Computers, Materials & Continua

Tech Science Press

Doi:10.32604/cmc.2025.064027

REVIEW

A Detailed Review of Current AI Solutions for Enhancing Security in Internet of Things Applications

Arshiya Sajid Ansari[1,*], **Ghadir Altuwaijri**[2], **Fahad Alodhyani**[1],
Moulay Ibrahim El-Khalil Ghembaza[3], **Shahabas Manakunnath Devasam Paramb**[3] and
Mohammad Sajid Mohammadi[3]

[1]Department of Information Technology, College of Computer and Information Sciences, Majmaah University, Al-Majmaah, 11952, Saudi Arabia

[2]Department of Computer Engineering, College of Computer and Information Sciences, Majmaah University, Al-Majmaah, 11952, Saudi Arabia

[3]Department of Computer Science, College of Engineering and Information Technology, Onaizah Colleges, Qassim, 56447, Saudi Arabia

*Corresponding Author: Arshiya Sajid Ansari. Email: ar.ansari@mu.edu.sa

Received: 02 February 2025; Accepted: 09 April 2025; Published: 19 May 2025

ABSTRACT: IoT has emerged as a game-changing technology that connects numerous gadgets to networks for communication, processing, and real-time monitoring across diverse applications. Due to their heterogeneous nature and constrained resources, as well as the growing trend of using smart gadgets, there are privacy and security issues that are not adequately managed by conventional security measures. This review offers a thorough analysis of contemporary AI solutions designed to enhance security within IoT ecosystems. The intersection of AI technologies, including ML, and blockchain, with IoT privacy and security is systematically examined, focusing on their efficacy in addressing core security issues. The methodology involves a detailed exploration of existing literature and research on AI-driven privacy-preserving security mechanisms in IoT. The reviewed solutions are categorized based on their ability to tackle specific security challenges. The review highlights key advancements, evaluates their practical applications, and identifies prevailing research gaps and challenges. The findings indicate that AI solutions, particularly those leveraging ML and blockchain, offer promising enhancements to IoT privacy and security by improving threat detection capabilities and ensuring data integrity. This paper highlights how AI technologies might strengthen IoT privacy and security and offer suggestions for upcoming studies intended to address enduring problems and improve the robustness of IoT networks.

KEYWORDS: Security in IoT applications; privacy-preserving; blockchain; AI-driven security mechanisms

1 Introduction

The IoT a network of networked devices, is one of the most widely utilized technologies of the contemporary era, varied parts that enable intelligent devices and services to identify, gather, share, and analyze data, comprises smart devices that gather and exchange data, such as RFID, accelerometers, watches, refrigerators, smoke alarms, heartbeat monitors, phones, etc. [1]. The IoT concept has made it feasible for devices to connect at higher degrees of integrity, security, accessibility, scalability, interoperability, and availability. Attackers can use a variety of techniques to target various parts of the system and achieve different objectives when attacking IoT devices. Among these is the application of AI to protect IoT systems from intrusions [2].

Cyber security is one of the most crucial issues in an IoT ecosystem in smart cities. In particular, some of the present difficulties include preventing malware attacks on edge devices, restricting unauthorized access, and preserving private correspondence. Several academic publications propose automated methods for ensuring IoT security in terms of anomaly detection, fault diagnostics, and virus identification that make use of ML models [3]. It functions as a technological seismic event that occurs at the appropriate moment, enhancing human welfare and well-being. As AI develops at an exponential rate, ML, neural networks, and other technologies can process data quickly and produce meaningful choices [4]. The IoT uses information of things as a paradigm for connecting people and peripherals to the internet. Peripherals, such as intelligent automobiles, smart cars, and smart homes, can speak with one another. In several industries, the IoT provides options for efficient production optimization. Among the problems with IoT are hardware capabilities, GIS visualization, centralization, big data analytics, security, and networking [5].

The advantages, possibilities, and difficulties of combining AI with IoT in various applications and IoT systems that are user-cantered and use a bidirectional processing system for human knowledge, communication networks for observing outside experiences, and an arbitration system for large data analytics that is driven by uncertainty [6]. Applications of blockchain technology for AI are identified, along with open research issues, blockchain applications are summarized, and platform protocols focused on AI domains are addressed [7]. The use of smart technologies has increased dramatically, which has improved secure wireless transfers, dependable connectivity, and efficient processing. Nevertheless, there are yet several computational and communication hazards associated with data augmentation in networks [8]. However, there is a concentration paid to automated multi-homing solutions for the management, processing, and security of massive data. Furthermore, using automated and AI-based smart systems for information security and processing in multihoming networks can reduce a variety of security and management challenges by enhancing multiple network clustering, data processing, data management, and large-scale data distributions [9]. Big data has been created because of the advancement of innovative technologies like IoT in conjunction with cloud computing storage capacities. This resulted in a vast amount of data that people are producing through IoT-based gadgets and sensors, which is altering society and industry in many ways. However, asymmetric and symmetric data distributions have been used to classify these massive data in practical applications [10].

Effectively outlines the significance of the IoT and its associated security challenges, highlighting that interconnected devices enhance data sharing and analysis. However, the transition between discussing IoT applications and BC integration. While AI's role in securing IoT systems through advanced threat detection is acknowledged, the shift to BC applications lacks clarity in terms of these two technologies complementing each other in real-world IoT environments, it also highlights the potential benefits of AI and BC in addressing IoT security. It does not explore the practical challenges of implementing these solutions, such as energy consumption, cost, and scalability [11].

Security challenges: AI, BC, and IoT technologies play crucial roles in addressing security challenges within interconnected environments. AI enhances security by enabling advanced threat detection through ML algorithms that analyze vast amounts of data, identify patterns, and predict potential attacks in real time [12]. Blockchain adds an extra layer of security through its decentralized and immutable ledger, ensuring transparent and temper-proof records for transactions and communications, which is vital in securing IoT networks. IoT devices, being inherently vulnerable due to their widespread and often unprotected nature, benefit from AI-driven security measures and blockchain ability to secure data transmission and storage, reducing the risk of unauthorized access and data breaches. Together, these technologies can create more resilient, self-sustaining security frameworks for IoT ecosystems by combining AI adaptability, BC trust and transparency, and IoT real-time connectivity, thereby ensuring stronger protection against emerging cyber-attacks.

A thorough investigation of modern AI technologies targeted at improving security in IoT applications is the goal of the review paper. By systematically investigating IoT security issues with blockchain and ML, the review aims to assess how different AI-driven techniques manage fundamental concerns like threat detection, data interiority, and privacy. Additionally, the paper aims to categorize these solutions based on their effectiveness, highlight key advancements, and identify prevailing research gaps and challenges, providing insights into future research directions that could support IoT environments against emerging security threats.

Contribution of the Study

- To evaluate the integration of AI including ML and BC technologies, into the security framework of the IoT. By addressing the inherent challenges of IoT's heterogeneous and resource-constrained devices, AI-driven solutions significantly improve the protection of sensitive data and ensure secure communication across IoT systems. The contribution of AI, particularly in areas such as threat detection, anomaly detection, and privacy-preserving mechanisms are highlighted as key advancements that strengthen IoT security.
- To explore the benefits of BC integration in IoT ecosystems, it highlights its tamper-proof nature, which ensures data integrity, secure transactions, and decentralized control integration is particularly beneficial in applications like healthcare, finance, and smart cities that require high data interiority.
- To identify areas for further research and make recommendations for improving IoT security. It suggests advanced AI techniques like DL and reinforcement learning to adapt to dynamic threats, improving scalability and investigating AI role in real-time intrusion detection and predictive security analytics.
- To suggest that AI-driven IoT security solutions can play a pivotal role in enhancing educational security systems by monitoring and guiding sensitive student data, controlling access to online platforms, and preventing cyberattacks. By integrating BC for data verification and ML for anomaly detection, educational institutions can create more secure and resilient digital environments for students and faculty alike.
- To highlight the effectiveness of AI solutions in improving IoT performance matrices demonstrate improved accuracy, precision, recall, and f1-score. By utilizing ML algorithms and BC, IoT system can detect potential security breaches with greater accuracy, improve detection rates and reduce false positives, thereby enhancing the efficiency of IoT networks.

The remainder of the paper is as follows: Section 2 presents related works. There was a comprehensive methodology in Section 3. A result analysis is provided in Section 4, and a conclusion is presented in Section 5.

2 Related Works

2.1 IoT Paradigm

The study [13] described IoT as an internet communication and data exchange network made up of physically connected objects. Real-time task automation and monitoring were made possible by the devices' capacity to exchange and gather data. They usually contain electronics, applications, software, and a variety of other technologies. The main objective of the IoT was to seamlessly incorporate technology to increase efficiency, make wiser decisions, and give people more automated, pleasant experiences.

It has already been used for many purposes, including smart grids production lines, and product supply chains, demonstrating how it was incorporated into various aspects of society. Future modern applications of IoT technology, such as smart grids, smart cities, smart industries, and smart healthcare, were expected to be supported by IoT communication infrastructure [14] and the current condition of IoT architecture device shown in Fig. 1.

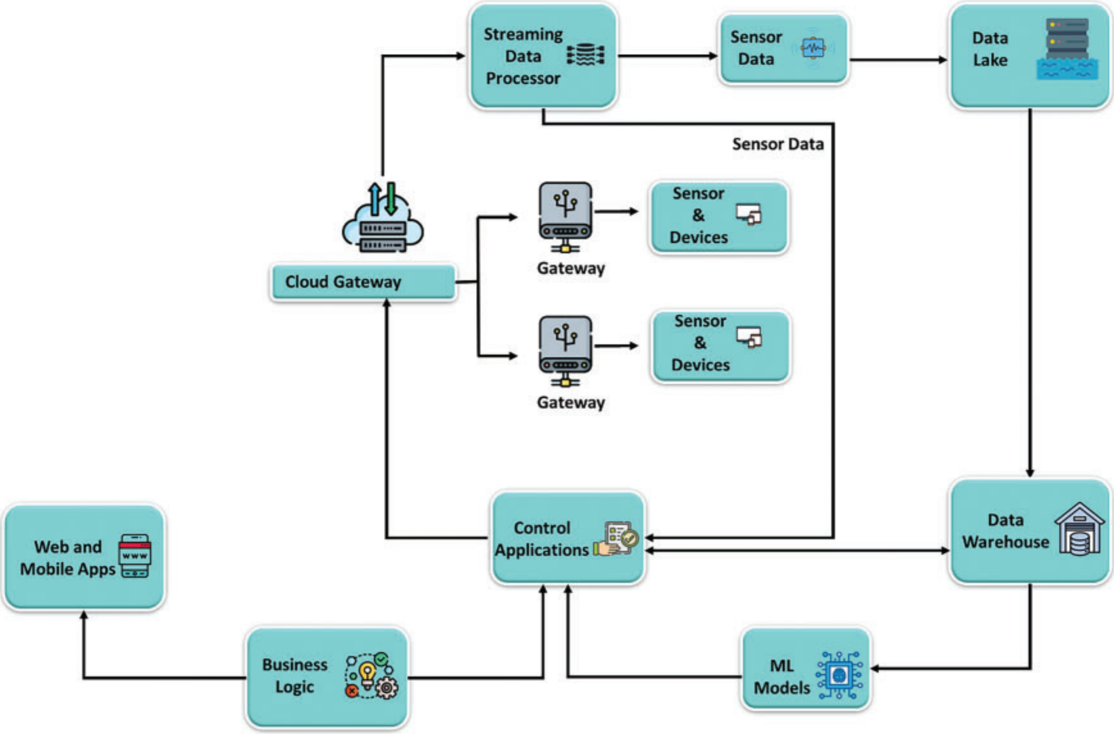


Figure 1: IoT architecture

Research [15] determined that IoT applications refer to the diverse range of practical uses and implementations of IoT technologies across various sectors and industries. It allows for automation, real-time monitoring, and better decision-making. Smart home systems, which let users manage lights and appliances from a distance, and medical devices that track patients' vital signs are a couple of examples of IoT applications. They aimed to create smart cities that optimize energy use and traffic flow as well as industrial automation that manufactures productivity. Through the incorporation of IoT technology into routine procedures, these applications are intended to improve overall quality of life, convenience, and efficiency.

The essential facets of society that comprise IoT applications were depicted in Fig. 2. The smart city was equipped with a wide range of instruments and technology that, when used for different purposes, enhanced people's lives. IoT was changing the demands on smart cities' security and revolutionizing the sector of education in the study [16].

The components of the IoT applications were categorized into several key areas: Smart water and energy management including water tap monitoring, population and leak detection in tanks, early identification of flooding and sewerage issues, and optimizing smart power regulation based on usage in [17]. In smart health, hospitalize utilizes sensor-based medical diagnostics, fall detection in residential settings, intelligent patient health monitoring, and environmental control of medicinal refrigerators [18].

In Agriculture, clever management of climate conditions in the greenhouse and controlled water levels in the field were key applications [19]. The home category allows for remote control of appliances, intelligent data exchange across devices to maximize performance, astute energy conversion, and the identification of intrusions with responsive self-prevention measures [20].

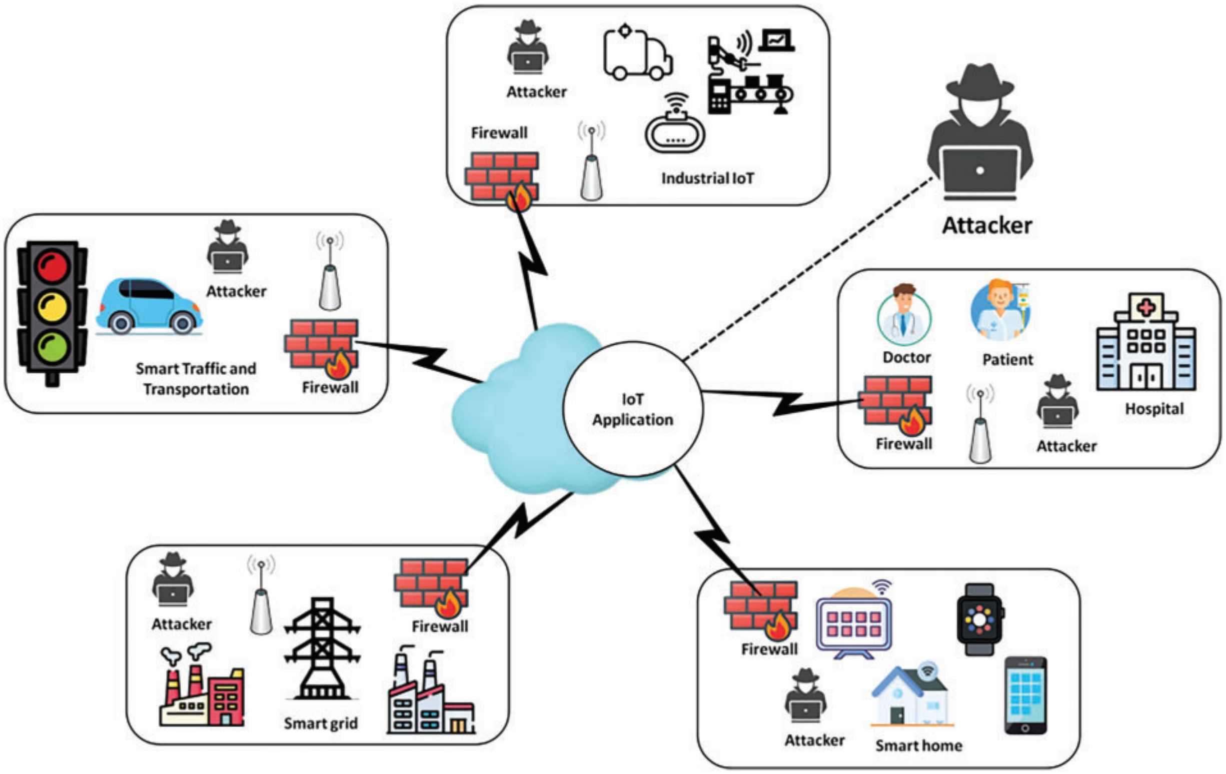


Figure 2: IoT applications

Transport innovations include smart parking, traffic monitoring, street smart light monitoring, adaptive route planning for garbage collection, intelligent roadways that can monitor traffic and accidents, and smart logistics systems [21]. In the environment category, applications focus on intelligent air pollution level monitoring, detection of fire outbreaks, and identification of landslides and earthquakes [22].

