DS Journal of Cyber Security
Volume 3 Issue 3, 15-38, Jul - Sep 2025
ISSN: 2584-0665 / https://doi.org/10.59232/CYS-V3I3P102

Review Article

Cybersecurity in the Internet of Things (IoT) - Review

Taban Habibu[1,2*], Ayo P. Julius[1]

[1]*Department of Computer and Information Science, Faculty of Technoscience, Muni University, Muni Arua, Uganda.*
[2]*Department of Computer Science, Faculty of Science, Islamic University in Uganda, Mbale, Uganda.*

*hamitech2019@gmail.com

Received: 08 June 2025; Revised: 07 July 2025; Accepted: 03 August 2025; Published: 15 August 2025

Abstract - The quick growth of the IoT has brought more ease, greater efficiency, and automation to industries. Still, connected systems in IoT bring up many cybersecurity challenges since IoT settings have many resources and a large variety of devices. This study helps to identify the key security problems, possible weaknesses, and dangers of IoT systems. It reviews IoT infrastructure security approaches, like encryption, authentication, intrusion detection, and blockchain, and studies their pluses and minuses. Important topics discussed in the paper are the scarcity of common security standards and the problem of securing devices and networks that work on the edges (peripheries) of the network. The article puts forward an approach to security that combines several defensive strategies, intelligent detection of threats, and tailored policies for different stakeholders to deal with these issues. It is emphasized that the security of IoT depends on the ability to change and work with different systems. With this assessment, the conversation about IoT cybersecurity is broadened by looking at the present state, noticing new trends, and helping set up future studies.

Keywords - Internet of Things (IoT), Cybersecurity, IoT Security Framework, Device Vulnerability, Data Privacy, Network Security, Intrusion Detection, Encryption Protocol, Theoretical Research, Security Challenge.

1. Introduction

Because of sensors, software, and network features in the Internet of Things, a physical device can now connect and exchange information with similar devices on its own [1]. For example, items at home, plus sophisticated equipment in business places, can all use the Internet to send and receive data for remote control and analysis anytime it is required. Devices or sensors in the IoT are equipped with sensors to obtain information. Such networks as Wi-Fi, Bluetooth, and cellular are part of connectivity, and these systems help gather data that is later examined and interpreted using Data Processing. User Interfaces offer people a way to use and interact with IoT devices [2].

In today's world, IoT helps a lot in different sectors, one of which is healthcare through monitoring patients at a distance by connecting medical devices; also at home by handling daily activities automatically and making them more convenient and energy-efficient; in managing cars and traffic safely and efficiently; and in making industrial tasks automatic, thus aiding the manufacturing sector. Because of IoT, industries are getting more efficient, saving money, and making choices based on data [3]. With IoT advancing, it will become common in different areas of life and business and keep transforming our surroundings [4]. Figure 1 shows the structure of the Internet of Things (IoT) and its main parts.

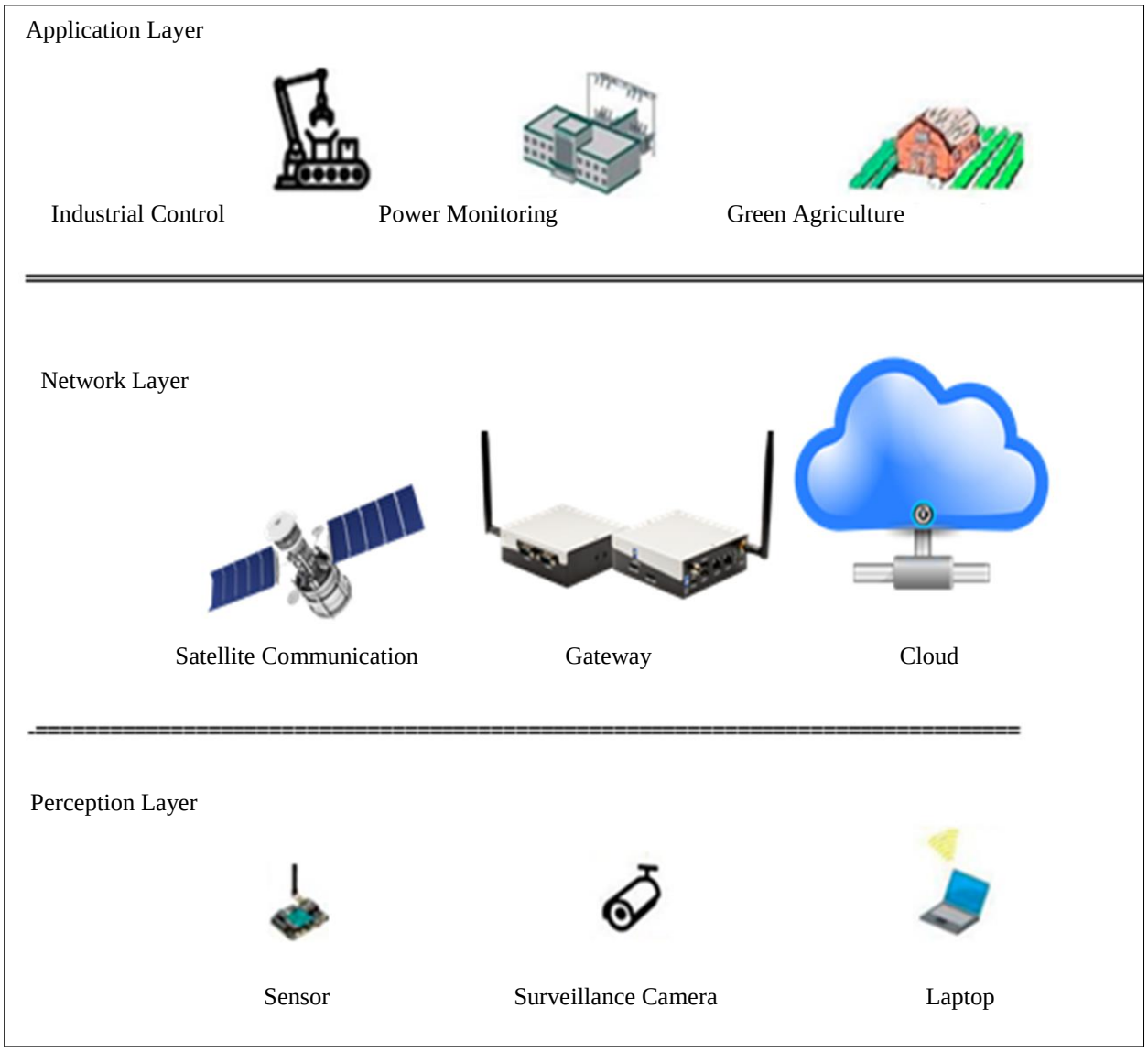

Fig. 1 General architecture of the IoT

1.1. IoT Growth and Trends

Because of more IoT devices, businesses can save time and operate more efficiently with ease and fast decisions using technology. Lately, the number of IoT devices has risen, and it is predicted that there will be more than 30 billion devices part of the IoT around the world by 2030. With the help of cloud, AI and 5G, IoT has become more valuable in healthcare, factories, planning cities and moving people around them [4]. Using the IoT in healthcare, doctors can watch their patient's distance and prevent possible health problems, while IIoT in manufacturing supports close supervision of factories and keeps devices running smoothly [5].

Still, the surge in IoT gadgets has given rise to many security risks, including cyber assaults, stolen information, and outsiders' control of critical systems. Since the number of IoT networks is rising, people must focus on strengthening their authentication, encryption and network protection. This can be achieved by making and following strong cybersecurity policies and relevant legislation [6]. Still, these hardships have not slowed IoT's role in aiding various sectors to become more digital, improve their business approaches and boost the efficiency of their daily operations. The Figure below, Figure 2, demonstrates this point.

