Computer Networks and Communications
https://ojs.wiserpub.com/index.php/CNC

UNIVERSAL WISER
PUBLISHER

Research Article

Security Issues in IoT: Perspective Review

Jeyalakshmi V.*, Vijayakumari Balan, Benitha V.S.

ECE Department, Mepco Schlenk Engineering College, Sivakasi, India
E-mail: jeyalakshmiv@mepcoeng.ac.in

Received: 25 November 2024; **Revised:** 24 February 2025; **Accepted:** 10 March 2025

Abstract: The Internet of Things (IoT) has revolutionized various sectors, including healthcare, wearables, automotive, smart cities, agriculture, manufacturing, business, and home automation. As technology continues to shape everyday life, ensuring the security of IoT systems has become a critical concern. IoT devices, equipped with multiple sensors and processors, collect vast amounts of data, making them vulnerable to cyber threats. Like other connected systems, these devices are susceptible to attacks such as credential theft, firmware exploits, and hardware-based intrusions. IoT security involves safeguarding physical components, data, and network connections against unauthorized access and malicious activities. Key security measures include software and firmware updates, credential protection, device authentication, encryption, disabling unnecessary IoT functionalities, and Domain Name System (DNS) filtering. However, securing IoT networks is challenging due to the diverse range of devices, lack of standardized security protocols, and the widespread use of open-source software. This article explores security vulnerabilities across different IoT layers, examines existing mitigation strategies, and discusses potential research directions for enhancing IoT security.

***Keywords*:** IoT devices, security, hackers, attackers, vulnerability, credential, privacy

1. Introduction

Internet of Things (IoT) is the inter-connection of physical devices that includes sensors, processors, and actuators to ease the elegance of human lives through enhancement in applications such as smart cities, smart farming, smart grid, banking, vehicular automation, intelligent healthcare, smart business, and education. IoT flourished due to the advancement in research technologies such as embedded systems, wireless sensor networks, and communication protocols for smart physical objects [1]. Considering the current rate of growth, the number of devices in the IoT network will become 38.6 billion by 2025 which will bring limitless opportunities in various significant domains [2]. IoT networks are vulnerable to security threats due to the heterogeneous nature of components, limitations in its power and computation facilities, and vast scalability. As the IoT device manufacturers are concentrating on time to market with enhanced usability features rather than security, the data communication between the devices in the IoT network is highly insecure. As the nodes are tiny and resource-constrained, they could not execute complex encryption and decryption algorithms and the data is more open to attacks and breaches.

Most IoT devices are manufactured with weak user names and passwords that cannot be reset and changed. Attackers easily guess these credentials and execute successful IoT thefts. A study shows that 98% of IoT data traffic that carries confidential information is not encrypted. Unsecured IoT devices can serve as a potential point of entry for attackers to

DOI: https://doi.org/10.37256/cnc.3120256140

expose the entire network to outside risks. A fully integrated autonomous system with sensors is an industrial IoT system that has challenges due to infrastructure limitations for data processing, storage, and communication.

Compared with computer networks and cellular networks, IoT networks are facing severe security challenges such as privacy and authentication issues. The penalties due to failure in IoT security would lead to the loss of many human lives and cause severe monetary loss. The different threats to security in current communication protocols for IoT is reviewed and various solutions to mitigate its effects are described.

In this study, the required literature are collected from IEEE explore, ACM digital library and science direct. The keywords used for search includes IoT security threats, cyberattacks in IoT, Machine learning for IoT security, security in smart devices. Relevant article in the duration from 2019 to 2024 that discussed security threats, attack models, or mitigation techniques in IoT networks are filtered manually excluding the irrelevant and outdated works (Table 1).

Table 1. Steps in analysing the survey of IoT security

Step	Procedure	Key actions
Define Research Scope & Objectives	Identify the focus of the review	What are the major IoT security challenges? What are the existing techniques to secure IoT devices and N/Ws? How effective are these security mechanisms?
Set time frame	Recent 5 years articles are collected and categorized	Relevant article from 2019 to 2024
Specify IoT security aspects	Grouping the existing research under key security aspects	Confidentiality, authentication, network security at various layers
Identify Reliable Sources	Collect relevant research papers	Search academic databases (IEEE Xplore, ACM, Springer, Elsevier)
Analyze and Compare Findings	Effectiveness, limitations, and implementation complexity of different techniques	Presented as barchart and table in Section VI
Summarize the emerging trends	AI-based IoT security solutions	ML, DL and quantum computing based security techniques are described
Identify the research gap	From the survey, the drawbacks and threats are analyzed	Future research direction presented in conclusion section

1.1 *Contributions*

The objectives of addressing security issues in IoT are to focus on protecting devices, networks, and data from cyber threats. Key objectives include: Ensuring Data Confidentiality, Maintaining Data Integrity, Ensuring Device Authentication, Securing Network Communication, Providing Access Control, Enhancing Device Security, Mitigating Privacy Risks, Detecting and Preventing Threats, Ensuring Availability and Reliability and Compliance with Security Standards. The key contributions of this review are

- Outlining the major IoT attacks and imposing the significance of IoT security.
- Summarizing the existing security techniques and their applications.
- Presenting the challenges in the current methodologies and paving the directions to future research.

2. Requirements of IoT security

Various applications of IoT focussing on improved smartness for home/industry allow many inanimate sensors to interact with each other, decide, and act without human intervention. Each connected device in the IoT network has a unique address and has the communication ability to transfer data into the network. IoT devices are more prone to malware attacks as their operating systems are not built with security mechanisms as in high-end machines. Due to the minimalistic and ease-of-use design feature of IoT components, they could not support software security controls such as anti-virus, anti-malware protection, and 'software whitelisting', in which the device permits only specific software installation and updates.

If the nodes in the network are not properly protected, then it leads to severe cybercrime. Data breaches can remotely control IoT devices and steal data in the IoT network. The various threats to IoT networks and devices include the intrusion of viruses, worms, malware, spyware, Trojans, malicious code, and backdoor attacks. IoT security concentrates on securing the network and protecting the devices.

Mirai attack on IoT devices is a Distributed Denial of Service (DDoS) attack carried out by a few college-aged kids which aims at crashing or slowing down the Domain Name server, Dyn through multiple compromised systems. Mirai is a type of malware that brings a group of IoT devices in the network under the control of a malicious actor. It targets IoT devices such as cameras, printers, and routers with poor security features, to execute the DDoS attack. The dynamic analysis of the Mirai attack on resource consumption such as processor utilization, memory usage, energy consumption, and Ethernet Input Output performance of resource-constrainedcompromised and victim IoT devices is carried out in [3]. The attacker introduced the malware through the smart camera which is a consumer IoT device to perform DDoS attack on the US Brian Krebs' website in September 2016. It disturbed the services of many prominent websites such as Twitter, Netflix, and Github for more than 8 h by increasing the network traffic to 1 Tbps [4].

Followed by Mirai, WannaCry and NotPetya attacks disrupted the IoT systems meant for smart infrastructure and manufacturing. WannaCry infected more than a quarter million IoT devices on May 12, 2017 in more than 150 countries across the world. The National Health Service (NHS) in England and Scotland turned standstill for several days as WannaCry attacked many hospitals and General Practice (GP) surgeries. It is one of the largest ransomware attacksthat weaponized the Eternal Blue which is software vulnerability in Microsoft Windows OS. The cyber attackers utilized the vulnerability in Microsoft's implementation of the Server Message Block (SMB) protocol [5]. The National Security Agency in the UK warned NHS that hackers are targeting the health records as they worth ten times more than other data like banking information, industrial data, etc. The attack triggered the government to invest more in the nation's cyber security.

NotPetya ransomware attacked many organizations in Ukraine infecting the victim's entire hard disk so that none of the files could be accessed. It quickly spreads over the entire network, exploiting the various vulnerabilities and executing the credential forgeries. Unlike other ransomware attacks which prevent access to files until a ransom is exchanged with victims, NotPetya permanently damages the files in the hard disks which ensure that the attacker's aim is entire system disruption and not the financial gain. The security practices for scanning an organization's emails for malware and blocking email attachments from foreign objects could protect the Firm. The attack vectors could be blocked by updating the software and patches [6].

Integrating security through machine learning techniques to identify the DDoS attack by training the algorithm through IoT datasets which are both real-time and simulated for various IoT environments is discussed in [7]. Deep learning based on ensemble methods can predict anomalies in network traffic when trained through complex patterns of IoT data transfer. The authors suggested that trained machine learning models can be embedded in the edge devices or fog nodes of IoT systems, to analyze the network traffic locally with faster response times. IoT-based datasets created as open source would be a valuable contribution which enables the data analyst to create ML/DL models to detect DDoS attacks efficiently [8], [9]. When the cloud provides the necessary computation, storage and power requirements for the nodes in the IoT network, this intersection of cloud with nodes is called as Cloud of Things (CoT) [10]. But the cloud centralized IoT architecture suffers from latency due to the data traffic back and forth between the nodes and cloud. Fog computing IoT architecture is introduced to resolve the latency issue where the computing cloud nodes are at theedges of network.