2.2 Difficulties in Integrating Blockchain Technology with IoT Network

IoT's capabilities and range of applications might be expanded by the incorporation of Blockchain technology. Nevertheless, because each network technology has unique constraints, integrating many technologies might present some difficulties [23]. Technology integration could be impacted by the limitations of the IoT, such as the vast volume of data involved in the network [24]. Blockchain integration with IoT networks presented several challenges, including smart contracts, scalability, storage, inexperience, and legal issues [25]. Although storage and scalability were already blockchain issues, they became even more problematic in the context of the IoT [26]. IoT networks have a lot of nodes, and blockchain technology does not scale well in networks with a lot of nodes. Despite the modest storage capacity of IoT devices, the distributed ledger has a memory that rises with the number of nodes over time. A significant barrier to integrating blockchain with IoT was a lack of competence, as IoT was used in every industry [27]. A common misconception was that blockchain technology was exclusive to Bitcoin. The fact that blockchain was a novel technology that links with other nations without any established legal or regulatory precedents was a significant challenge for service providers and manufacturers. The difficulty is also a significant barrier to blockchain and IoT integration.

Although IoT has helped users, there were disadvantages as well. Experts and security professionals on the list say that privacy issues and cyber security were the main concerns. These two present a serious challenge for both public and private organizations. The vulnerabilities of IoT technologies have been exposed by frequent, widely reported cyber security breaches. This risk arises from the interconnectedness of the IoT, which makes anonymous and untrustworthy content available and demands the creation of novel security measures. A range of research areas regarding the proliferation of IoT devices are depicted in Fig. 3. IoT devices are difficult to secure and react adversely to standard security methods because of their modest processors. Location and power resources were crucial factors to consider while putting security measures into action. For linked, or smart, cars, mobility is a major problem.

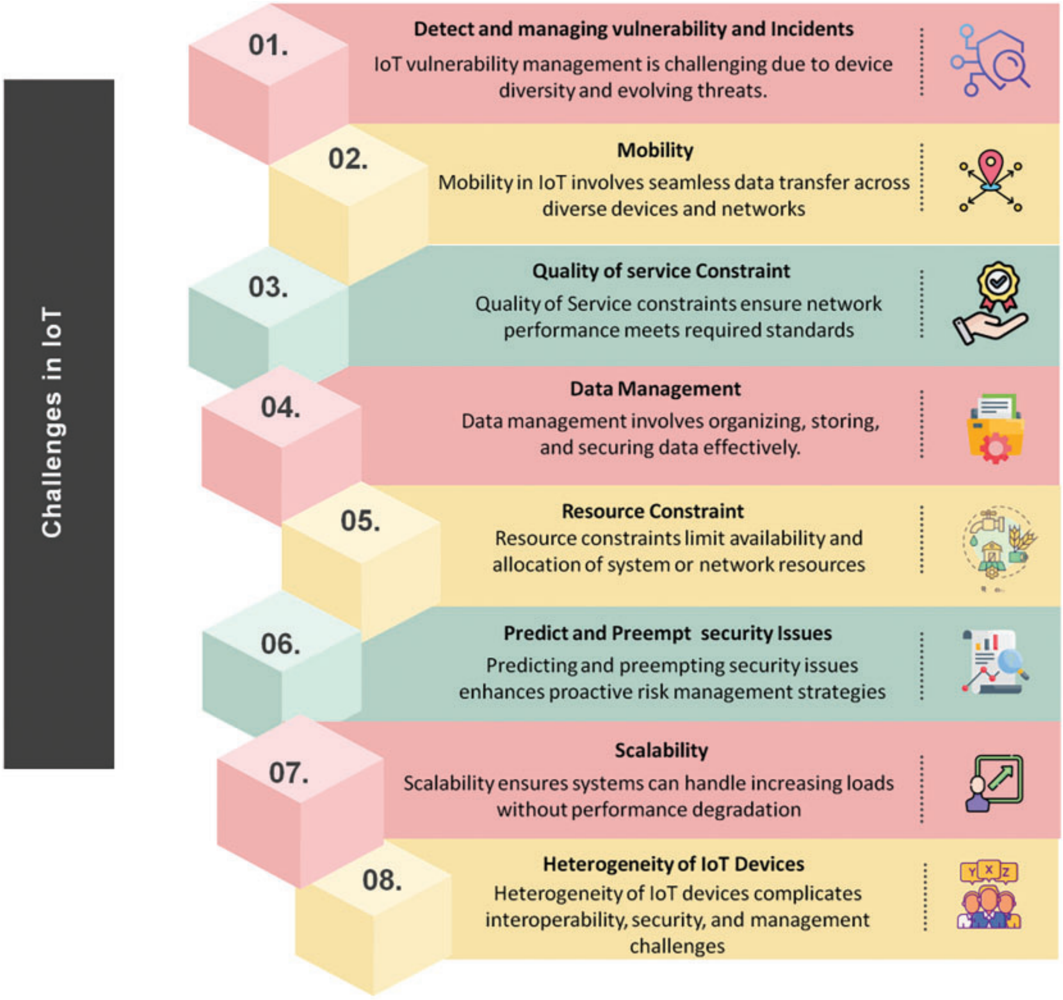

Challenges in IoT
01.
Detect and managing vulnerability and Incidents
IoT vulnerability management is challenging due to device diversity and evolving threats.
02.
Mobility
Mobility in IoT involves seamless data transfer across diverse devices and networks
03.
Quality of service Constraint
Quality of Service constraints ensure network performance meets required standards
04.
Data Management
Data management involves organizing, storing, and securing data effectively.
05.
Resource Constraint
Resource constraints limit availability and allocation of system or network resources
06.
Predict and Preempt security Issues
Predicting and preempting security issues enhances proactive risk management strategies
07.
Scalability
Scalability ensures systems can handle increasing loads without performance degradation
08.
Heterogeneity of IoT Devices
Heterogeneity of IoT devices complicates interoperability, security, and management challenges
Y
X
Z

Figure 3: IoT challenges

There was no uniformity in the security protocols. Every gadget has a different solution based on the supplier. Additionally, protocols were not standardized since a variety of devices make up the IoT network. Establishing trust was easier in applications with less mobility than in linked cars that move quickly. Cost, power, and space limits are only a few of the many aspects of IoT that present serious resource constraints for IoT devices.

2.3 The Advantages of IoT

IoT applications offer previously unattainable cost reductions, automation, data-driven operations, efficiency, and resource savings. The advantages of IoT are in various areas like healthcare, agriculture, education, finance, etc. IoT-capable improved product quality, growth, output, cost savings, agility, and cleaner practices were just a few of the many advantages that smart agriculture provides. Several studies have examined the benefits of deploying the IoT [28–30].

- **Superior efficiency:** Agriculture was a competitive industry. Farmers must increase their productivity despite poor soil conditions, a declining amount of available land, and rising weather variability [31]. Real-time monitoring of farms and environmental factors is made possible by IoT-based agriculture. Additionally, IoT-based agricultural solutions were adding automation, such as automated harvesting, fertilization, and irrigation.
- **Reduced resources:** Many IoT-based agricultural solutions were designed to optimize utilizing resources such as land, water, and electricity [32]. Precision farming powered by IoT helps farmers precisely allocate the right number of resources by using data collected from several field sensors.
- **Expansion:** Nine billion people will inhabit the earth in the next years, with 70% of them residing in urban areas [33]. These people can acquire fruits and veggies because of IoT-based systems, particularly those that feed food supply chains.
- **Cleaner method:** IoT-enabled smart agriculture can cut down on fertilizer and pesticide use [34]. In addition to significantly lowering the demand for pesticides and herbicides, intelligent agriculture assists farmers in conserving energy, water, and natural resources.
- **Agility:** IoT in agriculture has the benefit of expediting a number of processes. Real-time forecasting and monitoring technologies allowed farmers to react quickly to significant changes in the climate, moisture, pollution, blazes, and the state of specific crops and soil in the field [35].

2.4 IoT and Cloud Computing in Privacy Concerns

The possibility of data leaking, insufficient user permission procedures and unlawful data collecting have all been recurring topics. To address the particular issues raised by the extensive and diverse IoT ecosystem, robust privacy protections were required. Privacy concerns are heightened by the interaction between cloud computing and IoT. According to the research, cloud systems that centralize data can become more vulnerable. As cloud-related privacy issues become more widely recognized, research focused on topics including data access management, safe data transfer, and insider threat prevention [36–38].

Important Difficulties with Privacy-Preserving Methods

- **Scalability and Efficiency:** The study found that one persistent issue was the adaptability of secure techniques for IoT-based cloud systems. Making sure privacy safeguards can effectively scale to accommodate. Data volume and variety are becoming increasingly crucial as the number of linked devices keeps growing [39]. Optimal algorithms, distributed systems, and effective cryptographic protocols were investigated as remedies.
- **IoT Device Heterogeneity:** The variety of IoT devices, from powerful edge devices to sensors with little resources, makes it difficult to apply consistent privacy-preserving procedures [40]. The literature highlights the necessity of adaptable methods that can accommodate the various device classes' differing communication protocols, energy limitations, and processing capacities.

- **Standardization and Interoperability:** According to the research, the smooth integration of privacy-preserving strategies was hampered by the lack of standardized security frameworks. The field of study investigates the creation of universally applicable interoperable solutions for a variety of IoT platforms and devices [41].
- **Dynamic Character of IoT Settings:** Consistent privacy-preserving procedures were difficult to maintain in IoT settings due to the devices' frequent additions and deletions from networks. The research highlights the necessity of adaptive strategies that can easily respond to shifts in device ownership, connection, and network engagement [42].

2.5 Data Privacy and Encryption in IoT

In IoT, data privacy is still crucial, particularly as more devices manage confidential data like location, financial, and medical records. The transfer of enormous volumes of confidential information between devices in IoT networks leads to several vulnerabilities that must be fixed as they get bigger and more complicated. To preserve user confidence and adhere to privacy laws, it was vital to ensure that the information was protected from unauthorized access, modification, or misuse [43].

AI was essential to improving encryption and data privacy in IoT environments. Despite their effectiveness, traditional cryptographic techniques cannot be able to keep up with the size and dynamic nature of IoT networks [44]. AI-powered encryption systems have a more adaptive approach using ML techniques to dynamically adjust encryption algorithms and keys based on the data being transmitted and the context in which it was being used [45]. For instance, AI can identify the sensitivity of the data being exchanged and choose the most appropriate encryption methods, strengthening security without significantly impacting the performance of efficiency and also enabling advanced techniques like homographic encryption and differential privacy [46].

Numerous aspects of modern life, such as transportation, healthcare, industrial control systems, and home automation, have been altered by the IoT. However, there are also more security flaws as a result of more linked devices, especially from botnets. Several ML and DL methods for detecting IoT botnet attacks have been published to allay these worries. This systematic study aims to identify the best ML and DL methods for detecting IoT botnets by closely examining data pre-processing methods, assessment criteria, and benchmark datasets [47]. The rapid proliferation of IoT devices has increased the probability of malware attacks, necessitating the use of advanced detection and forensic methods. DL methods for forensic analysis and virus detection in IoT scenarios are examined in this comprehensive study. It points out research needs, including the requirement for extensive datasets, multidisciplinary approaches, real-time detection systems, and sophisticated countermeasures [48].

2.6 Problem Statement

There is a substantial research gap in the integration of blockchain technology with IoT, namely regarding scalability, storage, and knowledge gaps about the application of blockchain in different industries. Although blockchain can enhance IoT capabilities, its application faces challenges, such as the inability to manage large IoT networks with many nodes and the absence of standardized security standards. Additionally, the increasing interconnectivity and complexity of IoT devices, combined with privacy concerns, necessitate the creation of scalable, flexible privacy-preserving methods that can adapt to changing network conditions and varied device contexts. Additionally, nothing is known about how AI can improve data privacy and encryption in IoT networks, particularly when it comes to real-time data interchange and decision-making. These limitations underscore the need for more reliable, effective solutions to enhance scalability, data protection, and blockchain-IoT integration across various sectors.

3 Methodology

Fig. 4 shows the comprehensive review's roadmap. The study that is being conducted focuses on IoT security analysis, and IoT security characteristics that are crucial. To that purpose, a comprehensive literature review is carried out.

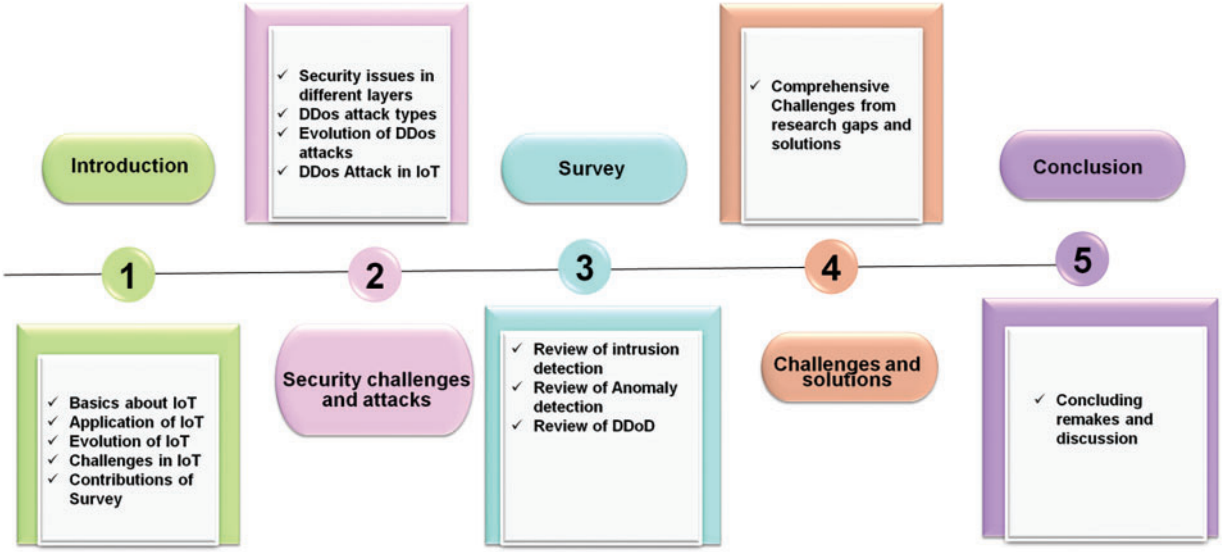

Introduction
1
✓ Basics about IoT
✓ Application of IoT
✓ Evolution of IoT
✓ Challenges in IoT
✓ Contributions of Survey
✓ Security issues in different layers
✓ DDos attack types
✓ Evolution of DDos attacks
✓ DDos Attack in IoT
2
Security challenges and attacks
Survey
3
✓ Review of intrusion detection
✓ Review of Anomaly detection
✓ Review of DDoD
✓ Comprehensive Challenges from research gaps and solutions
4
Challenges and solutions
Conclusion
5
✓ Concluding remakes and discussion

Figure 4: A schedule of the tasks completed for the review

The methodology section provides valuable insights into the sources reviewed such as IEEE, MDPI, springer Elsevier, and others. However, it lacks specific details in the selection criteria, such as database, keywords, or inclusion criteria used. Including these aspects would enhance the transparency and reproducibility of the review process.

3.1 Concerns about Security in the IoT Space

IoT devices are getting increasingly widespread, and due to their lack of protection, criminal activity has been able to perfect itself on them. Various Cybersecurity threats that could impact the IoT's perception, support, network, and application levels are depicted in Fig. 5. A widely accepted four-layer design is considered during the assessment process.