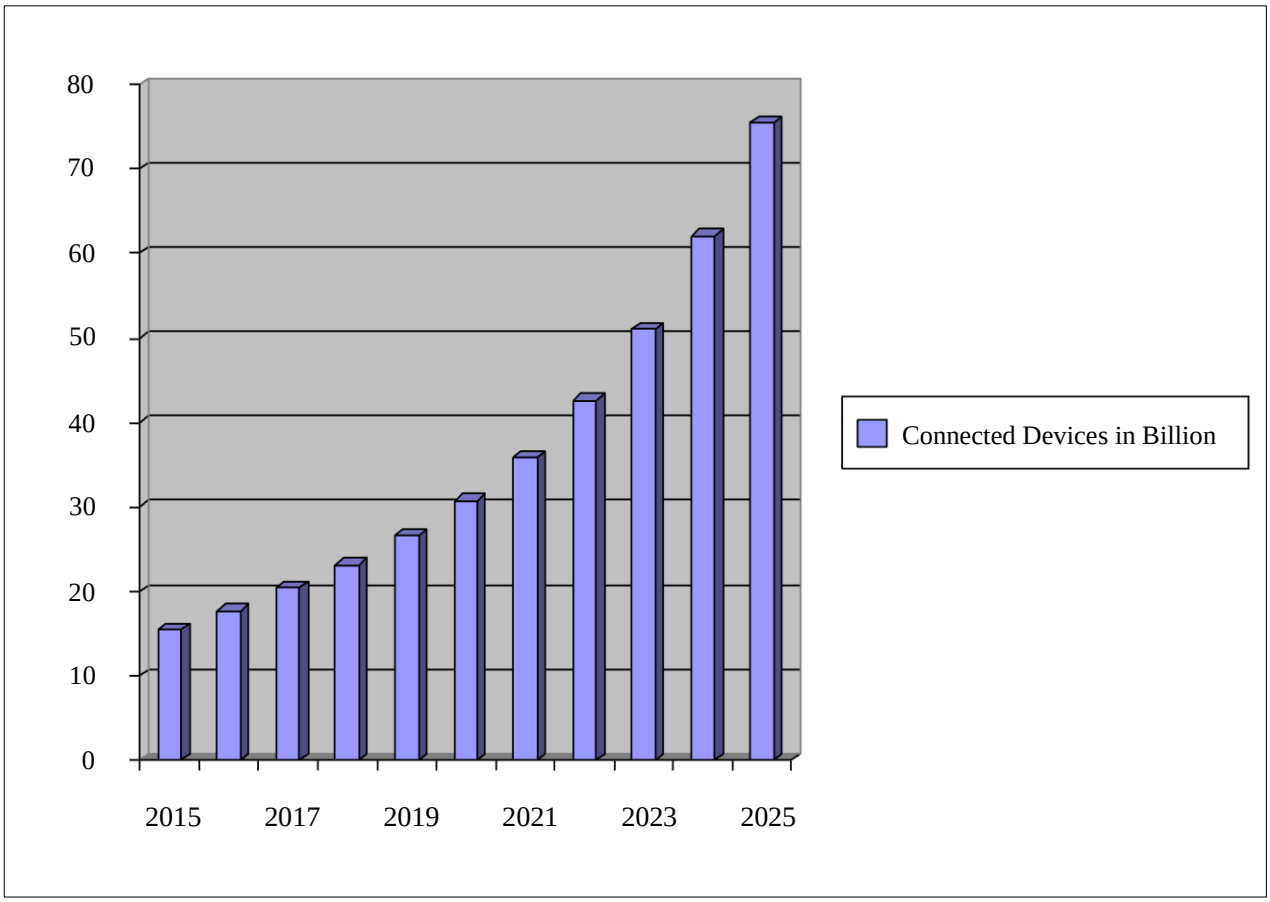

Fig. 2 Growth trends of IoT devices (2015-2025)

1.2. Cybersecurity in IoT: Essential Issues and Key Challenges

The rapid growth of IoT has made it possible for billions of online gadgets, which now adds to cybersecurity problems. Since encrypting and securing these IoT devices is not entirely possible because of lack of power, many security-related issues exist [7]. Manufacturers usually value low costs and how a device performs instead of carefully crafting its security. Therefore, their firmware might be vulnerable, they may use weak passwords by default, and outdated programs help hackers successfully target them [7].

Many companies struggle to protect and track gadgets since they are spread among many networks. Because cybersecurity laws and rules are still not strong enough, organizations should use network division, keep monitoring, and depend on artificial intelligence to deal with threats [8]. As more IoT devices are used, solving cybersecurity issues becomes important to defend data user privacy and improve the reliability of the whole system [9].

1.3. Risks and Consequences of IoT Vulnerabilities

Relying more on connected devices in organisations has increased cyberattack threats; if successful, such attacks might severely harm a business. On top of other problems, data breaches are very dangerous since they allow access to IoT devices, letting others view your personal, financial and health information and use it for identity theft or robbing you [10].

Sometimes, it is unclear to users how much privacy these devices take from them, creating concerns over ethics and laws [11]. Since an attack on IoT systems might bring down whole systems, failures in services like intelligent

networks, medical systems, and self-driving vehicles are a severe issue [12]. It is especially concerning that vulnerabilities in IoT can give attackers access to vital systems like power grids and water suppliers and make the public and the country unsafe [13]. Because IoT technology is widely used, it cannot do without firm security plans, regular updates for software, and better methods for noticing attacks against IoT devices [14].

1.4. The Critical Need for Cybersecurity in the Internet of Things

Millions of daily interactions that the Internet of Things supports make privacy and risk prevention more important. Since IoT devices send and collect lots of information, it makes personal, banking and health details vulnerable, encouraging hackers to attack [15]. Since security in many IoT devices is not correctly done, anyone can gain access, steal user data, and perform identity theft, resulting in significant losses [16]. Protecting self-driving cars, hospitals, and industrial equipment requires good cybersecurity [17]. As more cities and the nation rely on IoT, issues related to attacks on their power, water supplies, and emergency response systems become more important for people to keep in mind, as such attacks might endanger the public and weaken the economy [18]. If no proper security measures, regular updates, or strong regulations are used, IoT systems are vulnerable to attack, so taking action in advance is necessary.

As more devices connected through the Internet of Things are circulated in healthcare, cities, industry and even homes, security is a big concern because much of their cloud and edge computing are involved [19]. This research wants to uncover the main problems in the IoT security system, such as when an attacker steals someone's login, uses destructive programs, or targets IoT devices with DoS attacks. It looks into ways to safely store data, including using blockchain for verification and encryption that does not require many computing resources [20]. One major part of the research calls for enhancing technologies, including artificial intelligence, quantum encryption, and zero-trust techniques that help secure IoT structures from cyber hazards [21]. As a result of this study, cybersecurity has improved, Internet of Things systems have become stronger, and everyone's digital environments are safer [22].

1.5. Primary Focus of the Study

The research aims to point out IoT security problems and recommend ways of safeguarding the systems. The primary purpose of this research is to discuss key security challenges in IoT situations, such as having devices with limited strength and lacking proper authentication and encryption. Besides, it looks at how the existing rules and future developments, such as blockchain, AI for security purposes, and full trust networks, aid in protecting IoT networks. Researchers also examine the role of policies and rules in making people use standard security steps for IoT products. In addition, the study recommends using light encryption, having authentication for users decentralized across the network, and setting up intrusion detection right away to strengthen defence against cyber-attacks [23]. Since these goals are important, the work leads to safer internet systems and IoT usage in different areas, including keeping information private and safe communication [24].

1.5.1. Critical Questions Addressed by the Study

This study examines IoT cybersecurity's main gaps and challenges by asking the following key questions.

- Which IoT security issues often occur the most?
- Are IoTs covered adequately by the present cybersecurity regulations?
- What are some of the new technologies that can boost the safety and confidentiality of IoT systems?
- How do businesses face the security problems of handling many IoT devices?
- How can access to IoT devices undermine important infrastructure and invade people's privacy?

