep learning techniques for anomaly detection. It also discusses the need to improve existing systems to make them more scalable and testable. It also addresses challenges, such as identifying intrusion sites and intrusions in IoT systems. A comprehensive review of the latest relevant work is provided, and all the studies are summarized in a single table. However, the study did not provide a detailed discussion of specific attack-targeting devices within the IoT architecture [19].

Unlike the aforementioned studies, this research offers a unique contribution to this field, comprehensively covering three dimensions of IoT research: machine learning, deep learning methods, and the challenges and attacks associated with each layer of the IoT architecture. Previous research papers have provided a comprehensive review of various machine learning and deep learning techniques for anomaly detection in different domains. Although each study discusses the potential of these methods, empirical evidence and case studies demonstrating the effectiveness of machine learning and deep learning in enhancing and improving the security of IoT devices and attacks that may affect each layer of the IoT architecture have not been extensively discussed in the literature. By integrating these aspects, this survey paves the way for the exploration of new research avenues. This study includes a review of the latest arti-

©2026 The Author(s). This article is licensed under CC By 4.0

cles in the field, covering publications up to the present. This study is based on an inference of the latest trends and developments in the IoT space. Therefore, this work provides an updated overview of the latest research, including recent peer-reviewed articles, leveraging machine learning and deep learning techniques for anomaly detection in diverse IoT domains, such as healthcare, industry, and transportation. It also provides an updated overview of various attacks on IoT layers that can negatively impact the security of the IoT environment. Table 1 summarizes and lists relevant studies on these techniques, identifying the algorithms used, datasets, results, features, and challenges.

3. INTERNET OF THINGS OVERVIEW

In the modern era, the Internet of Things (IoT) has developed rapidly, revolutionizing modern technology through the widespread interconnection of devices, networks, and services [20]. IoT is a network of connected physical devices, software, vehicles, home appliances [21], and motors that can exchange information over communication networks such as the Internet [20]. IoT devices connected by sensors are used to connect homes, schools, universities, hospitals, and people [22]. These objects are capable of networking to collect and exchange data efficiently for control and management [21]. IoT is also defined as an object that exchanges and shares information with other objects or platforms over the Internet [22]. IoT is considered a network infrastructure [7]. The number of connected devices has reached 17 billion, making IoT an essential component of an interconnected society [23]. IoT consists of a set of basic elements: identification, sensing, communications, services, and semantics. With the increasing applications of IoT, devices could become less energy intensive, lower cost, and smaller [22].

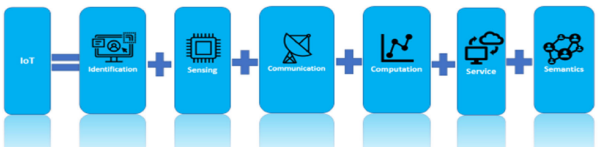


Figure 1. IOT component

IoT is also a network for exchanging data between various devices [15], and large amounts of data are transmitted over the network using the Internet as a basis for communication and minimal human intervention [3], which is primarily responsible for consumer requirements, as well as interactions between machines and users, and the relationship between the client and the server [15].

Through IoT systems, companies collect real-time data to improve operational efficiency, stimulate innovation, and increase decision-making capacity. The IoT, coupled with its computing capabilities, facilitates communication between physical objects and digital systems [24]. IoT is also designed to facilitate communication between real and digital sciences (also called digital transformation or cyber-physical systems) [22]. The use of IoT is increasing in most and various areas of life, as illustrated in Figure 2, such as homes, cars, hospitals, the agricultural sector, schools, and cities [22]. This leads to radical changes in everyday objects [25] and several industries, including manufacturing, transportation, agriculture, healthcare, and the military [24].

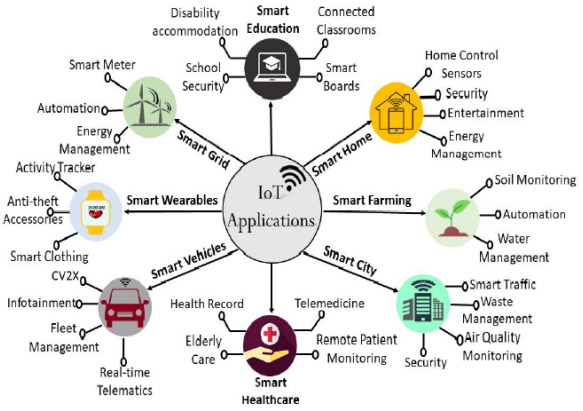


Figure 2. IOT Application

The IoT aims to improve human life, increase the availability of different applications and services [22], and provide efficiency and convenience through automation [20, 26]. Smart devices communicate with each other to perform various tasks [26]. However, they face numerous difficulties and security threats [20].

Radio-frequency identification (RFID) technology has been widely used since the 1980s in several industries such as supply chain management, retail, logistics, and pharmaceutical manufacturing. Wireless sensor networks (WSNs), which use networked smart sensors to collect data and monitor the surrounding environment, constitute another core IoT technology. The applications of these networks are numerous and include traffic monitoring, industrial control, healthcare monitoring, and environmental monitoring. Advances in RFID and WSN technology have significantly contributed to the development of IoT. Other technologies also support the IoT, including cloud computing, social media, smartphones, and barcodes [7].

The rapid growth of IoT devices has raised numerous security concerns such as unauthorized access, hacks, and vulnerabilities [27].

I. Architecture

The Internet of Things (IoT) environment consists of an ever-increasing number of smart devices and sensors connected and interconnected wirelessly and au-

©2026 The Author(s). This article is licensed under CC By 4.0

tonomously, anytime, anywhere [28] via a popular Internet Protocol called Internet Protocol (IP) [29]. This increase leads to increased data traffic and the processing and storage of large amounts of data [30]. Architecture is defined as the framework by which the physical components of the network, their organization, and operational procedures are defined, organized, and configured. Each layer of the IoT has associated security issues and vulnerabilities [28].

The IoT includes many heterogeneous and limited devices [4]. Consequently, it faces numerous challenges related to quality of service, privacy, and security [30].

Internet architecture consists of multiple layers that work together to perform tasks and achieve goals. There is no fixed standard for IoT architecture and researchers, authors, and practitioners have proposed various architectural models. Researchers developed five architectural models that share similar components. An IoT system consists of three layers: (1) the physical perception layer, (2) the network layer, and (3) the application layer. Reference [31] described this phenomenon. Other researchers have reported that an IoT technology stack consists of three basic layers: (1) the device layer, (2) the communication layer, and (3) the IoT cloud layer [32].

IoT consists of three layers: (1) device layer, (2) communication layer, and (3) application layer, as mentioned in [7]. The IoT architecture consists of three layers: edge perception, network, and application, as stated in [5]. In other research, researchers have analyzed an additional support layer located between the application layer and the network layer, which is included in the latest IoT architecture, consisting of fog computing and cloud computing [29]. While IoT has been classified into three-, four-, five-, or seven-layer architectures [1], in general, the basic component of IoT architecture consists of four layers. These four layers are the perception, network, middleware, and application layers, as stated in [19].

The network layer connects the IoT system to a perception layer. The perception layer consists of physical devices, such as actuators and sensors, that process data. The middleware layer in this layer processes, stores, and manages data collected from the perception layer. The application layer contains user applications that store the processed data. Some studies have shown that other layers are components of the IoT architecture, such as the management, environment, business, and security layers [19].

The International Telecommunication Union (ITU) considers IoT architecture to consist of five layers: application, sensing, networking, access, and middleware; it also adds an alternative architecture for the IoT, where the model consists of three layers: the application layer, the network layer, and the sensor layer. The architecture of IoT in another model consists of a network layer, perception layer, and application or service layer [7].

Each of the proposed IoT architectures fails to cover all the features of the IoT and presents several common drawbacks, summarized as follows.

a. **Distributedness:** IoT models are developed in a distributed environment, and data are collected from a variety of sources and can then be processed by distinct smart entities in a distributed process.
b. **Interoperability:** Systems and protocols must be designed to allow smart devices to exchange data in balanced ways to achieve common goals.
c. **Scalability:** Systems and applications operating in IoT environments must be able to process and manage massive amounts of data owing to the expansion and proliferation of devices in IoT environments.
d. **Resource Scarcity:** Computing units and power are extremely scarce resources.
e. **Security:** Devices can be taken over by an unknown external device, which can leave users feeling helpless and intimidated. [30]

To overcome these problems, similar functions, technologies, and services are consolidated at each layer, facilitating the development and improvement of each layer [30].

This study focuses on a specific model, the three-layer architecture (network, application, and perception), excluding other architecture models. Each layer of the IoT architecture is designed to perform a specific task or function. Each layer is exposed to various security issues and attacks, which are addressed in section 4

a. Application layer

The application architecture is a structure in which the data collected from IoT devices are processed [7]. In IoT architecture, the application layer is located at the top level and provides user interfaces [16]. This layer includes smart applications, such as smart homes, healthcare, and smart cars. This layer interacts with end users; therefore, maintaining data privacy and confidentiality is critical, as it may be exposed to serious security concerns [5]. Application layer protocols define the application interface with lower-layer protocols for sending data over a network. Application layer protocols facilitate interprocess communication using ports. Some application layer protocols include HTTP, CoAP, WebSocket, MQTT, XMPP, DDS, and AMQP [33] Security concerns that this layer may be exposed to, including eavesdropping through spying on traffic data, data breaches [17], denial of service, injection attacks, manipulation, scripting attacks, and others [5].

b. Network layer

Network architecture is a structure that connects and shares information between interconnected devices [7]. The network layer acts as the central nervous system (CNS) of the entire network. Its primary purpose is to route and transmit data to various IoT hubs and

©2026 The Author(s). This article is licensed under CC By 4.0

devices over the internet [33]. It also collects data from various IT infrastructure [7]. In this layer, data are received from the perception layer and transmitted to the processing systems in the middleware layer [5]. The network ensures efficient and seamless communication between the devices. The network manages data routing using MQTT, IPv6, and CoAP protocols. Network topology management and system performance can also be improved through protocols such as RPL, which optimizes resources [34] Cloud computing platforms, routing, switching, internet gateways, and other devices in this area operate using technologies such as Bluetooth, ZigBee, Wi-Fi, LTE, 3G, and more [33]. This layer is highly vulnerable to attacks, including a range of Internet of Things (IoT) devices, such as denial-of-service attacks, phishing attacks, wormhole attacks, and deep holes. Data are more vulnerable during transmission because of their importance and ease with which they can be hacked [17].

c. **Perception layer**

The perception layer, also called the "physical layer" or the "sensing layer," [16] is a group of interconnected devices that enable communication and remote control [7]. It establishes a physical connection with objects and transmits their data to a receiver or a gateway [16]. The main objective of this layer is to obtain and collect information from the environment using sensors and actuators and transmit it to the network layer for further processing [33]. It was also designed to perform feature-based identification and program smart devices to perform mechanical functions, reduce human interaction, and enhance scalability [35]. The role of the IoT in healthcare, which connects stakeholders such as doctors, nurses, patients, medical devices, and pharmacists, is considered part of the perception layer [16]. The security of this layer is measured in terms of complexity, energy efficiency, speed, channel state information (CSI), bit error rate (BER), SINR, maximum error coefficient (MSE), and more, for legitimate and illegitimate users [36].

In summary, the network layer connects the IoT system to the perception layer. The perception layer consists of physical devices, such as actuators and sensors, that process data. The application layer contains user applications that store the processed data. Some studies have also shown that other layers are components of the IoT architecture, such as the management, environment, business, and security layers [19].

4. IOT SECURITY ATTACKS CLASSIFICATION

The increasing scope of the IoT exposes it to various types of vulnerabilities and security threats. Because the IoT is based on the Internet, Internet security issues arise. As previously mentioned, IoT consists of three main layers: the perception layer, network layer, and application layer, each of which presents its own unique security issues and threats [28]. This issue is addressed in this section.

A. Application Layer Attacks

The primary objective of this layer is to intelligently and accurately analyze and process the information obtained from the network layer[28]. This layer is responsible for managing applications based on the information processed in the middleware layer. These devices are simple, lightweight, and low-power, making them vulnerable to attack [37]. This layer includes a range of applications, including smart mail, smart glasses, logistics, retail, smart independent living, safety and monitoring, and resource and energy management [28, 35]. These attacks may replace software code with malicious code, disrupt applications, and render them more vulnerable to hacking. Common threats in this layer include malicious code attacks, spear-phishing attacks, software vulnerabilities (inability to receive security patches), and hacking of smart meters/grids [37]. The Internet of Things (IoT) has become easier to implement because of its ease of use and accessibility through a range of smart portable devices [35]. Figure 3 illustrates the primary security attacks on IoT applications [16].