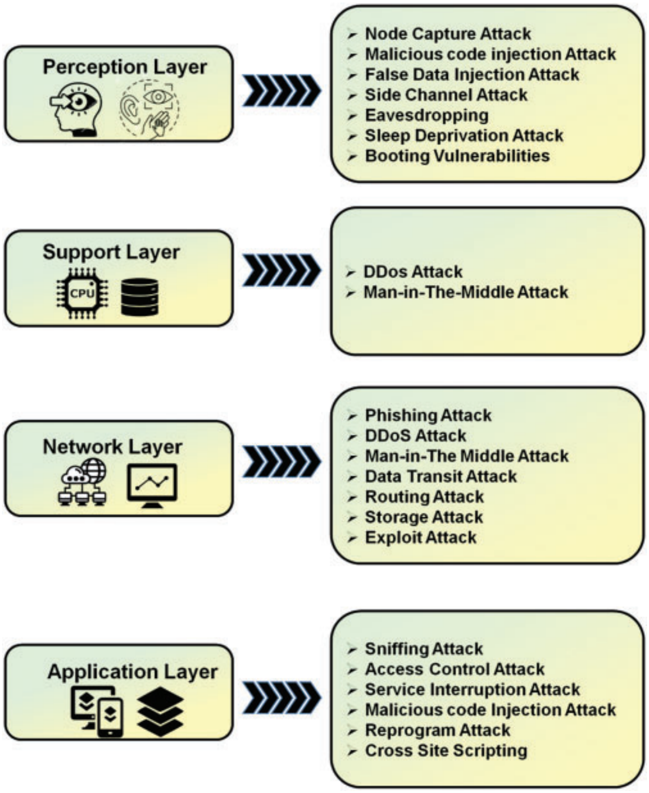


Figure 5: A visual depiction of diverse security breaches across multiple IoT layers

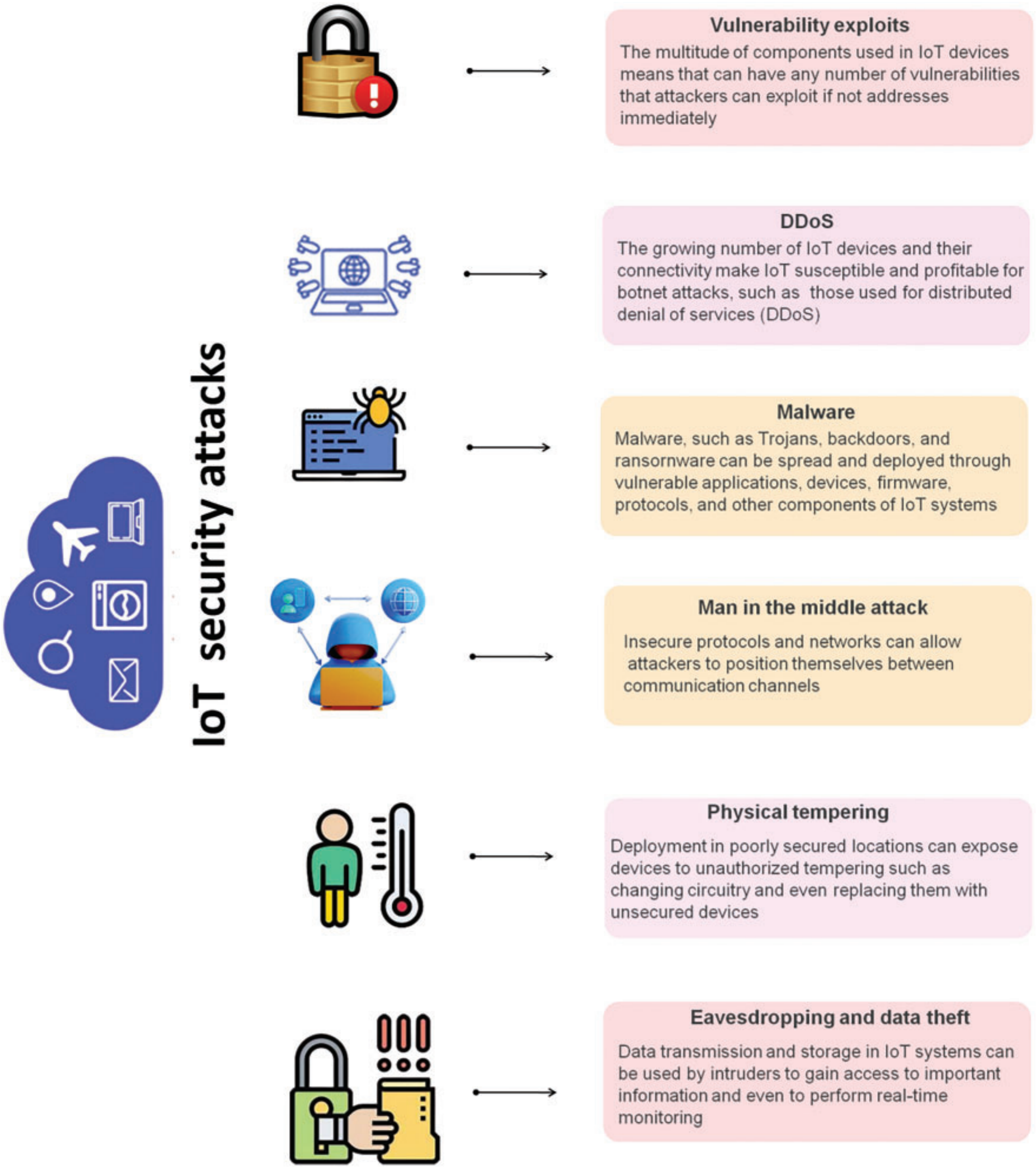
- ***Perception Layer:*** Among the many components of IoT network layer security are *ad hoc*, Wi-Fi, basic, and access network security. The security of cloud computing platforms and middleware technologies are two areas covered by application layer security. For the IoT perception layer, to suggest a layer-based security model in which the security of the perception layer is categorized using several enabling technologies [49]. The perception layer's primary responsibility is to perceive environmental data. The provision of services is the application layer's primary responsibility. Many IoT applications and blockchain are currently being developed for several industries, including industrial automation, air pollution, healthcare, and structural health monitoring [50]. It performs several tasks, such as gathering and displaying data. The lifting machine room's industrial computer is linked to the sensors; as a result, the configuration software gathers the characteristic parameters, which are saved to the server via the mining local area network and relate to the physical quantities that are observed [51].
- ***Network Layer:*** It permits data transfer to perception layer devices to finalize the operation of various applications on the application layer. It could be security faults that compromise the operation of the overall IoT architecture because this layer connects other levels [52]. Network communication software and hardware, such as servers and nodes, make up the network layer, which is a communication layer. It functions as a transmission layer and helps devices communicate with one another by delivering data to end devices. It serves as a bridge to transmit data over great distances and is mostly utilized in mobile telephony and the Internet. Through this layer, networks and devices are connected [53]. Depending on the needs, network and support layers are frequently used to build IoT designs. Moreover, several studies on IoT systems and blockchain have used the idea of cloud-based computing for the support layer [54].

- ***Support Layer:*** The layer encompasses several essential components, including middleware, communication protocols, data storage, and cloud services, enabling devices to connect share, and process information effectively [55]. By acting as a bridge between software and hardware, middleware offers crucial features like analytics, device control, and data aggregation. Additionally, on-premises and cloud-based data storage systems enable the safe collection and analysis of massive volumes of data generated by IoT devices. They facilitate decision-making and provide spontaneous discoveries [56]. The support layer also addresses scalability and flexibility, allowing IoT systems and blockchain to adapt to changing requirements and accommodate a growing quantity of gadgets. Given the circumstances, Enhancing the effectiveness, reliability, and security of blockchain and IoT networks requires a support layer, ensuring that devices can interact and collaborate effectively to deliver valuable insights and services [57].
- ***Application Layer:*** This layer's function is to handle application-specific features, such as those related to smart cities and health. This layer is realized as two sections in certain architecture. The business layer, which manages applications and handles security and privacy, is the outermost layer [58]. This layer's importance can be understood from its capacity to offer first-rate services that satisfy customer demands. This degree of IoT and blockchain could lead to the development of numerous innovative ecosystems, including smart factories, smart orangeries, and smart cities [59]. This layer has the power to confirm whether applications are receiving services. By data collected by sensors, it is also able to provide numerous services to various applications. Even with all its problems, security is the most important consideration [60].

3.2 IoT Security Breaches

Malicious actions intended to jeopardize the reliability, security, or accessibility of IoT networks and devices can take many different forms within the IoT framework. Poor security procedures might be the source of these assaults, which target IoT systems, insufficient authentication systems, or unsecured communications methods are described in Table 1. Unauthorized device access, data interception during transmission, DDoS attacks that overwhelm devices or networks, and malware infections that can cause disruptions or steal confidential information are examples of common security threats.

Security breaches categorized as either mild or critical, pose a continuous risk to all systems. Therefore, immediate action is required to prevent irreversible issues that can compromise availability, integrity, or confidentiality. Because of several limitations, small developers are unable to apply a traditional security setup for IoT devices because of memory constraints, a network that is active and diverse, as well as a battery that is restricted. As a result, the way this type of system is implemented needs to be revised. A typical strategy used against IoT platforms is to create a DoS attack on Fig. 6. One such is the Mirai-attack, which involves leveraging shared credentials to access Telnet, secure shell, or other services and then taking control of the device. The attacker typically uses this technique to overcome a target, in this instance, the victim, with the use of several gadgets. Port scanning is often conducted before attacking the target. The attacker can create and send packets, decipher the answers, and run port scans. This considers both port scans and DoS attacks in the application scenario because they are both highly frequent [61].



Vulnerability exploits

The multitude of components used in IoT devices means that can have any number of vulnerabilities that attackers can exploit if not addresses immediately

DDoS

The growing number of IoT devices and their connectivity make IoT susceptible and profitable for botnet attacks, such as those used for distributed denial of services (DDoS)

Malware

Malware, such as Trojans, backdoors, and ransomware can be spread and deployed through vulnerable applications, devices, firmware, protocols, and other components of IoT systems

Man in the middle attack

Insecure protocols and networks can allow attackers to position themselves between communication channels

Physical tempering

Deployment in poorly secured locations can expose devices to unauthorized tempering such as changing circuitry and even replacing them with unsecured devices

Eavesdropping and data theft

Data transmission and storage in IoT systems can be used by intruders to gain access to important information and even to perform real-time monitoring

Figure 6: Security attacks in IoT

Table 1: Security attacks

Category	Description	Real-world example
Unauthorized access	To gain unauthorized access to IoT devices, attackers take advantage of lax authentication procedures, which could compromise private information or allow them to remotely control devices [62].	Smartphone hacking: Exploiting weak passwords to access a device and steal data.

(Continued)

Table 1 (continued)

Category	Description	Real-world example
DDoS attacks	DDoS attacks can be launched by IoT devices that have been compromised and utilized as a botnet, overwhelming targeted servers and interfering with services [63].	Mirai botnet: IoT devices like cameras and routes were compromised to attack major websites.
Data interception	Insecure communication protocols can allow attackers to intercept data transmitted between IoT devices, resulting in privacy violations and data breaches [61].	Wi-Fi sniffing: Attackers intercept data from an insecure public Wi-Fi network.
Firmware exploitation	Vulnerabilities in the firmware of IoT gadgets can be misused for evil or exploited to give attackers control over the device, enabling them to change its behavior [64].	Smart TV hacking: Manipulating the firmware to control the TV remotely or collect data.
MITM attacks	Attackers can endanger data integrity and authenticity by intercepting and changing communications between IoT devices and their servers [65]. Identifies external assaults with no false positives. Unable to identify an insider threat.	Smart home devices: Intercepting communication between devices and their hubs.
Ransomware and malware	IoT devices can be compromised with ransomware or malware, which can cause operational disruptions or require payment of a ransom to return to functioning [61].	Smart Lock ransomware: Locking users out of their smart locks and demanding payment to region access.
Physical tampering	Attackers can physically access IoT devices to alter their functionality, gain unauthorized data access, or disable security features [66].	Datacenter attacks: physically tempering with servers to steal sensitive data.

- ***Instruction detection system (IDS) in IoT using AI solutions***

An IDS system's objective is to prevent unwanted access. An unauthorized infiltration potentially jeopardizes information availability, confidentiality, or integrity [67]. It is designed to protect an information system against unwanted access. Data integrity, confidentiality, and availability may be harmed by an unauthorized intrusion. In terms of intrusion detection methods, IDSs can be divided into two primary classes. A particular team compares observed events to a database of intrusion tactics, whereas another monitors ordinary conduct and records any odd occurrences [68].

ML algorithms-based AI solutions: Although a signature-driven intrusion detection system has a low false alarm rate and high accuracy, it is unable to detect new threats. A specification-based network intrusion detection system compares traffic patterns to a predetermined set of values and principles to detect malicious activity. A security specialist [69] manually specifies these requirements. Based on anomalies IDS constantly monitors network traffic to look for deviations from the standard network profile, in contrast to signature and specification-based IDS. An alert is sounded to indicate the detection of an assault if a deviation is beyond the threshold. ML techniques are used to learn the typical network profile. The capacity of anomaly-based IDS to identify novel threats makes them superior to signature and specification-based

IDS [70]. Since the IoT and blockchain environment consists of several devices with different protocols and limited computational resources, IDS uses lightweight algorithms and anomaly detection methods to identify threats such as command ML models or rule-based detection to analyze traffic patterns, instructing, and device behaviors, ensuring the system responds promptly to potential attacks while maintain minimal latency to support the seamless operations of IoT ecosystems as described in Fig. 7. The IoT captures noisy network traffic with a wide variety of traffic characteristics. IDS performance is impacted by ML models, which take longer to create due to the complexity of IoT network data. Consequently, feature selection is necessary for IoT intrusion detection to create models more rapidly and effectively [71]. The data can be accurately classified by the algorithms. It is suggested that IDS for IoT networks can be constructed using ML algorithms. The difficult part of developing IDS with ML principles is creating a realistic and excellent training dataset, as interception is only feasible [72]. Building the ML model considers a variety of data because the network will be run by a variety of heterogeneous devices. Appropriate IDS for an IoT context can be developed by addressing these obstacles [73].

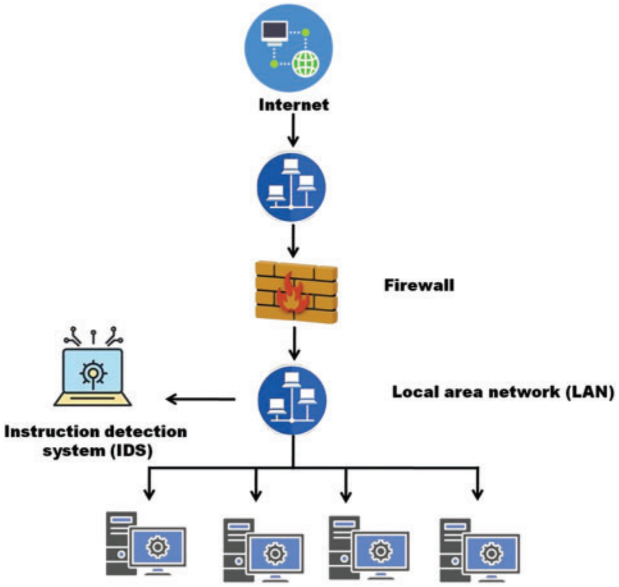


Figure 7: Architecture of IDS

DL algorithms-based AI solutions: In the IoT, IDS are security architectures created to keep an eye on and identify fraudulent or unauthorized activity across networks and connected devices [74]. Understanding the rationale behind the choice made by their DL-based IDS is one of the primary goals of this approach [75]. In addition to protecting terminal users, IDS will also safeguard service providers, therefore, when internet threats increase, IDS approaches should also be updated. IDS methods can be divided into two categories: anomaly detection and misuse detection. The ability of anomaly detection technology to identify undiscovered threats makes it a hot spot [76].

Depending on how intrusions are found, the IDSs fall into one of two main groups. While one team looks at recorded events and compares them to a database of intrusion techniques, another team looks at typical conduct and flags any anomalies as shown in Table 2.

Table 2: An illustration of the progression of IDS attack methods

Ref.	Year	Method and attack name	Parameters
Author [Balakrishnan N, Rajendran A, Pelusi D, Ponnusamy V] in [77]	2021	Deep Learning (DL) model DBN utilized in the study for IDS	The parameters used by DBN in the study for IDS include precision, recall, and F1-score
Author [Saravanan V, Madiajagan M, Rafee SM, Sanju P, Rehman TB, Pattanaik B] in [78]	2024	DL model RNN utilized in the study for IDS	Precision (98.65), recall (98.84%), F1-score (97.27%), Accuracy (98.32%), execution time (15)
Author [Mansour RF] in [79]	2022	The proposed model BAC-IDS used for IDS in the study	F1-score, precision, recall, accuracy, TNR, and AUC of 99.96%, 99.96%, and 99.96%
Author [Liang C, Shanmugam B, Azam S, Karim A, Islam A, Zamani M, et al.] in [80]	2021	The proposed model BC-HyIDS used for IDS in the study	88.375 accuracy rate and an 89.263 maximum recall measure

• ***Anomaly detection in IoT using AI solutions:*** It is essential for enhancing security and guaranteeing the dependability of networked systems and devices in IoT.

ML algorithms-based AI solutions: IoT and blockchain frameworks can use advanced ML algorithms and statistical techniques [81] to assess the enormous amounts of data that sensors and gadgets produce in real-time, as seen in Table 3. These techniques allow for the identification of trends and deviations that can indicate malicious actions or system problems. Implementing anomaly detection mechanisms enables proactive responses to potential threats, allowing for immediate isolation of compromised devices and minimizing risks to the entire network as shown in Fig. 8. Furthermore, these systems can adapt and become more accurate with time as they absorb fresh information to increase their forecasting power and provide a more robust security in increasingly complex IoT environments [82].

DL algorithms-based AI solutions: DL is a kind of ML that learns a good representation of data by using layers of abstractions. DL can outperform traditional ML techniques as data volume and heterogeneity increase. DL-powered anomaly detection methods have recently shown growing utility across a range of fields. To develop a DL-enabled framework for trustworthy IoT anomaly detection to get beyond the challenges presented by diverse IoT systems [83]. Although there are several anomaly-detection techniques, fewer attempts have been made to use CNNs for anomaly identification [84]. They concentrate on identifying anomalies in weighted graphs. The method can be used in a variety of situations, including social network abnormalities, spammer detection, intrusion detection, and more. Additionally, the problem of detecting anomalies in static, labeled networks is discussed. A few ego networks were studied in this context, and it was determined that when the sum over a specific label is abnormally high approximately the edge count of the network, the related individual may be acting abnormally [85].