They help choose the research focus, identify weak points, analyse defences, and recommend improvements. This article aims to explain IoT cybersecurity troubles and offer possible solutions. The introduction section tells readers when and why the study started and its main goals. Research papers on existing IoT security risks, approaching dangers, and ongoing ways to deal with them are studied in the literature study. In the methodology section, researchers describe the data collection and analysis strategies. In the results and discussion section, the

report studies serious IoT cybersecurity issues reviews the available security methods, and suggests different solutions. In the conclusion, the report mentions the main findings, shows why they matter, and proposes further studies in IoT security.

2. Literature Review

You will discover a thorough examination of the current development of IoT security here. It evaluates what has been studied earlier, explains the leading security challenges, and points out key achievements reached by the industry. Our research will show knowledge gaps, check the facility's security, and provide solutions for unresolved problems based on past investigations. This helps connect the study's aims to past studies and existing trends in IoT security.

2.1. Understanding IoT and Its Security Issues: Expansion and Implications

The speed at which IoT is expanding has made businesses use data immediately, automate certain functions, and select better decisions. Because of IoT, hospitals can now deliver better patient healthcare and work more efficiently [25]. These days, you can merge appliances, operate bright lights, and set temperature controls, leading to more comfort and security [26]. Vehicles, vehicle care predictions, and car safety technology have all improved because of the IoT [22]. Factories now rely on automation using networks of sensors, robots and advanced analyses to ensure more products are made while repair times are kept to a minimum. As companies and people use IoT more, they have started taking benefits by streamlining their tasks, reducing costs, and raising the quality of services in various sectors [27].

2.2. Security Risks and Vulnerabilities in IoT

Since various informally organized devices are part of IoT, security problems are prevalent. Since IoT devices have limited resources, they may be unable to implement high-level security [33]. Because there are insufficient prevention measures, too many devices are affected by cyber-attacks, such as being hacked, losing important data and being hit by viruses [24]. Also, setting several networks among devices allows cyber threats to get to more internet-connected devices, making it more complex to protect them [28]. Since IoT devices are always connected to big networks, hackers may target poor security measures in this field [36]. In such cases, anything that impacts the security of IoT could keep people from using different services, threaten their data, and introduce safety hazards [29].

2.3. Key Security Challenges in IoT

2.3.1. Device and Network Vulnerabilities

Many IoT devices lack proper security because of weak authentication, encryption, insecure ways of communication, and lack of strong access management. Many IoT devices are in danger of attack because they use default passwords [30]. Weak data encryption in IoT networks makes them easy to access, watch over and attack by an outside party [31]. When no security is used with MQTT or HTTP traffic, others may manipulate the information shared among devices [32]. IoT equipment rarely uses advanced user authentication measures, making it open to different attacks [33]. Without intervention, these problems could affect every device in an IoT system, steal vital information and interrupt activities in various industries.

2.3.2. Scalability and Complexity

As more IoT devices go online, it is harder for companies to ensure that networks are secure. Since so many devices are connected to the Internet, keeping data secure, access, and correctness is now more difficult than before [34]. It is hard to perform tasks such as login verification, key management and spot attacks on a large scale because regular security tools are not designed for big and heterogeneous environments [35]. Besides, due to the difference between all types of devices, security needs to be adjusted for each type, which is not simple to achieve [36, 37]. Adding new devices to the Internet of Things increases the chances of security problems and possible attacks. It is

necessary to have security systems that are flexible enough to adapt to changing demands and apply proper security rules according to the situation.

2.3.3. Data Privacy Concerns

IoT devices being used more commonly concern people about privacy since they always collect, study, and send personal and health information. Types of IoT, like smart home assistants, wearables for health monitoring, and sensors in industries, often store vast amounts of user data, which can be accessible to anyone who intends to misuse it [38]. Data users send to many IoT devices stays unprotected because these gadgets do not have strong privacy measures [39].

Additionally, because third-party service providers handle data, questions come up about who owns the data, what permission is given, and how transparent everything is [39]. If laws and security standards are not strictly in place, IoT-created data might result in identity theft, cyberattacks aimed at individuals, or incorrect profile creation, creating huge risks for people and organizations [40]. In order to deal with these problems, IoT systems should use strong encryption, obey strict rules, and educate users to improve their data security [41]. As shown in Figure 3, this is the Taxonomy of IoT Security Threats, and you can refer to Table 1 for a summary of security risks and their effects.

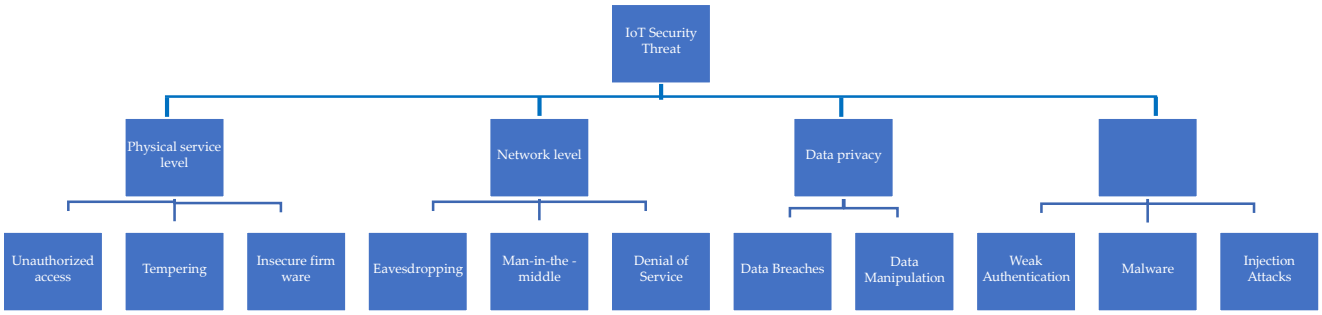

Fig. 3 Taxonomy of IoT security threats

Table 1. Summary of security risks and their impact

Security Threat	Affected IoT Component(s)	Potential Consequences
Unauthorized Access	Devices, User Interfaces	Data breaches and hackers getting into someone else's devices
Man-in-the-Middle Attacks	Communication Channels	Taking or intercepting data, changing it improperly, or losing the security of private information
Malware and Botnets	Embedded Devices, Firmware	When devices are hijacked, DDoS attacks occur, or network congestion occurs.
Weak Authentication	User Management Systems	Identity theft, imitating someone else, and losing control
Data Leakage	Cloud Storage, Data Transmission	Sensitive data privacy breaches facing users
Insecure Firmware Updates	Device software	Problems arise when difficulties are introduced, and the system gets compromised.
Physical Tampering	Sensor, Edge Devices	Carrying out destruction, modifying data, interfering with the system
Scalability Issues	Entire Network Architecture	System performance loss and monitoring devices' behavior are both issues that need to be addressed.

2.4. Current Approaches and Solutions for IoT Security

2.4.1. Authentication and Access Control

Deploying strong authentication and permissions is necessary to ensure that unauthorized people cannot use the systems and devices connected to the network. Various methods are created to handle the identification and authentication problems in IoT networks. To secure their communications, various industries depend on PKI to create digital certificates that confirm the identity of devices and safeguard their information [42]. Having multiple identifiers like a password and a fingerprint improves security improved through MFA [42].

New authentication approaches for IoT devices are also designed to work efficiently and use limited resources. They include Extensible Authentication Protocol (EAP) and using blockchain for identity, which may help make things more secure without affecting speed [43]. However, enforcing security on authentication for many and various IoT networks has not been achieved easily. Authorizations can be adjusted using AI to find unusual actions that enhance security and stop unauthorized access.