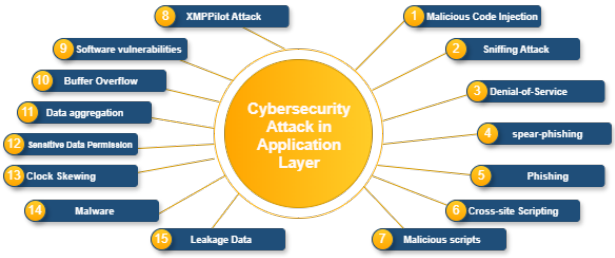


Figure 3. security attack in the application layer

Here, we summarize some Application-Layer Security Attacks:

1- **Malicious Code Injection:**
In this type of attack, an attacker uses certain programs and techniques to inject any type of malicious code into the system to steal data from the user [28]. Attackers can include malicious SQL commands in web form, page requests, or URLs, resulting in unwanted database access[16].

2- **Sniffing Attack:**
An attacker inserts a sniffing application into the

©2026 The Author(s). This article is licensed under CC By 4.0

system, allowing it to obtain network information, which in turn leads to system corruption [28]. It provides integrated security by combining an application layer and middleware [33].

3- **Denial-of-Service (DoS) Attack:**
Denial-of-service (DoS) attacks have become increasingly complex and challenging, and are being carried out to breach defense systems [28] through a group of compromised computers operating from multiple locations [16]. The main goal of this attack is to overwhelm the server, website, or online service and render it unavailable [16]. These attacks trick the victim into believing that the attack is occurring elsewhere, exposing personal and sensitive user data to attackers and leading to service unavailability [28, 36].

4- **spear-phishing attack:**
In this attack, the victim is lured into an email opening, which allows the attacker to access the victim's data. The attacker then pretends to retrieve sensitive information, [28] which is a common threat to the application layer [37].

5- **Phishing Attack:**
Owing to the rapid spread of digital services and internet access, phishing attacks have become a significant threat to cybersecurity [38]. This threat primarily affects the application layer [34]. The attacker uses malicious email and a phishing website [36], where the attacker impersonates the legitimate user by logging into the victim's email account [36] and pretends to be unaware of personal and sensitive information, such as passwords and credit card details, [34] to obtain the victim's credentials and use them for criminal purposes and corrupt data [33]. Attackers can use compromised devices such as smartphones, home appliances, and smart cars to launch these attacks at the application layer [16]. For example, Irish cyberattacks on the Health and Safety Executive (HSE Conti) have escalated [16].

6- **Cross-site Scripting (XSS) Attacks:**
In this type of attack, an attacker injects malicious code into legitimate and trusted websites, compromising the security of users, the system, and data. [16, 34] This technique is used in the IoT to exploit the web interfaces of connected devices [34], which allows an attacker to change the content of an application [16]. Because the browser is unable to distinguish between malicious and legitimate codes, the infected code is executed, thus enabling them to access session IDs, cookies, or other confidential information. Furthermore, attackers can control the device and send users to other malicious websites, or cause the device to malfunction or be damaged [16].

7- **Malicious scripts:**
These scripts infect an application and deliberately harm an IoT system. An attacker sends a malicious script to a user when they request a service from the Internet, because all IoT applications rely on the Internet. Examples of these scripts include ActiveX and Java. An attacker can cause a system crash by accessing confidential data [36].

8- **XMPPilot Attack:**
This attack was launched using the XMPPilot command-line tool on the XMPP connection established between the client and server. This attack allows the attacker to monitor communications because it prevents encryption on the client-side [36].

9- **Software vulnerabilities:**
They are considered a major threat because they are weaknesses in software that attackers exploit for malicious purposes. Owing to a lack of security standards, software engineers and developers do not attach much importance to writing secure software. This, in turn, enables attackers to launch attacks such as buffer overflow [36].

10- **Buffer Overflow Attacks:**
Some programs suffer from memory problems previously allocated to a particular program [36]. Buffers hold data as they are transferred from one location to another; if the buffer capacity is exceeded, the data exceeds the buffer capacity [16]. An attacker writes a piece of code that is larger than the memory previously allocated to a particular program, thus modifying the information stored in other memory locations, executing malicious software that redirects the stack pointer, disrupts the control flow, and crashes the application. Memory-access errors or incorrect results can occur [36]. The goal of this attack is to enable attackers to exploit memory overwriting vulnerabilities that negatively impact execution paths, leak confidential information, and corrupt numerous files. Older systems are the most vulnerable to this type of attack because of their limited memory [16].

11- **Data aggregation distortion:**
The attacker alters the data collected from multiple nodes and sends it to the base station, which then gathers incorrect information regarding the surrounding environment [36].

12- **Sensitive Data Permission/Manipulation:**
This attack exploits vulnerabilities in IoT design, particularly in terms of permissions and authorizations for controlling applications. The primary goal is to communicate between smart applications and smart devices. Sensitive data are sent to the application that is being monitored by the smart device. This type of attack poses significant risks, especially in terms of user privacy [36].

13- **Clock Skewing:**

©2026 The Author(s). This article is licensed under CC By 4.0

In this type, the attacker generates incorrect time information and desyncs IoT devices, which in turn causes the victim's devices to desync with aggregation nodes [36].

14- **Malware:**
Malware is used to commit cybercrime using IoT applications, and recently, this attack has occurred when an attacker attempts to access IoT devices using a default SSH or Telnet account [39]. Many types of malware have been released to attack IoT devices, including spyware, rootkits, and hardware. Malware in national security (such as the Red October virus), finance (BaFin), social (transportation, telecommunications, energy, water), and economic (manufacturing, fintech) sectors negatively impacts these sectors and human lives [16]. The most common example of malware is the Trojan horse attack, which refers to the use of malicious software hidden within secure and legitimate applications to compromise security. The attack affects the application layer. To improve the security of IoT applications, strong authentication, security practices, data encryption, and security mechanisms must be implemented [34].

15- **Data Leakage:**
An attacker aims to access sensitive and confidential data by exploiting the vulnerabilities in IoT services and applications [36].

B. Network Layer Attacks:

This layer also contains all network devices, such as routers, switches, bridges, and firewalls, that work with communication and routing protocols, such as ZigBee, Infrared, Wi-Fi, 3G, 4G, and 5G [30]. UMTS, WiMAX, Satellite and RFID [28]. At the network layer, security is provided by IP Security Protocols (IPSec), which provide complete security with integrity, authentication, replay protection, and confidentiality. Multiple intrusion detection systems can detect intruders and malicious activity in a network. Firewalls are critical for preventing unauthorized access to networks. 6LoWPAN IoT networks are vulnerable to many attacks, both from within the network and from the Internet [40]. The presence of any malicious node or behavior may disrupt the normal functioning of the network, triggering attacks, such as hello flooding, black holes, selective rerouting, recursion attacks, and wormholes [41]. Figure 4 illustrates basic security attacks at the IoT network layer. [16].

Here, we summarize some Network-Layer Security Attacks:

1- **Dos/DDoS Attacks:**
This is one of the most common attacks, and is a type of cyberattack that disrupts a system, network, or application. When an attack originates from multiple compromised nodes, it is called DDoS [16]. In

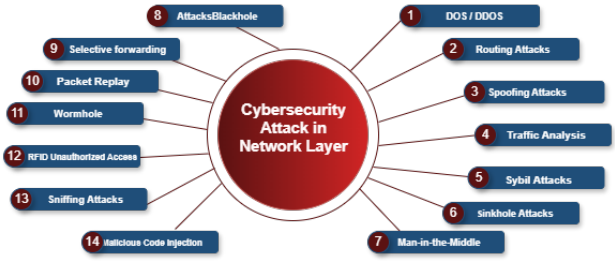


Figure 4. security attacks at the IoT network layer

the Internet of Things (IoT), a DDoS attack occurs when an attacker adds a massive amount of invalid data to the network, rendering it unable to process valid data. [34] The network is flooded with malicious and useless code messages, which in turn renders the targeted users unavailable [37], which prevents them from accessing websites, emails, network services, or data, making the targeted networks extremely slow, often leading to their shutdown and denial of service to authorized users [37]. Furthermore, DDoS attacks can be used as a means for other types of attacks such as data theft or malware installation [34]. In these attacks, a series of data packets is continuously sent to the targeted IoT devices via an IP address, rendering the targeted device unusable after a period of inactivity. This includes many attacks such as SYN flooding, dead-end testing, and UDP flooding [36]. To counter these attacks, intrusion detection systems and routing tables have been used. Attacks based on the network layer affect smart buildings, e-health, and smart-city applications [42]. Owing to the small size of IoT node batteries, an attacker drains the battery to shut down the node, preventing it from functioning and reporting emergencies. Keeping the nodes awake and preventing them from entering sleep mode could trigger a DoS attack [36]. Furthermore, one of the main threats is leakage of unencrypted user information [36].
These attacks have become more sophisticated and are a method for executing attacks to breach defense systems, placing the unencrypted personal data of the user at the hacker's disposal [28].

2- **Routing Attacks:**
This type of attack targets routing protocols used in IoT systems [36]. IPv6 is used throughout the IoT, such as in wireless sensor networks, which are more vulnerable to routing attacks and impersonation [36]. Altered routing information can lead to packet drops, routing loops, increased latency, misdirected rerouting, or network fragmentation [36]. An attacker uses this attack to reroute, impersonate, or send misleading messages to the system. There are many routing

©2026 The Author(s). This article is licensed under CC By 4.0

attacks such as wormholes, blackholes, routing information changes, Sybil attacks, grayholes, and hello floods. These attacks are carried out at the ISP, and ICT providers must be NIS2-D compliant [16].

3- **SPOOFING ATTACKS:**
Spoofing attacks are used to spread malicious information in the IoT systems. Spoofing includes several types such as email, frame spoofing, and URL spoofing. IP or MAC address spoofing was the most common type [36] of spoofing [16]. An attacker impersonates the IP address of a device or node to access the IoT system, sending suspicious data that appears to originate from a legitimate and trusted device [36]. The MAC address is used in IoT to authenticate wireless networks at the data link layer. An attacker spoofs the MAC addresses of legitimate users to gain unauthorized access to the network, which in turn negatively affects the confidentiality and integrity of the data [16]. In Radio Frequency Identification (RFID) technology, an attacker uses fake information for a legitimate RFID tag and disseminates data that appear to have originated from an authentic RFID tag to carry out malicious activity or behavior. They also used RFID information to transmit their data as if they were legitimate owners, allowing them to gain access to the system [36].

4- **Traffic Analysis:**
The wireless media features of IoT rely on radio-frequency identification (RFID) technology [36]. The network traffic was analyzed to detect and monitor anomalies and abnormal behavior [16]. An attacker uses a spy tool to analyze traffic and obtain confidential information [16]. An abnormally high traffic volume also indicates traffic analysis or a denial-of-service attack [36]. These types of analyses include vulnerability scanning, network monitoring, and port scanning [36]. Criminals monitor traffic to obtain passwords by analyzing packets during each keystroke and the time between them [36]. The greater the amount of traffic, the greater the possibility of extracting data from the obtained packets [36].

5- **Sybil Attacks:**
In this attack, legitimate nodes are impersonated using malware to redirect data traffic to malicious nodes [36] within the network and to deceive and manipulate the behavior of the system for their benefit [34]. In this attack, malicious nodes possess multiple identities, potentially outnumbering legitimate nodes in the network [15]. Owing to the different identities, the compromised device sends fake data to neighboring devices [36]. This attack impacts data integrity and resource allocation owing to its ability to control information flow within the network [15].

6- **Sinkhole Attacks:**
In this attack, false metrics (such as optimal bandwidth, minimum delay, and shortest path) are sent from a compromised IoT node or device to neighboring nodes, allowing them to use this node as a routing node along their path [36]. The attacker redirects or ignores the traffic, preventing the base station from receiving the entire data transmission and reducing network robustness and draining energy [16]. Through these attacks, an attacker can eavesdrop on communications, intercept and obtain sensitive information, or manipulate data and collect confidential data, such as login credentials and financial information. They can also modify data or inject malicious content [34].
This type of attack leads to unauthorized actions and [34]. Affects the integrity, availability, and reliability of the network [16].