Table 3: An illustration of the progression of Anomaly detection

Ref.	Year	Method and attack name	Parameters
Author [Yang X, Chen Y, Qian X, Li T, Lv X] in [86]	2021	To develop BCEAD techniques to prevent Anomaly detection	The parameters used by BCEAD in the study for this attack include precision, recall, and F1-score
Author [Kim J, Nakashima M, Fan W, Wuthier S, Zhou X, Kim I, et al.] in [87]	2022	ML was used in the study to find anomalies	The research employed ML parameters for Anomaly detection to determine accuracy and F1-score
Author [Seifi S, Beaubrun R, Bellaiche M, Halabi T] in [88]	2021	The proposed model RL used for Anomaly detection in the study	The parameters used by RL utilized in the study for Anomaly detection for accuracy and F1-score

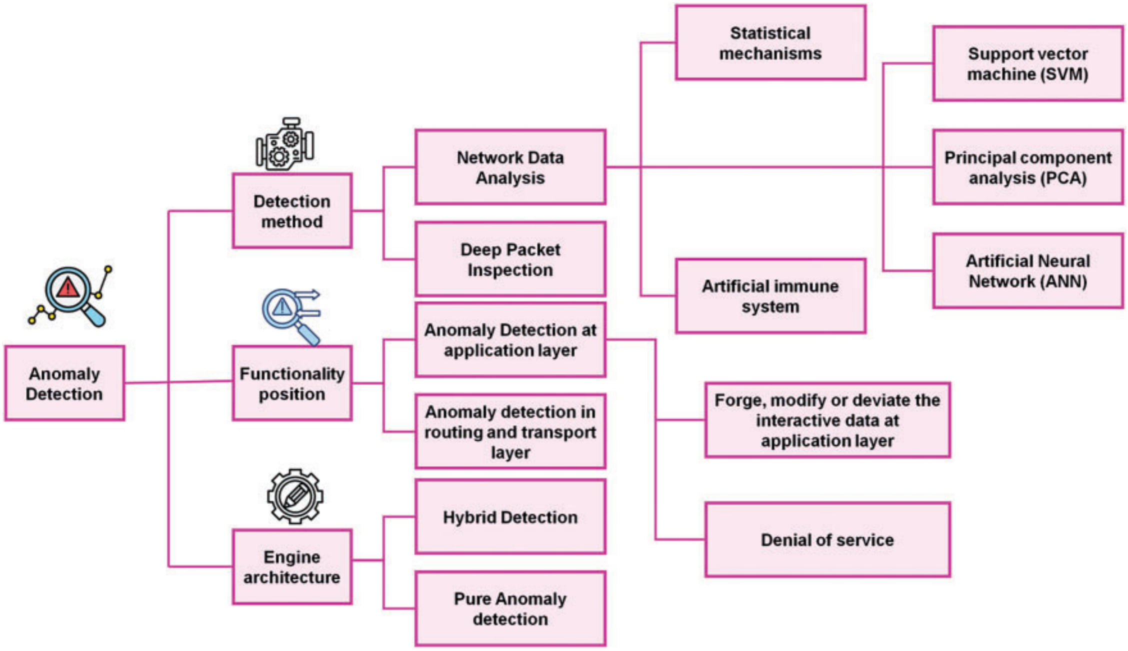

Anomaly Detection
Detection method
Functionality position
Engine architecture
Network Data Analysis
Deep Packet Inspection
Anomaly Detection at application layer
Anomaly detection in routing and transport layer
Hybrid Detection
Pure Anomaly detection
Statistical mechanisms
Artificial immune system
Support vector machine (SVM)
Principal component analysis (PCA)
Artificial Neural Network (ANN)
Forge, modify or deviate the interactive data at application layer
Denial of service

Figure 8: Architecture of Anomaly detection

- ***Distributes denial of services (DDoS) in IoT using AI solutions***

DDoS attacks are malicious efforts to disrupt a service or network's normal operation by overloading it with traffic from the internet. It is appropriate for multi-targeted attacks, nevertheless, because a network-wide deluge necessitates mitigating measures before it reaches the victims. Software fixes and appliance deployments cannot completely stop or block DDoS attacks. As a result, internet service providers either overprovision their networks or employ cleaning services. Both approaches are not financially viable [89].

ML algorithms-based AI solutions: A DDoS involves the use of several hijacked computer systems, frequently comprising a botnet, to make an excessive number of requests to the intended recipient, exhausting its assets and hindering it from reacting to users who are doing it legally [90]. These assaults have the potential to cause serious disruptions, monetary losses, and reputational harm. Black diagram DDoS as shown in Fig. 9. The size of unconfirmed transactions increases, giving attackers an opportunity, and real users must pay more mining fees to prioritize their unconfirmed transactions. Therefore, a strong and effective security mechanism is needed to identify DDoS attacks [91].

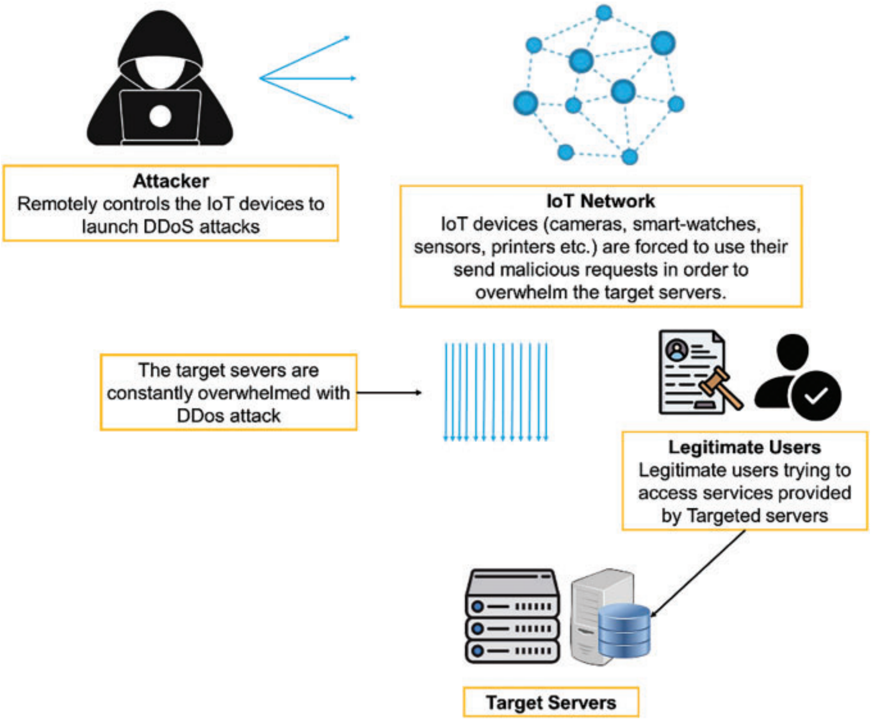

Attacker
Remotely controls the IoT devices to launch DDoS attacks
IoT Network
IoT devices (cameras, smart-watches, sensors, printers etc.) are forced to use their send malicious requests in order to overwhelm the target servers.
The target severs are constantly overwhelmed with DDos attack
Legitimate Users
Legitimate users trying to access services provided by Targeted servers
Target Servers

Figure 9: Architecture of DDOS

DL algorithms-based AI solutions: Three types of DDoS assaults are distinguished: brute force, spoofing, and flooding. The most frequent and harmful attacks are flooding attacks, which limit network bandwidth and block all valid requests. Every focus of survival is on single-target victims, who must recognize and control the attack on their own [92]. IoT devices can be weaponized and hijacked for targeted code injection, MITM attacks, DDoS attacks, and pose estimation. Additionally, malicious actors can remotely influence IoT devices, which significantly impact network data transfer. Thus, it is particularly crucial to maintain and safeguard IoT security to lower intermediate hazards in a networked setting. The entire network, IoT device segmentation, monitoring, inspection, and policy enforcement, as well as the implementation of prompt, automated responses if an attack affects the network, all contribute to the reduction of security threats [93]. DDoS attacks use a variety of techniques, such as volume-based, protocol-based, and application-layer assaults illustrated in Table 4. Mitigating DDoS attacks requires a combination of strategies including traffic analysis, risk limiting, and employing DDoS protection on services to detect and eliminate harmful traffic while preserving the availability of trustworthy services [94].

Table 4: An illustration of the progression of DDOS attacks

Ref.	Year	Method	Parameters
Author [Yin X, Fang W, Liu Z, Liu D] in [95]	2024	The proposed model CNN and Bi-LSTM used for DDoS in the study	Recall rate (96.74), accuracy (96.74), precision (96.77), and detection time (5.83 m.s./batch)
Author [Alghazzawi D, Bamasag O, Ullah H, Asghar MZ] in [96]	2021	The proposed model CNN and Bi-LSTM used for DDoS in the study	Error rate (91.31), false alarm rate (5.66), and detection rate (5.47)
Author [Cheng J, Liu Y, Tang X, Sheng VS, Li M, Li J] in [97]	2020	DL model CNN utilized in the study for DDoS	F1-score (93.44), recall (92.04), precision (94.74), and Accuracy (94.52)
Author [Hairab BI, Elsayed MS, Jurcut AD, Azer MA] in [98]	2022	DL model CNN utilized in the study for DDoS	Statistical and Analytical Methods, Accuracy (87.27), precision (81.07), recall (72.25), F1-score (76.46)
Author [Issa ASA, Albayrak Z] in [99]	2023	CNN and Bi-LSTM, the suggested model, were employed for DDoS	The accuracy, precision, and recall, were 99.31, 99.18, and 99.18, respectively

- ***Man in the middle attack (MITM) attack in IoT using AI solutions***

A Man-in-the-Middle (MITM) attack is an illegal attack that intercepts and maybe modifies communications between two valid IoT devices or between a device and a server, as shown in Table 5. By placing themselves between the two parties, the attacker can listen to confidential information, inject malicious comments, or manipulate the information being exchanged without either party realizing it [100].

ML algorithms-based AI solutions: With the interconnected nature of IoT, such attacks pose significant risks, as they can exploit vulnerabilities in communication protocols, weak encryption, or unsecured networks. For instance, an attacker cloud intercept data from a smart home device, such as a thermostat or security camera, and either manipulates the data or steals confidential information [101]. Mitigating MITM attacks in IoT involves using robust encryption techniques, Effective authentication procedures, and secure communication protocols to ensure that data is kept private and unchanged during transmission [102]. The Benefits of mitigating MITM attacks in IoT are significant, primarily enhancing data privacy, integrity, and trust in interconnected devices by securing communications with strong encryption and authentication mechanisms [103].

DL algorithms-based AI solutions: Additionally, mitigating MITM attacks helps maintain the integrity of the IoT ecosystem by preventing malicious actors from injecting harmful commands or altering device behaviors [104]. They promote user confidence in IoT technologies, encouraging widespread adoption and integration across various sectors, ultimately, effective MITM defense strengthens the security posture of IoT systems, reducing vulnerabilities and enhancing their resilience against cyber threats. However, MQTT depends on SSL/TLS to encrypt MQTT communications because it lacks an advanced security mechanism of its own [105]. Regretfully, IoT installations are not adequately enforced. An attacker can change the data being sent between two endpoints of a network by intercepting the connection. This type of cyber-attack is called MITM attack [106]. A technically capable attacker with the presence and power to execute an MITM attack on a user's mobile device is taken into consideration [107]. IoT devices have unique characteristics, such as the requirement to function as tiny computing systems and be energy efficient [108]. Many IoT devices can share a network, and because of their constrained computing power, these devices employ a variety of lightweight protocols. MQTT is an application layer protocol that is frequently used in IoT devices [109].

Table 5: An illustration of the progression of MITM attacks

Ref.	Year	Method	Parameters
Author [Hashimyar ME, Aiash M, Khoshkholghi A, Nalli G] in [110]	2024	The suggested XGB model	Recall (0.995), F1-score (0.9948), accuracy (0.9960), and precision (0.9955)
Author [Toutsop O, Harvey P, Kornegay K] in [111]	2020	The proposed model PSO-RF	Accuracy (99.76), F1-score (96.45), Precision (99.5), MCC (99.51)
Author [Rihan SDA, Anbar M, Alabsi BA] in [112]	2023	The suggested DL models (RNN, LSTM, CNN, and GRU) were assessed	Recall (97.95%), Precision (97.95%), F1 measure (998.87%), and accuracy (97.87%)

3.3 AI Is Supporting IoT for Security

AI enhances IoT security by providing intelligent, adaptive technologies that can manage the difficulties presented by IoT contexts, such as resource constraints, device heterogeneity, and the need for real-time threat detection. Below are key ways AI supports IoT security.

- **Anomaly detection and threat identification:** IoT systems can identify strange data flow patterns that can indicate security lapses connected to AI, especially those employing ML algorithms are support vector machine (SVM), naïve Bayes (NB), K-nearest neighbor (KNN), Random Forest (RF), decision tree (DT) [113]. Substantial amounts of data produced by IoT devices can be analyzed by AI models to identify typical activity and highlight abnormalities. It allows for early detection of cyber-attacks, such as DDoS or unauthorized access that can otherwise be unnoticed by traditional security protocols.
- **Predictive security:** It is extremely difficult to protect IoT devices from any security breaches due to the large amount of communication traffic data between them [114]. This problem is made worse by the existence of unbalanced network traffic data. AI technologies, particularly machine and deep learning, have demonstrated promise in identifying and mitigating these security risks that target IoT networks.
- **Automates security response:** The design of AI-based security approaches and an understanding of the cyber threat landscape of IoT networks have garnered a lot of attention [115], instead the lack of distributed architecture has resulted in the creation of heterogeneous datasets that include complex cyber threat scenarios and the real-world behaviors of IoT networks to assess the new systems' credibility.
- **Data integrity with blockchain integration:** Combining blockchain technology with AI can increase the security and dependability of data transfers in IoT devices [116]. By utilizing blockchain's decentralized, tamperproof nature, AI can ensure that IoT communications remain secure, transparent, and resistant to cyber-attacks. Smart contracts powered by AI can automatically enforce security policies and manage general proposed access control without the need for intermediaries.
- **Adaptability to resource constraints:** IoT devices are limited in terms of memory, processing power, and bandwidth [117]. AI powered security solutions are being developed to operate efficiently within these constraints, ensuring that security mechanisms do not overload the system or drain resources.

Lightweight AI models, such as edge computing-based solutions enable device-level real-time threat analysis, which eliminates the requirement for continuous contact with central servers.

3.4 Blockchain and IoT Integration for Enhancing and Education Security Systems

Technologies like blockchain and IoT can improve security and lessen assaults on systems used in healthcare and education. Healthcare uses IoT devices for remote patient monitoring, but centralized data storage exposes patient information to potential breaches. Blockchain provides a decentralized ledger for secure storage and transfer of medical data, while IoT collects sensitive student information, ensuring privacy and unauthorized access.

Increasingly patients are being admitted to hospitals around the country as a result of the emergence of blockchain and IoT innovations in healthcare, making it increasingly difficult to provide complete medical care [118]. Monitoring patients remotely is the main strategy for handling healthcare issues. Smart watches and IoT devices are essential for remote patient monitoring, data collecting, and hospital data transmission [119,120]. These gadgets' primary goals are to give medical professionals vital information including a patient's blood pressure, blood glucose level, and breathing patterns [121]. To safeguard patient data, the IoT application of healthcare has unique requirements, including data transfer and interoperability. The technique of sharing data across several sources is known as interoperability. The inability to establish interoperability is one facet of the centralization concept [122]. Centralization is the cornerstone of the IoT, and data is stored on the insecure cloud. Integrating blockchain technology with IoT helps address security problems in healthcare applications [123,124]. IoT-based educational services include security and privacy in the classroom: Systems that rely on these modern technologies safeguard a range of data that are sent over the Internet. They are mostly made up of several interconnected devices, and when these devices begin to monitor and collect data from pupils, the privacy of the students is at risk. Any security lapse might expose a student's personal information linked to their family's financial situation, medical history, or any other confidential information [125]. Reliable wireless connection (Wi-Fi) and high-speed wireless networks are the most crucial of these technologies, providing bandwidth for the orderly and high-quality delivery of educational classes via audio and video. The importance of contemporary technology for education and its continuous necessity without sudden pauses or disruptions are undeniable [126,127]. Several variables, including smart classrooms, may make it challenging for educational institutions and industries to adopt this innovative technology. Informational institutions can profit from investigating and testing IoT possibilities, even though there are possible hazards and challenges associated with technology [128,129]. Cost, these innovative modern technologies, together with all the equipment required to form an integrated educational system, can be used to fully prepare the current educational institution at an excessive cost. Thus, another issue facing educational institutions and sectors is the expense of gadgets and equipment [130]. Health, the student's medical record can be updated by using remote sensors and surveillance cameras to monitor the ill student and determine whether he has a temperature or a shift [131].