2.4.2. Encryption and Secure Communication Protocols

To guarantee that data transfers between IoT devices are safe and uncompromising, the data should be encrypted and reliable communication methods must be used. Because of TLS, many users feel comfortable that their private information cannot be accessed by unwelcome people or eavesdroppers [44]. Data security is increased with VPNs because they send it through private routes and protect it from being uncovered by others [45]. The protection of messages communicated between devices and cloud servers at the network stage is managed by Internet Protocol Security (IPSec) [46].

IEEE 802.15.4 standards recommend ECC and AES since they are handy tools for IoT devices due to their excellent security and low power usage [43]. Even so, using encryption throughout large-scale IoT networks leads to problems in key handling, speed of calculations, and ability to use with different types of devices [44]. In the future, better quantum-resistant algorithms and security systems in blockchain can support more secure communication for the IoT [47].

2.4.3. Intrusion Detection and Prevention Systems (IDPS)

IDPS serves an important role in IoT by noticing and preventing cyberattacks, such as DDoS, man-in-the-middle attacks, and malware infestations. Such systems watch the network and activities on the systems in real time, spot unusual changes, and stop unauthorized access using signatures, spotting anomalies, or both [48]. Using known attack patterns, signature-based IDPS systems differ from anomaly-based ones that look for unusual activity with the help of machine learning. Because linked devices in IoT have limited resources, lightweight IDPS solutions are essential.

Also, if AI and blockchain are used in IDPS, it can address threats automatically and manage security through distributed networks [49]. However, identifying new threats in large-scale networks, avoiding false alarms, and making frequent updates are the main drawbacks of IDPS in IoT [51]. Future studies are expected to boost IDPS effectiveness by adopting federated learning, edge computing, and adaptive cybersecurity mechanisms for IoT [50, 51].

2.4.4. Blockchain and Decentralized Security

Some emerging strategies, including lightweight blockchain frameworks, sharding, and separate processing outside the blockchain, are being looked into to improve how IoT devices use blockchain. Because IoT is growing, integrating blockchain with AI and edge computing is expected to help secure the network and overcome new cyber threats [52, 53]. The following Figure shows a Thematic Map of the current technologies used to secure the IoT. Table 2 gives a summary of the reviewed IoT security solutions.

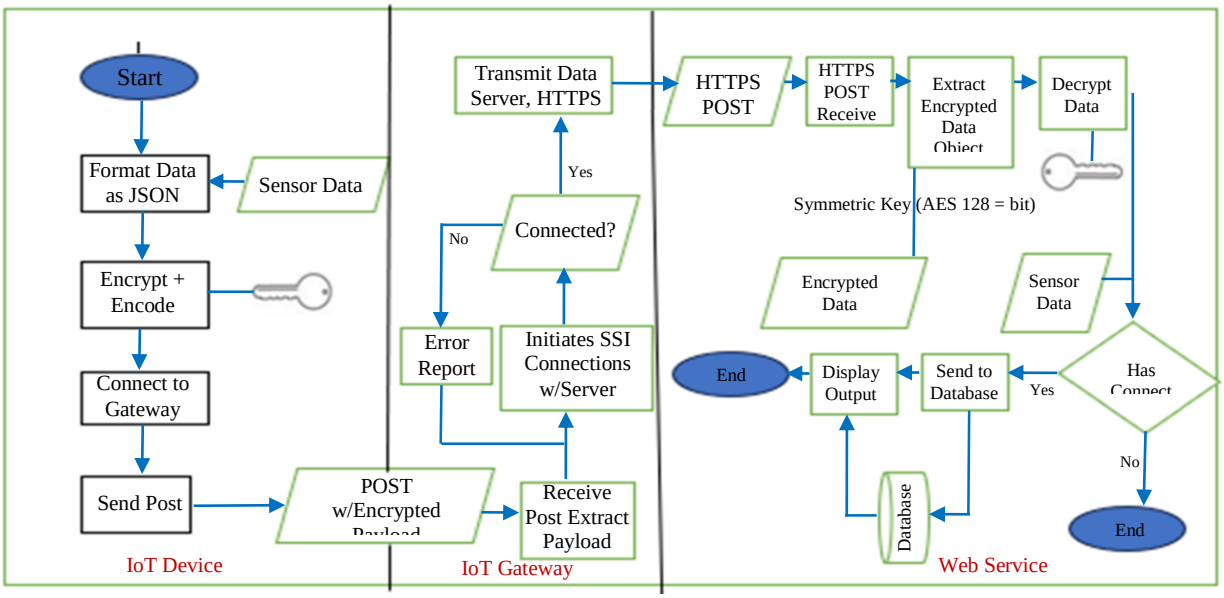

Fig. 4 Thematic map of current IoT security solution

Table 2. Comparative review of IoT security solutions

Security Approach	Pros	Cons	Implementation Complexity	Common Application Areas
Encryption (e.g., AES, TLS)	- Data safety confidentiality and integrity - Widely supported	- Computationally intensive for low - power IoT devices	Medium	Secure communication, data transmission
Authentication & Access Control	- Prevents unauthorized access - Flexible user/device verification	- Can be bypassed if credentials are weak or stolen	Low to Medium	Device login, network access, identity management
Blockchain	- Provides decentralized trust - Tamper-proof data ledger	- High resource usage - Not scalable for high-speed transactions	High	Secure device identities, audit logs, smart contracts

2.5. Emerging Technologies and Future Directions

2.5.1. Artificial Intelligence and Machine Learning in IoT Security

AI and Machine Learning help keep IoT networks secure thanks to their threat-recognising, securing and quick-responding abilities. Since IoT networks are expanding and becoming more complicated, security systems are insufficient, and AI must be used to prevent upcoming issues. ML algorithms look through vast amounts of data coming from IoT daily to discover strange patterns, note any security issues, and set apart incidents of intrusions [54]. Because of real-time processing, algorithms can review large IoT information and find anything suspicious, raise alarms for security concerns, and keep track of unwanted access [54].

Because of the capabilities of AI, Intrusion Detection Systems and Intrusion Prevention Systems can monitor the network at all times and respond to new cyber threats [55]. In addition, thanks to CNNs and RNNs, detecting threats in IoT becomes more accurate since they can spot complicated attacks [56]. Still, any practical use of AI will depend on solving issues related to model explanation, confidentiality, and severe attacks on the system [54]. As federated learning and edge AI develops, threats will be found faster, data will be better protected, and the response time for IoT devices will decrease [54].

2.5.2. Edge Computing and Fog Computing in IoT Security

These processes have made IoT systems safer because most data is processed on-site, and cloud usage has decreased. When sending information to a central server, you face security risks, and the system services can be delayed, or the network resources may be occupied. Since data processing happens close to the devices, less chance exists for private information to be stolen by hackers [55]. In the same way, fog computing makes things better by processing some of the data at intermediate locations, forming several layers of security [57]. Since a single entity does not control them, they have less chance of vulnerabilities, and it is easy to discover and tackle security issues [52]. They also secure the exchange of user information to the cloud so that data breaches do not happen before files are stored [55]. However, edge computing needs to be adapted more to conquer issues related to sparse resources and needing security in all places.

2.5.3. Security Standards and Regulatory Frameworks

With more devices connected to the Internet due to IoT, authorities have ensured that rules and guidelines keep information safe and cyber threats are reduced. The Internet Engineering Task Force (IETF) and the National Institute of Standards and Technology (NIST) recently released advice for improving the security of IoT devices. The IETF allows data protection for IoT devices using protocols such as Datagram Transport Layer Security and Constrained Application Protocol [58]. At the same time, NIST has developed a cybersecurity framework for IoT with directions on identifying risks, choosing encryption, and ensuring identification [59].

Besides IETF and GFCE, ENISA and ISO have produced security guidelines for joint systems to safeguard their data and comply with the General Data Protection Regulation (GDPR) [60]. At the same time, it is hard to apply these standards around the globe since every IoT system is unique and technology changes fast. It is necessary to make standard rules in different countries and to persuade companies to use security in the design of IoT devices [60-62].