7- **Man-in-the-Middle (MITM) Attacks:**
A cyberattack involves secretly intercepting the communication between two devices [16, 34]. The attacker gains unauthorized access to eavesdrops, manipulates data, or collects sensitive information [34]. The main goal of this attack is to steal users' confidential information or to modify messages or data [37]. Attackers exploit existing or new vulnerabilities in IoT systems to perform such attacks. Examples include device malfunction and temperature sensor reading, which enables hackers to steal sensitive information [16].

8- **Blackhole Attack:**
This attack involves inserting malicious nodes into the network and providing false routing information to their neighbors, indicating that they have the shortest path to the interface where the malicious node processes or drops the packets. The attacker captures packets at one location in the network and sends them to another [12].

9- **Selective forwarding:**
In this type of attack, the attacker drops some or all packets destined for IoT nodes and delays their routing. They can also disrupt communication between devices by selectively routing packets [36].

10- **Packet Replay Attack:** In this type of attack, the attacker retransmits and replays previously received packets to a group of nodes in the IoT system or the entire network [36]. An attacker copies a key or part of the messages exchanged between two parties and steals the information. The authenticated information is then sent maliciously to the recipient for malicious purposes. The authenticated message is sent repeatedly and is considered legitimate, meeting the attacker's requirements and goals [37]. This, in turn, degrades

©2026 The Author(s). This article is licensed under CC By 4.0

the system owing to the consumption of resources, such as memory, bandwidth, and power. This is considered a type of phishing attack [36].

11- **Wormhole Attacks:**
In this type of attack, two malicious devices are placed in separate locations within the same geographic area of the IoT system with a private, one-hop link between them. IoT devices select these devices or nodes as the next hop in their routing paths. Once data flows through the tunnel between two malicious nodes, an attacker can delay or drop the data, which is very dangerous for mission-critical applications. This attack is performed either by compromising the IoT device, known as an out-of-band wormhole, or by in-band wormholes using a high-gain directional antenna [36].

12- **RFID unauthorized access**
This type of attack arises owing to the lack of an authentication process for RFID tags, easy accessibility, and easy manipulation. An attacker can easily modify or delete information contained in the tag [36].

13- **Sniffing attack:**
In this attack, the attacker uses specific applications, programs, or devices to capture the network traffic and analyze it to carry out a real attack [36].

14- **Malicious code injection:**
In this type of attack, an attacker takes over a working node and injects it with malicious code to gain access to and control over the network. This often leads to network shutdown [37]. The network layer plays a significant role in the application layer. Artificial neural networks (ANNs) are used to detect IP-based intrusions in IoT devices [42].

C. Perception layer Attacks:

The function of this layer is to perceive and collect information using devices such as pressure sensors, temperature sensors, and Radio Frequency Identification (RFID) tags. These challenges arise due to the presence of IoT devices in an open, unprotected environment, as well as the limited resources of IoT nodes and devices. These challenges include physical damage and tampering with IoT devices. Attacks in this layer focus on falsification of information [35, 36].

This layer is exposed to significant security risks, as shown in Figure 5 [16].

Here, we summarize some Network-Layer Security Attacks:

1- **Eavesdropping:**
An attacker secretly intercepts private communications (wireless communication channels) between sensors in order to obtain confidential information [34]. Exchange between devices or radio frequency identification (RFID) tags and readers [16]. This attack is considered passive because the attacker does nothing but eavesdrop [36]. Eavesdropping attacks may have other malicious intent, such as capturing biometric and genomic data for personal gain or using personally identifiable information/genetic data for espionage. These attacks were successful in the past. [16]. Once the RF signal is interfered with by noise, communication between nodes becomes difficult, which in turn disrupts the network and leads to denial of service [36].

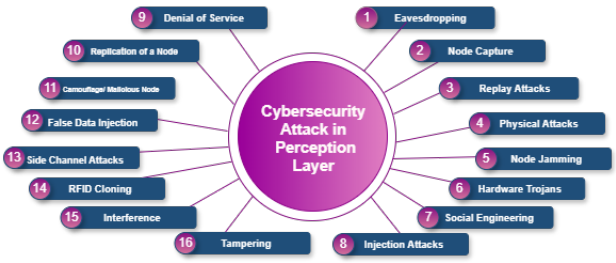


Figure 5. Security attack in the perception layer

2- **Node Capture Attacks:**
In this type of attack, an attacker can gain access to a node or device within an IoT system, seize its control, and take it over. This attack involves completely replacing a node or manipulating the hardware components of the targeted node. The attacker can also copy information to malicious nodes that connect to the network or IoT system as authorized nodes and perform malicious actions [34]. and reconfigure or extract the encryption information. This is because IoT nodes operate in an unprotected external environment, which makes them more vulnerable to these attacks [36].

3- **Replay attacks:**
In this type of attack, an attacker hijacks network traffic and causes a malicious node or device to gain the trust of other nodes, pretending to be the original sender using legitimate identification information previously communicated with the destination node or device. These attacks are launched through authentication processes to delegate the integrity of the certificates [34, 36].

4- **Physical attacks:**
These attacks focus on the perception or physical layers of the IoT architecture [16]. The attacker accesses or modifies information from the tag for forgery and sabotage [36]. To attack this layer, proximity to the network infrastructure and unauthorized access are required to execute the attack [16]. These tags include circuit tampering, probe attacks, clock tampering, and material removal tags [36].

5- **Node jamming attack:**

©2026 The Author(s). This article is licensed under CC By 4.0

An attacker sends jamming signals through the IoT wireless signaling channel, thus occupying the transmission medium and causing interference [36]. This causes energy consumption, leading to rapid resource depletion [36], which ultimately leads to a service outage and complete shutdown [16]. This ultimately leads to a denial of service (DoS) attack on an IoT node. Jamming is a common type of attack in this layer. This type of attack can be catastrophic, especially in healthcare, as it can disrupt ongoing surgeries and medical diagnoses, thereby impacting human lives [16].

6- **Hardware Trojans:**
An attacker accesses the data and programs installed in an integrated circuit (IC). The attacker alters the design of these circuits during or before production to add hardware trojans. To activate this mechanism, an attacker can create a specific operating system. Hardware Trojan attacks include both external and internally enabled attacks [36].

7- **Social engineering:**
In this type of attack, an attacker manipulates the IoT users to perform specific actions. The attacker must then interact with the IoT users to perform a particular action or obtain related information [36].

8- **Injection attacks:**
These attacks involve injecting malicious code and modifying the software of the IoT devices. They provide attackers with complete control and access to IoT systems [36]. These attacks can be devastating to the infrastructure, as a malicious node can spread across the entire network, infecting it and draining network resources [16, 36], causing complete operational damage [16]. Viruses can also be injected into the nodes [36].

9- **Denial of Service (DoS) Attacks:**
The Internet of Things (IoT) is vulnerable to this type of attack owing to its limited resources such as batteries, power, memory, and processing capabilities. Owing to its small size, an attacker can drain the battery to shut down nodes, which has dire consequences in emergencies where a node is unable to operate and report an emergency. In addition, a DoS attack can cause a denial of service attack by preventing nodes from sleeping, keeping them awake, and preventing them from entering the sleep mode. In DoS attacks against RFID tags, the user cannot read the tags because of interference with the wireless communication channel, rendering them unavailable [36].

10- **Replication/duplication of a node:**
In this type of attack, malicious nodes that appear authentic are embedded in the system by duplicating information from the original nodes. This attack uses duplicate nodes to intercept packets, reroute data, or access sensitive information such as shared encryption keys [36].

11- **Camouflage/Corrupted/Malicious Node Attack:**
In this attack, legitimate nodes are attacked or malicious and fraudulent nodes are introduced to hide at the edge. These nodes are used to send and reroute packets and perform trac analysis. The attacker aims to gain access to the system, other nodes, network, and their connections using malicious and corrupted nodes. This can lead to a network shutdown [36].

12- **False data injection attacks**
In this type of attack, an attacker injects information to replace the correct information initially collected from the IoT device. The attacker then sends the false information to the target [36].

13- **Side Channel Attacks:**
In this attack, the attacker aims to obtain the encryption key by predicting it through the plaintext or ciphertext of the communication. Some techniques have been applied to obtain the encryption key, such as timing techniques, which analyze the time spent in the encryption process and then predict the encryption key. A side-channel attack is launched against an RFID tag, where the attacker extracts information by attacking wireless communications between the parties. In a non-network-side channel attack, private information about the nodes is provided, enabling continuous transmission of electromagnetic waves [36].

14- **RFID Cloning:**
In this type of attack, the attacker deceives the reader using duplicate tags that mimic the original tag to gain unauthorized access to information [16]. The reader cannot distinguish between the original RFID tag and compromised RFID tag [36]. This includes various methods, such as RFID cloning and tag cloning. The goal of these attacks is to obfuscate and confuse the reader, giving the attacker access to sensitive information via RFID spoofing [36]. This compromises the integrity of the system and increases the risk of biometric intrusion [16].

15- **Interference:**
In this type of attack, network communication is disrupted by interrupting traffic and broadcasting radio waves to spread misinformation and cause panic [16].

16- **Tampering:**
In this type of attack, the memory of a node is manipulated and its functions are altered. An attacker may manipulate a device by shutting it down, starting it up, restarting it, tampering with data, or stealing sensitive information. Individuals can suffer severe consequences if their personal information is misused. Because of the misuse of generative AI, adversaries repeatedly plan and execute these attacks. Misuse of an individual's personal

©2026 The Author(s). This article is licensed under CC By 4.0

information can have severe consequences [16].

5. METHODOLOGY

The research was conducted from 2018 to include early access publications to obtain the most recently published studies. The search included four major academic databases: IEEE Xplore (44 studies), Springer (10 studies), MDPI (seven studies), ScienceDirect (Elsevier) (two studies), River Publishers (1study) and Sana'a University Journal of Applied Sciences and Technology (five studies).
The search strategy used the following keywords:

- **In the technical field**: - "Internet of Things," "IoT," "IoT layers," "Industrial IoT," "IIoT," "Smart City," "Internet of Medical Things," "IoMT," "Internet of Vehicles."
- **In the field of security**: "Security," "Intrusion Detection," "Intrusion Detection System (IDS)," "Anomaly Detection," "Cyber Attacks," "Threats," "Botnet Attacks," "DDoS," "Spoofing," "Privacy."

–

- **Technologies used**: - "Machine Learning," "Deep Learning," "Federated Learning," "Hybrid Model," "Artificial Intelligence," "AI."

This research included studies published in peer-reviewed journals and conferences, focusing primarily on IoT security and anomaly detection, studies using machine learning and deep learning techniques in anomaly detection, and studies that discuss IoT security from the perspective of the underlying layers of IoT (Layered Architecture). It also included papers that provided experimental evaluations and mentioned clear performance metrics (such as precision and recall).
This study also excluded studies that did not focus on IoT security (such as studies that only addressed performance or energy consumption improvements without focusing on security), as well as studies that did not use machine and deep learning techniques as a primary method for increasing IoT security. This study also excluded studies and unpeer-reviewed research, as well as duplicate papers published in more than one source.

6. IOT DOMAIN

The Internet of Things (IoT) is a vast ecosystem in which devices and systems are interconnected across multiple domains to communicate, share [43], and perform various tasks [26]. The IoT encompasses diverse applications and is rapidly expanding [5]. These applications include emergency services, logistics, retail controls, smart industries [3], security and healthcare applications, object tracking, home automation, military applications, industrial automation, smart cities [5], traffic management, shopping, sustainability, transportation, manufacturing, delivery, smart communities, smart street lighting, urban life safety, urban protection, traffic signals, waste management, vehicle networks [26], and everyday consumer devices such as home assistants and smart watches [24].
Security is one of the most significant challenges across all applications.