Table 1 shows the issues and solutions for the recent attacks in IoT networks happened all over the globe [11]-[14]

Table 2. Recent security attacks in IoT networks

Security threat in IoT networks	Issue	Impact	Solution
Jeep Cherokee Cyberattack (2015)	Remote exploitation of connected vehicle systems	Hackers could manipulate critical car functions like braking, steering, and acceleration	Strengthen automotive cybersecurity with robust security protocols and Over-the-Air (OTA) updates
Mirai Botnet Incident (2016)	IoT devices compromised to launch large-scale DDoS attacks	Disruption of major online services such as Twitter and Netflix	Eliminate default passwords, enforce strong authentication, and apply regular security patches
St. Jude Medical Device Vulnerability (2017)	Security loopholes in connected medical devices	Potential life-threatening cyber intrusions in pacemakers and defibrillators	Implement rigorous security evaluations and ensure timely firmware updates in medical IoT
Amazon Ring Security Breach (2019)	Unauthorized access to smart home cameras	Users faced privacy violations and security threats	Strengthen security with two-factor authentication (2FA), unique passwords, and regular firmware updates
Smart Thermostat Ransomware Attack (2020)	Ransomware affecting smart home devices	Devices locked, with attackers demanding cryptocurrency for access restoration	Secure IoT devices with encryption, strong authentication, and frequent security updates
Rise in IoT Malware Attacks (2023)	Significant spike in malware targeting IoT devices	400% surge in attacks due to unpatched vulnerabilities	Emphasize regular updates, strong authentication, and proactive security monitoring
Cyber Intrusions in U.S. Utility Systems (2024)	Increased cyberattacks on IoT-based infrastructure	70% rise in attacks exploiting outdated software and expanding digital networks	Enhance cybersecurity defenses and ensure continuous software maintenance in critical systems
Roku Credential Breach (2024)	Account takeover via credential stuffing	Over 576,000 accounts compromised, exposing financial and personal data	Promote unique password usage and enforce two-factor authentication for account protection
Healthcare IoT Ransomware Incident (2024)	Ransomware attack on IoT-powered medical systems	Disruptions in critical patient care devices, forcing hospitals to revert to manual operations	Deploy regular security patches and implement network segmentation to mitigate risks
Smart City Infrastructure DDoS Attack (2024)	Large-scale DDoS assault on smart city IoT networks	Disruptions in traffic control, surveillance, and waste management, leading to urban chaos	Strengthen cybersecurity frameworks and conduct regular updates for smart city infrastructure

2.1 *Authentication and authorization*

Authentication refers to the real identity of a node or a device in the IoT network, whereas authorization represents the different levels of accessing the network information. The access privilege of a subject to an object is termed as authorization and is provided by authentication mechanism which means the verification of the subject's identity. Weak authentication can make the intruders to gain control over the network nodes leading to information theft or even stealing of the nodes itself and utilizing them for malicious purposes [15]. The personal and financial information of individuals and confidential business information are breached by frauds due to the poor authorization control.

As single parameter verification of an IoT node may lead to compensating nodes into the network causing unauthorized access, multifactor identification could strengthen the authentication mechanism.

Authentication and authorization are fundamental components of IoT security, ensuring that only trusted entities can access IoT resources and perform authorized actions while safeguarding sensitive data and maintaining system integrity.

Certificate-based authentication is a security mechanism used in IoT networks to verify device identities through digital certificates issued by a trusted Certificate Authority (CA). Each IoT device holds a private key, paired with a public key embedded in its certificate. When a device attempts to connect to a network, it presents its certificate, which the server validates against trusted CAs. If the certificate is verified, the device is granted access. This method offers strong security, scalability, and non-repudiation, but requires careful management of certificates and keys. It is commonly used for device-to-device communication, secure cloud access, and ensuring trusted firmware updates. Several authentication methods [16] commonly used in IoT are shown in Figure 1 are explained below:

Password-based authentication: Devices are assigned credentials (e.g., username/password) that they must provide to authenticate themselves before accessing the network or services.

Certificate-based authentication: Devices are issued digital certificates, typically signed by a trusted certificate authority (CA). These certificates are used to authenticate the device's identity during communication with other devices or servers.

Token-based authentication: Devices obtain tokens after successful authentication, which they then use to access resources or services. These tokens typically have an expiration time and are used to avoid repeatedly sending sensitive credentials over the network.

Biometric authentication: Some IoT devices may incorporate biometric sensors (e.g., fingerprint scanners) to authenticate users before granting access to the device or its functions [17], [18].

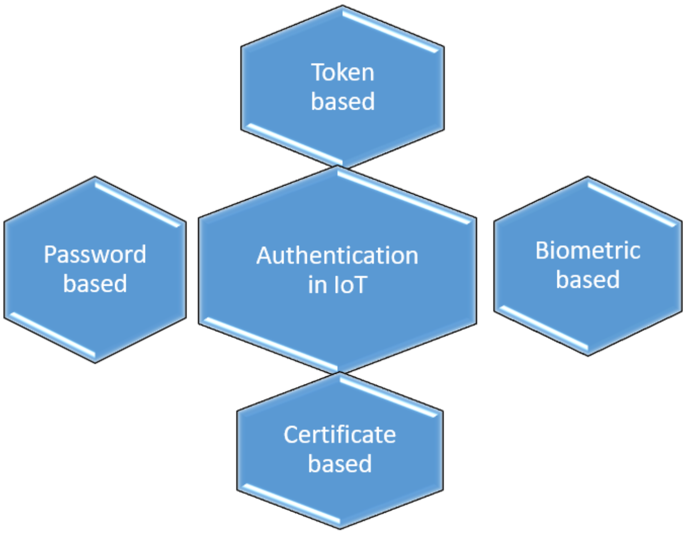
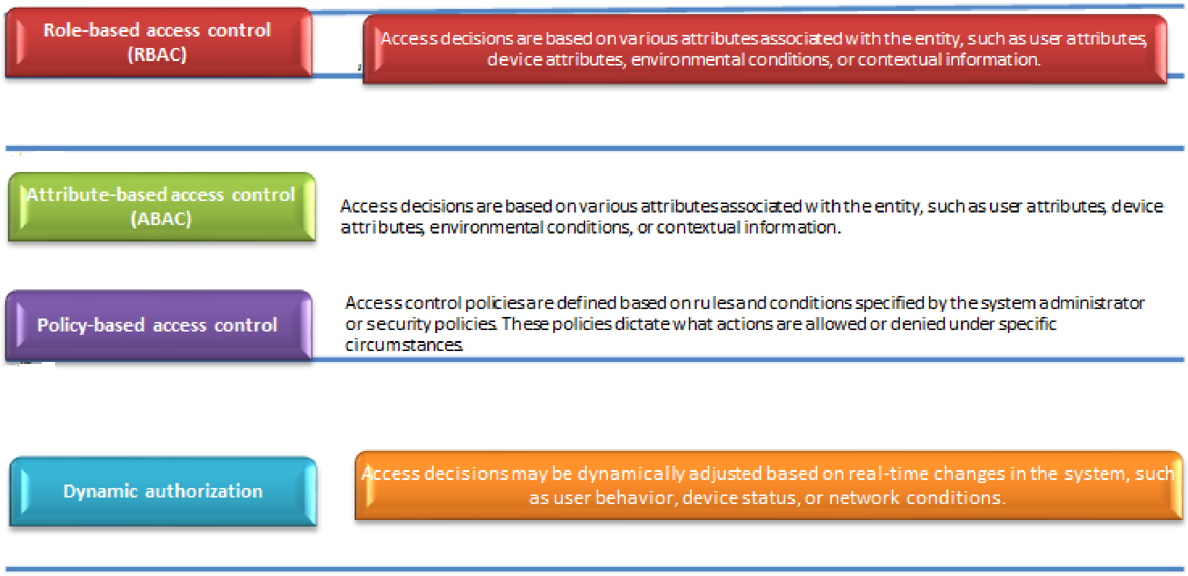


Figure 1. Authentication methods in IoT

Few commonly used authorization methods are summarized in Figure 2. To achieve authentication and authorization in IoT devices various security measures should be implemented [19] to verify the identity of entities and control their access to resources. Figure 3 shows some common methods and strategies to achieve authentication and authorization in IoT devices:



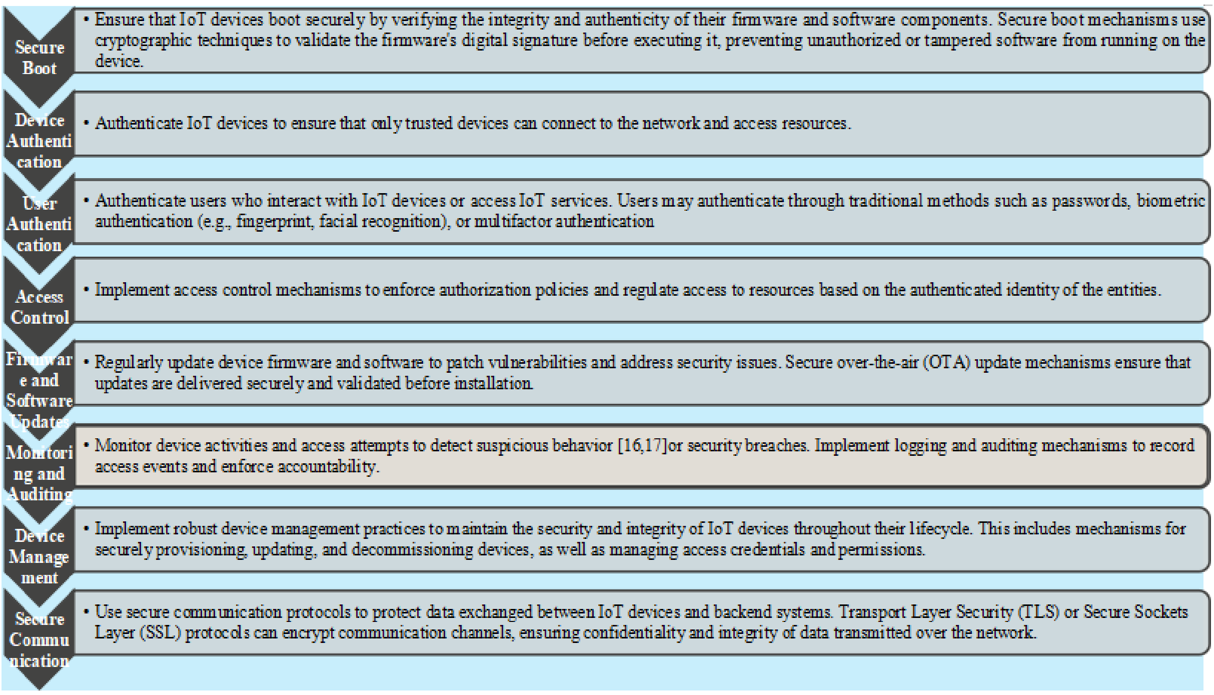
Role-based access control (RBAC) — Access decisions are based on various attributes associated with the entity, such as user attributes, device attributes, environmental conditions, or contextual information.