2.6. Gaps in Current Research and Knowledge

2.6.1. Limitations of Existing Security Solutions

Even though progress is being made, security in IoT is still not robust in research and practice. Since every manufacturer and sector follows different security approaches, it is hard for them to cooperate. Because IoT devices use different security codes, it is usually difficult to secure them and connect them [45]. It is hard to make security systems expand to meet the needs of growing numbers of connected devices [62].As IoT networks have many devices, using passwords as the primary authentication is not safe anymore, so biometric authentication and decentralized identity controls are better choices. *It is also hard to add advanced encryption to systems restricted by limited sensors and hardware [63]. Most IDPS systems use signature matching, so they cannot recognize new threats, such as those created by AI or against zero-day issues. As IoT continues to grow, we should create security arrangements that are easy to change, adapt and stick to its standards for complete protection [63-65].

2.6.2. Need for Comprehensive IoT Security Frameworks

Because IoT devices are used in many areas of work, we must ensure that comprehensive systems deal with all the problems with IoT. At present, security methods mostly deal with individual factors, but no single plan includes device makers, service providers and users all at once [54].

Architectures for the Internet of Things should always consist of standard security, tough encryption and constant updates for security prevention [55]. Also, it is necessary to ensure that IoT devices follow the necessary rules and meet major global security standards for safety.

Since IoT is used in healthcare and city services, developing security models equipped with AI and blockchain could make IoT systems safer. As long as complete security systems are lacking in IoT, it remains possible for big cyberattacks, data leakages, and operational disturbances to occur [54]. The following table lists the gaps that were identified from the literature.

Table 3. Research gaps identified in literature

Identified Limitation	Implication	Need for New frameworks
Fragmented security approaches that address specific issues (e.g., only encryption or access control	Leaves IoT systems vulnerable to multi-layered and coordinated attacks	A mixture of technology and policies is important to keep all the layers of IoT systems secure
Lack of scalability in existing security solutions	Security mechanisms may fail as the number of connected IoT devices grows	Frameworks have to ensure scalability and smart distribution of resources over time.
Limited support for low-power, resource-constrained devices	Traditional security tools are often too heavy for IoT devices	Security protocols that use less energy and are light should be included in different frameworks.
Minimal integration of AI/ ML for proactive security	Most systems are reactive, detecting threats after they occur	Building a predictive threat analysis using artificial intelligence and machine learning should be part of the framework.
In consisted or missing regulatory compliance mechanisms	Varying global standards lead to security loopholes and legal uncertainty	It should follow the changes in international standards and give access to compliance solutions.

3. Materials and Methods

3.1. Research Design

3.1.1. Overview of the Research Approach

This paper uses theory to examine cybersecurity issues in the Internet of Things. Studying the existing literature, security standards, and advisory guides with a theoretical approach to finding weak points and suitable answers is important. The analysis in this paper uses earlier findings to check alternative models, encryption procedures, ways to authenticate users, and international laws dealing with IoT security threats [55].

This study of cybersecurity in the Internet of Things is done by applying theories. When using a theoretical approach, we look closely at works, security guidelines, and industry standards to learn what puts IoT security at risk and worth fixing.

Research in this paper discusses studies from the past, investigates new ways to guard the IoT, analyzes encryption techniques, identifies secure authentication solutions, and looks into the laws managing IoT security [55]. Due to this strategy, we can determine which security issues are most important in IoT so we can develop better solutions instead of collecting data or experimenting. As threats in IoT security change rapidly, theories are beneficial for keeping up with them [54]. Figure 5 shows the main model used in the work.

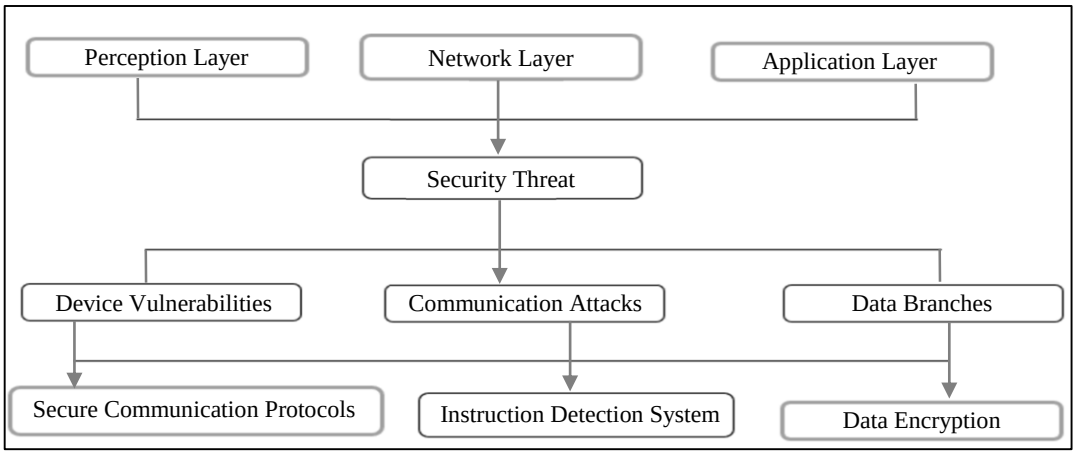

Fig. 5 Theoretical framework

3.1.2. Justification of Approach

Since no data was collected in our work, we used the theoretical research method to carefully analyze cybersecurity in the Internet of Things (IoT) [55]. Since new IoT risks and ways to handle them are appearing, it is important to study and analyze existing security systems, encryption techniques, types of authentications, and their legal factors. In particular, it makes it possible to find flaws in current security approaches and develop effective IoT defence techniques. In addition, if data from various sources is combined, it provides a clear picture of cybersecurity challenges and leads to advice for clearing many areas in the IoT. When testing experiments is impossible because of money, other problems, or real-life complications, theories are fundamental [54].

3.2. IoT Devices and Systems

3.2.1. Selection of IoT Devices

The study focused on IoT devices as they play a significant role in cybersecurity and are used everywhere [56]. Most of the study concentrates on smart home devices, medical Internet of Things, and industrial sensors because these areas of IoT are hazardous if problems are discovered. Since many people use linked thermostats, security cameras, and voice assistants, exposing them to risks, they are listed in the study. Since they have unique features, remote patient monitoring systems and health trackers will likely be their victims when cyberattacks happen [57]. Also, protecting IO sensors on industrial networks is important since it stops potential problems caused by security breaches [56, 57].

3.2.2. Device Specifications and Features

As not all IoT devices are alike, they can be more or less protected from cybersecurity threats [56]. You can find both Real-Time Operating Systems (RTOS) on sensors used in industry and embedded Linux and Android on smart home and medical equipment [58]. Since each connectivity protocol has unique problems, they are all evaluated for security. It is possible to listen in on Wi-Fi and Bluetooth devices, while private LoRaWAN and Zigbee devices are not that secure. Hardware capacities are extended further by using microcontrollers for simple IoT products and more powerful System-on-Chip for advanced projects [59]. The process of updating firmware, using biometrics for identification, and built-in encryption is checked for its ability to stop cyber threats [59].

3.3. Security Assessment Techniques

3.3.1. Vulnerability Scanning and Penetration Testing

To spot any possible weaknesses in hardware and software, security in IoT devices requires vulnerability scanning and penetration testing [53]. Vulnerability scanning uses tools like Nmap, OpenVAS, and Nessus to discover errors and old firmware and recognize security issues in devices and network protocol settings [65]. In

penetration testing (ethical hacking), testing is done using methods similar to real cyberattacks to find and test risks, such as those coming from weak login systems, unsecured communication between devices, and APIs that are not secured [65]. During fuzz testing, the IoT device's firmware is tested by giving it invalid or malicious data to look for hidden security problems. Professionals use the same techniques to determine if the present security measures are enough and find where defence measures can be improved [64].