4 Performance Matrices

4.1 Deep Learning-Based Experimental Validation

The performance metrics that are most frequently used for DDOS, anomaly detection, and IDS are covered below. According to the research's findings, CNN routinely outperforms alternative models in terms of recall, F1-score, accuracy, and precision, which are important security criteria. The findings demonstrate CNN's excellent capacity to identify and reduce hazards in IoT contexts, as it obtains the greatest values for precision (97.70%), recall (98.30%), accuracy (98.82%), and F1-score (98.8%). In contrast, classifiers like DCNN and FCFFN show significantly lower performance. These findings highlight how crucial it is to use the right classifiers depending on the particular security metric being optimized. Blockchain technology combined with IoT has also been recognized as a viable way to improve security by tackling concerns about resource constraints, privacy, and transparency. Finally, the study explores the distribution of IoT applications, with smart cities dominating the market share, followed by healthcare and business applications. The capacity of CNN's convolutional layers to efficiently capture spatial hierarchies and patterns in data accounts for its superior accuracy when compared to FCFFN. Unlike FCFFN, which treats all input features independently, CNN utilized local receptive fields to identify local features and progressively combine them to form higher-level representations. The hierarchical feature extraction allows CNN to better generalize from data, particularly when dealing with complex patterns such as images or sequential data, leading to improved accuracy. Additionally, CNN typically requires fewer parameters and can manage overfitting more effectively, contributing to their superior performance in tasks like classification.

4.1.1 Accuracy

The percentage of all forecasts that contain correct predictions is known as accuracy. This statistic works best when the dataset is balanced. The outcomes of this statistic could not accurately represent the performance of the model when a majority class is present in the dataset as shown in Eq. (1).

$$Accuracy = \frac{TP + TN}{TP + TN + FN + FB} \tag{1}$$

Table 6 and Fig. 10 present the accuracy percentage of different classifiers as reported in various studies. The classifiers listed include deep Convolutional neural network (DCNN) with an accuracy of 77.55%, full connected feed-forward network (FCFFN) at 93.74%, deep autoencoder deep neural network (DAE-DNN) with 83.33%, focal loss-based feed-forward neural network (FNN-focal) at 91.55% and Convolutional neural network (CNN) achieving the highest accuracy of 98.82%.

Table 6: Outcomes of accuracy

Ref.	Classifiers	Accuracy (%)
Author [Ullah S, Ahmad J, Khan MA, Alkhammash EH, Hadjouni M, Ghadi YY, et al.] in [132]	DCNN	77.55
Author [Awajan A] in [133]	FCFFN	93.74
Author [Novaria Kunang Y, Nurmaini S, Stiawan D, Suprapto B] in [134]	DAE-DNN	83.33
Author [Raoufi P, Hemmati A, Rahmani AM] in [135]	FNN-Focal	91.55
Author [Aswad FM, Ahmed AM, Alhammadi NA, Khalaf BA, Mostafa SA] in [136]	CNN	98.82

4.1.2 Precision

The ML model's precision is a metric that indicates how accurate it is in determining the proportion of actual positives to all anticipated positives. This measure is helpful in cases where the cost of a false positive is significant for the model's quality, such as in spam detection models as shown in Eq. (2).

$$Precision = \frac{TP}{TP + FP} \tag{2}$$

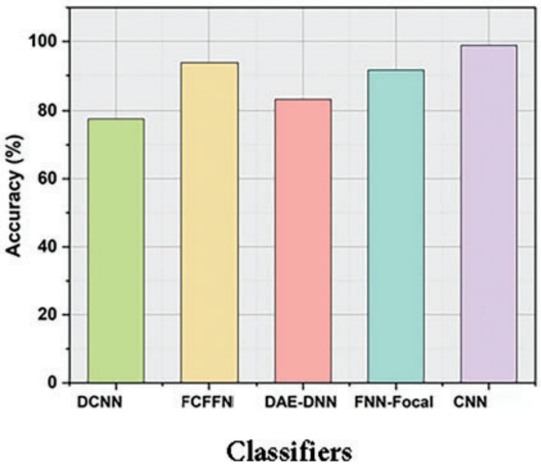


Figure 10: Comparison of accuracy

Table 7 and Fig. 11 present the precision percentage of difference classifiers as reported in various studied. The classifiers listed include DCNN with a precision of 78.76%, FCFFN at 93.71%, DAE-DNN with 86.02%, FNN-focal at 55.59% and CNN achieving the highest precision of 97.70%.

Table 7: Outcomes of precision

Ref.	Classifiers	Precision (%)
Author [Ullah S, Ahmad J, Khan MA, Alkhammash EH, Hadjouni M, Ghadi YY, et al.] in [132]	DCNN	78.76
Author [Awajan A] in [133]	FCFFN	93.71
Author [Novaria Kunang Y, Nurmaini S, Stiawan D, Suprapto B] in [134]	DAE-DNN	86.02
Author [Raoufi P, Hemmati A, Rahmani AM] in [135]	FNN-Focal	55.59
Author [Aswad FM, Ahmed AM, Alhammadi NA, Khalaf BA, Mostafa SA] in [136]	CNN	97.70

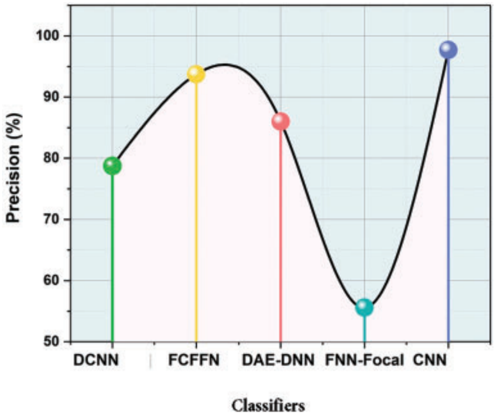


Figure 11: Comparison of precision

4.1.3 Recall

Recall is a metric used to quantify how well an ML model approximates the ratio of true positives to total positives. This measure is useful when False Negative is extremely expensive for model quality, as it is in the fraud detection Model, as Eq. (3) illustrates.

$$Recall = \frac{TP}{TP + FN} \tag{3}$$

Table 8 and Fig. 12 present the recall percentage of difference classifiers as reported in various studied. The classifiers listed include DCNN with a recall of 73.43%, FCFFN at 93.82%, DAE-DNN with 83.33%, FNN-focal at 63.80% and CNN achieving the highest recall of 98.30%.

Table 8: Outcomes of recall

Ref.	Classifiers	Recall (%)
Author [Ullah S, Ahmad J, Khan MA, Alkhammash EH, Hadjouni M, Ghadi YY, et al.] in [132]	DCNN	73.43
Author [Awajan A] in [133]	FCFFN	93.82
Author [Novaria Kunang Y, Nurmaini S, Stiawan D, Suprapto B] in [134]	DAE-DNN	83.33
Author [Raoufi P, Hemmati A, Rahmani AM] in [135]	FNN-Focal	63.80
Author [Aswad FM, Ahmed AM, Alhammadi NA, Khalaf BA, Mostafa SA] in [136]	CNN	98.30

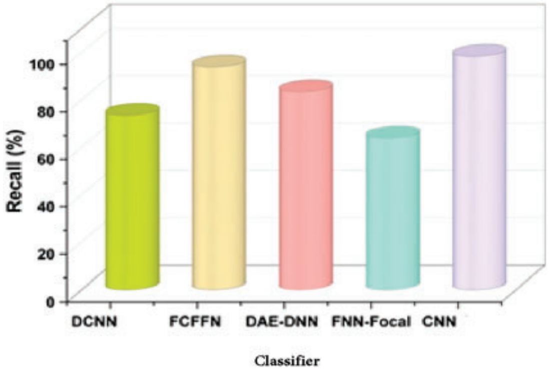


Figure 12: Comparison of recall

4.1.4 F1-score

The model's performance is evaluated more precisely by calculating the Harmonic Mean of the accuracy and recall metrics. This statistic is significant for an unbalanced dataset like this one since it assigns equal weight to precision and recall as shown in Eq. (4).

$$F1 - score = \frac{2 \times precision \times Recall}{Precision + Recall} \tag{4}$$

Table 9 and Fig. 13 present the F1-score percentage of difference classifiers as reported in various studies. The classifiers listed include DCNN with an F1-score of 76.80%, FCFFN at 93.47%, DAE-DNN with 82.04%, FNN-focal at 82.04% and CNN achieving the highest F1-score of 98%.

Table 9: Outcomes of F1-score

Ref.	Classifiers	F1-score (%)
Author [Ullah S, Ahmad J, Khan MA, Alkhammash EH, Hadjouni M, Ghadi YY, et al.] in [132]	DCNN	76.80
Author [Awajan A] in [133]	FCFFN	93.47
Author [Novaria Kunang Y, Nurmaini S, Stiawan D, Suprapto B] in [134]	DAE-DNN	82.04
Author [Raoufi P, Hemmati A, Rahmani AM] in [135]	FNN-Focal	82.04
Author [Aswad FM, Ahmed AM, Alhammadi NA, Khalaf BA, Mostafa SA] in [136]	CNN	98

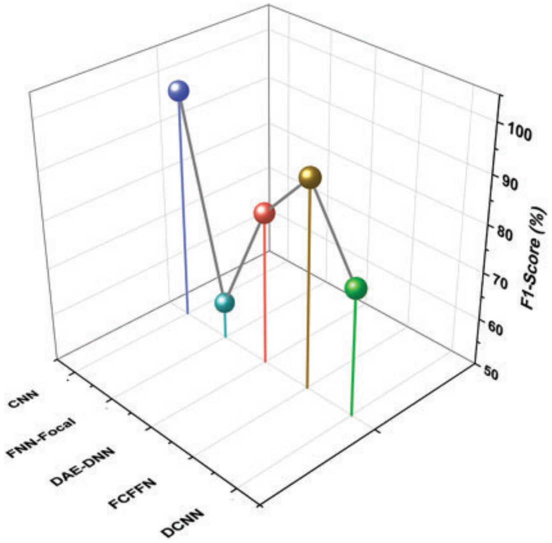


Figure 13: Comparison of F1-score

IoT and blockchain technologies complement each other to deal with the issues of resource limitations, privacy, and security. Blockchain's decentralized structure enhances IoT security by ensuring transparent, tamper-proof data exchanges, mitigating the risk of cyber breaches and untrustworthy content. Smart contracts automate trust without intermediaries, making security protocols more uniform and scalable across different IoT devices, even in environments with high mobility, like enhancing privacy. Additionally, the lightweight blockchain protocols being developed address IoT's limited processing power and energy constraints, making security solutions more feasible for resource-constrained devices.

4.2 Machine Learning-Based Experimental Validation

Table 10 and Fig. 14 present the performance metrics of various classifiers, including RF, DT, XGBoost, AdaBoost, and an ensemble model combining RF-BPNN. All classifiers demonstrate excellent performance, with accuracy and precision values predominantly at near 99.9%. The DT and XGBoost classifiers stand out with perfect precision of 100%, indicating their highly accurate predictions for positive classes. Overall, these classifiers exhibit comparable and prominent levels of accuracy and precision, suggesting their robustness in the given task.

Table 10: Numerical outcomes of ML methods (Accuracy and Precision)

Metrics	Accuracy (%)	Precision (%)
RF [137]	99.9	99.9
DT [137]	99.9	100.0
XGBoost [137]	99.9	100.0
AdaBoost [137]	99.9	99.9
Ensembled RF-BPNN [137]	99.9	99.9

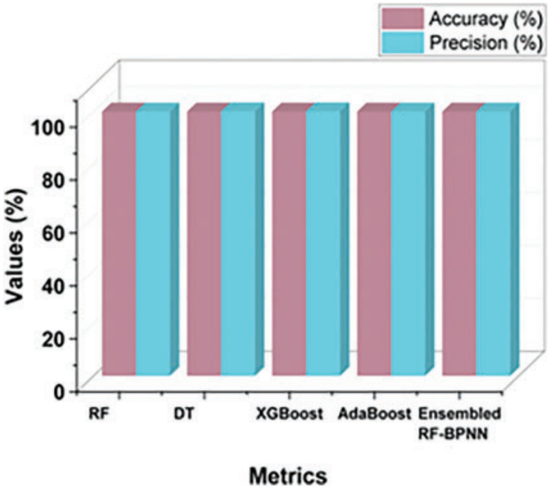


Figure 14: Comparison of ML methods (Accuracy and Precision)

Table 11 and Fig. 15 present the performance metrics of various classifiers, including RF, DT, XGBoost, AdaBoost, and an ensemble model combining RF-BPNN. Most models, particularly RF, AdaBoost, and the ensemble model RF-BPNN achieve a recall. An F1-score of 99.9%, indicating excellent performance in identifying true positives and balancing precision and recall DT and XGBoost show slightly lower recall (99.1%) but maintain high F1-score (99.5% and 9.9%) respectively, demonstrating their ability to maintain a strong tradeoff between precision and recall. Overall, these classifiers perform excellently across both metrics, with minimal variation in performance.

4.3 Bloch Chain-Based Experimental Validation

Latency [138]: To the time taken for a data packet to travel from the source to the destination, in the context of a blockchain-based experimental validation, latency is crucial to measure the quick information or control signals propagating through the system. Lower latency indicates that the system can react more swiftly, which is particularly important for real-time applications in IoT, and other communications networks as shown in Fig. 16.

Table 11: Numerical outcomes of ML methods (Recall and F1-score)

Metrics	Recall (%)	F1-score (%)
RF [137]	99.9	99.9
DT [137]	99.1	99.5
XGBoost [137]	99.1	99.9
AdaBoost [137]	99.9	99.9
Ensembled RF-BPNN [137]	99.9	99.9

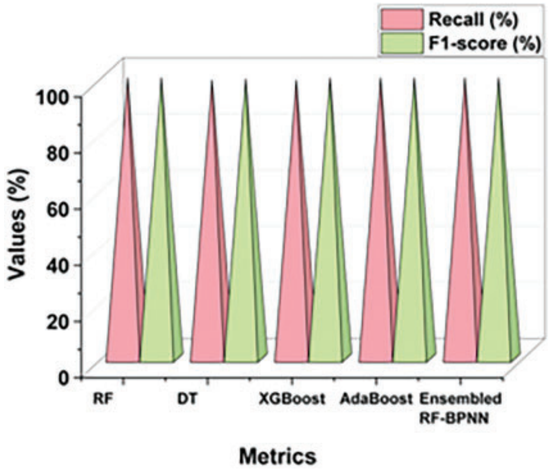


Figure 15: Comparison of ML methods (Recall and F1-score)

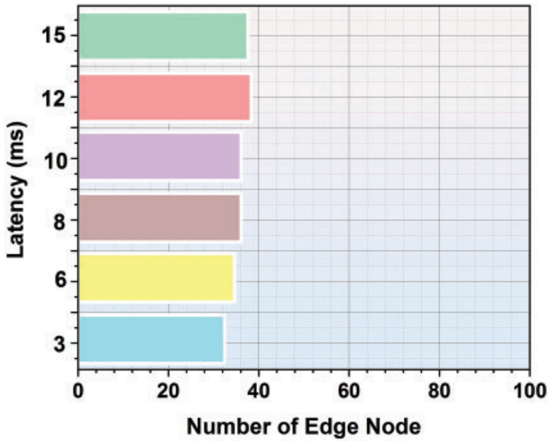


Figure 16: Comparison of latency

Accuracy [138]**:** In the context of a block chain experiment, it refers to the correctness of the transmitted or processed information in comparison to the expected outcome. It indicated the well the systems perform in terms of data integrity, minimizing errors during the communications or processing phases, ensuring that the system delivers precise results as shown in Fig. 17.

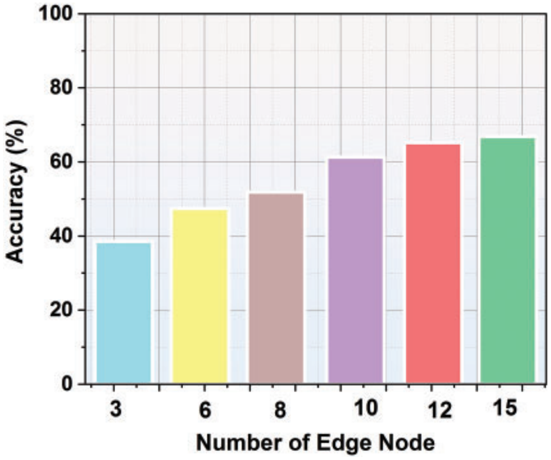


Figure 17: Comparison of accuracy

Throughput [139]**:** The quantity of data that is successfully sent over a network in a specific length of time is known as throughput. Throughput, which reflects the total bandwidth and the system's ability to handle several jobs or communications at once, gauges the system's ability to efficiently manage data flow in a blockchain setting. High throughput ensures effective data transmission even under heavy load conditions as shown in Fig. 18.