Attribute-based access control (ABAC) — Access decisions are based on various attributes associated with the entity, such as user attributes, device attributes, environmental conditions, or contextual information.

Policy-based access control — Access control policies are defined based on rules and conditions specified by the system administrator or security policies. These policies dictate what actions are allowed or denied under specific circumstances.

Dynamic authorization — Access decisions may be dynamically adjusted based on real-time changes in the system, such as user behavior, device status, or network conditions.

Figure 2. Authorization methods in IoT



Secure Boot	• Ensure that IoT devices boot securely by verifying the integrity and authenticity of their firmware and software components. Secure boot mechanisms use cryptographic techniques to validate the firmware's digital signature before executing it, preventing unauthorized or tampered software from running on the device.
Device Authentication	• Authenticate IoT devices to ensure that only trusted devices can connect to the network and access resources.
User Authentication	• Authenticate users who interact with IoT devices or access IoT services. Users may authenticate through traditional methods such as passwords, biometric authentication (e.g., fingerprint, facial recognition), or multifactor authentication
Access Control	• Implement access control mechanisms to enforce authorization policies and regulate access to resources based on the authenticated identity of the entities.
Firmware and Software Update	• Regularly update device firmware and software to patch vulnerabilities and address security issues. Secure over-the-air (OTA) update mechanisms ensure that updates are delivered securely and validated before installation.
Monitoring and Auditing	• Monitor device activities and access attempts to detect suspicious behavior [16,17]or security breaches. Implement logging and auditing mechanisms to record access events and enforce accountability.
Device Management	• Implement robust device management practices to maintain the security and integrity of IoT devices throughout their lifecycle. This includes mechanisms for securely provisioning, updating, and decommissioning devices, as well as managing access credentials and permissions.
Secure Communication	• Use secure communication protocols to protect data exchanged between IoT devices and backend systems. Transport Layer Security (TLS) or Secure Sockets Layer (SSL) protocols can encrypt communication channels, ensuring confidentiality and integrity of data transmitted over the network.

Figure 3. Strategies to achieve authorization and authentication [20], [21]

2.2 *Privacy and integrity*

With the development of new technology and methods, the internet is expanding quite quickly these days. A few years back, the internet was not as sophisticated, thus it is not necessary to have an effective security system for networking devices [22]. In a 2017 survey, 51% of large organizations said they didn't even consider device security since they believed their devices wouldn't be attacked by hackers. Currently, approximately 96% of companies believe that assaults on IoT devices will likely increase significantly in the future years [23]. Attacks on internet-connected devices are becoming more frequent and frequent at a very fast rate as technology advances. Security and privacy are now crucial considerations. The field of Internet of Things (IoT) security is concerned with safeguarding, detecting, and keeping an eye on hazards to prevent threats and breaches against linked devices and networks, including SCADA systems, home automation, and security cameras [24]. To ensure the availability, integrity, and confidentiality of the physical elements, applications, data, and network connections inside IoT ecosystems, security measures are taken. IoT security comprises the subsequent elements: strategies for security that keep Internet of Things devices safe, methods for tracking threats and vulnerabilities in IoT security, techniques to lessen or address found IoT security issues [25].

IoT security is essential since these systems are widely used and vulnerable, which makes them a prime target for attacks [26]-[28].

Device Vulnerabilities: 41% of cyberattacks are based on vulnerabilities in devices. This underscores the importance of regularly updating and patching devices to mitigate known weaknesses.

Targeting Imaging Equipment: Healthcare organization's imaging equipment is the target of 51% of cyber assaults. This is alarming as it not only jeopardizes patient care but also provides hackers access to sensitive patient data stored on these devices.

IoT Vulnerabilities: Cybercriminals target IoT devices with medium or high severity attacks in 57% of cases. IoT devices are often considered easy targets due to negligent security measures compared to traditional IT assets.

Spread of Malware: IoT and IT assets are present in 72% of healthcare VLANs. This interconnectedness increases the risk of malware spreading from user laptops to vulnerable IoT devices, potentially causing widespread damage.

Addressing these vulnerabilities requires a multi-faceted approach, including regular security audits, updating firmware and software, implementing network segmentation, and educating staff on cybersecurity best practices. Additionally, investing in advanced threat detection and response mechanisms can help healthcare organizations better protect their network infrastructure and sensitive patient data [29], [30].

The main reasons for implementing IoT security [31], [32]:

- Reputational Harm: Breaches in IoT devices can lead to negative publicity, damaging the company's reputation in the long run.

- Financial Losses: Insecure IoT systems can be prone to fraud and revenue loss, especially with features like remote activation and usage-based business models.

- Theft of Intellectual Property: With millions invested in IoT technology, inadequate security measures can lead to the theft of valuable intellectual property.

- Faulty Data, Poor Decisions: Insufficiently protected data can be manipulated, leading to inaccurate insights and bad business decisions, ultimately negating the benefits of IoT initiatives.

- Regulatory Penalties: Compliance with data protection regulations is crucial. Failure to secure IoT systems can lead to significant penalties from regulatory bodies.

- Liabilities and Litigation: Inadequate security measures can expose companies to lawsuits, especially if customer data is compromised due to insufficient protection.

Implementing robust IoT security measures is essential not only to protect sensitive data but also to safeguard the company's reputation, financial stability, and legal standing.

On the other hand secure boot and firmware integrity are crucial aspects of IoT device security. Secure Boot is a security feature that ensures only trusted software is loaded and executed during the boot process of a device. It establishes a chain of trust from the hardware to the operating system, preventing unauthorized or malicious software from being executed during startup. Hackers may attempt to compromise the boot process by injecting malware or unauthorized code, which can lead to device takeover or data breaches. Secure Boot verifies the digital signatures of boot components against known trusted signatures, ensuring their integrity before allowing execution.

Firmware integrity refers to the assurance that the firmware running on an IoT device has not been tampered with or altered. Since firmware controls the behaviour and functionality of the device, ensuring its authenticity is critical to maintaining device security and functionality. Attackers may attempt to modify firmware to introduce backdoors, malware, or other malicious functionality, compromising the device's security and stability. Techniques such as cryptographic signing are used to verify the authenticity of firmware. Cryptographic signatures ensure that the firmware has not been altered since it was signed by the manufacturer. If compromised firmware is installed on a device, it can lead to various security risks, including unauthorized access, data breaches, and disruption of device functionality. By implementing secure boot mechanisms and ensuring firmware integrity through rigorous verification processes, IoT device manufacturers can mitigate the risk of unauthorized access, data breaches, and other security threats, thereby enhancing the overall security posture of IoT deployments.

3. Attacks at different layers

Most IoT network follows four-layered architecture, but it may vary depending on the applications and business models for which the network is devised. Figure 4 depicts the four layers with their functionalities and the possible threats that can happen in that layer.

3.1 *Security threats in the sensing layer*

The hardware components in the IoT network are disturbed by the attacker and based on the level of interaction with components, the attack is classified as invasive, non-invasive, and semi-invasive attacks. The invasive attack is characterized by the chip-level attack on the Integrated Circuits (ICs) embedded in the smart cards, smartphones, and other identity cards to steal the sensitive information stored in their memory [33]. Well-trained software and hardware experts are utilized to perform invasive attacks either with or without detaching the component from the system. Non-invasive attack is carried out through the interfaces of the targeted component which does not cause any physical damage during data breach. Without harming the device, the intruder creates contact with the internal wires or pads it to a test circuit to steal the data. In a semi-invasive attack, the chip is de-packaged from the IoT device, but the passivation layer of the chip which serves for electronic isolation, remains intact with the device.

Hardware Trojan attack in IoT network introduces a malicious circuit or modifies the existing circuit in the physical hardware devices to alter its programmed function. This type of attack aims to snip the network information by bypassing the authentication and access control mechanisms [34].

3.2 *Security threats in the network layer*

Jamming attacks blocks the wireless communication channel for IoT networks by malicious node that introduces noise in the channel blocking the reliable reception [35]. A malicious node introduced by the intruder, presents itself to other communicating nodes in the network as it provides the best routing path for the information [36]. Hence, all the information in the network flows through that malicious node and hence the network performance such as efficiency and reliability are affected due to congestion. Such attack is termed as sinkhole attack as the cruel node “sinks” all the information that flows in the targeted IoT network. The recent jamming attack suspected to be created by Russia during April 2024, disrupted the Global Navigation Satellite System signals in the Baltic region aimed at affecting hundreds of aircrafts flying in that region and also the shipping in that region.