3.3.2. Network Traffic Analysis

Checking network traffic allows one to detect issues with communication, lost data, and dangers present in IoT devices [56]. Data transferring between different Internet of Things devices and cloud platforms is watched over and examined to catch any unusual activity or sensitive words [58]. To analyze network traffic, researchers can use Wireshark, Zeek (before known as Bro), and tcpdump, and this allows them to spot poor encryption, transfer of unauthorized data, and data that lacks encryption [57]. IoT experts pay close attention to MQTT, CoAP, and HTTP since these protocols have weak encryption and unsuitable authentication. Also, deep packet inspection collects data to study traffic patterns in case they detect illegal actions regarding data [59]. Checking traffic logs can help experts understand IoT devices' risks and develop stronger security ways to deal with them.

3.3.3. Security Protocol Evaluation

Security in IoT devices should be examined so that our data remains confidential, intact and safe. This review mainly seeks to understand IoT systems' encryption, authentication and access control. TLS, AES, and ECC are tested for blocking unauthorised access and adjusting data in transit. For all these authentication systems, including PKI, MFA and identity verification based on blockchain, methods used for illegal access are carefully reviewed. To answer this question, both RBAC and ABAC are analyzed to find out how they could stop unapproved communications from devices [66]. Specialists perform penetration testing and review the protocols to confirm that the system is protected from errors such as missing mutual authentication, applying easy-to-crack cryptography, or keeping passwords unchanged [66, 67]. The different approaches to assessment are discussed in Table 4.

Table 4. Summary of assessment techniques

Assessment Technique	Description	Purpose of IoT Security	Theoretical Application
Vulnerability Scanning	Automated systems go through systems to identify known security flaws	Identities recognize outdated programs, errors in the system setup, and available services.	Used for picturing the level of danger at each layer of the IoT system
Penetration Testing	Using a simulated attack to spot methods of attack	Evaluate outside dangers and confirm the security strategies.	Proposed as a technique to see whether particular security mechanisms are effective
Network Traffic Analysis	Watching network traffic to find possible harmful activity	The software identifies anything that appears suspicious and warns about it.	Offers a basis for formulating theories for IDS tools
Security Protocol Evaluation	Review of the existing encryption/ authentication methods	It helps create communication and data privacy that cannot be easily breached	Application of comparing how well TLS, DTLS, and other existing protocols are working
Threat modelling	Looking into the details of each system component, possible threats, and related controls	It helps spot possible threats and decide on how to respond to them first	It gives insights to assist in designing a well-structured framework

3.4. Security Solution Implementation

3.4.1. Security Measures Tested

Various security options were offered and looked at, especially in encryption, authentication, and Intrusion Detection Systems (IDS), to solve the issues found in IoT systems. The data was isolated from copying or viewing, bypassing the rules by securing communication with TLS and storing it with AES [68]. All these methods were added to ensure that the identification and security of devices improved. IDS and IPS were also built to use machine learning and detect anomalies so they could instantly prevent cyberattacks. RBAC and ABAC were implemented to stop undesired interactions from getting into IoT networks. For this reason, data breaches, unauthorized gain of access and cyberattacks became less likely, stressing the significance of compatible IoT security approaches [68].

3.4.2. Testing Security Frameworks and Protocols

Various testing methods were performed on the devices to determine how IoT security strategies reduced the risks [69]. Data communication was private with TLS and DTLS, so users could not be spied on [64]. The introduction of PKI and ECC made authentication of devices in the network easier. Employing RBAC and ABAC, deciding which people and devices are permitted on the IoT network [66] is possible. Using machine learning algorithms, ID and IPS security tools were placed on networks to spot abnormal activities [70].

Evaluation checked the security features for the delay, speed, and resistance to cyber-attacks, and it turned out that some do better than others depending on the support provided by the device and the network they are on [70, 71]. The research shows that for IoT security to work effectively, multiple layers of protection should be applied [70, 71]. Steps taken so far to review security measures and protocols are shown in Table 5.

Table 5. Security measures and protocols reviewed

Security Measure / Protocol	Description	Theoretical Evaluation	Relevance to IoT Security
Transport Layer Security (TLS)	Used for picturing the level of danger at each layer of the IoT system	Assessed by how it works on IoT devices that have limited resources and for how it handles two-way authentication.	Since it is so secure, it is a favourite choice for maintaining data security in various IoT applications.
Datagram TLS (DTLS)	Proposed as a technique to see whether particular security mechanisms are effective	Researchers looked into the issue of timing in IoT contexts.	Helpful when there is a need for quick and instant communication
OAuth 2.0	Offers a basis for formulating theories for IDS tools	Discussed for the proper way to manage and regulate access controls among devices and users	It helps manage how users can use different devices connected to an IoT system.
IPSec	Application of comparing how well TLS, DTLS, and other existing protocols are working	Take care of communication security at the network layer	Beneficial for IoT systems that start with an IoT gateway
Lightweight Cryptography (e.g. ECC) Blockchain-based Security	It gives insights to assist in designing a well-structured framework	Studied for the comparison between energy requirements and safety aspects.	Required for the security of sensors and embedded devices that use low power. This method can be used for secure recording of events and proper authentication in IoT networks.

3.5. Data Collection and Analysis

3.5.1. Data Collection Methods

A planned review and interpretation of already available sources were used as the data collection method since this study followed a theoretical research strategy. The process gathered and compiled significant Internet of Things (IoT) security material from other literature, standards, and published cases. A lot of valuable data was evaluated in the analysis.

- Papers and conference proceedings on IoT security frameworks, types of threats, and possible ways to fix them.
- Supply information documents and articles about network security protocols and how to defend them.
- There are records of device logs, network traffic overview statistics, and previously found attack results from earlier IoT security experiments and simulations [67].

This collection has details of examinations on logs that show how the devices communicate, what protocols are found, and what results penetration tests produced [68]. They explained how some forms of danger surface in real life and whether established security measures were sufficient. Furthermore, we relied on SLRs to ensure we analysed both old but effective theories and the latest advances in IoT cyber security. For every aspect to be covered, data was gathered bit by bit, and each focus dealt with a different element, for example, network activity, intrusion detection, or access control [69]. We kept reviewing and updating our data collection to include the latest articles and innovations. For this reason, the authors were able to incorporate the freshest IoT security advances in their framework.

3.5.2. Data Analysis Techniques

Data for this research was synthesized, and ethnographic information was used to compare and understand information from various educational materials and descriptions. We concentrated on determining which IoT security issues, trends, and holes appear in various implementations. Most of the research utilized thematic analysis by plotting the data into groups: encryption, authentication, access control, and intrusion detection. Because of this strategy, it was possible to see which design flaws appeared in multiple tumor models and find tested and confirmed solutions from previous experiments [72]. Besides, each security framework was measured according to the efficiency of its protocols, how advanced its cryptography was, and whether it was scalable for future needs.

They matched what was found in research, experiments, and simulations to work out which tools and steps were most helpful in enhancing security [59]. With time, the collected information was examined to follow the changes in risks and their solutions. The study recommends new strategies since it is believed that dangers will increase. To ensure the results, aspects from academic research, industry publications, and simulations of cyber-attacks were used. As a result of using these techniques, trust in the process grew, which made it possible to develop a reliable security plan for IoT [72].

3.6. Ethical Considerations

3.6.1. Ethical Approval

Every piece of research was conducted correctly by paying attention to ethics and data protection [66]. Since security is an important concern for IoT, steps were taken to guarantee sensitive data and user privacy [67]. The review board checked and approved the study to ensure it was conducted ethically, especially regarding how data was kept and examined [68]. All the IoT equipment was tried out in suitable ways, the stakeholders agreed to be a part of the research, and personal records were changed so personal details could not be revealed [66]. During the project, the author used NIST and GDPR standards to guarantee ethical actions from everyone involved.