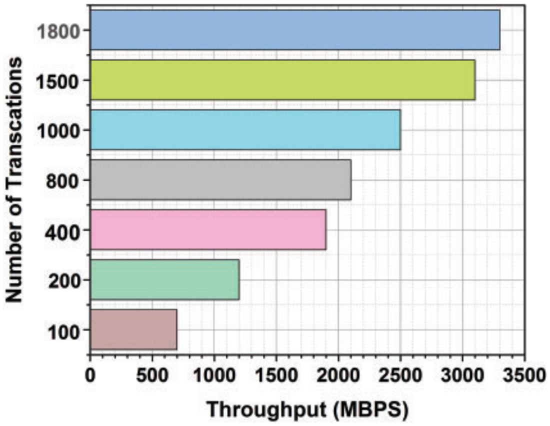


Figure 18: Comparison of throughput

End to end delay [139]**:** It explains the total amount of time an information packet takes to travel from its source to its destination, accounting for all intermediate steps. End-to-end delays include and delays caused by processing, transmission, queuing along the path. In block chain systems, minimizing end-to-end delay is critical for applications requiring rapid decision making and low latency communications are as shown in Fig. 19.

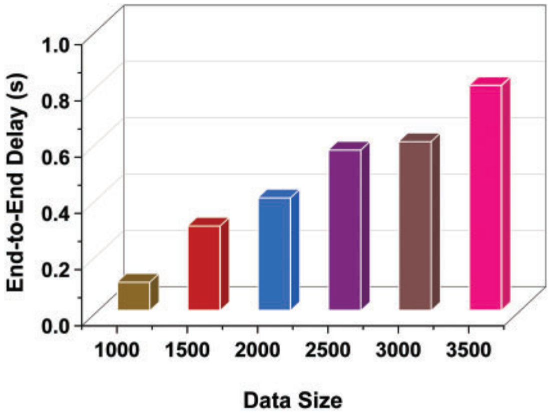


Figure 19: Comparison of end-to-end delay

4.4 IoT Applications

For example, Fig. 20 [140] compares the percentage of IoT applications to date by taxonomy. It looked at six IoT application domains. According to the literature, the smart city strategy has the largest percentage of application domains (30%). Applications for the IoT are divided as follows: business uses 14%, health care uses 20%, general uses 12%, environmental uses 12%, and industrial uses 10%.

4.5 Global Share of IoT Projects

Fig. 21 [141] displays the market share of IoT projects worldwide. IoT programmers centered on business, cities that are smart, connected power, and smart vehicles have a larger market share than other initiatives.

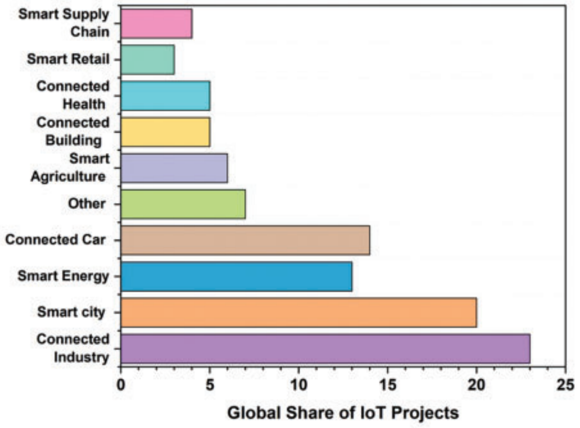


Figure 20: The proportion of IoT apps that were displayed

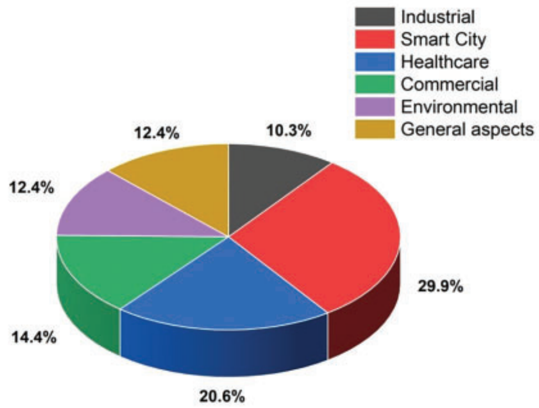


Figure 21: The proportion of IoT projects worldwide

Fig. 22 shows the publisher and year-by-year details of the surveyed articles from reputable publishers, such as IEEE, MDPI, Springer, and Elsevier, which are specifically targeted. Most of the examined publications are from recent years, specifically 2020 and 2019, and are indexed [142].

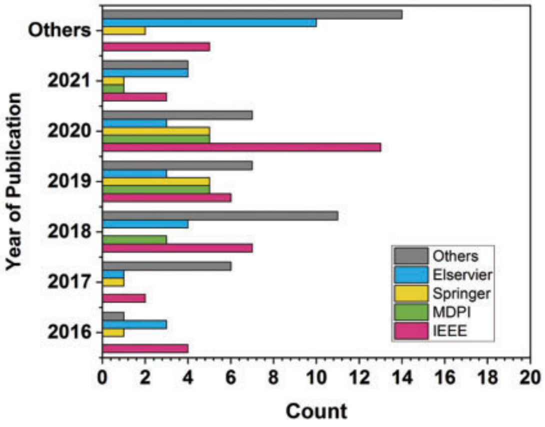


Figure 22: Graphical display of the examined articles' year-by-year details

4.6 Future Suggestions on How Using AI Can Further Increase IoT Security

- **Federated Learning Enhancements**

Future Direction: The main goal of federated learning advancements should be to address current issues with model convergence, security threats, and communication overhead. Future research can concentrate on privacy-preserving technologies and adaptive federated learning strategies designed specifically for decentralized IoT environments [143]. The potential of federated learning enhances IoT security, but the suggestions remain abstract and would benefit from concrete examples or case studies demonstrating their feasibility and impact. For instance, illustrating that privacy-preserving technologies can be applied in real-world decentralized IoT environments would make the argument more practical. Additionally, while the research acknowledges the rapid evolution of IoT and AI technologies, it does not fully explore how the dynamic landscape might affect the long-term validity of the findings or the adaptability of the proposed solutions.

Rationale: In situations where data decentralization is a basic necessity, improved federated learning techniques can greatly aid in protecting privacy. For federated learning in the IoT to be successful, communication issues must be resolved, and strong security measures must be in place.

- **Standards and Regulations Protecting Privacy**

Future Direction: Research should also focus on creating standards and laws that protect privacy for cloud systems that are based on IoT. This entails working with industry stakeholders, regulatory agencies, and privacy specialists to create standards that guarantee the uniform implementation of privacy safeguards in IoT contexts.

Rationale: Standardized laws and policies can give companies a framework to work within and serve as a benchmark for evaluating how well privacy-preserving practices are performing.

4.7 Discussion

A significant limitation in evaluating the classifiers (DCNN, FCFFN, DAE-DNN, FNN-Focal, CNN) and ensemble techniques (RF, DT, XGBoost, AdaBoost, ensemble RF-BRNN) in terms of performance metrics like throughput, end-to-end delay, and latency is a lack of a clear understanding of how the model's dimension in actual network and internet of things (IoT) environments. Real-time processing, computing expenses, and resource limitations could limit the practical applicability of the models, considering that the models can demonstrate beneficial accuracy and precision in controlled circumstances. The systems with limited resources, the deep learning (DL) models such as CNN and DCNN are effective at extracting the features and frequently demand a large processing time and computational power, which results in high latency and decreased throughput. Faster processing speeds could be provided by the traditional machine learning (ML) models like RF and AdaBoost, whereas there could be limitations on performance that the DL algorithms are efficient at capturing the complex patterns.

The ensemble approaches can include further layers of complexity, which could lead to significant increases in the computational load and network latency as it enhances accuracy. As a result, the primary complexity in implementing these models in dynamic IoT and network systems is maintaining high performance while addressing issues like low latency, scalability, and real-time throughput. This type of assault has been studied and identified using ML methods like k-nearest neighbor (KNN) and decision trees. The accuracy of the two suggested algorithms is noticeably higher when compared to widely utilized techniques. Furthermore, the outcomes show that the two suggested algorithms have outperformed alternative categorization techniques by a significant margin. Furthermore, for these two techniques, greater p-values correspond to increased detection accuracy. This issue demonstrates that the detectors can identify fake data injection assaults that result in more serious system disruptions [144]. A framework for safe data management that includes a strong data flow architecture, encryption, integrity checking, and an integrated communication network. We examine the various facets of data integrity, security, and privacy as well as viable solutions in the context of blockchain and IoT integration. With an emphasis on algorithmic, mathematical, and cryptographic viewpoints, the paper also explores the safe transaction procedure. To fully address the associated security and privacy concerns, we utilized flow charts to demonstrate how blockchain technology might be applied in the nuclear energy sector. It emphasizes the importance of our approach to the nuclear industry and also acknowledges its limitations, such as the requirement for real-world validation, challenges in IoT contexts with limited resources, the rise in cyber risks, and the absence of real-time data availability [145].

5 Conclusion

The review aimed to explore modern AI technologies, particularly ML and BC for enhancing security in IoT ecosystems. The objective was to systematically investigate IoT security challenges, focusing on privacy preservation, threat detection, and data integrity, and to assess the efficacy of AL-driven solutions in addressing these core concerns. Additionally, it wanted to categorize these solutions based on their performance and provide insights into directions that could further enhance IoT security. The approach used comprised a thorough analysis of the body of research on AI-powered privacy-preserving IoT security measures. It examined a variety of security issues within IoT networks, including vulnerabilities related to device heterogeneity and resource constraints. Various AI techniques, particularly ML algorithms and BC were explored for their effectiveness in mitigating these issues. Solutions were categorized according to their capability to address specific security challenges, with an emphasis on advancement in threat detection, Anomaly identification, and data integrity. The findings of the research indicate that AI solutions, especially those incorporating ML and BC technologies, have significantly advanced the security landscape of IoT ecosystems. It improves data threat detection, enhances privacy preservation, and ensures the integrity of data exchanges within IoT networks. The integration of BC is particularly beneficial in providing tamper-proof data transactions and decentralized control, which is crucial for sectors such as healthcare, fiancé and smart cities, furthermore, the review demonstrated that AI-enhanced IoT systems exhibit improvements in key performance metrics such as accuracy, precision, recall, and f1-score, with AI techniques showing potential to reduce false positives and enhance detection rates.

5.1 Limitations

The review acknowledges the limitations of IoT and AI technologies, including the rapid evolution, complexity of standardized AI solutions due to diverse IoT applications and devices, and the need for more empirical studies to validate the effectiveness of AI-driven mechanisms across different IoT contexts. The research limitations include that, while it conducts significant analysis of current literature, it does not present particular case studies and experiences with AI-driven cyber security solutions for IoT. Although it highlights a few potential AI technologies, such as machine learning and blockchain, it fails to address any scalability issues that could occur in large, heterogeneous IoT networks. The assessment finds no trade-offs in terms of resource usage that would prevent the practical implementation of stronger AI-based security approaches, particularly for restricted devices. Also, because IoT and AI technologies are continually changing, many of their conclusions may become obsolete as discoveries emerge. Furthermore, it does not investigate the other possible hazards of deploying AI models, such as adversarial assaults on AI algorithms, which might undoubtedly impair their effective operation to safeguard IoT networks. Finally, the limited exploration of cross-disciplinary approaches might constrain a deeper conceptualization of broader ramifications on IoT security.

5.2 Future Work

Future studies should focus on developing AI systems that utilize techniques such as reinforcement learning and self-optimization, enabling them to dynamically adjust to the evolving demands of IoT environments. These AI models should be capable of continually learning from real-time data, adapting their behavior based on changes in network conditions, device states, and user interactions. Incorporating federated learning will allow these systems to learn from decentralized data while maintaining privacy and edge computing will enable quicker, localized decision making, reducing latency. Moreover, attention should be on creating AI models that can generalize across various applications, ensuring they are not robust enough to manage diverse environments while addressing challenges related to data security, integrity and quality.

Acknowledgement: The author Dr. Arshiya Sajid Ansari extends appreciation to the Deanship of Postgraduate Studies and Scientific Research at Majmaah University for funding this research work through project number (R-2025-1706).

Funding Statement: The author Dr. Arshiya Sajid Ansari extends the appreciation to the Deanship of Postgraduate Studies and Scientific Research at Majmaah University for funding this research work through the project number (R-2025-1706).

Author Contributions: Data collection: Arshiya Sajid Ansari & Mohammad Sajid Mohammadi; Analysis and interpretation of results: Mohammad Sajid Mohammadi & Arshiya Sajid Ansari; Draft manuscript preparation: Fahad Alodhyani, Ghadir Altuwaijri, Moulay Ibrahim El-Khalil Ghembaza & Shahabas Manakunnath Devasam Paramb. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Not applicable.

Ethics Approval: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest to report regarding the present study.

Abbreviations

Acronyms	Description
IoT	Internet of Things
AI	Artificial Intelligence
ML	Machine Learning
RFID	Radio Frequency Identification
IIoT	Industrial IoT
DNN	Deep Neural Networks
DoS	Denial of Service
GIS	Geographic Information System
DDoS	Distributed DoS
NLP	Natural Language Processing
EC-IoT	Edge Computing-Internet of Things
VR	Virtual Reality
DL	Deep Learning
IoV	Internet of Vehicles
NPU	Network Processing Unit
SCM	Supply Chain Management
FATL	Federated Active Transfer Learning
H-IoT	Healthcare IoT
IDS	Intrusion Detection System
DL	Deep Learning
RNN	Recurrent Nural Network
DBN	Deep Belief Network
BAC-IDS	Blockchain-Assisted Clustering with IDS
CNN	Convolutional Neural Network
Bi-LSTM	Bidirectional Long Short-Term Memory
BCEAD	Blockchain-Based Ensemble Anomaly Detection
RL	Reinforcement-Learning
ROC	Receiver Operating Characteristic
AUC	Area Under Curve
MITM	Man In the Middle

BC-HyIDS	Blockchain-based Hybrid Intrusion Detection System
SSL/TLS	Secure Socket Layer/Transport Layer Security
MQTT	Message Queuing Telemetry Transport
XGB	XGBoost
PSO-RF	Particle Swarm Optimization-Random Forest
GRU	Gated Recurrent Unit

References

1. Sarker IH, Khan AI, Abushark YB, Alsolami F. Internet of Things (IoT) security intelligence: a comprehensive overview, machine learning solutions and research directions. Mob Netw Appl. 2023;28(1):296–312. doi:10.1007/s11036-022-01937-3.
2. Goje SS, Asutkar SM, Asutkar GM. Study of various AI based security model for threat analysis in communication and IoT network. In: AIP Conference Proceedings. Melville, NY, USA: AIP Publishing; 2025. doi:10.1063/5.0254197.
3. Magaia N, Fonseca R, Muhammad K, Segundo AHFN, Lira Neto AV, de Albuquerque VHC. Industrial Internet-of-things security enhanced with deep learning approaches for smart cities. IEEE Internet Things J. 2021;8(8):6393–405. doi:10.1109/JIOT.2020.3042174.
4. Shi F, Ning H, Huangfu W, Zhang F, Wei D, Hong T, et al. Recent progress on the convergence of the Internet of Things and artificial intelligence. IEEE Netw. 2020;34(5):8–15. doi:10.1109/MNET.011.2000009.
5. Ahmed I, Zhang Y, Jeon G, Lin W, Khosravi MR, Qi L. A blockchain- and artificial intelligence-enabled smart IoT framework for sustainable city. Int J Intelligent Sys. 2022;37(9):6493–507. doi:10.1002/int.22852.
6. Aldoseri A, Al-Khalifa KN, Hamouda AM. Re-thinking data strategy and integration for artificial intelligence: concepts, opportunities, and challenges. Appl Sci. 2023;13(12):7082. doi:10.3390/app13127082.
7. Saxena R, Gayathri E, Surya Kumari L. Semantic analysis of blockchain intelligence with proposed agenda for future issues. Int J Syst Assur Eng Manag. 2023;14(S1):34–54. doi:10.1007/s13198-023-01862-y.
8. Rathee G, Khelifi A, Iqbal R. Artificial intelligence-(AI-) enabled Internet of Things (IoT) for secure big data processing in multihoming networks. Wirel Commun Mob Comput. 2021;2021(1):5754322. doi:10.1155/2021/5754322.
9. Basaure A, Vesselkov A, Töyli J. Internet of Things (IoT) platform competition: consumer switching versus provider multihoming. Technovation. 2020;90(1):102101. doi:10.1016/j.technovation.2019.102101.
10. Ajani SN, Khobragade P, Jadhav PV, Mahajan RA, Ganguly B, Parati N. Frontiers of computing—evolutionary trends and cutting-edge technologies in computer science and next generation application. J Electr Syst. 2024;20(1s):28–45. doi:10.52783/jes.750.
11. Mazhar T, Talpur DB, Shloul TA, Ghadi YY, Haq I, Ullah I, et al. Analysis of IoT security challenges and its solutions using artificial intelligence. Brain Sci. 2023;13(4):683. doi:10.3390/brainsci13040683.
12. Ahmed U, Nazir M, Sarwar A, Ali T, Aggoune EM, Shahzad T, et al. Signature-based intrusion detection using machine learning and deep learning approaches empowered with fuzzy clustering. Sci Rep. 2025;15(1):1726. doi:10.1038/s41598-025-85866-7.
13. Kizza JM. Internet of Things (IoT): growth, challenges, and security. In: Guide to computer network security. Berlin/Heidelberg, Germany: Springer; 2024. p. 557–73. doi:10.1007/978-3-031-47549-8_25.
14. Shehu Yalli J, Hilmi Hasan M, Abubakar Badawi A. Internet of Things (IoT): origins, embedded technologies, smart applications, and its growth in the last decade. IEEE Access. 2024;12(1):91357–82. doi:10.1109/ACCESS.2024.3418995.
15. Ghosh A, Edwards DJ, Hosseini MR. Patterns and trends in Internet of Things (IoT) research: future applications in the construction industry. Eng Constr Archit Manag. 2020;28(2):457–81. doi:10.1108/ECAM-04-2020-0271.
16. Bajaj K, Sharma B, Singh R. Integration of WSN with IoT applications: a vision, architecture, and future challenges. In: Integration of WSN and IoT for smart cities. Berlin/Heidelberg, Germany: Springer; 2020. p. 79–102. doi:10.1007/978-3-030-38516-3_5.