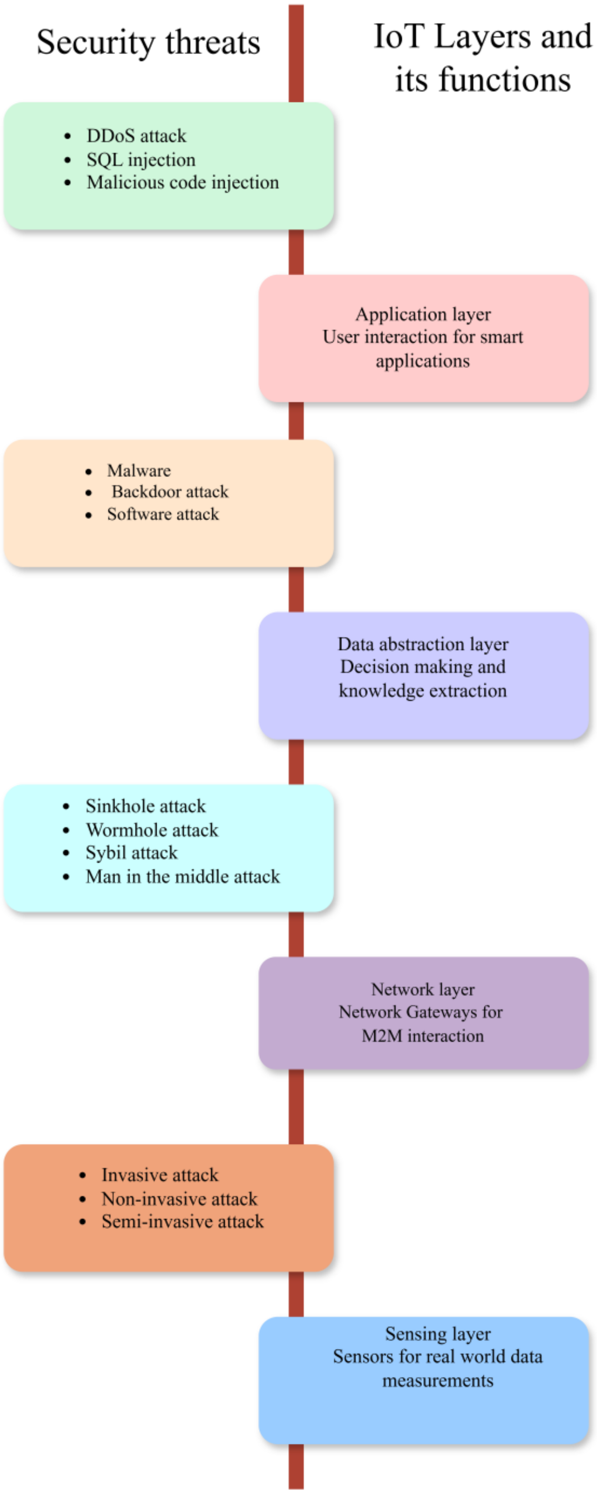


Figure 4. Functions IOT layers and security threats

On the other hand, in wormhole attack, the malicious node or code injected by the victim selectively forwards the information to the destination by establishing a private channel between any communicating devices in the IoT network [37]. In traffic analysis and routing information attacks, the routing information such as the distance between the transmitting nodes, packet length etc. are notified to the attacker by a malicious node introduced by him [38]. The attacker can spoof, misguide or drop the information before it reaches the intended receiver. During February 2022, the malicious attacker exploited $325 million crypto currency through Solana pay app that bypassed the verification process by injecting a fake sysvar account that issued the malicious message of 120,000 Wormhole Ethereum (WeETH)

3.3 *Security threats in the data abstraction layer*

Backdoor or Brute force attack planned to remotely access resources in the IoT network by breaking the IoT security mechanism and bypassing the authentication procedure. The attack is carried out by launching malicious code to break the established weak cryptographic technique in the IoT network [39]. Malware and spyware attack steal the sensitive information such as passwords, banking information and other personal data without the user's knowledge. The open ports in the devices of the IoT network are identified and utilized by the attacker to gain access the network content. These attacks do not cause any physical damage to the nodes [40]. Outage attack shutdown the remote IoT devices and prevent them to do their regular routines. Stuxnet is an outage attack introduced into the Iran's nuclear process control where the node failed to predict the emergency conditions and therefore, didn't turn-off for protection purpose [41]. The attack was launched into the Natanz power plant network through a compromised USB drive. Stuxnet was believed to be designed by USA to delay or stop the sensitive nuclear program in an Iranian computer.

3.4 *Security threats in the application layer*

Worms, Viruses and Trojan horses are software attacks in the IoT network that replicates itself to create copies to fill the disk or the entire memory space of the weak processing units in the IoT nodes. This hinders the device from rebooting by affecting the boot loader in the IoT gadgets. They are malicious program appears to be harmless while downloaded and installed. Later it infects the files and gets transferred through the entire network through wired or wireless transmission [42], [43].

In reverse engineering attack, the intruder distracts the IoT firmware embedded in the IoT device thus generating serious issues to the IoT applicants and users. He reverse engineered the program to identify the security risks and accounts to corrupt the code. Then, he advertises himself to resolve the issue, get access to the network and steals the sensitive information from the network [44].

Mirai botnet is malicious software designed to remotely control vulnerable IoT devices like webcams and other industrial sensors that have open ports, default user names and passwords. It is a type of distributed Denial of Service attack created by forming many remotely controlled bots. Once a bot is created in the network, it is capable of infecting all devices connected with it leading to devastating attacks. The methods for avoiding security threats in the application layer is shown in Figure 5.

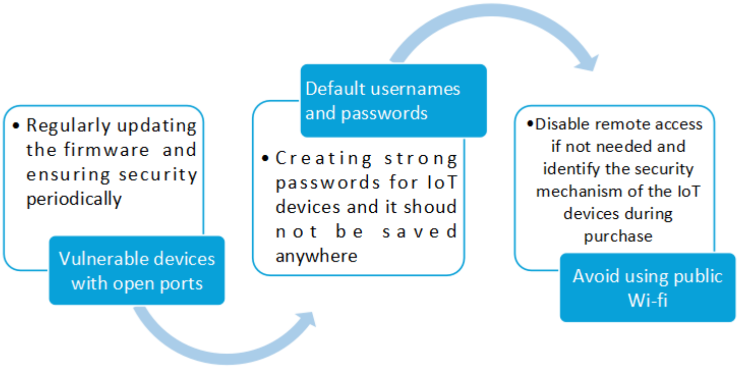

• Regularly updating the firmware and ensuring security periodically
Vulnerable devices with open ports
Default usernames and passwords
• Creating strong passwords for IoT devices and it shoud not be saved anywhere
•Disable remote access if not needed and identify the security mechanism of the IoT devices during purchase
Avoid using public Wi-fi

Figure 5. Security threats in application layer

3.5 *Other security-related issues*

It has been predicted by researchers that the IoT device utility for most of applications has been drastically increasing. Hackers are capitalizing on this growth by targeting various organizations and industries with simple cyber-attacks [45]. Hence, security issues are of major concern due to the proliferation of connected devices and the potential impact of security breaches on individuals, organizations, and society as a whole [46]. Some of the key security issues are shown in Figure 6.

Many IoT devices have inadequate or default authentication credentials [47], making them vulnerable to unauthorized access. A lack of robust authentication and authorization mechanisms can result in unauthorized users gaining control over IoT devices, leading to data breaches or malicious activities. IoT devices often communicate over unencrypted or insecure channels, exposing sensitive data to interception and tampering. Insecure communication protocols may allow attackers to eavesdrop on communication between devices or inject malicious commands, compromising the integrity and confidentiality of data. IoT devices may contain vulnerabilities in their firmware or software, either due to coding errors, design flaws, or outdated components. Attackers can exploit these vulnerabilities to execute remote code execution, denial-of-service (DoS) attacks, or install malware on IoT devices, potentially compromising their functionality and security.

IoT devices collect and process vast amounts of data, including personal and sensitive information about users and their environments. Poorly designed IoT systems may fail to adequately protect user privacy, leading to unauthorized data collection, profiling, or surveillance [48]. IoT devices deployed in uncontrolled or hostile environments are susceptible to physical tampering, theft, or sabotage. Attackers may physically access IoT devices to extract sensitive information, manipulate device behaviour, or compromise their functionality. IoT devices often comprise components sourced from various vendors and manufacturers, introducing supply chain risks. Malicious actors may compromise the supply chain by injecting counterfeit components, backdoors, or malware into IoT devices during manufacturing, assembly, or distribution. Managing security in large-scale IoT deployments poses challenges due to the sheer number and diversity of connected devices. The complexity of IoT ecosystems, involving heterogeneous devices, protocols, and platforms, increases the attack surface and makes it difficult to implement consistent security measures.

Many IoT devices lack mechanisms for receiving and applying security updates and patches, leaving them vulnerable to known vulnerabilities. Manufacturers and vendors may neglect security updates for IoT devices, especially for legacy or low-cost devices, exacerbating the risk of exploitation over time.

Few more emerging issues that have to be taken care are shown in Figure 7. IoT devices often collect vast amounts of personal data. Ensuring the privacy of this data is crucial to prevent unauthorized access or misuse. Complex IoT environment is an interconnected web of at least 10 IoT devices. It is really hard to tackle and control the interconnected functions, which will put household security at risk. During pandemic situations, work-from-home control must be done around the globe, which again puts IoT security at risk. The transition to 5G comes with much anticipation and expectations nowadays. Hence while adapting it, security issues should be taken care.

Addressing these security issues requires a multi-faceted approach involving collaboration among stakeholders, including device manufacturers, developers, regulators, and end-users. Measures such as implementing strong authentication and encryption, conducting regular security audits and assessments, promoting security awareness and education, and establishing industry standards and regulations can help to mitigate the security risks in IoT ecosystems. Additionally, embracing principles of privacy by design and adopting security best practices throughout the lifecycle of IoT devices can enhance resilience and trust in connected systems.