A. Healthcare:

The Internet of Things (IoT) is a data-driven infrastructure that relies on smart sensors (such as temperature sensors and blood pressure monitors) to increase response times, diagnoses, and treatments. The Internet of Things (IoT) in healthcare is also known as digital healthcare [16]. With the increase in IoT devices in this field and the development of cybersecurity threats, these devices have become vulnerable to various attacks, such as those associated with generative artificial intelligence and the fifth-generation Internet of Things (5G IoT). These risks can lead to data theft, unauthorized access, a lack of control, management, security, and potential harm [16].
The integration of a range of medical devices into the IoT, also known as Healthcare 5.0, has created the IoT in healthcare, which in turn has paved the way for a new era of medical practice and patient care. The Internet of Medical Things (IoT) has led to the integration of advanced technologies, and has played a role in improving medical processes and procedures, developing services, and improving patient outcomes [44]. Recently, many biomedical devices have been developed to assist patients in monitoring and diagnosing diseases. Information recorded from biomedical devices is stored and processed on the central platform to which these devices are connected [22].

B. Smart Home:

One of the most common applications of IoT is smart homes, which consist of a variety of interconnected devices, including doors, thermostats, and light switches, which can be controlled via smart speakers or smartphones [14]. These devices have brought convenience and comfort to human life and have made many tasks easier. These devices consist of various computing devices connected to sensors that can communicate, share data, and be controlled remotely via the Internet or other types of networks. By the end of 2025, the total number of IoT devices is expected to reach 20 billion [14].
These devices are small and therefore consume relatively little power and resources, making it eas-

©2026 The Author(s). This article is licensed under CC By 4.0

ier for attackers to penetrate. Therefore, it is essential to protect the features and integrity of a smart home environment from external intrusions and attacks [22].

C. Smart Cities:

Smart cities consist of a set of IoT devices, such as lighting, connected meters, and sensors, to collect and analyze data owing to the complex networks and variety of devices. These devices control, manage, and implement a range of daily tasks and services to improve the quality of human life [45].

D. UAVs:

Unmanned aerial vehicles (UAVs) are also known as drones. Drones have become an important and influential role in many different sectors, such as agriculture, the military, trade, and police, in improving the quality of life. They are also exposed to numerous risks as hostile actors exploit security vulnerabilities to launch various attacks that can cause significant damage. These vulnerabilities include weak communication channels, hardware and software risks, network threats, and authorization risks [12].

E. Industry:

IoT plays a significant role in monitoring and managing the health of industrial machinery to improve the efficiency and quality of industrial operations [14]. The Industrial Internet of Things (IIoT) is an important concept in Industry 4.0, connecting industrial assets such as machinery and control systems to information systems and business processes. Integrating production IoT devices enables communication and data exchange within the production systems. Adding sensors to legacy equipment provides cost-effective upgrades to the industrial infrastructure within the IIoT [15]. IoT-enabled systems have been used in manufacturing environments and a range of commercial applications [26].

Detection is critical in smart industries to reduce downtime, improve safety, and prevent equipment failure from increasing production. The IoT has led to the provision and collection of a large amount of data from industrial machines. This information can be used to automatically detect anomalies that are difficult for humans to detect manually owing to their size and complexity. Machine learning (ML) algorithms are a method for detecting anomalies in industrial machines by analyzing the data generated by these devices [15].

Smart systems possess a wide range of capabilities, ranging from smart homes and buildings to power generation, transportation networks, and smart facilities, such as factory automation and management [26]. Internet of Things (IoT) devices represent 40.2% of the industry and manufacturing. The medical sector uses IoT equipment at a rate of 30.3%, retail sector uses IoT devices at 8.3%, security sector uses IoT devices at 7.7%, and transportation sector uses IoT devices at 4.1% [10]. The amount of data generated by IoT devices can reach large amounts. The amount of data generated by these devices is increasing dramatically, and they may contain sensitive and confidential information. By the end of 2025, the amount of data generated by the IoT is expected to reach 73.1 zettabytes [10].

7. ANOMALY DETECTION AND ALGORITHMS

An anomaly is a deviation from the normal, expected, or standard, and may refer to something unusual, irregular, or problematic. Anomaly detection is the process of identifying abnormal or unusual events or trends in the data (anomalies). Anomaly detection finds errors, tracks the status, and detects attacks and security breaches. Anomaly detection is a security method for identifying when a system's behavior deviates from normal [19], potentially leading to malicious activity [46]. Anomaly based detection can be classified into model-based and case-based methods [2]. Depending on the situation, anomaly detection can be performed at the context level, where unusual data points are detected through their surrounding context; [21] the group level, where groups of data elements that do not conform to the norm are detected; [21] or the point level, where data points that do not conform to the norm are analyzed to prevent patterns [21].

Anomaly detection involves training the system on normal behavior and traffic patterns. Anomalies are considered abnormal if they deviate from normal behavior. To train the system, we require a large and complex amount of Internet of Things (IoT) data and normal network traffic patterns, as well as significant time to build a profile of these data [19]. Monitoring network traffic, which is the primary goal of anomaly detection, is important for maintaining network security [47]. Anomaly and attack detection are critical issues in Internet of Things (IoT) systems. The advancement and expansion of IoT systems across a variety of different sectors has led to an increase in attacks, threats, and anomalies targeting these infrastructures, which can disrupt these systems and their components and impact their outcomes [48].

Malware detection methods can be divided into two groups: signature-based identification and anomaly based identification. Typically, anomaly based detection determines whether a program

©2026 The Author(s). This article is licensed under CC By 4.0

is malicious or not [49]. Attacks on the Internet of Things (IoT) are anomalous. For an attack to succeed, the system must exhibit an unusual behavior. Abnormal network traffic, malicious payloads, behavioral abnormalities, and other factors can cause anomalous data traffic [19]. The Internet of Things (IoT) environment has witnessed numerous attacks, which, due to their growth and expansion, have been classified into four types: physical attacks, encrypted attacks, network attacks, and software attacks. These include buffer overflow, brute force, DNS poisoning, injection, replay, distributed denial of service (DDoS), SQL injection, and backdoor vulnerabilities. Anomaly detection can prevent many IoT attacks by sending alerts when unusual or abnormal behaviors are detected. Anomaly detection can prevent IoT attacks by sending alerts when abnormal behavior is detected, which helps identify problems with system functions that could lead to system failure or shutdown [19]. When the availability, privacy, and security of the data are compromised, it is considered a deliberate attack [21].

Supervised algorithms require labeled data for training and testing to perform tasks such as classification and regression, To perform classification tasks, most studies used SVM, ANN, DT, and RF models [21, 50]. Supervised techniques have two additional categories: generative and discriminative techniques. Generative methods, such as Bayesian networks and hidden Markov models, describe the combined probability distribution of input data and output classes. Discriminative methods such as logistic regression and support vector machines model the conditional probability distribution of output classes by considering input characteristics. Unsupervised algorithms are used to perform tasks, such as fluidity and dimensionality reduction. Clustering is the process of arranging data points into groups according to a similarity measure such as cosine similarity or Euclidean distance. Dimensionality reduction techniques such as autoencoders and principal component analysis can be used to simplify complex datasets without compromising important information. Labeled and unlabeled data can be used to train semi-supervised algorithms jointly or self-train [19]. The word "self-training" refers to a process in which a pre-trained classifier is employed to confidently classify new examples placed in the training set. Two classifiers are simultaneously learned from two distinct views or subsets of features and then employed to cluster the unlabeled data simultaneously [21]. There are two types of anomaly detection based on deep learning: Internet of Things anomaly detection and attack detection. Anomalies are considered attacks [19].

Anomaly detection can be achieved through unsupervised learning that leverages the abundance of natural traffic using individual or machine-based models. One approach to ensemble anomaly detection is iForest, which isolates anomalies by repeatedly partitioning data to create a forest of trees. An unsupervised machine-learning algorithm, OCSVM, was designed for novelty detection. It identifies anomalies and learns decision boundaries to encapsulate normal data points. By calculating the distances between data points, the density-based anomaly detection (LOF) technique determines the density of data points and classifies denser regions as normal and less-dense regions as anomalies [5]. Similar to the OCSVM, DeepSVDD separates data samples using a hypersphere and uses neural networks to learn feature representations that aid anomaly detection [51]. However, anomaly based detection can result in false positives, packet misclassification, and poor performance. The capabilities of anomaly detection systems have increased owing to recent advances in artificial intelligence. These systems use supervised machine learning techniques, such as support vector machines (SVMs) and decision trees (DTs), and unsupervised machine learning techniques, such as DBSCAN, K-nearest neighbors, and K-means.

These systems are highly sensitive to changes in the feature extraction and selection. On the other hand, deep learning techniques are much less sensitive to feature selection than machine learning. Deep-learning-powered intrusion detection systems have the ability to continuously evolve and adapt in response to new threats and accurately detect new and potential security breaches [2]. Using deep learning techniques, features can be automatically extracted from the data rather than relying on manual extraction [52]. The emergence of specialized systems, such as the Internet of Things (IoT) underscores the need for a robust and highly adaptable intrusion detection system [2]. The ways in which anomalies or attacks can threaten the security and privacy of IoT networks and users are data loss, corruption, leakage, outages, degradation, theft, fraud, and physical damage. Therefore, anomalies and attacks must be identified and stopped quickly before they cause further damage [21]. Real-time monitoring systems must include anomaly-detection techniques and predictive modeling to detect and mitigate security threats [24].

Emerging technologies, such as blockchain, generative artificial intelligence (AI), and quantum computing, are increasingly being explored to un-

©2026 The Author(s). This article is licensed under CC By 4.0

cover anomalies in the Internet of Things. For example, hybrid frameworks combining deep neural networks and blockchain-based logging have proven effective in improving the detection accuracy and integrity of anomaly logs in IoT deployment [53]. Decentralized detection approaches, such as CIoTA, also leverage blockchains to coordinate model updates across devices in a collaborative and tamper-resistant manner [54]. With regard to generative artificial intelligence, modern businesses use GANs, VAEs, and auto-coding-based generative models to collect attack-like data or to represent rare anomaly patterns in IoT traffic flows [55]. Furthermore, quantum machine learning (QML) offers new opportunities. Systematic reviews identify QML as a promising approach for detecting IoT anomalies, particularly for handling complex, high-dimensional datasets and enabling more adaptive detection models [56]. In addition, quantum deep learning frameworks have been proposed to detect network attacks using quantum support vector-based techniques and quantum auto-cryptage devices [57]. Integrating these emerging technologies into IoT anomaly detection frameworks can lead to smarter, scalable, and more secure detection systems in future IoT environments.

Recently, several anomaly detection methods and techniques have been developed, such as machine learning and deep learning algorithms [12]. This is because breach detection has received significant attention in many academic and industrial circles for addressing these threats [12]. This is a major source of motivation for many researchers to explore these techniques because of their ability to identify new threats [26].

However, traditional methods are not effective in detecting new security threats and breaches, and require longer updates. This can be mitigated using machine learning (ML) and deep learning (DL), which are artificial intelligence techniques [19].

Table 1 presents related studies on the use of machine learning and deep learning techniques to detect anomalies and attacks in the IoT, identifying the algorithms used, dataset, results, features, and challenges.

By analyzing the twenty-five studies presented in the table, it becomes clear that the field of intelligent anomaly detection in the Internet of Things (IoT) is witnessing a remarkable diversity of methods and technologies. These methodologies can be classified into several distinct types: machine learning (ML) (including "supervised machine learning"), deep learning (DL), hybrid models (including "hybrid deep learning," "hybrid (ML & DL)", and"hybrid (GNN + Metaheuristic Optimization)"), and specific variants of deep learning such as "generative deep learning."

The results showed that the machine learning (ML) category was the most representative among the studies, appearing in at least ten studies (e.g., [1, 3, 5–7, 9, 15, 18–20]). These studies achieved remarkably high accuracies, often exceeding 99% in many cases (e.g., 99.999% in [1], 100% in [9], 99.99% in [5] using RF, and 100% in [19] using DT/RF for binary classification). The F1 score for prominent ML models, such as Random Forest and Decision Tree, was consistently high, often at or close to 100%, in several studies. In contrast, the deep learning (DL) class showed strong but sometimes variable performance, with accuracy ranging from 82.58% (LSTM on UNSW-NB15 in [5]) to 100% (LSTM on Edge-IIoTset in [13]). The hybrid deep learning class, which combines algorithms such as CNN-LSTM (e.g., [8, 23]), ACLR [16][16], and IMFOHDL-ID [24], showed generally high and robust performance with accuracy frequently ranging between 98% and 99.9%. The main challenge observed for these hybrid models, particularly in [8, 11, 16], is their increased computational complexity, which may limit their application in resource-limited IoT devices.