17. Maraveas C, Piromalis D, Arvanitis KG, Bartzanas T, Loukatos D. Applications of IoT for optimized greenhouse environment and resources management. Comput Electron Agric. 2022;198(10):106993. doi:10.1016/j.compag.2022.106993.
18. Choppara P, Lokesh B. Efficient task scheduling and load balancing in fog computing for crucial healthcare through deep reinforcement learning. IEEE Access. 2025;13:26542–63. doi:10.1109/ACCESS.2025.3539336.
19. Quy VK, Hau NV, Anh DV, Quy NM, Ban NT, Lanza S, et al. IoT-enabled smart agriculture: architecture, applications, and challenges. Appl Sci. 2022;12(7):3396. doi:10.3390/app12073396.
20. Stolojescu-Crisan C, Crisan C, Butunoi BP. An IoT-based smart home automation system. Sensors. 2021;21(11):3784. doi:10.3390/s21113784.
21. Ajay P, Nagaraj B, Pillai BM, Suthakorn J, Bradha M. Intelligent ecofriendly transport management system based on IoT in urban areas. Environ Dev Sustain. 2022;10(3):1–8. doi:10.1007/s10668-021-02010-x.
22. Goudarzi M, Wu H, Palaniswami M, Buyya R. An application placement technique for concurrent IoT applications in edge and fog computing environments. IEEE Trans Mob Comput. 2021;20(4):1298–311. doi:10.1109/TMC.2020.2967041.
23. Le Nguyen B, Laxmi Lydia E, Elhoseny M, Pustokhina IV, Pustokhin DA, Mohamed Selim M, et al. Privacy preserving blockchain technique to achieve secure and reliable sharing of IoT data. Comput Mater Contin. 2020;65(1):87–107. doi:10.32604/cmc.2020.011599.
24. Li C, Xu G, Chen Y, Ahmad H, Li J. A new anti-quantum proxy blind signature for blockchain-enabled Internet of Things. Comput Mater Contin. 2019;61(2):711–26. doi:10.32604/cmc.2019.06279.
25. Chen H, Wan W, Xia J, Zhang S, Zhang J, Peng X, et al. Task-attribute-based access control scheme for IoT *via* blockchain. Comput Mater Contin. 2020;65(3):2441–53. doi:10.32604/cmc.2020.011824.
26. Atlam HF, Alenezi A, Alassafi MO, Wills GB. Blockchain with Internet of Things: benefits, challenges, and future directions. Int J Intell Syst Appl. 2018;10(6):40–8. doi:10.5815/ijisa.2018.06.05.
27. Reyna A, Martín C, Chen J, Soler E, Díaz M. On blockchain and its integration with IoT. Challenges and opportunities. Future Gener Comput Syst. 2018;88(3):173–90. doi:10.1016/j.future.2018.05.046.
28. Acharya B, Garikapati K, Yarlagadda A, Dash S. Internet of Things (IoT) and data analytics in smart agriculture: benefits and challenges. In: AI, Edge and IoT-based smart agriculture. Amsterdam, The Netherlands: Elsevier; 2022. p. 3–16. doi:10.1016/b978-0-12-823694-9.00013-x.
29. Obaideen K, Yousef BAA, AlMallahi MN, Tan YC, Mahmoud M, Jaber H, et al. An overview of smart irrigation systems using IoT. Energy Nexus. 2022;7(8):100124. doi:10.1016/j.nexus.2022.100124.
30. Sinha BB, Dhanalakshmi R. Recent advancements and challenges of Internet of Things in smart agriculture: a survey. Future Gener Comput Syst. 2022;126(4):169–84. doi:10.1016/j.future.2021.08.006.
31. Dhanaraju M, Chenniappan P, Ramalingam K, Pazhanivelan S, Kaliaperumal R. Smart farming: Internet of Things (IoT)-based sustainable agriculture. Agriculture. 2022;12(10):1745. doi:10.3390/agriculture12101745.
32. Jani KA, Chaubey NK. A novel model for optimization of resource utilization in smart agriculture system using IoT (SMAIoT). IEEE Internet Things J. 2022;9(13):11275–82. doi:10.1109/JIOT.2021.3128161.
33. Hassan RJ, Zeebaree SRM, Ameen SY, Kak SF, Sadeeq MAM, Ageed ZS, et al. State of art survey for IoT effects on smart city technology: challenges, opportunities, and solutions. Asian J Res Comput Sci. 2021;2021:32–48. doi:10.9734/ajrcos/2021/v8i330202.
34. Polymeni S, Skoutas DN, Sarigiannidis P, Kormentzas G, Skianis C. Smart agriculture and greenhouse gas emission mitigation: a 6G-IoT perspective. Electronics. 2024;13(8):1480. doi:10.3390/electronics13081480.
35. Selvam AP, Al-Humairi SNS. The impact of IoT and sensor integration on real-time weather monitoring systems: a systematic review. [cited 2025 Jan 1]. Available from: https://doi.org/10.21203/rs.3.rs-3579172/v1.
36. Dhinakaran D, Joe Prathap PM. Preserving data confidentiality in association rule mining using data share allocator algorithm. arXiv:230414605. 2023. doi:10.32604/iasc.2022.024509.
37. Dhinakaran D, Sankar S, Selvaraj D, Raja SE. Privacy-preserving data in IoT-based cloud systems: a comprehensive survey with AI integration. arXiv:240100794. 2024. doi:10.32604/iasc.2022.024509.
38. Zhang J, Wang Z, Shang L, Lu D, Ma J. BTNC: a blockchain-based trusted network connection protocol in IoT. J Parallel Distrib Comput. 2020;143(1):1–16. doi:10.1016/j.jpdc.2020.04.004.

39. Onik MMH, Kim CS, Yang J. Personal data privacy challenges of the fourth industrial revolution. In: 2019 21st International Conference on Advanced Communication Technology (ICACT); 2019 Feb 17–20; PyeongChang, Republic of Korea.

40. Selvaraj D, Udhay Sankar SM, Dhinakaran D, Anish TP. Outsourced analysis of encrypted graphs in the cloud with privacy protection. arXiv:230410833. 2023. doi:10.14445/23488379/ijeee-v10i1p105.

41. Chen H, Huang Z, Laine K, Rindal P. Labeled PSI from fully homomorphic encryption with malicious security. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security; 2018 Oct 15–19; Toronto, ON, Canada. doi:10.1145/3243734.3243836.

42. Mkpa A. A dynamic configurable model for addressing trust and privacy in IoT networks: anglia ruskin research online (ARRO) [master's thesis]. Cambridge, UK: Anglia Ruskin University; 2024.

43. Awotunde JB, Jimoh RG, Folorunso SO, Adeniyi EA, Abiodun KM, Banjo OO. Privacy and security concerns in IoT-based healthcare systems. In: The fusion of internet of things, artificial intelligence, and cloud computing in health care. Berlin/Heidelberg, Germany: Springer; 2021. p. 105–34. doi:10.1007/978-3-030-75220-0_6.

44. Malhotra P, Singh Y, Anand P, Bangotra DK, Singh PK, Hong WC. Internet of Things: evolution, concerns and security challenges. Sensors. 2021;21(5):1809. doi:10.3390/s21051809.

45. Ali Qasem M, Thabit F, Can O, Naji E, Alkhzaimi HA, Patil PR, et al. Cryptography algorithms for improving the security of cloud-based Internet of Things. Secur Priv. 2024;7(4):e378. doi:10.1002/spy2.378.

46. Arulmurugan L, Thakur S, Dayana R, Thenappan S, Nagesh B, Sri RK. Advancing security: exploring AI-driven data encryption solutions for wireless sensor networks. In: 2024 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI); 2024 May 9–10; Chennai, India. doi:10.1109/ACCAI61061.2024.10602020.

47. Nazir A, He J, Zhu N, Wajahat A, Ma X, Ullah F, et al. Advancing IoT security: a systematic review of machine learning approaches for the detection of IoT botnets. J King Saud Univ Comput Inf Sci. 2023;35(10):101820. doi:10.1016/j.jksuci.2023.101820.

48. Qureshi SU, He J, Tunio S, Zhu N, Nazir A, Wajahat A, et al. Systematic review of deep learning solutions for malware detection and forensic analysis in IoT. J King Saud Univ Comput Inf Sci. 2024;36(8):102164. doi:10.1016/j.jksuci.2024.102164.

49. Ali Khattak H, Ali Shah M, Khan S, Ali I, Imran M. Perception layer security in Internet of Things. Future Gener Comput Syst. 2019;100(7):144–64. doi:10.1016/j.future.2019.04.038.

50. Cheng CF, Chen YC, Lin JC. A carrier-based sensor deployment algorithm for perception layer in the IoT architecture. IEEE Sens J. 2020;20(17):10295–305. doi:10.1109/JSEN.2020.2989871.

51. Jurcut AD, Ranaweera P, Xu L. Introduction to IoT security. In: IoT security: advances in authentication. Hoboken, NJ, USA: John Wiley & Sons, Inc; 2020. p. 27–64. doi:10.1002/9781119527978.ch2.

52. Ande R, Adebisi B, Hammoudeh M, Saleem J. Internet of Things: evolution and technologies from a security perspective. Sustain Cities Soc. 2020;54(5):101728. doi:10.1016/j.scs.2019.101728.

53. Hu S, Chen X, Ni W, Hossain E, Wang X. Distributed machine learning for wireless communication networks: techniques, architectures, and applications. IEEE Commun Surv Tutor. 2021;23(3):1458–93. doi:10.1109/COMST.2021.3086014.

54. Zhang J, Rajendran S, Sun Z, Woods R, Hanzo L. Physical layer security for the Internet of Things: authentication and key generation. IEEE Wirel Commun. 2019;26(5):92–8. doi:10.1109/MWC.2019.1800455.

55. Altwoyan W, Alsukayti IS. A novel IoT architecture for seamless IoT integration into university systems. Int J Adv Comput Sci Appl. 2022;13(4):109–16. doi:10.14569/ijacsa.2022.0130413.

56. Rahman A, Islam J, Kundu D, Karim R, Rahman Z, Band SS, et al. Impacts of blockchain in software-defined Internet of Things ecosystem with Network Function Virtualization for smart applications: present perspectives and future directions. Int J Communication. 2025;38(1):e5429. doi:10.1002/dac.5429.

57. Swamy SN, Kota SR. An empirical study on system level aspects of Internet of Things (IoT). IEEE Access. 2020;8:188082–134. doi:10.1109/ACCESS.2020.3029847.

58. Tewari A, Gupta BB. Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. Future Gener Comput Syst. 2020;108(4):909–20. doi:10.1016/j.future.2018.04.027.

59. Ahlawat B, Sangwan A, Sindhu V. IoT system model, challenges and threats. Int J Sci Technol Res. 2020;9(3):6771–6.

60. Touqeer H, Zaman S, Amin R, Hussain M, Al-Turjman F, Bilal M. Smart home security: challenges, issues and solutions at different IoT layers. J Supercomput. 2021;77(12):14053–89. doi:10.1007/s11227-021-03825-1.

61. Quy VK, Hau NV, Anh DV, Ngoc LA. Smart healthcare IoT applications based on fog computing: architecture, applications and challenges. Complex Intell Systems. 2022;8(5):3805–15. doi:10.1007/s40747-021-00582-9.

62. Jamshidi S, Nikanjam A, Nafi KW, Khomh F, Rasta R. Application of deep reinforcement learning for intrusion detection in Internet of Things: a systematic review. Internet Things. 2025;31(8):101531. doi:10.1016/j.iot.2025.101531.

63. Abdulrahman NF, Jit Singh MS. Deep learning approaches for DDoS attack detection in communication networks and IoT: a comprehensive review. J Kejuruter. 2025;37(1):323–33. doi:10.17576/jkukm-2025-37(1)-22.

64. Kaushik K, Bhardwaj A, Dahiya S. Framework to analyze and exploit the smart home IoT firmware. Meas Sens. 2025;37(10):101406. doi:10.1016/j.measen.2024.101406.

65. Abosata N, Al-Rubaye S, Inalhan G, Emmanouilidis C. Internet of Things for system integrity: a comprehensive survey on security, attacks and countermeasures for industrial applications. Sensors. 2021;21(11):3654. doi:10.3390/s21113654.

66. Khanam S, Ahmedy IB, Idris MY, Jaward MH, Sabri AQ. A survey of security challenges, attacks taxonomy and advanced countermeasures in the Internet of Things. IEEE Access. 2020;8:219709–43. doi:10.1109/ACCESS.2020.3037359.

67. Vaigandla K, Azmi N, Karne R. Investigation on intrusion detection systems (IDSs) in IoT. Int J Emerg Trends Eng Res. 2022;10(3):158–66. doi:10.30534/ijeter/2022/041032022.

68. Logeswari G, Deepika Roselind J, Tamilarasi K, Nivethitha V. A comprehensive approach to intrusion detection in IoT environments using hybrid feature selection and multi-stage classification techniques. IEEE Access. 2025;13(4):24970–87. doi:10.1109/ACCESS.2025.3532895.

69. Verma A, Ranga V. Machine learning based intrusion detection systems for IoT applications. Wirel Pers Commun. 2020;111(4):2287–310. doi:10.1007/s11277-019-06986-8.

70. Smys DS, Basar DA, Wang DH. Hybrid intrusion detection system for Internet of Things (IoT). J ISMAC. 2020;2(4):190–9. doi:10.36548/jismac.2020.4.002.

71. Heidari A, Ali Jabraeil Jamali M. Internet of Things intrusion detection systems: a comprehensive review and future directions. Clust Comput. 2023;26(6):3753–80. doi:10.1007/s10586-022-03776-z.

72. Almiani M, AbuGhazleh A, Al-Rahayfeh A, Atiewi S, Razaque A. Deep recurrent neural network for IoT intrusion detection system. Simul Model Pract Theory. 2020;101:102031. doi:10.1016/j.simpat.2019.102031.

73. Sai Kiran KVVNL, Kamakshi Devisetty RN, Kalyan NP, Mukundini K, Karthi R. Building a intrusion detection system for IoT environment using machine learning techniques. Procedia Comput Sci. 2020;171(7):2372–9. doi:10.1016/j.procs.2020.04.257.

74. Vargas H, Lozano-Garzon C, Montoya GA, Donoso Y. Detection of security attacks in industrial IoT networks: a blockchain and machine learning approach. Electronics. 2021;10(21):2662. doi:10.3390/electronics10212662.

75. Al-Shurbaji T, Anbar M, Manickam S, Hasbullah IH, Alfriehat N, Ahmad Alabsi B, et al. Deep learning-based intrusion detection system for detecting IoT botnet attacks: a review. IEEE Access. 2025;13(8):11792–822. doi:10.1109/ACCESS.2025.3526711.

76. Bhavsar M, Roy K, Kelly J, Olusola O. Anomaly-based intrusion detection system for IoT application. Discov Internet Things. 2023;3(1):5. doi:10.1007/s43926-023-00034-5.

77. Balakrishnan N, Rajendran A, Pelusi D, Ponnusamy V. Deep Belief Network enhanced intrusion detection system to prevent security breach in the Internet of Things. Internet Things. 2021;14(4):100112. doi:10.1016/j.iot.2019.100112.