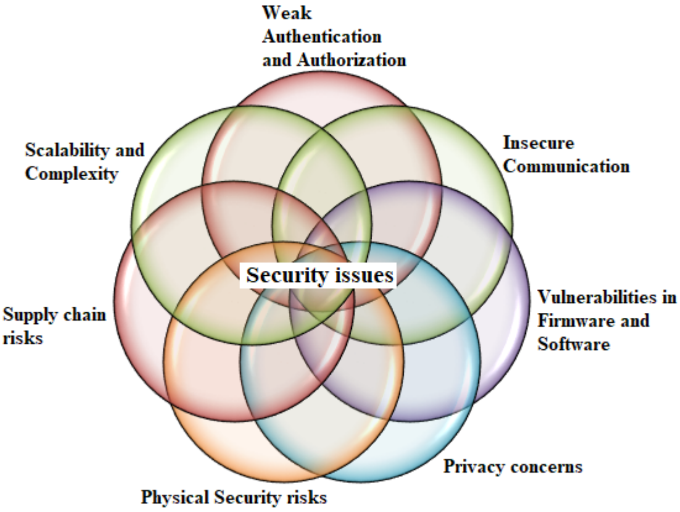

Weak Authentication and Authorization
Insecure Communication
Scalability and Complexity
Security issues
Supply chain risks
Vulnerabilities in Firmware and Software
Privacy concerns
Physical Security risks

Figure 6. Key security issues

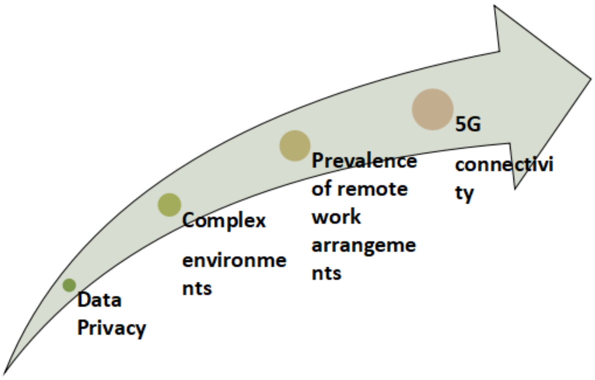


Figure 7. Emerging security issues

4. Solutions to mitigate security threats in IoT networks

The future of IoT holds immense potential for innovation and transformation across various industries and domains [49] as given in Figure 8. Edge computing [50] brings computational resources closer to the data source, reducing latency and bandwidth requirements for IoT applications. Integrating AI and machine learning algorithms at the edge enables real-time data processing, analysis, and decision-making, enhancing autonomy and intelligence of IoT devices. The deployment of 5G networks will provide ultra-fast connectivity with low latency, enabling new IoT applications and use cases that demand high-speed data transmission and real-time responsiveness [51].

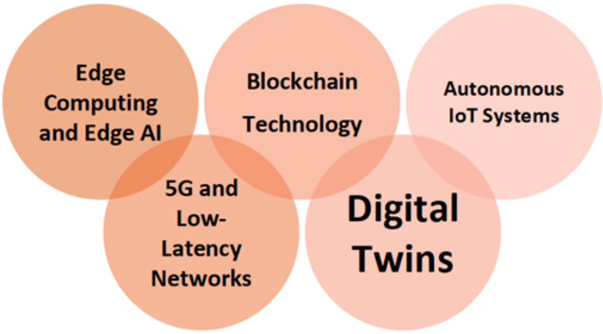


Figure 8. Domains exploring IoT

4.1 *Security by design*

Owing to the serious security breaches to the devices in the IoT networks, security by design during the manufacturing and deployment process is a critical requirement. Unlike computer communication, IoT is still in its beginnings, the security protocols and procedures are not yet standardized. For secured IoT communication, security risk analysis need to be carried out listing all possible issues and developing solutions during the development of the system.

The device credentials should never be revealed and manufacturing industries of hardware units need to ensure the safe storage of device identities. The device should not be cloned by the attackers to steal the data and data tampering should be avoided in critical applications. Layered defensive mechanism can be adapted in smart health, smart grid and banking applications that ensures the integrity of data at all levels-the devices, gateways, communication channel and at the user end. Efficient privilege management guarantees prevention of fraudulent activities and encryption mechanism safeguards from data tampering and making the stolen data useless for the hackers.

These systems adapt to changing environments, predict and prevent failures, and optimize resource utilization autonomously without human intervention. Green IoT [52] initiatives focus on energy-efficient design, resource optimization, and environmental sustainability in IoT deployments. Energy harvesting technologies, low-power devices, and eco-friendly manufacturing practices contribute to reducing the environmental footprint of IoT solutions. These future directions in IoT represent on-going trends and emerging technologies that will shape the next generation of connected systems, driving innovation, efficiency, and societal impact across various domains.

4.2 *Machine learning based IoT security*

Recently, machine learning and deep learning techniques are utilized for security. Securing Internet of Things (IoT) devices is a critical challenge due to their distributed nature, resource constraints, and susceptibility to various attacks. Machine learning techniques can play a significant role in enhancing IoT security [53] by detecting anomalies, identifying malicious activities, and mitigating threats.

Anomaly detection

Anomaly detection involves identifying patterns in data that deviate from expected behaviour. In the context of IoT security, anomaly detection can help identify unusual activities that may indicate a security breach or a compromised device. Techniques such as Isolation Forest, One-Class SVM, and Autoencoders can be used for anomaly detection in IoT data streams.

Intrusion Detection Systems (IDS)

Machine learning can be applied to build intrusion detection systems specifically tailored for IoT environments. These systems analyze network traffic, device behavior, and system logs to detect malicious activities such as DDoS attacks, malware infections, and unauthorized access. Techniques like Random Forests, Support Vector Machines (SVM), and Deep Learning models (e.g., Convolutional Neural Networks) can be employed for building IDS for IoT.

Predictive maintenance

Predictive maintenance uses machine learning algorithms to predict when IoT devices are likely to fail or require maintenance. By continuously monitoring device parameters and performance metrics, predictive maintenance models can detect anomalies indicative of potential security threats, such as tampering or attacks on device integrity.

Behavioural analysis

Machine learning can be used to establish baselines of normal behaviour for IoT devices and detect deviations from these baselines. By analyzing historical data and real-time sensor readings, behavioural analysis models can identify suspicious activities.

Secure authentication and access control

Machine learning algorithms can enhance authentication mechanisms by analyzing user behaviour patterns to detect unauthorized access attempts. Behavioral biometrics, such as keystroke dynamics or gait analysis, can be utilized to continuously authenticate users interacting with IoT devices will provide an additional layer of security.

Data encryption and privacy

Machine learning techniques can be applied to enhance data encryption mechanisms and protect sensitive information transmitted by IoT devices. Secure multi-party computation (SMPC) and homomorphic encryption, combined with machine learning models, can enable privacy-preserving analytics on encrypted IoT data without compromising data confidentiality.

Firmware and software security

Machine learning aids in identifying vulnerabilities in IoT device firmware and software by analyzing code patterns and detecting potential security weaknesses. Static and dynamic analysis techniques, coupled with machine learning algorithms, can automate the process of identifying and patching vulnerabilities in IoT device firmware and software.

Adaptive security

Machine learning models can continuously adapt to evolving threats and security challenges in IoT environments. By leveraging reinforcement learning techniques, security policies and defenses can be dynamically adjusted based on real-time threat intelligence and environmental changes, enhancing the resilience of IoT systems against emerging threats.

AI-powered systems detect anomalies and prevent cyberattacks in IoT networks such as industrial IoT and smart homes. AI analyzes global cybersecurity trends and predicts attack patterns before they occur and detects unusual behavior in IoT devices and isolates compromised nodes. AI-powered blockchain authentication prevents data tampering and ensures transaction integrity in IoT ecosystems. AI significantly enhances IoT security by predicting, detecting, and mitigating cyber threats autonomously. By integrating AI with blockchain, encryption, and adaptive security, IoT systems become more resilient to cyberattacks while maintaining autonomy and efficiency.

Table 3 presents the evaluation metrics and benchmarking datasts available for analysing ML in overcoming challenges in IoT security.

Table 3. Machine learning in IoT security

Reference	Key focus	Evaluation/Benchmarking methods
[54]	Evaluates different ML models for anomaly detection in IDS.	Uses benchmark datasets (e.g., NSL-KDD, CICIDS2017) and metrics like accuracy, precision, and recall.
[55]	Investigates the application of anomaly detection ML models in network intrusion detection.	Compares ML techniques using real-world network traffic and benchmark datasets.
[56]	Proposes ML-based IDS solutions for IoT security.	Tests multiple ML models in IoT environments and analyzes computational overhead.
[57]	Compares ML algorithms for anomaly detection in IoT networks.	Benchmarks ML models on real IoT traffic and simulated attacks.
[58]	Examines various IDS models and ML techniques for intrusion detection.	Compares supervised and unsupervised ML techniques using standard datasets.