At the individual algorithm level, the decision forest (RF) has consistently demonstrated exceptional accuracy, exceeding 99% in multiple studies and datasets (e.g., 99.71% on WSN-DS [5], 100% on IoTID20 [9], and 99.55% on CICIoT2023 [18]), reflecting its effectiveness in detecting trait-based anomalies with relatively low complexity. Similarly, decision TreDT has achieved 100% accuracy and a complete F1 score in studies such as [9] and [25]. In contrast, LSTM-based models (e.g., in [5, 8, 13, 23]) are efficient in temporal behavior analysis, although their performance is more dependent on the dataset. SVM algorithms have shown acceptable performance but are generally lower and more variable (e.g., accuracy: 97% in [6], and 88.29% in [9]), with an average accuracy significantly lower than their tree-based counterparts.

The most prominent datasets used across the studies were BoT-IoT (used in [13, 17, 24, 25]) and TON_IoT (used in [2, 4, 5, 7, 11, 12]) and UNSW-NB15 (used in [2, 5, 16, 17]) and CIC-IDS variables (used in [5, 6, 10, 11, 13, 17]) and IoT-23 (used in [4, 17]). Despite its prevalence, which covers a significant part of the reviewed research, this dependence on a common set of criteria may limit the ability of models to generalize, as it is manifested when tested in diverse or specialized IoT environments.

The results also highlight the use of more special-

©2026 The Author(s). This article is licensed under CC By 4.0

Table 1. summarizes related works on anomaly and attack detection in IoT using machine learning and deep learning techniques.

N	Year	Reference	Detection Algorithm	Algorithm Type	Domain	Dataset	Metrics				Advantage	Limitations
							Accuracy(%)	Precision (%)	Recall (%)	F1-score (%)		
1	2025	[43]	Fine Tree-Based Model	Machine Learning (ML)	Internet of Vehicles (IoV)	Benchmark hybrid dataset created using the 5G-LENA module in the NS-3 simulator to simulate vehicular networks in 5G/6G environments.	99.9%	99.9%	99.9%	99.9%	1. Achieves high accuracy in attack detection. 2. Operates computationally efficiently in resource-limited environments. 3. Explainability and facilitates decision-making. 4. Real-time detection speed.	1. Adapting to new attacks 2. Balancing performance and complexity 3. Dynamic data volume 4. Data noise
2	2025	[9]	Single-View AE Single-View CNN Multi-View CNN Multi-View AE DGCCA	Deep Learning (DL)	Cybersecurity (Anomaly Detection in Enterprise Networks)	TON_IoT , UNSW-NB15	_	_	_	- Single-View AE : TON_IoT = 72.0% UNSW-NB15 =79.7% - Single-View CNN : TON_IoT = 89.2% UNSW-NB15= 80.6% - Multi-View CNN : TON_IoT = 87.1% UNSW-NB15 = 84.8% - Multi-View AE : TON_IoT= 92.5% UNSW-NB15= 85.6% - DGCCA : TON_IoT= 86.0% UNSW-NB15 =80.0%	1.Multi-View models excel at integrating multi-source data. 2.Higher F1-score (0.925 on TON_IoT and 0.856 on UNSW-NB15). 3.Higher ability to detect complex attacks such as DDoS and MITM.	1.Computational complexity due to the integration of multiple data sets. 2.Poor performance if the data is not integrated. 3.The need for fine-tuning parameters such as kernel size in CNNs.
3	2025	[58]	AIDS and its integration with (OCSVM, LOF, G_KDE, PW_KDE, B_GMM, MCD, Iso-Forest)	Machine Learning (ML)	the Internet of Medical Things (IoMT)	1. The LDE dataset 2. The CDE behavior dataset 3. The CDE network dataset.	1. The LDE DS = 98.0%. 2. The CDE behavior DS= 97.0%. 3. The CDE network DS= 94.0%.	_	_	_	1.Detecting known and unknown attacks. 2.Lightweight in terms of computational consumption.	1.Lack of compatible datasets. 2.The need for lightweight algorithms due to limited IoMT hardware resources. 3.Difficulty obtaining training data representing unknown attacks.
4	2025	[2]	Fed-MLDL (Federated Multi-Layered Deep Learning)with FedRIME	Deep Learning(DL)	Network security, intrusion detection in IoT networks.	CICIoT23 , CICIoT22 , ToN_IoT ,Edge_IIoTset and IoT-23	1- IID: 99.7% (two-class) 99.5% (8 classes) 99.3% (34 classes) 2- Non-IID: 99.4% (two-class) 99.3% (7 classes) 99.1% (34 classes)	Values ranging (99.0% - 99.5%)	Values ranging (99.1% - 99.5%) depending on the data distribution.	Values ranging (99.0% - 99.5%)	1.High performance 2.Improved convergence speed 3.Customize the model for each client 4.Privacy protection	1.Heterogeneous data distribution 2.Limitations of resource-limited IoT devices 3.Balancing performance and privacy
5	2025	[59]	Random Forest (RF) Long Short-Term Memory (LSTM)	Machine Learning (RF) Deep Learning (LSTM)	IoT Security (Network Intrusion Detection Systems - NIDS)	WSN-DS UNSW-NB15 CIC-IDS 2017	WSN-DS: -RF =99.7% -LSTM= 99.4% UNSW-NB15 -RF =90.2% -LSTM= 82.6% CIC-IDS 2017 -RF =99.9% -LSTM= 99.9%	WSN-DS: -RF = 99.7% -LSTM = 99.4% UNSW-NB15 -RF = 90.1% -LSTM = 82.4% CIC-IDS 2017 -RF = 99.9% -LSTM = 99.9%	WSN-DS: -RF =99.7% -LSTM = 99.4% UNSW-NB15 -RF =90.1% -LSTM = 82.5% CIC-IDS 2017 -RF =99.9% -LSTM= 99.9%	WSN-DS: -RF = 99.7% -LSTM = 99.4% UNSW-NB15 -RF =90.1% -LSTM = 80.8% CIC-IDS 2017 -RF =99.9% -LSTM = 99.9%	1.Multi-Dataset Evaluation 2.Feature Selection 3.Handling Imbalanced Data 4.Performance: RF outperforms LSTM in accuracy and computational efficiency 5.Robustness	1.LSTM Performance 2.Computational Cost that requires longer training times 3.Threshold Sensitivity 4.Dataset Bias 5.Noise Sensitivity

© 2026 The Author(s). This article is licensed under CC By 4.0

© 2026 The Author(s). This article is licensed under CC By 4.0

Table 1. (Follow the table 1) summarizes related works on anomaly and attack detection in IoT using machine

N	Year	Reference	Detection Algorithm	Algorithm Type	Domain	Dataset	Metrics				Advantage	Limitations
							Accuracy(%)	Precision (%)	Recall (%)	F1-score (%)		
6	2025	[24]	-Isolation Forest (Anomaly Detection) -Logistic Regression (LR) (Binary Classification) -Support Vector Machine (SVM) (Binary Classification) - Random Forest (RF) (Multiclass Classification) -XGBoost (Multiclass Classification)	Machine Learning (ML)	IoT and Smart City Wireless Networks	Penetration Test-Generated Dataset (20,421 entries from "Tenda_476300" WiFi network) CIC-IDS2017	SVM = 97.1% LR = 92.0% XGBoost = 99.0% RF = 95.0%	SVM= 98.0% LR = 95.0% XGBoost = 99.0% RF = 95.0%	SVM = 95.0% LR = 89.0% XGBoost = 100.0% RF = 99.0%	SVM = 97.0% LR = 92.0% XGBoost = 100.0% RF = 99.0%	1. Comprehensive Framework 2. High Performance 3. Real-World Applicability 4. Scalability 5. Interpretability	1. Dataset Scope 2. Computational Cost 3. False Positives 4. Dynamic Networks 5. Ethical Constraints
7	2025	[20]	Random Forest (RF), Explainable Boosted Linear Regression (EBLR)	Machine Learning (ML)	(IoT Intrusion Detection Systems)	ToN-IoT	99.0%	99.9%	98.8%	99.4%	1. Simplicity and Efficiency 2. Interpretability 3. Imbalanced Data Handling 4. Intelligent Feature Generation	1. Poor performance in MITM attacks 2. Heavy reliance on feature engineering 3. Lack of flexibility in deep learning
8	2025	[44]	Hybrid CNN-LSTM (HIDS-RPL)	Deep Learning (Hybrid)	Internet of Medical Things (IoMT)	CIC-DDoS2019	99.8%	98.5%	98.6%	98.5%	1. Combines CNN and LSTM 2. Achieves high performance metrics 3. Designed for resource-constrained IoMT environments 4. Explicitly incorporates RPL protocol awareness	1. Computational complexity. 2. Relies on a fixed threshold (= 500 ms) for malicious node detection 3. Real-world performance may vary due to dynamic network conditions
9	2024	[8]	Decision Tree (DT), Random Forest (RF), K Nearest Neighbor (kNN), Support Vector Machine (SVM)	Machine Learning (Supervised Machine Learning)	IoT Networks	IoTID20	- DT & RF with GA = 100.0% - SVM with GA = 88.2% - kNN with GA = 99.9%	- DT & RF with GA= 100.0% - SVM with GA = 83.7% - kNN with GA = 99.9%	- DT & RF with GA I= 100.0% - SVM with GA= 99.7% - kNN with GA = 99.8%	- DT & RF with GA = 100.0% - SVM with GA= 99.7% - kNN with GA = 99.8%	1. High Accuracy with DT and RF. 2. Efficient feature selection using GA. 3. Uses a modern dataset (IoTID20)	1. SVM performs poorly with large datasets. 2. Limited to DoS attacks. 3. Requires further validation in real IoT environments.
10	2024	[60]	SWM-IDS (BWO-GraphSAGE)	Hybrid (GNN + Metaheuristic Optimization)	Smart City (IoT)	CIC-IDS-2018, CIC-DDoS-2019	CIC-IDS =99.7% CIC-DDoS =99.6%	_	CIC-IDS =99.6% CIC-DDoS =99.5%	CIC-IDS = 99.6% CIC-DDoS = 99.5%	1. High accuracy and detection rate. 2. Effective feature selection using BWO. 3. Adaptable to IoT constraints.	1. Scalability issues in large-scale IoT networks. 2. Limited to binary classification. 3. Dependency on dataset quality
11	2024	[61]	DEEPShield (CNN + LSTM + Pruning)	deep learning (Hybrid (Deep Ensemble Learning + Pruning))	IoT Networks	HL-IoT, CICIDS-17, ISCX-12, ToN-IoT	>90.0%	>90.0%	_	93.00%	1. High accuracy for both high/low-volume attacks. 2. Optimized for edge devices via pruning. 3. Novel HL-IoT dataset.	1. Slightly higher FPR for low-volume attacks. 2. Scalability limits on edge devices (e.g., Raspberry Pi). 3. Requires balanced datasets for training
12	2024	[11]	Random Forest (RF) K-Nearest Neighbors SVM Logistic Regression Deep Learning (ANN)	Machine Learning & Deep Learning	IoT Security (Tamper Data, Injection, DoS, Backdoor attacks)	TON_IoT Dataset	ANN = 99.0%	ANN= 99.8%	RF= 98.4%	ANN & RF= High	1. High accuracy 2. Early threat detection at the sensing layer 3. Combines ML, fog computing, and blockchain 4. Enhanced features improve classification	1. High computational overhead (DL models) 3. Real-time scalability needs validation 4. Focuses mainly on security, not privacy threats 5. Not flexible for all new attack types

Table 1. (Follow the table 1) summarizes related works on anomaly and attack detection in IoT using machine learning and deep learning techniques.