4. Results and Discussion

The team presents the outcomes, carefully examines the research findings, and explores the study's consequences. The aim is to go through the data without bias and see what the results show about IoT's security.

4.1. Summary of Results

4.1.1. An Overview of Key Findings

It is seen in these results that devices connected to the Internet have significant vulnerabilities in authentication, encryption, and securing network communication. The research of the collected data revealed that many IoT devices are protected by encryption standards that a star attack can disrupt. Access issues and breaches of data are some problems encountered. Also, according to the analysis, some data was not secured by encryption, so attackers might easily steal it. It was found from Figure 6 that MFA and end-to-end encryption play significant roles in increasing mobile device security when they were studied within the context of security frameworks.

However, security measures that need advanced resources tend to slow down how IoT devices function. The evidence suggests that IT systems should be standard, adaptable, and able to grow with new problems found online. The Model of the Proposed Comprehensive IoT Security Framework appears in Figure 6, and the Theoretical Findings are shown in Table 6.

Table 6. Summary of theoretical findings

IoT Security Threat	Evaluated Method(s)	Strengths Identified	Gaps/Limitations
Unauthorized Access	Access Control takes place with the use of OAuth 2.0.	Offers the ability to assign limited access to different individuals; makes user and device management possible.	The features may not work correctly because of their complex token leakage risks.
Data Interception (Eavesdropping)	TLS, DTLS, Lightweight Encryption är alternatives lügend	Offers strong encryption for transferring data and can work on smart devices	Some constrained devices may experience more delay or use extra power because of encryption.
Firmware/Software Exploits	Vulnerability Scanning and the Idea of Patch Management	Found known holes in the software before they could be exploited	The system only works with regular updates since it does not detect zero-day flaws.
Device Spoofing/ impersonation	Mutual Authentication and ID based on blockchain	Blockchain assures that everything stays unchanged, and only those with the proper permissions can access the technology.	Concerns about increasing the size of IoT systems and using less energy
Denial-of-Service (DOS) Attacks	Reviewing the elements in your network and putting limits on bandwidth usage	Is capable of finding and stopping suspicious network activities	There is a possibility they might experience DDoS attacks in real-time.
Data Privacy Violation	Another thing to focus on is data encryption, anonymizing data, and designing access policies.	Improves how well a service follows regulations and earns users' confidence	It is not always easy to ensure that our online experience is easy to use and secure simultaneously.

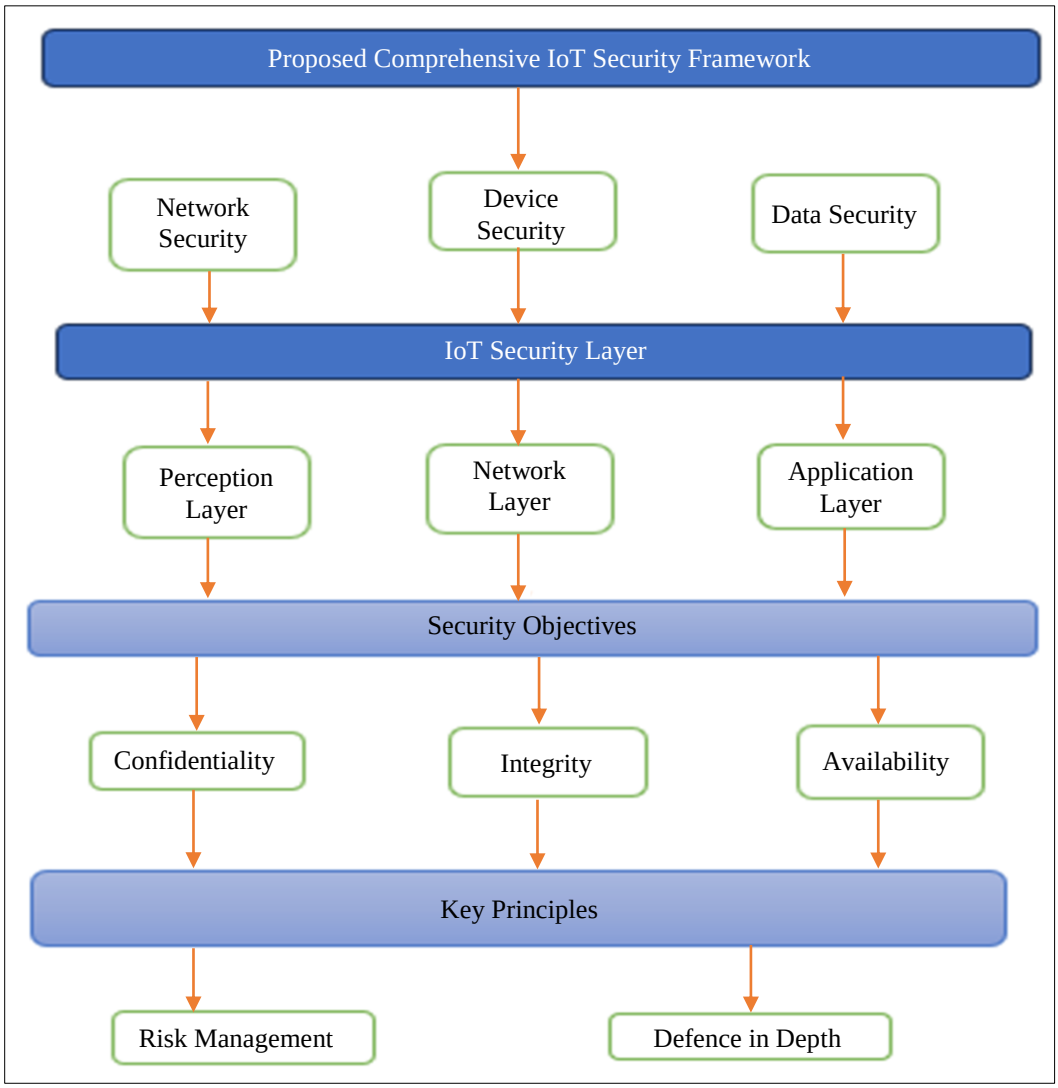

Fig. 6 Model of proposed comprehensive IoT security framework

4.2. Interpretation of Results

4.2.1. Analysis of Findings

Most of the problems in IoT security are caused by poor authentication, weak encryption, and open connections to the network [69]. The primary aim of developing IoT devices is economy and performance, while security is given less importance, which helps attacks still work [70]. These problems can vary, and others might access your data without encryption while having weak passwords makes it simple for someone to enter your devices [66]. They may lead to organizations being breached, losing funds, and not obeying rules while placing individuals' security and privacy at significant risk [69]. As reported by the studies, following general security rules set by manufacturers and well-implemented actions from businesses are necessary to monitor IoT risks [66, 70].

4.3. Comparison with Previous Research

This study shows that its results are connected to earlier studies about the ongoing problems of unreliable authentication systems, weak encryption, and unprotected networks for communication [69]. For example, Smith and Kumar [69] have stated that there are also issues with interoperability and scalability when securing IoT devices, which is what this study also found.

Also, according to Zhao et al. [70], most IoT systems lack proper security standards, showing that careful rules and guidelines must be implemented. Still, our studies highlight that these vulnerabilities can matter significantly in the Internet of Things networks for healthcare since insecure data could lower confidence in the services and create serious issues with patient information [66]. This indicates that we need security approaches that rely on AI for spotting danger and blockchain for user authentication to strengthen resistance to modern cyber threats [66, 70]. Table 7 shows how these ideas differ from previous concepts.