4.3 *Deep learning based IoT security*

Deep learning techniques offer advanced capabilities for IoT security by enabling the analysis of large and complex datasets [59], identifying intricate patterns, and detecting subtle anomalies indicative of security threats. Deep neural networks, such as Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs), can be employed for various security tasks in IoT. CNNs are effective for image-based security tasks like object detection in video surveillance systems, while RNNs are suitable for sequential data analysis, such as analyzing network traffic patterns for intrusion detection. GANs consist of two neural networks, a generator and a discriminator, trained simultaneously in a competitive setting. GANs can be used for generating synthetic data to augment training datasets for anomaly detection or simulating attack scenarios to assess the robustness of IoT security systems. Auto encoders are neural network architectures used for unsupervised learning, where the network is trained to reconstruct input data. In the context of IoT security, auto encoders can be employed for anomaly detection by reconstructing normal patterns and identifying deviations as anomalies, indicating potential security threats. Reinforcement Learning (RL) algorithms learn optimal decision-making strategies by interacting with an environment to maximize cumulative rewards. RL techniques can be applied for adaptive security in IoT systems, where security policies are dynamically adjusted based on real-time feedback and environmental changes to mitigate emerging threats effectively. Deep Reinforcement Learning (DRL) combines deep learning with reinforcement learning techniques, enabling the training of deep neural networks to learn complex security policies and strategies autonomously. DRL can be used for adaptive intrusion detection, threat response, and dynamic access control in IoT environments. Transfer learning involves leveraging pre-trained deep learning models on large datasets and fine-tuning them for specific tasks with limited labeled data. Deep transfer learning can be applied in IoT security to utilize pre-trained models for related domains (e.g., computer vision or natural language processing) and adapt them to detect security threats in IoT data. Deep learning techniques can be extended to work with encrypted data, preserving privacy while enabling secure analysis of sensitive information transmitted by IoT devices. Homomorphic encryption and secure multi-party computation (SMPC) techniques can be combined with deep learning models to perform computations on encrypted IoT data without compromising confidentiality. Deep learning models can be trained for deep packet inspection to analyze network traffic at the packet level and identify malicious activities, such as DDoS attacks, intrusion attempts, or data exfiltration, in real-time, enhancing the security of IoT networks and devices. Deep learning techniques aid in analyzing IoT device firmware for vulnerabilities and malicious code. By training deep learning models on labeled datasets of benign and malicious firmware samples, it's possible to automatically detect and classify suspicious firmware behaviour, helping prevent attacks targeting IoT device integrity. Deep learning models can be employed for biometric authentication in IoT systems, utilizing techniques such as facial recognition, voice authentication, or behavioural biometrics to authenticate users and devices securely.

4.4 *Role of quantum computing in IoT security*

Quantum computing could disrupt current IoT security by breaking traditional encryption methods like RSA and ECC, which rely on the difficulty of certain mathematical problems. This makes IoT systems vulnerable to attacks. However, researchers are developing post-quantum cryptography (PQC) to create new encryption algorithms resistant to quantum threats. On the positive side, quantum key distribution (QKD) could enhance IoT security by ensuring that communications remain secure through the principles of quantum mechanics. Additionally, quantum technologies could improve device authentication and integrity. The transition to quantum-safe methods is challenging for resource-constrained IoT devices, but it's necessary for long-term security. Furthermore, quantum computing could both help and hinder network defense capabilities. Privacy risks may arise as quantum advancements could potentially expose previously secure data. As quantum computing develops, IoT systems will need to adapt with new cryptographic solutions to stay secure.

5. IoT security framework

The regulatory frameworks are designed to reduce IoT security risks by establishing standards for device makers, service providers, and users. However, IoT security regulations are still in development, and on-going adjustments will be necessary to keep up with new threats and technological advancements. Ensuring proper implementation and adherence to these regulations will be essential for safeguarding the expanding IoT landscape. Table 4 lists few of the regulatory frameworks of IoT security

Table 4. Regulatory frameworks of IoT security

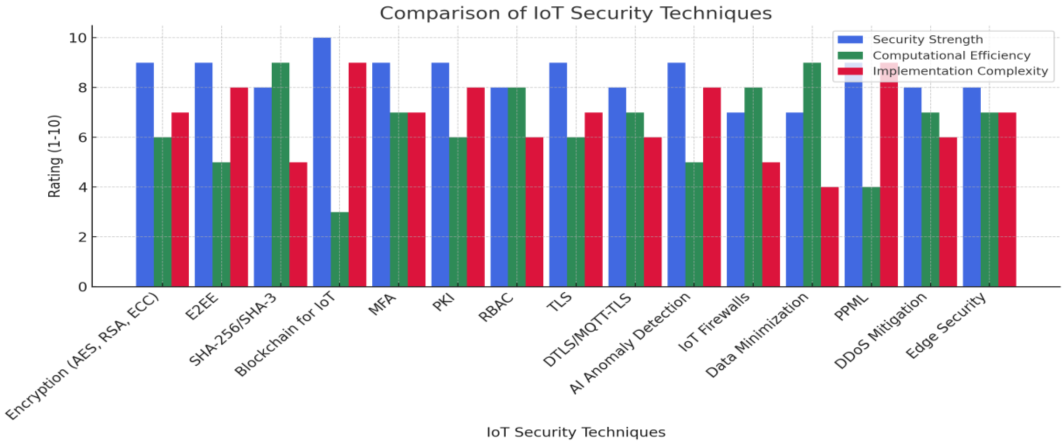
Regulatory framework	**Region**	**Focus**
General Data Protection Regulation (GDPR)	European union	Ensures protection of personal data collected by IoT devices and establishes privacy standards.
Network and Information Systems Directive (NIS)	European union	Outlines cybersecurity requirements for critical infrastructure, including IoT networks.
IoT cybersecurity improvement act	United States	Sets security standards for IoT devices used by U.S. federal agencies, such as encryption and authentication.
California Consumer Privacy Act (CCPA)	United States (California)	Focuses on consumer data protection, including that collected by IoT devices.
Australia's cybersecurity strategy 2020	Australia	National framework to enhance cybersecurity, with specific measures for IoT security risks.
ISO/IEC 27001:2013	Global	Standard for managing information security, including guidelines for securing IoT devices and systems.
UK's code of practice for consumer IoT security	United Kingdom	Provides recommendations for securing consumer IoT devices, including strong passwords and software updates.
Cybersecurity Act of 2015	United States	Promotes collaboration in cybersecurity and encourages IoT security practices, including risk management.
ITU-T X.1205 (IoT security framework)	Global	Offers global standards for securing IoT systems and devices, focusing on industry best practices.
The Internet of Things cybersecurity improvement act	United States	Sets minimum security standards for IoT devices used by federal agencies, including secure authentication and patching.

6. Comparison of security techniques in IoT

The effectiveness of different IoT security techniques based on key factors such as security strength, computational efficiency, and implementation complexity is shown in the chart below and elaborated in Table 5. Higher value of security strength, computational efficiency, and implementation complexity indicates stronger security, less computational burden and more challenging to implement.

Table 5. Comparison of IoT security techniques

Security Aspect	Techniques	Advantages	Challenges
Data confidentiality	Encryption (AES, RSA, ECC)	Strong protection against data breaches	Computational overhead for resource-limited devices
	End-to-End Encryption (E2EE)	Prevents data interception in transit	Implementation complexity in constrained networks
Data integrity	Cryptographic hashing (SHA-256, SHA-3)	Ensures data authenticity and integrity	Cannot prevent initial tampering; only detects changes
	Blockchain for IoT	Provides decentralized and tamper-proof records	High processing and storage requirements
Authentication & Access control	Multi-Factor Authentication (MFA)	Stronger security against credential theft	User convenience can be affected
	Public Key Infrastructure (PKI)	Secure and scalable authentication	Requires proper certificate management
	Role-Based Access Control (RBAC)	Restricts access based on user roles	Complexity in managing roles at a large scale
Network security	Transport Layer Security (TLS)	Encrypts data in transit for secure communication	Can be resource-intensive for IoT devices
	Lightweight Cryptographic Protocols (DTLS, MQTT with TLS)	Optimized for constrained IoT devices	May still introduce latency in real-time communication
Intrusion detection & Prevention	AI-based anomaly detection	Identifies unknown cyber threats in real-time	Requires training datasets and continuous updates
	IoT firewalls	Filters and blocks malicious traffic	Needs to be updated frequently against new threats
Privacy protection	Data minimization	Reduces exposure of sensitive data	May limit analytics capabilities
	Privacy-Preserving Machine Learning (PPML)	Enables AI-based IoT security without exposing raw data	Implementation complexity and high processing requirements



The Table 6 elaborates the applications of existing security techniques in practical domains highlighting their challenges and achieved benefits [60, 61].

Table 6. Summary on applications of IoT security techniques

Security technique	Deployment domain	Challenges	Outcomes achieved
Intrusion detection & Prevention (IDPS)	Smart homes (Google nest secure), Industrial IoT (Siemens SCADA), smart cities (Cisco Cyber Vision)	High false positives, scalability in large networks, detection of zero-day attacks	20-30% improved threat detection, reduced false alarms, real-time anomaly detection
Blockchain for secure IoT	IBM food trust (supply chain), power ledger (smart grids), MedRec (healthcare)	High computational cost, latency issues, blockchain scalability	Data integrity ensured, 40% reduction in fraudulent activities, improved transaction trust
AI-driven threat intelligence	Tesla OTA security, siemens industrial IoT, GE healthcare	Requires large datasets, AI model explainability, high resource consumption	90% attack detection accuracy, 35% fewer security breaches, improved proactive threat mitigation
Secure boot & Firmware integrity	Apple HomeKit (smart home), Philips (medical devices), Siemens PLCs (industrial)	Firmware update delays, device compatibility issues, key management complexity	80% reduction in firmware-based attacks, improved IoT device reliability
Zero Trust Architecture (ZTA) & Network segmentation	Cisco/Palo alto in industrial IoT, walmart IoT POS security, healthcare IoT segmentation	Complex implementation, integration with legacy systems, increased authentication overhead	50% reduction in unauthorized access, improved security of critical infrastructure
Lightweight cryptography for IoT	Apple Watch & Fitbit (wearables), Toyota V2V communication, schneider electric IIoT sensors	Balancing security & low power consumption, compatibility with legacy encryption methods	60% lower energy consumption with secure data transmission, strong encryption with minimal latency

7. Challenges in existing techniques and Future research direction

Future IoT security research must go beyond traditional encryption and firewalls to embrace AI, quantum security, federated learning, bio-inspired models, and Zero Trust architectures. These next-gen security solutions will enhance resilience, privacy, and scalability in autonomous IoT systems. Sections below elaborate on the area where the future researchers have to make their contribution to enhance IoT security.