N	Year	Reference	Detection Algorithm	Algorithm Type	Domain	Dataset	Metrics				Advantage	Limitations
							Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)		
13	2024	[45]	Long Short-Term Memory Feature Engineering (AE, IG, GA)	Deep Learning (DL) Binary & Multiclass Classification	Smart Cities	BoT-IoT Edge-IIoT NSL-KDD	BoT-IoT = 99.9% Edge-IIoT =100.0% NSL-KDD =99.7%	BoT-IoT =99.9% Edge-IIoT =100.0%	BoT-IoT =99.9% Edge-IIoT= 100.0%	_	1. High accuracy 2. Fast detection time (5-8 ms) 3. Use of feature engineering 4. Effective for binary and multi-class classification 5. Accelerated TPU training (approximately 100-616 ms)	1. High cost of training deep learning models 2. Limited on other IoT datasets 3. Reliance on feature engineering 4. Requires labeled data for supervised learning 5. May struggle with some attacks, such as zero-day attacks
14	2024	[25]	Random Forest (RF) Decision Tree (DT) Transformers LSTM CNN FFNN	Hybrid (ML & DL)	IoT Security (RPL Protocol Attacks)	ROUT-4-2023	RF/DT =99.0% LSTM =98.0%	Transformers =97.0%	_	_	1. High accuracy (99%) with RF/DT 2. Efficient training (Transformers) 3. Comprehensive attack coverage 4. Feature engineering for anomaly detection 5. Balanced dataset analysis	1. Computational overhead for DL models 2. Limited validation 3. Dependency on labeled data 4.Difficulty detecting and countering zero-day attacks. 5.IoT devices increase resource usage.
15	2024	[23]	Decision Trees (DT), k-nearest neighbors (KNN), Gaussian SVM	Machine Learning (ML)	Industrial IoT (IIoT)	IOTID20	DT: 99.9% ACC (binary), 97.6% ACC (multi-class) KNN: 99.0% ACC (multi-class) Gaussian SVM: 96.0% ACC (PCA, 12 features)	_	_	_	1- High accuracy with reduced features (12/79) 2- Lower computational complexity 3- Balanced model size and speed	1. Longer training times for KNN/Gaussian SVM 2. Limited comparison with deep learning methods 3. Real-world applicability not tested
16	2024	[62]	ACLR (ANN + CNN + LSTM + RNN)	Deep Learning (Hybrid)	IoT Security Botnet Detection	UNSW-NB15	96.9% (97.4 % with K-fold)	96.90%	96.90%	96.90%	1. Combines strengths of multiple DL models 2. High detection accuracy 3. Robust to evolving botnet threats 4. Effective for imbalanced data	1. High computational complexity 2. Longer training time 3. Requires large labeled dataset 4. Less interpretability due to ensemble nature
17	2024	[63]	DNN, CNN, RNN/LSTM/GRU, AE, DBN, STL	Deep Learning (DL)	IoT Security / Intrusion Detection	KDD Cup99, NSL-KDD, UNSW-NB15, CICIDS2017, Bot-IoT, IoT-23	DNN =up to 99.5% CNN =97.0% LSTM =99.5% AE =99.1% DBN =99.9%	_	_	_	1. Comprehensive coverage of DL models 2- Addresses data imbalance solutions	1. No unified performance benchmark 2. Challenges in IoT-specific adaptations 3. Computational complexity not quantified

© 2026 The Author(s). This article is licensed under CC By 4.0

© 2026 The Author(s). This article is licensed under CC By 4.0

Table 1. (Follow the table 1) summarizes related works on anomaly and attack detection in IoT using machine learning and deep learning techniques.

N	Year	Reference	Detection Algorithm	Algorithm Type	Domain	Dataset	Metrics				Advantage	Limitations
							Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)		
18	2024	[64]	Random Forest (RF), Logistic Regression (LR), Perceptron (PER), Deep Neural Network (DNN), Adaptive Boosting (AB	Machine Learning	IoT Healthcare	CICIoT2023	99.5% (2-Class) 95.5% (8-Class) 96.3% (34-Class)	99.5% (2-Class) 99.5% (8-Class) 96.2% (34-Class)	99.5% (2-Class) 95.5% (8-Class) 96.3% (34-Class)	99.5% (2-Class) 95.5% (8-Class) 96.2% (34-Class)	1. High accuracy and real-time detection. 2. Balanced dataset using SMOTE improves model generalization. 3. Reduced feature space speeds up training.	1. Recon and Spoofing attacks had lower detection rates. 2. Requires further analysis for certain attack subclasses.
19	2024	[65]	Random Forest (RF), Decision Tree (DT), Extra Tree Classifier (ETC), Support Vector Machine (SVM), k-Nearest Neighbor (KNN), Deep Neural Network (DNN)	Machine Learning and Deep Learning	Industrial IoT (IIoT)	Edge-IIoTset	DNN: 100.0% (2-Class) 96.1% (6-Class) 94.6% (15-Class) RF: 100.0% (2-Class) 85.6% (6-Class) 80.9% (15-Class) DT: 100.0% (2-Class) 84.7% (6-Class) 79.5% (15-Class)	_	_	_	1. High accuracy across binary and multiclass classification. 2. Uses SMOTE for handling class imbalance and PCA for feature reduction. 3. Low computational complexity for real-time deployment.	1. DNN requires significant computational resources. 2. Lower accuracy for certain attack subclasses (e.g., Malware). 3. Limited interpretability of DNN models.
20	2024	[66]	MLP, SVM, Random Forest, Naive Bayes + Neural Network, MobileNetV2, VGG16, InceptionV3, InceptionV3 + LSTM, VGG16 + Dense Layer	Machine Learning, Deep Learning and Hybrid Models	Smart Agriculture	-Dry Beans Dataset (2021) -Soil Type Dataset (2024)	-MLP= 88.0% -Naïve Bayes =77.0% -SVM =93.0% -Random Forest + Neural Network =92.0% -MobileNetV2 =97.0% -VGG16 =95.0% -InceptionV3 =97.0% -InceptionV3 + LSTM =91.0% -VGG16 + Dense Layer =80.0%	_	-MobileNetV2 =97.0% -VGG16 =94.0% -InceptionV3 =95.0% -InceptionV3 + LSTM =91.0% -VGG16 + Dense Layer =70.0%	MLP =89.0% Naïve Bayes =56.0% SVM =91.0% Random Forest + Neural Network =93.0%	1. High classification accuracy (up to 97%). 2. Combines IoT with ML/DL for real-time monitoring. 3. Hybrid models leverage the strengths of multiple algorithms. 4. Effective for resource-constrained environments.	1. Limited generalization to other agricultural datasets. 2. Complex hybrid models may be hard to implement in real-world farming. 3. No security measures for IoT networks (e.g., replay attacks, DoS). 4. Computational overhead for deep learning models.
21	2024	[67]	GAN and CNN	Deep Learning (DL)	IoT Security	collected dataset	Spoof Detection = 94.6% Authentication = 92.4% (all devices), 96.1% (Dragino devices)	Spoof Detection = 88.2%	_	_	1. No hardware / software modifications required for IoT devices. 2. Robust under NLoS conditions. 3. High accuracy in spoof detection and authentication. 4. Utilizes physical-layer imperfections for unique fingerprints.	1. Performance degrades at low SNR (<0 dB). 2. Limited generalization to other modulation schemes. 3. No evaluation under dynamic channel conditions. 4. Computational overhead for deep learning models

Table 1. (Follow the table 1) summarizes related works on anomaly and attack detection in IoT using machine learning and deep learning techniques.

N	Year	Reference	Detection Algorithm	Algorithm Type	Domain	Dataset	Metrics				Advantage	Limitations
							Accuracy (%)	Precision (%)	Recall (%)	F1-score (%)		
22	2024	[68]	Modified Variational Autoencoder (VAE)	Deep Learning (DL)	Green IoT Edge Networks	Public dataset with 18,448 observations (energy, link quality, and transmission parameters)	94.8%	95.2%	95.0%	_	1.Non-intrusive, no external devices needed. 2. High accuracy and reliability. - Focus on dominant features	1. Limited to overconsumption anomalies. 2. Requires short-term diagnostic overhead. 3. Not tested for underconsumption scenarios.
23	2024	[27]	CNN-LSTM and CNN-GRU with Grid Search Optimization	Deep Learning (Hybrid)	IoT Cybersecurity	Kitsune and TON-IoT	Kitsune =99.6% TON-IoT = 99.0%	_	Kitsune =99.3% TON-IoT= 99.0%	_	1. High accuracy and low false alert rates. 2. Combines spatial (CNN) and temporal (LSTM/GRU) feature extraction. 3. Optimized hyperparameters via Grid Search.	1. Computationally intensive due to hybrid architecture. 2. Requires large datasets for training. 3. Limited to known attack types in training data
24	2024	[69]	Improved Mayfly Optimization Algorithm with Hybrid Deep Learning(IMFOHDL-ID)	Deep Learning (Hybrid)	IoT Cybersecurity	BoT-IoT Dataset	TRAPS =98.3% TESPS =98.1%	TRAPS =92.0% TESPS =91.3%	TRAPS =91.7% TESPS =90.9%	TRAPS =91.9% TESPS =91.0%	1. Combines feature selection (IMFO) and hyperparameter tuning (DTOA) . 2. High detection accuracy across multiple attack classes. 3. Effective for IoT-specific challenges like heterogeneity and resource constraints.	1. Computational complexity due to hybrid optimization. 2. Limited evaluation on real-time IoT environments. 3. Dependency on dataset quality (BoT-IoT). 4. No outlier handling mechanism mentioned.
25	2023	[22]	Random Forest, Decision Tree, AdaBoost, ANN, LSTM, Autoencoder	Machine Learning	Smart Home	UNSW BoT-IoT Dataset	RF, DT, AdaBoost =100.0% ANN =95.7%	RF, DT, AdaBoost = 100.0% ANN =98.0%	RF, DT, AdaBoost =100.0% ANN =96.0%	RF, DT, AdaBoost =100.0% ANN =96.0%	1. High accuracy with simple ML models (RF, DT, AdaBoost). 2. Effective for multiclass attack detection. 3. Feature engineering (SMOTE, IQR) improves imbalance handling.	1. ANN underperforms compared to simpler models. 2. Limited to offline dataset (BoT-IoT). 3. No real-time deployment validation. 4. Computational cost of LSTM/Autoencoder not addressed.

© 2026 The Author(s). This article is licensed under CC By 4.0

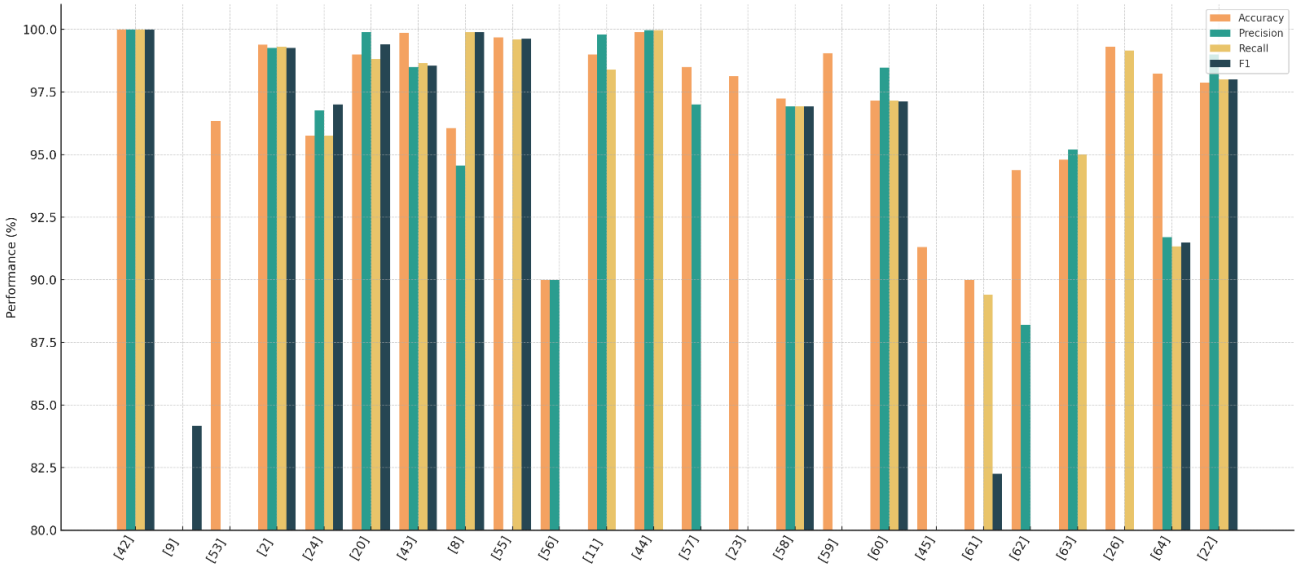


Figure 6. Performance metrics for the various anomaly detection algorithms of the scientific references mentioned in Table 1

ized datasets, albeit in a smaller number of studies. These include CICIoT2023 for industrial environments [18], Route-4-2023 for RPL protocol attacks [14], LDE/CDE for the Medical Internet of Things (IoMT) [3], and the LoRa dataset for physical layer impersonation [21].