78. Saravanan V, Madiajagan M, Rafee SM, Sanju P, Rehman TB, Pattanaik B. IoT-based blockchain intrusion detection using optimized recurrent neural network. Multimed Tools Appl. 2024;83(11):31505–26. doi:10.1007/s11042-023-16662-6.

79. Mansour RF. Blockchain assisted clustering with intrusion detection system for industrial Internet of Things environment. Expert Syst Appl. 2022;207(14):117995. doi:10.1016/j.eswa.2022.117995.

80. Liang C, Shanmugam B, Azam S, Karim A, Islam A, Zamani M, et al. Intrusion detection system for the Internet of Things based on blockchain and multi-agent systems. Electronics. 2020;9(7):1120. doi:10.3390/electronics9071120.
81. Tukur YM, Thakker D, Awan IU. Edge-based blockchain enabled anomaly detection for insider attack prevention in Internet of Things. Trans Emerging Tel Tech. 2021;32(6):e4158. doi:10.1002/ett.4158.
82. de Melo PHAD, Miani RS, Rosa PF. FamilyGuard: a security architecture for anomaly detection in home networks. Sensors. 2022;22(8):2895. doi:10.3390/s22082895.
83. Abusitta A, de Carvalho GHS, Abdel Wahab O, Halabi T, Fung BCM, Al Mamoori S. Deep learning-enabled anomaly detection for IoT systems. Internet Things. 2023;21(2):100656. doi:10.1016/j.iot.2022.100656.
84. Ullah I, Mahmoud QH. Design and development of RNN anomaly detection model for IoT networks. IEEE Access. 2022;10:62722–50. doi:10.1109/ACCESS.2022.3176317.
85. Cauteruccio F, Cinelli L, Corradini E, Terracina G, Ursino D, Virgili L, et al. A framework for anomaly detection and classification in Multiple IoT scenarios. Future Gener Comput Syst. 2021;114(1):322–35. doi:10.1016/j.future.2020.08.010.
86. Yang X, Chen Y, Qian X, Li T, Lv X. BCEAD: a blockchain-empowered ensemble anomaly detection for wireless sensor network *via* isolation forest. Secur Commun Netw. 2021;2021:9430132. doi:10.1155/2021/9430132.
87. Kim J, Nakashima M, Fan W, Wuthier S, Zhou X, Kim I, et al. Anomaly detection based on traffic monitoring for secure blockchain networking. In: 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC); 2021 May 3–6; Sydney, Australia. doi:10.1109/icbc51069.2021.9461119.
88. Seifi S, Beaubrun R, Bellaiche M, Halabi T. A study on the efficiency of intrusion detection systems in IoT networks. In: 2023 International Conference on Computer, Information and Telecommunication Systems (CITS); 2023 Jul 10–12; Genoa, Italy. doi:10.1109/CITS58301.2023.10188799.
89. Singh R, Tanwar S, Sharma TP. Utilization of blockchain for mitigating the distributed denial of service attacks. Secur Priv. 2020;3(3):e96. doi:10.1002/spy2.96.
90. Kumari P, Jain AK. A comprehensive study of DDoS attacks over IoT network and their countermeasures. Comput Secur. 2023;127(2):103096. doi:10.1016/j.cose.2023.103096.
91. Kumar R, Kumar P, Tripathi R, Gupta GP, Garg S, Hassan MM. A distributed intrusion detection system to detect DDoS attacks in blockchain-enabled IoT network. J Parallel Distrib Comput. 2022;164(2):55–68. doi:10.1016/j.jpdc.2022.01.030.
92. Wani S, Imthiyas M, Almohamedh H, Alhamed KM, Almotairi S, Gulzar Y. Distributed denial of service (DDoS) mitigation using blockchain—a comprehensive insight. Symmetry. 2021;13(2):227. doi:10.3390/sym13020227.
93. Ali MH, Jaber MM, Abd SK, Rehman A, Awan MJ, Damaševičius R, et al. Threat analysis and distributed denial of service (DDoS) attack recognition in the Internet of Things (IoT). Electronics. 2022;11(3):494. doi:10.3390/electronics11030494.
94. Ahmed S, Khan ZA, Mohsin SM, Latif S, Aslam S, Mujlid H, et al. Effective and efficient DDoS attack detection using deep learning algorithm, multi-layer perceptron. Future Internet. 2023;15(2):76. doi:10.3390/fi15020076.
95. Yin X, Fang W, Liu Z, Liu D. A novel multi-scale CNN and Bi-LSTM arbitration dense network model for low-rate DDoS attack detection. Sci Rep. 2024;14(1):5111. doi:10.1038/s41598-024-55814-y.
96. Alghazzawi D, Bamasag O, Ullah H, Asghar MZ. Efficient detection of DDoS attacks using a hybrid deep learning model with improved feature selection. Appl Sci. 2021;11(24):11634. doi:10.3390/app112411634.
97. Cheng J, Liu Y, Tang X, Sheng VS, Li M, Li J. DDoS attack detection via multi-scale convolutional neural network. Comput Mater Contin. 2020;62(3):1317–33. doi:10.32604/cmc.2020.06177.
98. Hairab BI, Said Elsayed M, Jurcut AD, Azer MA. Anomaly detection based on CNN and regularization techniques against zero-day attacks in IoT networks. IEEE Access. 2022;10(11):98427–40. doi:10.1109/ACCESS.2022.3206367.
99. Ahmed Issa AS, Albayrak Z. DDoS attack intrusion detection system based on hybridization of CNN and LSTM. Acta Polytech Hung. 2023;20(2):105–23. doi:10.12700/APH.20.2.2023.2.6.
100. Saadallah O, Nouar I. Feature selection methods for intrusion detection systems in IoT. In: 2025 IEEE 23rd World Symposium on Applied Machine Intelligence and Informatics (SAMI); 2025 Jan 23–25; Stará Lesná, Slovakia. doi:10.1109/SAMI63904.2025.10883062.

101. Madanian S, Chinbat T, Subasinghage M, Airehrour D, Hassandoust F, Yongchareon S. Health IoT threats: survey of risks and vulnerabilities. Future Internet. 2024;16(11):389. doi:10.3390/fi16110389.
102. Robert W, Denis A, Thomas A, Samuel A, Kabiito SP, Morish Z, et al. A comprehensive review on cryptographic techniques for securing Internet of medical things: a state-of-the-art, applications, security attacks, mitigation measures, and future research direction. Mesopotamian J Artif Intell Healthc. 2024;2024:135–69. doi:10.58496/MJAIH/2024/016.
103. Cherian MM, Varma SL. Mitigation of DDOS and MiTM attacks using belief based secure correlation approach in SDN-based IoT networks. Int J Comput Netw Inf Secur. 2021;14(1):52–68. doi:10.5815/ijcnis.2022.01.05.
104. Cecílio J, Souto A. Security issues in industrial Internet-of-things: threats, attacks and solutions. In: 2024 IEEE International Workshop on Metrology for Industry 4.0 & IoT (MetroInd4.0 & IoT); 2024 May 29–31; Firenze, Italy. doi:10.1109/MetroInd4.0IoT61288.2024.10584217.
105. Perwej Y, Akhtar N, Kulshrestha N, Mishra P. A methodical analysis of medical Internet of Things (MIoT) security and privacy in current and future trends. J Emerg Technol Innov Res. 2022;9(1):d346–71.
106. Wong H, Luo T. Man-in-the-middle attacks on mqtt-based IoT using bert-based adversarial message generation. In: KDD 2020 AIoT Workshop; 2020 Aug 24; Virtual.
107. OConnor TJ, Jessee D, Campos D. Through the spyglass: towards IoT companion app man-in-the-middle attacks. In: Proceedings of the 14th Cyber Security Experimentation and Test Workshop; 2021 Aug 9; Virtual. doi:10.1145/3474718.3474729.
108. Rihan SDA, Anbar M, Alabsi BA. Meta-learner-based approach for detecting attacks on Internet of Things networks. Sensors. 2023;23(19):8191. doi:10.3390/s23198191.
109. Michelena Á, Aveleira-Mata J, Jove E, Bayón-Gutiérrez M, Novais P, Romero OF, et al. A novel intelligent approach for man-in-the-middle attacks detection over Internet of Things environments based on message queuing telemetry transport. Expert Syst. 2024;41(2):e13263. doi:10.1111/exsy.13263.
110. Hashimyar ME, Aiash M, Khoshkholghi A, Nalli G. Signature-based security analysis and detection of IoT threats in advanced message queuing protocol. Network. 2025;5(1):5. doi:10.3390/network5010005.
111. Toutsop O, Harvey P, Kornegay K. Monitoring and detection time optimization of man in the middle attacks using machine learning. In: 2020 IEEE Applied Imagery Pattern Recognition Workshop (AIPR); 2020 Oct 13–15; Washington, DC, USA. doi:10.1109/AIPR50011.2020.9425304.
112. Rihan SDA, Anbar M, Alabsi BA. Approach for detecting attacks on IoT networks based on ensemble feature selection and deep learning models. Sensors. 2023;23(17):7342. doi:10.3390/s23177342.
113. Haji SH, Ameen SY. Attack and anomaly detection in IoT networks using machine learning techniques: a review. Asian J Res Comput Sci. 2021;9(2):30–46. doi:10.9734/ajrcos/2021/v9i230218.
114. Alkhudaydi OA, Krichen M, Alghamdi AD. A deep learning methodology for predicting cybersecurity attacks on the Internet of Things. Information. 2023;14(10):550. doi:10.3390/info14100550.
115. Moustafa N. A new distributed architecture for evaluating AI-based security systems at the edge: network TON_IoT datasets. Sustain Cities Soc. 2021;72:102994. doi:10.1016/j.scs.2021.102994.
116. Rane NL, Kaya Ö, Rane J. Integrating Internet of Things, blockchain, and artificial intelligence techniques for intelligent industry solutions. In: Artificial intelligence, machine learning, and deep learning for sustainable Industry 5.0. London, UK: Deep Science Publishing; 2024. doi:10.70593/978-81-981271-8-1_6.
117. Zahoor S, Mir RN. Resource management in pervasive Internet of Things: a survey. J King Saud Univ Comput Inf Sci. 2021;33(8):921–35. doi:10.1016/j.jksuci.2018.08.014.
118. Parvathavarthini S, Visalakshi N, Shanthi S, Mohan J. An improved crow search based intuitionistic fuzzy clustering algorithm for healthcare applications. Intell Autom Soft Comput. 2020;26(2):253–60. doi:10.31209/2019.100000155.
119. Babar ETR, Rahman MU. A smart, low cost, wearable technology for remote patient monitoring. IEEE Sens J. 2021;21(19):21947–55. doi:10.1109/JSEN.2021.3101146.
120. Naresh VS, Pericherla SS, Sita Rama Murty P, Reddi S. Internet of Things in healthcare: architecture, applications, challenges, and solutions. Comput Syst Sci Eng. 2020;35(6):411–21. doi:10.32604/csse.2020.35.411.

121. Yu P, Xia Z, Fei J, Kumar Jha S. An application review of artificial intelligence in prevention and cure of COVID-19 pandemic. Comput Mater Contin. 2020;65(1):743–60. doi:10.32604/cmc.2020.011391.

122. McGhin T, Choo KR, Liu CZ, He D. Blockchain in healthcare applications: research challenges and opportunities. J Netw Comput Appl. 2019;135(1):62–75. doi:10.1016/j.jnca.2019.02.027.

123. Ajaz F, Naseem M, Sharma S, Shabaz M, Dhiman G. COVID-19: challenges and its technological solutions using IoT. Curr Med Imaging. 2022;18(2):113–23. doi:10.2174/1573405617666210215143503.

124. Paul AK, Qu X, Wen Z. Blockchain-a promising solution to Internet of Things: a comprehensive analysis, opportunities, challenges and future research issues. Peer Peer Netw Appl. 2021;14(5):2926–51. doi:10.1007/s12083-021-01151-0.

125. Sollins KR. IoT big data security and privacy versus innovation. IEEE Internet Things J. 2019;6(2):1628–35. doi:10.1109/JIOT.2019.2898113.

126. Gupta BB, Quamara M. An overview of Internet of Things (IoT): architectural aspects, challenges, and protocols. Concurr Comput Pract Exp. 2020;32(21):e4946. doi:10.1002/cpe.4946.

127. Khorov E, Lyakhov A, Nasedkin I, Yusupov R, Famaey J, Akyildiz IF. Fast and reliable alert delivery in mission-critical Wi-Fi HaLow sensor networks. IEEE Access. 2020;8:14302–13. doi:10.1109/ACCESS.2020.2966147.

128. Sarker MFH, Al Mahmud R, Islam MS, Islam MK. Use of e-learning at higher educational institutions in Bangladesh: opportunities and challenges. J Appl Res High Educ. 2019;11(2):210–23. doi:10.1108/JARHE-06-2018-0099.

129. Stoyanova M, Nikoloudakis Y, Panagiotakis S, Pallis E, Markakis EK. A survey on the Internet of Things (IoT) forensics: challenges, approaches, and open issues. IEEE Commun Surv Tutor. 2020;22(2):1191–221.

130. Haleem A, Javaid M, Qadri MA, Suman R. Understanding the role of digital technologies in education: a review. Sustain Oper Comput. 2022;3(4):275–85. doi:10.1016/j.susoc.2022.05.004.

131. Verma P, Sood SK, Kalra S. Cloud-centric IoT based student healthcare monitoring framework. J Ambient Intell Humaniz Comput. 2018;9(5):1293–309. doi:10.1007/s12652-017-0520-6.

132. Ullah S, Ahmad J, Khan MA, Alkhammash EH, Hadjouni M, Ghadi YY, et al. A new intrusion detection system for the Internet of Things *via* deep convolutional neural network and feature engineering. Sensors. 2022;22(10):3607. doi:10.3390/s22103607.

133. Awajan A. A novel deep learning-based intrusion detection system for IoT networks. Computers. 2023;12(2):34. doi:10.3390/computers12020034.

134. Kunang YN, Nurmaini S, Stiawan D, Suprapto BY. Attack classification of an intrusion detection system using deep learning and hyperparameter optimization. J Inf Secur Appl. 2021;58(1):102804. doi:10.1016/j.jisa.2021.102804.

135. Raoufi P, Hemmati A, Rahmani AM. Deep learning applications in the Internet of Things: a review, tools, and future directions. Evol Intell. 2024;17(5):3621–54. doi:10.1007/s12065-024-00949-0.

136. Aswad FM, Ahmed AMS, Ali Majeed Alhammadi N, Ahmad Khalaf B, Mostafa SA. Deep learning in distributed denial-of-service attacks detection method for Internet of Things networks. J Intell Syst. 2023;32(1):20220155. doi:10.1515/jisys-2022-0155.

137. El-Sofany H, El-Seoud SA, Karam OH, Bouallegue B. Using machine learning algorithms to enhance IoT system security. Sci Rep. 2024;14(1):12077. doi:10.1038/s41598-024-62861-y.

138. Singh SK, Rathore S, Park JH. BlockIoTIntelligence: a blockchain-enabled intelligent IoT architecture with artificial intelligence. Future Gener Comput Syst. 2020;110(2):721–43. doi:10.1016/j.future.2019.09.002.

139. Latif SA, Wen FBX, Iwendi C, Wang LF, Mohsin SM, Han Z, et al. AI-empowered, blockchain and SDN integrated security architecture for IoT network of cyber physical systems. Comput Commun. 2022;181(6):274–83. doi:10.1016/j.comcom.2021.09.029.

140. Asghari P, Rahmani AM, Javadi HHS. Internet of Things applications: a systematic review. Comput Netw. 2019;148(7):241–61. doi:10.1016/j.comnet.2018.12.008.

141. Kumar S, Tiwari P, Zymbler M. Internet of Things is a revolutionary approach for future technology enhancement: a review. J Big Data. 2019;6(1):111. doi:10.1186/s40537-019-0268-2.

142. Mishra N, Pandya S. Internet of Things applications, security challenges, attacks, intrusion detection, and future visions: a systematic review. IEEE Access. 2021;9:59353–77. doi:10.1109/ACCESS.2021.3073408.

143. Ghimire B, Rawat DB. Recent advances on federated learning for cybersecurity and cybersecurity for federated learning for Internet of Things. IEEE Internet Things J. 2022;9(11):8229–49. doi:10.1109/JIOT.2022.3150363.
144. Tightiz L, Nasimov R, Nasab MA. Implementing AI solutions for advanced cyber-attack detection in smart grid. Int J Energy Res. 2024;2024(1):6969383. doi:10.1155/2024/6969383.
145. Rai HM, Shukla KK, Tightiz L, Padmanaban S. Enhancing data security and privacy in energy applications: integrating IoT and blockchain technologies. Heliyon. 2024;10(19):e38917. doi:10.1016/j.heliyon.2024.e38917.