7.1 *AI-driven self-adaptive security systems*

Future research should focus on developing AI-powered security frameworks that autonomously adapt to evolving cyber threats in real-time. These frameworks will use machine learning models to detect, predict, and neutralize threats before they impact IoT networks, reducing reliance on manual interventions. By integrating AI-driven self-healing mechanisms, IoT systems can dynamically adjust security policies and configurations based on behavioral analysis.

7.2 *Quantum-resistant cryptography for IoT*

As quantum computing advances, existing encryption algorithms like RSA and ECC will become vulnerable, requiring post-quantum cryptographic solutions for IoT security. Future research should explore lightweight quantum-resistant algorithms, such as lattice-based and hash-based encryption, to ensure secure communication in resource-constrained IoT devices. These algorithms must be optimized for low-power environments while maintaining strong cryptographic resistance against quantum attacks.

7.3 *Blockchain 2.0 for IoT security*

Traditional blockchain implementations are computationally expensive and struggle with scalability, making them unsuitable for IoT environments. Future blockchain-based IoT security should focus on energy-efficient consensus mechanisms like Proof-of-Elapsed-Time (PoET) and Directed Acyclic Graphs (DAG) to improve transaction speed and reduce overhead. Additionally, integrating smart contracts with AI-driven anomaly detection can enable trustless, self-enforcing security policies across IoT ecosystems.

7.4 *Federated learning-based threat intelligence*

Federated Learning (FL) enables distributed attack detection without centralizing sensitive IoT data, preserving privacy while improving threat intelligence. Future research should enhance FL models by incorporating real-time, cross-network training to detect global attack patterns across multiple IoT environments. By leveraging edge AI for localized decision-making, IoT networks can achieve faster threat response times while maintaining decentralized security.

7.5 *Bio-inspired & neuromorphic IoT security models*

Future IoT security research should explore self-learning, adaptive defense mechanisms that mimic the human body's response to infections. These models could integrate neuromorphic computing to enable real-time, ultra-low-power attack detection and mitigation. By continuously evolving in response to new cyber threats, bio-inspired IoT security systems could offer self-healing capabilities with minimal human intervention.

7.6 *Zero trust IoT security frameworks*

Zero Trust security eliminates implicit trust and enforces continuous authentication for every IoT device, reducing unauthorized access risks. Future research should focus on integrating behavior-based authentication, where AI models analyze user and device behavior patterns in real time to dynamically adjust access permissions. Additionally, implementing context-aware Zero Trust policies can enhance IoT security by ensuring access decisions are based on real-time risk assessments.

7.7 *Next-generation IoT cyber-resilience models*

Traditional security measures focus on attack prevention, but future IoT systems need self-recovering, cyber-resilient frameworks that maintain functionality during and after cyberattacks. Research should explore digital twins for IoT security, allowing virtual simulations of real-world attacks to develop proactive defense strategies. By combining AI-driven anomaly detection with automated recovery mechanisms, future IoT systems can autonomously detect, mitigate, and recover from cyber threats in real time.

8. Conclusions

This study conducts a systematic literature review to explore security threats in IoT networks, assess existing countermeasures, and identify research gaps. The analysis highlights key vulnerabilities, including authentication weaknesses, anomaly detection challenges, and communication security issues. While various solutions have been proposed, concerns regarding scalability, standardization, and real-time threat mitigation persist. Future research should prioritize the development of AI-driven, adaptive security frameworks that enhance protection while considering efficiency and resource constraints in IoT environments.

Low-power wide-area networks (LPWANs) like NB-IoT and LTE-M will enable long-range, low-power communication for IoT devices in remote or energy-constrained environments. Blockchain technology offers secure and transparent data transactions, enhancing trust, and integrity in IoT ecosystems. Applications of blockchain in IoT include secure device identity management, tamper-proof data logging, and decentralized device coordination. Digital twins are virtual representations of physical IoT devices, systems, or processes, enabling real-time monitoring, analysis, and optimization. Simulation and modelling techniques allow for predictive maintenance, scenario testing, and optimization of IoT deployments before implementation in the physical world. Autonomous IoT systems leverage AI, machine learning and robotics to enable self-configuring, self-optimizing, and self-healing capabilities.

Declaration

The authors have no relevant financial or non-financial interests to disclose. The authors have no conflicts of interest to declare that are relevant to the content of this article.

References

[1] J. Gubbi, R. Buyya, S. Marusic, and M. Palaniswami, "Internet of things (IoT): A vision, architectural elements, and future directions," *Future Generation Computer Systems*, vol. 29, no. 7, pp. 1645-1660, 2013.

[2] N. Sharma, M. Shamkuwar, and I. Singh, "The history, present and future with IoT," in *Internet of Things and Big Data Analytics for Smart Generation*. Heidelberg, Germany: Springer, 2019, pp. 27-51.

[3] B. Tushir, H. Sehgal, R. Nair, B. Dezfouli, Y. Liu, "The impact of DiS attacks on resource-constrained IoT devices: A study on the Mirai attack," *arXiv*, 2021, Available: https://arxiv.org/abs/2104.09041. [Accessed Apr. 9, 2021].

[4] M. De Donno, N. Dragoni, A. Giaretta, and A. Spognardi, "DDoS-capable IoT malwares: Comparative analysis and Mirai investigation," *Security and Communication Networks*, vol. 2018, no. 1, p. 7178164, 2018, https://doi.org/10.1155/2018/7178164.

[5] J. Wang, Y. Liu, and H. Feng, "IFACNN: Efficient DDoS attack detection based on improved firefly algorithm to optimize convolutional neural networks," *Mathematical Biosciences and Engineering*, vol. 19, pp. 1280-1303, 2021.

[6] I. Ullah and Q. H. Mahmoud, "A scheme for generating a dataset for anomalous activity detection in IoT networks," in *Advances in Artificial Intelligence*. Cham, Switzerland: Springer, 2020.

[7] A. A. Alahmadi, M. Aljabri, F. Alhaidari, D. J. Alharthi, G. E. Rayani, L. A. Marghalani, et al., "DDoS attack detection in IoT-based networks using machine learning models: A survey and research directions," *Electronics*, vol. 12, no. 14, p. 3103, 2023, https://doi.org/10.3390/electronics12143103.

[8] N. Sharma, M. Shamkuwar, and I. Singh, "The history, present and future with IoT," in *Internet of Things and Big Data Analytics for Smart Generation*. Heidelberg, Germany: Springer, 2019, pp. 27-51.

[9] G. S. Hukkeri and R. H. Goudar, "IoT: Issues, challenges, tools, security, solutions and best practices," *International Journal of Pure and Applied Mathematics*, vol. 120, no. 6, pp. 12099-12109, 2019.

[10] R. A. Lika, D. Murugiah, S. N. Brohi, and D. Ramasamy, "NotPetya: Cyber attack prevention through awareness via gamification," in Proc. International Conference on Smart Computing and Electronic Enterprise (ICSCEE), Shah Alam, Malaysia, Jul. 11-12, 2018, pp. 1-6, https://doi.org/10.1109/ICSCEE.2018.8538431.

[11] A. K. Sikder, A. Acar, H. Aksu, A. S. Uluagac, M. Conti, and A. S. Tosun, "Consumer IoT: Security vulnerability case studies and solutions," *IEEE Consumer Electronics Magazine*, vol. 9, no. 2, pp. 17-25, 2020.

[12] C. Xenofontos, I. Zografopoulos, C. Konstantinou, A. Jolfaei, M. K. Khan, and K. K. R. Choo, "Consumer, commercial, and industrial IoT (In) Security: Attack taxonomy and case studies," *IEEE Internet of Things Journal*, vol. 8, no. 12, pp. 9531-9541, 2021.

[13] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose, “SoK: Security evaluation of home-based IoT deployments,” in Proc. 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, May 19-23, 2019, pp. 1362-1380.

[14] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, “Securing IoT devices against emerging security threats,” *Journal of Cyber Security and Mobility*, vol. 12, no. 1, pp. 1-24, 2023.

[15] W. H. Hassan, “Current research on Internet of Things (IoT) security: A survey,” *Computer Networks*, vol. 148, pp. 283-294, 2019.

[16] F. Meneghello, M. Calore, D. Zucchetto, M. Polese, and A. Zanella, “IoT: Internet of threats? A survey of practical security vulnerabilities in real IoT devices,” *IEEE Internet of Things Journal*, vol. 6, pp. 8182-8201, 2019.

[17] A. Yadav, A. Tripathi, N. Rakesh, and S. Pandey, “Protecting composite IoT server by secure secret key exchange for XEN intra virtual machines,” *International Journal of Information and Computer Security*, vol. 12, no. 1, pp. 53-69, 2020.

[18] W. Yang, S. Wang, N. M. Sahri, N. M. Karie, M. Ahmed, and C. Valli, “Biometrics for Internet-of-Things security: A review,” *Sensors*, vol. 21, no. 18, p. 6163, 2021.

[19] S. Ebrahimi and S. Bayat-Sarmadi, “Lightweight fuzzy extractor based on LPN for device and biometric authentication in IoT,” *IEEE Internet of Things Journal*, vol. 8, pp. 10706-10713, 2021.

[20] S. Duraibi, “Voice biometric identity authentication model for IoT devices,” *International Journal of Security, Privacy and Trust Management (IJSPTM)*, vol. 9, no. 2, p. 9201, 2020.