Based on this analysis, this field requires a unified assessment framework. This framework should standardize the reporting of key statistical metrics (e.g., accuracy, precision, recall, F1 score, AUC, and FPR), promote transparency regarding data sources and preprocessing steps, and mandate rigorous evaluation across multiple datasets (Cross-dataset Evaluation) to assess the ability of models to generalize across IoT environments and different attack scenarios.

8. IOT SECURITY : OPEN CHALLENGES

The increasing use of the Internet of Things (IoT) in various fields, including transportation networks, smart grids, healthcare, and drones, has raised significant security concerns. The following are the most notable unresolved issues and potential areas for IoT security research:

A. Authentication and Privacy Enhancement

- Drone Security: Research into biometric authentication (physiological/behavioral), natural language processing (NLP), and image-based verification to improve detection and network security [12].
- Hybrid authentication systems: Combining machine learning with programmable metasurfaces such as smart overlays (SIMs) to enhance intrusion detection efficiency [19].

B. Advanced Intrusion Detection Systems (IDS)

- Hybrid Deep Learning Models: To detect asymmetric attacks, such as insider threats and ransomware, HIDS-RPL must be scaled while reducing computational complexity [45].
- Exploratory and graph-based approaches: To address data imbalances and enhance input-output security, accurate tree models must be improved. [17].
- Multiview CNNs and GNNs: These are scalable models designed for large datasets. Distributed frameworks are enhanced by integrating knowledge graphs to handle structured and unstructured data [9].

***C.* Real-time threat detection and response**

- Deep learning for anomaly detection: Improving and developing real-time response systems capable of predicting various attacks [14].
- Enhancing heterogeneous datasets and tests: Using diverse datasets improves adaptability in IoT [14].

D. Federated Learning and Explainable Artificial Intelligence (XAI)

- Federated multitask learning (FMTL): Improving and enhancing model training across multiple tasks in VANETs while preserving privacy [2].
- XAI for Transparency: Detecting privacy threats and improving explainability in intrusion detection by combining federated learning and explainable AI. [11].

E. Integrating Blockchain Technology and Artificial Intelligence

- Smart grid security: The combination of AI and blockchain to combat false data injection,

©2026 The Author(s). This article is licensed under CC By 4.0

topology attacks, and big data vulnerabilities [20].

- Preventing Zero-Day Attacks: Combining SDN, Blockchain, and Deep Learning to Secure IoT Devices from Advanced Threats [5].

F. Optimizing Endpoint Resources

- Lightweight Machine Learning: To detect denial-of-service attacks, models are deployed on endpoint devices (such as the Raspberry Pi) [8].

- Computational Efficiency: Reducing power consumption and response time in intrusion detection systems (IDS) (e.g., via SIM cards and enhanced AIDS systems) [69].

G. Emerging IoT Areas

- Industrial Internet of Things (IIoT): Detection of sensor failures and discovery of innovative AI and IIoT solutions [58].

- New Datasets and Algorithms: Testing models on new datasets while incorporating unsupervised techniques such as CIPMAIDS2023-1 and CIDIDS [62].

H. Explainability and Transparency

- Augmented AI with Reinforcement Learning: To detect IoT intrusions in an explainable manner [4].

9. CONCLUSION AND FUTURE RESEARCH DIRECTIONS

This review was thoroughly subjected to 69 peer-reviewed studies on intelligent anomaly detection in IoT Security published between 2018 and the present. The comparison focused on three main algorithm families: machine learning (ML), Deep Learning (DL), and hybrid/advanced models, which also addressed the accuracy of the reported models, their recall, and F1 score.

Consolidated analysis revealed that ML-based approaches achieved remarkably high precision (99.38%) and recall (98.62%), confirming their robustness and interpretability in lightweight IoT environments. However, their average accuracy (82.92%) was noticeably lower than that of more advanced architectures.Deep learning-based technologies, despite their computational intensity, achieved improved accuracy of 88.88% and demonstrated superior adaptability to complex and high-dimensional Internet of Things traffic, albeit with a slight decrease in recall rate (84.30%) due to data imbalance and over-processing risks. In contrast, the hybrid and combined architectures, which integrate machine learning and deep learning models, outperformed all other categories, achieving an average accuracy of 99.35% and an F1 score of 99.60%, confirming their ability to balance efficiency, scalability, and detection quality.

These results indicate a gradual shift from traditional machine-learning classifiers to hybrid and deep frameworks capable of capturing nonlinear dependencies and time features in IoT data streams. Despite the outstanding performance of these models, deep learning and hybrid systems still face persistent challenges related to the computational cost, energy consumption, and model interpretability, all of which are critical in constrained IoT environments. Therefore, hybrid models that combine ML simplicity with DL robustness, such as CNN–LSTM and Federated Learning-based designs, have emerged as promising research directions for lightweight, adaptive, and privacy-preserving anomaly detection.

To address these challenges and enhance and improve the security of IoT, future research should focus on the following three strategic areas:

1- Algorithmic Optimization involves creating explainable and resource-efficient models that combine Federated Learning and Explainable AI (XAI) to improve privacy and interpretability, while preserving high detection accuracy.

2- Architectural Integration: In large-scale IoT ecosystems, utilizing Edge/Fog computing for localized, real-time detection and blockchain for tamper-proof communication can reduce the latency and bandwidth overhead.

3- Standardization and Collaboration by establishing unified datasets, performance benchmarks, and evaluation protocols through interdisciplinary collaboration among academia, industry, and government to ensure reproducibility, transparency, and global security standards.

In conclusion, no single algorithmic paradigm provides a universal solution for the IoT anomaly detection. The future of secure IoT environments will depend on hybrid, federated, and explainable AI frameworks that harmonize accuracy, transparency, and scalability, paving the way for resilient, trustworthy, and energy-efficient IoT security systems over the next decade.

REFERENCES

[1] N. A. Al-Shaibany, T. A. B. Al-Sofi, G. H. Al-Gaphari, Nagi, and A. Al-Shaibany, “A model for enhancing the information security management systems in yemen banks,” 2023, Online. [Online]. Available: https://jpurnals.su.edu.ye/jast.

[2] C. J. Chandnani, V. Agarwal, S. C. Kulkarni, A. Aren, G. B. Amali, and K. Srinivasan, “A physics based hyper parameter optimized federated multi-layered deep learning model for intrusion detection in iot networks,” *IEEE Access*, 2025. DOI: 10.1109/ACCESS.2025.3535952.

©2026 The Author(s). This article is licensed under CC By 4.0

[3] P. L. S. Jayalaxmi, R. Saha, G. Kumar, M. Conti, and T. H. Kim, "Machine and deep learning solutions for intrusion detection and prevention in iots: A survey," *IEEE Access*, vol. 10, pp. 121 173–121 192, 2022. DOI: 10.1109/ACCESS.2022.3220622.

[4] M. Saied, S. Guirguis, and M. Madbouly, "A comparative study of using boosting-based machine learning algorithms for iot network intrusion detection," *Int. J. Comput. Intell. Syst.*, vol. 16, no. 1, 2023. DOI: 10.1007/s44196-023-00355-x.

[5] A. Ghaffari, N. Jelodari, S. Pouralish, N. Derakhshanfard, and B. Arasteh, "Securing internet of things using machine and deep learning methods: A survey," *Clust. Comput.*, vol. 27, no. 7, pp. 9065–9089, 2024. DOI: 10.1007/s10586-024-04509-0.

[6] M. A. Al-Hadi, G. H. Al-Gaphari, I. A. Al-Baltah, and F. B. Julian, "A promising smart healthcare monitoring model based on internet of things and deep learning techniques," *Sana'a Univ. J. Appl. Sci. Technol.*, vol. 2, no. 2, pp. 147–153, 2024. DOI: 10.59628/jast.v2i2.811.

[7] T. Al-Shurbaji et al., "Deep learning-based intrusion detection system for detecting iot botnet attacks: A review," *IEEE Access*, 2025. DOI: 10.1109/ACCESS.2025.3526711.

[8] E. Altulaihan, M. A. Almaiah, and A. Aljughaiman, "Anomaly detection ids for detecting dos attacks in iot networks based on machine learning algorithms," *Sensors*, vol. 24, no. 2, 2024. DOI: 10.3390/s24020713.

[9] M. Li, Y. Qiao, and B. Lee, "A comparative analysis of single and multi-view deep learning for cybersecurity anomaly detection," *IEEE Access*, 2025. DOI: 10.1109/ACCESS.2025.3564066.

[10] I. Ullah and Q. H. Mahmoud, "Design and development of a deep learning-based model for anomaly detection in iot networks," *IEEE Access*, vol. 9, pp. 103 906–103 926, 2021. DOI: 10.1109/ACCESS.2021.3094024.

[11] A. M. Almasabi, M. Khemakhem, F. E. Eassa, A. A. Abi Sen, A. B. Alkhodre, and A. Harbaoui, "A smart framework to detect threats and protect data of iot based on machine learning," *IEEE Access*, vol. 12, pp. 176 833–176 844, 2024. DOI: 10.1109/ACCESS.2024.3498603.

[12] A. A. Alzubaidi, "Systematic literature review for detecting intrusions in unmanned aerial vehicles using machine and deep learning," *IEEE Access*, 2025. DOI: 10.1109/ACCESS.2025.3552329.

[13] S. H. Mohammed et al., "A review on the evaluation of feature selection using machine learning for cyber-attack detection in smart grid," *IEEE Access*, vol. 12, pp. 44 023–44 042, 2024. DOI: 10.1109/ACCESS.2024.3370911.

[14] K. S. Awaisi, Q. Ye, and S. Sampalli, "A survey of industrial aiot: Opportunities, challenges, and directions," *IEEE Access*, vol. 12, pp. 96 946–96 996, 2024. DOI: 10.1109/ACCESS.2024.3426279.

[15] S. F. Chevtchenko et al., "Anomaly detection in industrial machinery using iot devices and machine learning: A systematic mapping," *IEEE Access*, vol. 11, pp. 128 288–128 305, 2023. DOI: 10.1109/ACCESS.2023.3333242.

[16] M. A. Khatun, S. F. Memon, C. Eising, and L. L. Dhirani, "Machine learning for healthcare-iot security: A review and risk mitigation," *IEEE Access*, vol. 11, pp. 145 869–145 896, 2023. DOI: 10.1109/ACCESS.2023.3346320.

[17] N. Mishra and S. Pandya, "Internet of things applications, security challenges, attacks, intrusion detection, and future visions: A systematic review," *IEEE Access*, 2021. DOI: 10.1109/ACCESS.2021.3073408.

[18] M. A. Al-Garadi, A. Mohamed, A. K. Al-Ali, X. Du, I. Ali, and M. Guizani, "A survey of machine and deep learning methods for internet of things (iot) security," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 3, pp. 1646–1685, 2020. DOI: 10.1109/COMST.2020.2988293.

[19] S. H. Rafique, A. Abdallah, N. S. Musa, and T. Murugan, "Machine learning and deep learning techniques for internet of things network anomaly detection—current research trends," *Sensors*, 2024. DOI: 10.3390/s24061968.

[20] K. K. Eren, K. Kucuk, F. Ozyurt, and O. H. Alhazmi, "Simple yet powerful: Machine learning-based iot intrusion system with smart preprocessing and feature generation rivals deep learning," *IEEE Access*, 2025. DOI: 10.1109/ACCESS.2025.3547642.

[21] M. M. Inuwa and R. Das, "A comparative analysis of various machine learning methods for anomaly detection in cyber attacks on iot networks," *Internet Things*, vol. 26, 2024. DOI: 10.1016/j.iot.2024.101162.

[22] N. Sarwar, I. S. Bajwa, M. Z. Hussain, M. Ibrahim, and K. Saleem, "Iot network anomaly detection in smart homes using machine learning," *IEEE Access*, vol. 11, pp. 119 462–119 480, 2023. DOI: 10.1109/ACCESS.2023.3325929.

[23] A. Houkan et al., "Enhancing security in industrial iot networks: Machine learning solutions for feature selection and reduction," *IEEE Access*, 2024. DOI: 10.1109/ACCESS.2024.3481459.

[24] T. Zhukabayeva, Z. Ahmad, A. Adamova, N. Karabayev, Y. Mardenov, and S. Satybaldina, "Penetration testing and machine learning-driven cybersecurity framework for iot and smart city wireless networks," *IEEE Access*, 2025. DOI: 10.1109/ACCESS.2025.3569965.