[21] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, “A survey on IoT security: Application areas, security threats, and solution architectures,” *IEEE Access*, vol. 7, pp. 82721-82743, 2019.

[22] G. Kumar and K. Kumar, “Network security-an updated perspective,” *Systems Science and Control Engineering*, vol. 2, no. 1, pp. 325-334, 2014.

[23] N. N. Srinidhi, S. M. Dilip Kumar, and K. R. Venugopal, “Network optimizations in the Internet of Things: A review,” *Engineering Science and Technology, an International Journal*, vol. 22, no. 1, pp. 1-21, February 2019.

[24] P. K. Sadhu, V. P. Yanambaka, and A. Abdelgawad, “Internet of Things: Security and solutions survey,” *Sensors*, vol. 22, no. 19, p. 7433, 2022, https://doi.org/10.3390/s22197433.

[25] P. Williams, I. K. Dutta, H. Daoud, and M. Bayoumi, “A survey on security in internet of things with a focus on the impact of emerging technologies,” *Internet of Things*, vol. 19, p. 100564, August 2022.

[26] B. I. Mukhtar, M. S. Elsayed, A. D. Jurcut, and M. A. Azer, “IoT vulnerabilities and attacks: SILEX malware case study,” *Symmetry*, vol. 15, no. 11, p. 1978, 2023, https://doi.org/10.3390/sym15111978.

[27] M. A. Al Kabir, W. Elmedany, and M. S. Sharif, “Securing IoT devices against emerging security threats: Challenges and mitigation techniques,” *Journal of Cyber Security Technology*, vol. 7, no. 4, pp. 199-223, 2023, doi: https: //doi.org/10.1080/23742917.2023.2228053.

[28] H. Pourrahmani, A. Yavarinasab, A. M. Hosseini Monazzah, and J. Van herle, “A review of the security vulnerabilities and countermeasures in the Internet of Things solutions: A bright future for the Blockchain,” *Internet of Things*, vol. 23, p. 100888, October 2023.

[29] M. S. Jalali and J. P. Kaiser, “Cybersecurity in hospitals: A systematic, organizational perspective,” *Journal of Medical Internet Research*, vol. 20, no. 5, e10059, 2018, https://doi.org/10.2196/10059.

[30] M. Javaid, A. Haleem, R. P. Singh, and R. Suman, “Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends,” *Cyber Security and Applications*, vol. 1, p. 100016, December 2023.

[31] H. Taherdoost, “Security and Internet of Things: Benefits, challenges, and future perspectives,” *Electronics*, vol. 12, no. 8, p. 1901, 2023, https://doi.org/10.3390/electronics12081901.

[32] T. Mazhar, D. B. Talpur, T. A. Shloul, Y. Y. Ghadi, I. Haq, I. Ullah, et al., “Analysis of IoT security challenges and its solutions using artificial intelligence,” *Brain Sciences*, vol. 13, no. 4, p. 683, 2023, https://doi.org/10.3390/brainsci13040683.

[33] S. Bhunia and M. Tehranipoor, (Eds.), “Physical attacks and countermeasures,” in *Hardware Security*. San Francisco, CA, USA: Morgan Kaufmann, 2019, pp. 245-290.

[34] M. El-hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, “A survey of Internet of Things (IoT) authentication schemes,” *Sensors*, vol. 19, no. 5, 2019.

[35] A. Fadele, M. Othman, I. Hashem, I. Yaqoob, M. Imran, and M. Shoaib, “A novel countermeasure technique for reactive jamming attack in Internet of Things,” *Multimedia Tools and Applications*, vol. 78, pp. 29899-29920, 2019.

[36] I. Butun, P. Österberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures," *IEEE Communications Surveys and Tutorials*, vol. 22, no. 1, pp. 616-644, 2020.

[37] A. Mosenia and N. K. Jha, "A comprehensive study of security of Internet-of-Things," *IEEE Transactions on Emerging Topics in Computing*, vol. 5, no. 4, pp. 586-602, 2017.

[38] A. Mayzaud, R. Badonnel, and I. Chrisment, "A taxonomy of attacks in RPL-based Internet of Things," *International Journal of Network Security*, vol. 18, no. 3, pp. 459-473, 2016.

[39] L. Sha, F. Xiao, W. Chen, and J. Sun, "IIoT-SI defender: Detecting and defense against the sensitive information leakage in industry IoT," *World Wide Web*, vol. 21, no. 1, pp. 59-88, 2018.

[40] Q. D. Ngo, H. T. Nguyen, V. H. Le, and D. H. Nguyen, "A survey of IoT malware and detection methods based on static features," *ICT Express*, vol. 6, no. 4, pp. 280-286, 2020.

[41] A. Matrosov, E. Rodionov, D. Harley, and J. Malcho, "Stuxnet under the microscope," San Diego, CA, USA: ESET LLC, 2010.

[42] M. M. Ogonji, G. Okeyo, and J. M. Wafula, "A survey on privacy and security of Internet of Things," *Computer Science Review*, vol. 38, p. 100312, 2020.

[43] C. Dong, G. He, X. Liu, Y. Yang, and W. Guo, "A multi-layer hardware trojan protection framework for IoT chips," *IEEE Access*, vol. 7, pp. 23628-23639, 2019.

[44] M. R. Naqvi, M. Aslam, M. W. Iqbal, S. K. Shahzad, M. Malik, and M. U. Tahir, "Study of block chain and its impact on Internet of Health Things (IoHT): Challenges and opportunities," in Proc. International Congress on Human-Computer Interaction, Optimization and Robotic Applications, Ankara, Turkey, Jun. 26-28, 2020, pp. 1-6.

[45] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, "A survey on IoT security: Application areas, security threats, and solution architectures," *IEEE Access*, vol. 7, pp. 82721-82743, 2019.

[46] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT privacy and security: Challenges and solutions," *Applied Sciences*, vol. 10, no. 11, p. 4102, 2020.

[47] J. Y. Lee and J. Lee, "Current research trends in IoT security: A systematic mapping study," *Mobile Information Systems*, vol. 2021, p. 8847099, 25 pages, 2021.

[48] D. Fang, Y. Qian, and R. Q. Hu, "A flexible and efficient authentication and secure data transmission scheme for IoT applications," *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3474-3484, 2020.

[49] M. Yahuza, M. Y. I. B. Idris, A. W. B. A. Wahab, A. T. Ho, S. Khan, S. N. B. Musa, and A. Z. B. Taha, "Systematic review on security and privacy requirements in edge computing: State of the art and future research opportunities," *IEEE Access*, vol. 8, pp. 76541-76567, 2020.

[50] H. Elazhary, "Internet of Things (IoT), mobile cloud, cloudlet, mobile IoT, IoT cloud, fog, mobile edge, and edge emerging computing paradigms: Disambiguation and research directions," *Journal of Network and Computer Applications*, vol. 128, pp. 105-140, 2019.

[51] N. M. Karie, N. M. Sahri, and P. Haskell-Dowland, "IoT threat detection advances, challenges and future directions," in Proc. Workshop on Emerging Technologies for Security of IoT (ETSecIoT), Sydney, NSW, Australia, Apr. 21, 2020, pp. 22-29.

[52] M. A. Ferrag, L. Shu, X. Yang, A. Derhab, and L. Maglaras, "Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges," *IEEE Access*, vol. 8, pp. 32031-32053, 2020.

[53] F. Alwahedi, A. Aldhaheri, M. A. Ferrag, A. Battah, and N. Tihanyi, "Machine learning techniques for IoT security: Current research and future vision with generative AI and large language models," *Internet of Things and Cyber-Physical Systems*, vol. 4, pp. 167-185, 2024.

[54] J. Doe and A. Smith, "Benchmarking of machine learning for anomaly-based intrusion detection systems," *IEEE Transactions on Network and Service Management*, vol. 18, no. 3, pp. 1234-1245, 2023.

[55] M. Brown and K. Lee, "Anomaly-based intrusion detection by machine learning: a case study," *IEEE Internet of Things Journal*, vol. 9, no. 5, pp. 3456-3468, 2022.

[56] L. Sana, M. M. Nazir, J. Yang, L. Hussain, Y. L. Chen, C. S. Ku, M. Alatiyyah, L. Y. Por, "Securing the IoT cyber environment: enhancing intrusion anomaly detection systems using machine learning," *IEEE Access*, vol. 11, pp. 56789-56801, 2023.

[57] L. Zhang and R. Kumar, "A comprehensive analysis of the machine learning algorithms in IoT anomaly detection," *IEEE Communications Surveys & Tutorials*, vol. 25, no. 1, pp. 112-130, 2024.

[58] H. Patel and J. Thompson, "Comparative analysis of intrusion detection systems and machine learning algorithms," *IEEE Transactions on Information Forensics and Security*, vol. 19, no. 2, pp. 654-667, 2024.

[59] E. C. P. Neto, S. Dadkhah, S. Sadeghi, H. Molyneaux, and A. A. Ghorbani, “A review of Machine Learning (ML)-based IoT security in healthcare: A dataset perspective,” *Computer Communications*, vol. 213, pp. 61-77, 2024.

[60] M. T. Talpur, D. B. Shloul, T. A. Ghadi, Y. Y. Haq, I. Ullah, K. Ouahada, and H. Hamam, “Analysis of IoT security challenges and its solutions using artificial intelligence,” *Brain Sciences*, vol. 13, no. 4, 2023, https://doi.org/10.3390/brainsci13040683.

[61] M. A. Khan and K. Salah, “Security and internet of things: benefits, challenges, and future directions,” *Electronics*, vol. 12, no. 8, 2020. Available: https://doi.org/10.3390/electronics12081901. [Accessed Apr. 19, 2023].