[25] U. Shahid, M. Z. Hussain, M. Z. Hasan, A. Haider, J. Ali, and J. Altaf, "Hybrid intrusion detection system for rpl iot networks using machine learning and deep learning," *IEEE Access*, vol. 12, pp. 113 099–113 112, 2024. DOI: 10.1109/ACCESS.2024.3442529.

[26] I. Ullah, A. Ullah, and M. Sajjad, "Towards a hybrid deep learning model for anomalous activities detection in internet of things networks," *Internet Things*, vol. 2, no. 3, pp. 428–448, 2021. DOI: 10.3390/iot2030022.

[27] M. Maaz, G. Ahmed, A. S. Al-Shamayleh, A. Akhunzada, S. Siddiqui, and A. H. Al-Ghushami, "Empowering iot resilience: Hybrid deep learning techniques for enhanced security," *IEEE Access*, 2024. DOI: 10.1109/ACCESS.2024.3482005.

[28] S. Vashi, J. Ram, J. Modi, S. Verma, and C. Prakash, "Internet of things (iot): A vision, architectural elements, and security issues," in *Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud (I-SMAC)*, 2017, pp. 492–496. DOI: 10.1109/I-SMAC.2017.8058399.

©2026 The Author(s). This article is licensed under CC By 4.0

[29] M. Bilal, *A review of internet of things architecture, technologies and analysis smartphone-based attacks against 3d printers*, Incomplete reference: publication details missing.

[30] W. Kassab and K. A. Darabkh, "A–z survey of internet of things: Architectures, protocols, applications, recent advances, future directions and recommendations," *J. Netw. Comput. Appl.*, vol. 163, 2020. DOI: 10.1016/j.jnca.2020.102663.

[31] F. Wortmann and K. Flüchter, "Internet of things: Technology and value added," *Bus. & Inf. Syst. Eng.*, 2015. DOI: 10.1007/s12599-015-0383-3.

[32] S. Bandyopadhyay, P. Balamuralidhar, and A. Pal, "Interoperation among iot standards," *J. ICT Stand.*, vol. 1, no. 2, pp. 253–270, 2013. DOI: 10.13052/jicts2245-800X.12a9.

[33] S. N. Swamy, D. Jadhav, and N. Kulkarni, "Security threats in the application layer in iot applications," in *Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud (I-SMAC)*, 2017, pp. 477–480. DOI: 10.1109/I-SMAC.2017.8058395.

[34] M. El Hanine, A. El-Yahyaoui, and R. Es-Sadaoui, "Three layer iot architecture: Attacks and security mechanisms," in *Proceedings of the 11th International Conference on Future Internet of Things and Cloud (FiCloud)*, 2024, pp. 32–38. DOI: 10.1109/FiCloud62933.2024.00014.

[35] Y. Khan, M. B. M. Su'ud, M. M. Alam, S. F. Ahmad, N. A. Salim, and N. Khan, "Architectural threats to security and privacy: A challenge for internet of things (iot) applications," *Electronics*, 2023. DOI: 10.3390/electronics12010088.

[36] M. A. Obaidat, S. Obeidat, J. Holst, A. Al Hayajneh, and J. Brown, "A comprehensive and systematic survey on the internet of things: Security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures," *Computers*, vol. 9, no. 2, 2020. DOI: 10.3390/computers9020044.

[37] S. Deep, X. Zheng, A. Jolfaei, D. Yu, P. Ostovari, and A. K. Bashir, *A survey of security and privacy issues in the internet of things from the layered context*, arXiv preprint, 2020. [Online]. Available: http://arxiv.org/abs/1903.00846.

[38] A. A. Alsabri and M. A. Al-Hadi, "A hybrid cnn-blstm model for phishing attack detection using deep learning to strengthen internet security," *Sana'a Univ. J. Appl. Sci. Technol.*, vol. 3, no. 4, pp. 964–972, 2025. DOI: 10.59628/jast.v3i4.1822.

[39] H. Mrabet, S. Belguith, A. Alhomoud, and A. Jemai, "A survey of iot security based on a layered architecture of sensing and data analysis," *Sensors*, 2020. DOI: 10.3390/s20133625.

[40] D. Singh, G. Tripathi, and A. Jara, "Secure layers based architecture for internet of things," in *IEEE World Forum on Internet of Things (WF-IoT)*, 2015, pp. 321–326. DOI: 10.1109/WF-IoT.2015.7389074.

[41] G. Sharma, S. Vidalis, N. Anand, C. Menon, and S. Kumar, "A survey on layer-wise security attacks in iot: Attacks, countermeasures, and open issues," *Electronics*, 2021. DOI: 10.3390/electronics10192365.

[42] A. N. Ozalp, Z. Albayrak, M. Cakmak, and E. Ozdogan, "Layer-based examination of cyber-attacks in iot," in *Proceedings of the 4th International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, 2022. DOI: 10.1109/HORA55278.2022.9800047.

[43] P. K. Tiwari et al., "A secure and robust machine learning model for intrusion detection in internet of vehicles," *IEEE Access*, 2025. DOI: 10.1109/ACCESS.2025.3532716.

[44] A. Berguiga, A. Harchay, and A. Massaoudi, "Hids-rpl: A hybrid deep learning-based intrusion detection system for rpl in internet of medical thing networks," *IEEE Access*, 2025. DOI: 10.1109/ACCESS.2025.3545918.

[45] C. Hazman, A. Guezzaz, S. Benkirane, and M. Azrour, "Enhanced ids with deep learning for iot-based smart cities security," *Tsinghua Sci. Technol.*, vol. 29, no. 4, pp. 929–947, 2024. DOI: 10.26599/TST.2023.9010033.

[46] P. Russell, M. A. Elsayed, B. Nandy, N. Seddigh, and N. Zincir-Heywood, "On the fence: Anomaly detection in iot networks," in *Proceedings of the IEEE/IFIP Network Operations and Management Symposium (NOMS)*, 2023. DOI: 10.1109/NOMS56928.2023.10154271.

[47] A. Huc and D. Trcek, "Anomaly detection in iot networks: From architectures to machine learning transparency," *IEEE Access*, vol. 9, pp. 60 607–60 616, 2021. DOI: 10.1109/ACCESS.2021.3073785.

[48] S. Panja, S. Das, and A. Pal, "Assessing the effectiveness of anomaly detection in iot data streams with machine learning," in *Proceedings of the 4th International Conference on Computer, Communication, Control and Information Technology (C3IT)*, 2024. DOI: 10.1109/C3IT60531.2024.10829458.

[49] S. S. Hussain, M. F. A. Razak, and A. Firdaus, "Deep learning based hybrid analysis of malware detection and classification: A recent review," *J. Cyber Secur. Mobil.*, 2024. DOI: 10.13052/jcsm2245-1439.1314.

[50] *Breast cancer risk factors and prediction using machine learning*, Online resource, bibliographic details unavailable.

[51] S. Golestani and D. Makaroff, "Device-specific anomaly detection models for iot systems," in *2024 IEEE Conference on Communications and Network Security (CNS)*, 2024. DOI: 10.1109/CNS62487.2024.10735608.

[52] M. Algabri, E. N. A. Abu Huliqah, M. Ghurab, A. A. G. Al-Khulaidi, and G. H. Al-Gaphari, "Fake news detection on social media: Review of literature," *Sana'a Univ. J. Appl. Sci. Technol.*, vol. 2, no. 1, pp. 7–15, 2024. DOI: 10.59628/jast.v2i1.369.

[53] S. A. R. and J. Katiravan, "Enhancing anomaly detection and prevention in internet of things (iot) using deep neural networks and blockchain based cyber security," *Sci. Reports*, vol. 15, no. 1, 2025. DOI: 10.1038/s41598-025-04164-4.

[54] T. Golomb, Y. Mirsky, and Y. Elovici, "Ciota: Collaborative anomaly detection via blockchain," in *Internet Society Symposium on Security and Privacy*, 2018. DOI: 10.14722/diss.2018.23003.

[55] Y. R. Siwakoti, D. B. Rawat, and S.-H. Loke, "Adgam: Anomaly detection in iot using generative ai models," in *SPIE Proceedings*, 2025. DOI: 10.1117/12.3058632.

[56] A. J. Aparcana-Tasayco, X. Deng, and J. H. Park, "A systematic review of anomaly detection in iot security: Towards quantum machine learning approach," *The Eur. Phys. J. Quantum Technol.*, 2025. DOI: 10.1140/epjqt/s40507-025-00414-6.

©2026 The Author(s). This article is licensed under CC By 4.0

[57] M. Hdaib, S. Rajasegarar, and L. Pan, "Quantum deep learning-based anomaly detection for enhanced network security," *Quantum Mach. Intell.*, vol. 6, no. 1, 2024. DOI: 10.1007/s42484-024-00163-2.

[58] G. Zachos, G. Mantas, K. Porfyrakis, J. M. C. S. Bastos, and J. Rodriguez, "Anomaly-based intrusion detection for iomt networks: Design, implementation, dataset generation and ml algorithms evaluation," *IEEE Access*, 2025. DOI: 10.1109/ACCESS.2025.3547572.

[59] H. Hakami, M. Faheem, and M. B. Ahmad, "Machine learning techniques for enhanced intrusion detection in iot security," *IEEE Access*, vol. 13, pp. 31 140–31 158, 2025. DOI: 10.1109/ACCESS.2025.3542227.

[60] M. M. Aborokbah, "A novel intrusion detection model for enhancing security in smart city," *IEEE Access*, vol. 12, pp. 107 431–107 444, 2024. DOI: 10.1109/ACCESS.2024.3438619.

[61] M. F. Saiyedand and I. Al-Anbagi, "Deep ensemble learning with pruning for ddos attack detection in iot networks," *IEEE Trans. on Mach. Learn. Commun. Netw.*, vol. 2, pp. 596–616, Apr. 2024. DOI: 10.1109/TMLCN.2024.3395419.

[62] M. Ali, M. Shahroz, M. F. Mushtaq, S. Alfarhood, M. Safran, and I. Ashraf, "Hybrid machine learning model for efficient botnet attack detection in iot environment," *IEEE Access*, vol. 12, pp. 40 682–40 699, 2024. DOI: 10.1109/ACCESS.2024.3376400.

[63] H. Liao et al., "A survey of deep learning technologies for intrusion detection in internet of things," *IEEE Access*, vol. 12, pp. 4745–4761, 2024. DOI: 10.1109/ACCESS.2023.3349287.

[64] M. M. Khan and M. Alkhathami, "Anomaly detection in iot-based healthcare: Machine learning for enhanced security," *Sci. Reports*, vol. 14, no. 1, 2024. DOI: 10.1038/s41598-024-56126-x.

[65] S. Sadhwani, U. K. Modi, R. Muthalagu, and P. M. Pawar, "Smartsentry: Cyber threat intelligence in industrial iot," *IEEE Access*, vol. 12, pp. 34 720–34 740, 2024. DOI: 10.1109/ACCESS.2024.3371996.

[66] M. Aldossary, H. A. Alharbi, and C. A. Ul Hassan, "Internet of things (iot)-enabled machine learning models for efficient monitoring of smart agriculture," *IEEE Access*, vol. 12, pp. 75 718–75 734, 2024. DOI: 10.1109/ACCESS.2024.3404651.

[67] D. Huang and A. Al-Hourani, "Physical layer spoof detection and authentication for iot devices using deep learning methods," *IEEE Trans. on Mach. Learn. Commun. Netw.*, vol. 2, pp. 841–854, Jun. 2024. DOI: 10.1109/TMLCN.2024.3417806.

[68] A. Shahnejat Bushehri, A. Amirnia, A. Belkhiri, S. Keivanpour, F. G. De Magalhaes, and G. Nicolescu, "Deep learning-driven anomaly detection for green iot edge networks," *IEEE Trans. on Green Commun. Netw.*, vol. 8, no. 1, pp. 498–513, Mar. 2024. DOI: 10.1109/TGCN.2023.3335342.

[69] S. Duraibi and A. M. Alashjaee, "Enhancing cyberattack detection using dimensionality reduction with hybrid deep learning on internet of things environment," *IEEE Access*, vol. 12, pp. 84 752–84 762, 2024. DOI: 10.1109/ACCESS.2024.3411612.

©2026 The Author(s). This article is licensed under CC By 4.0