Table 7. Comparison with prior frameworks

Aspect	Existing Frameworks (Literature)	Proposed Framework (This Study)	Improvement / Contribution
Architecture focus	When authentication is managed either by devices or cloud services (for example, by using a central server).	Holistic includes the device, edge, network, and cloud layers.	Protects the entire system involved in IoT, including all parts of its security.
Security Mechanisms Emphasized	Simple ways of encryption and managing who can access information	In addition, blockchain, lightweight cryptography, and AI-based systems are designed to find malicious behavior.	Adaptable, advanced and handled by several parties
Flexibility/Scalability	Commonly, there is insufficient future-proofing for extensive and varied IoT use cases.	Developed to work well and integrate in any expanding or connected setting	Improving IoT systems' ability to grow and change according to their needs
Threat Coverage	When creating the strategy, deal mainly with dangers such as DoS and data leakage.	Protection against a wide range of issues (for example, spoofing, zero-day, concerns about privacy, firmware).	Able to handle more kinds of cyber attacks
Theoretical Grounding	The research is mainly done by examining cases and relying less on modeling theory.	Model relations among things by using conceptual modeling.	Improved platform for improving understanding with research.
Standard and compliance	Maybe it does not meet the emerging standards for security.	Follows and uses the standards provided by government agencies such as NIST, ISO and GDPR.	Can function properly in environments driven by policies.
Adaptability to Emerging Tech	Those topics receive only minor attention.	Provides security using AI, edge, and fog aspects.	Makes certain that policing technology can be used together effectively.

4.4. Implications for IoT Security, Risk and Challenges

It highlights how its results match previous research that pointed out issues with insufficient authentication, weak encryption, and exposed communication networks [69]. The study arrived at the same findings as those by Smith and Kumar [69], who pointed out that many security issues in IoT devices are linked to interoperability and scalability. Plus, Zhao et al. [70] noticed that IoT systems lack proper security standards in most cases, so clearly,

more specific guidelines are required. Nevertheless, our research clarifies that these issues can influence patients' safety and the reliability of IoT healthcare systems when a cyber-incident happens [66]. As a result, companies should start using AI and blockchain technologies together to defend themselves against modern cyber-attacks [66, 70]. You can see from Table 7 that this framework's application differs from that of different prior frameworks.

5. Recommendations

Following, we have a list of recommendations that may help with the problems that have been outlined. They should cover security issues and suggest ways to decrease threats.

5.1. Recommendations for Device Manufacturers

5.1.1. Improved Security Standards

It is important to apply more advanced authorization tests, improved encryption and regular updates to software to secure IoT devices [69]. Adding Multi-Factor Authentication (MFA) to the system ensures no unauthorized individual can enter the network, and all transfer of data inside the network ought to be protected with TLS and AES technology. Because of this, companies should pay attention to updating their firmware and software whenever there is a new problem or hazard [66]. You can ensure reliable security for IoT devices by combining hardware with zero-trust when they are being made [67]. According to NIST and IETF, using the guidelines from the International Security Organization ensures that different security systems can work together and that cybersecurity is improved. If manufacturers depend on strong encryption, they can minimize risks and improve confidence among people involved in the IoT [68].

5.2. Recommendations for IoT Network Administrators

5.2.1. Network Security Best Practices

Managers should protect IoT networks by applying many security measures [69]. Protecting valuable systems from IoT devices makes them more secure against getting infected by those devices [66]. Various verification methods, such as multi-factor and certificates [66], make your network more secure. WPA3 encryption should be used for Wi-Fi, and VPN access is recommended for downloading via the Internet [69]. Firmware must be fixed and upgraded as often as possible to solve new problems [70]. IDPS should be established to check for any unusual activity the network carries. In addition, creating firewall rules, closing additional services and searching for vulnerabilities can prevent possible threats [70]. Using NIST and ISO/IEC 27001 standards can strengthen networks to deal with new risks.

5.3. Recommendations for Users

5.3.1. User Awareness and Training

It is important to show people how to protect their internet-connected devices and confidential info. Organizations and producers of things like drones should guide customers on how to secure passwords and why it helps to set up multi-factor authentication [69]. Allowing users to attend training classes, workshops, and online tools can make them aware of phishing and other dangers [68]. Users of IoT devices become more alert to security matters because of the alarms and step-by-step instructions included in the devices' interfaces [68]. It is possible for cybersecurity teams and the government to advice people on staying safe when using IoT [64, 68]. When people are more aware of security, the number of data breaches, illegal access and cyberattacks will likely decrease [66, 68].

5.4. Policy and Regulatory Recommendations

5.4.1. Government and Regulatory Bodies

The security level of IoT can be improved when the government and regulatory organizations call for secure designs in every IoT device [66]. Often, using encryption, asking for secure login and offering regular updates for their software can enhance security in both industries and businesses [67]. NIST, ENISA, and IETF should work on

creating a set of guidelines that could be applied worldwide to ensure interoperability and privacy and to respond to security attacks [66]. Governments should enforce laws in business through certification, auditing, and the assignment of fines to offenders [66]. If businesses get some tax or other aid to secure their IoT systems, they may adopt better security steps [67]. Creating IoT security laws globally would keep everyone's digital spaces safe [66]. An explanation of recommendations towards stakeholders based on the findings is seen in both Figure 7 and Table 8.

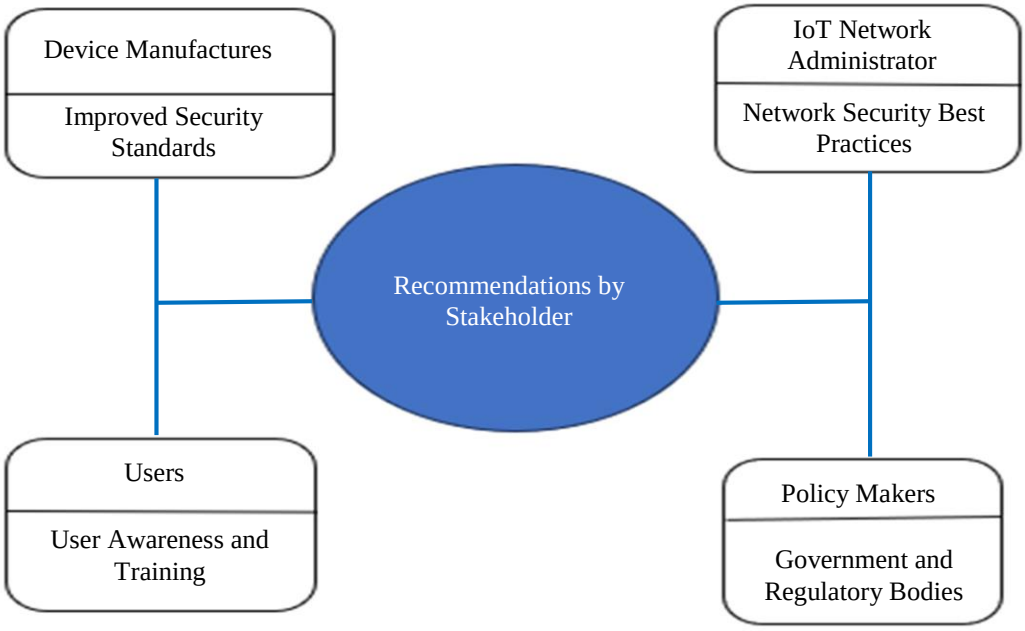

Fig. 7 Stakeholder based recommendation map

Table 8. Summary of recommendation by target audience

Target Audience	Recommendation	Rationale
Device Manufactures	- Use the factory security functions, which may be called secure boot and firmware validation. - Get security compliant by acquiring standard certifications	- Do not let tampering happen and lower chances of hardware-related threats
Network Administrators	- Use instant intrusion prevention systems. - he process of detecting and breaking up networks	- Improves how potential threats are seen. - Controls the movement laterally - Networks - Updates systems to defend against known exploits
IoT Users	- Help users learn how to use the system safely. - Having employees work on trusted devices and secure system is important	- Helps prevent problems related to human mistakes, phishing scams and weak password habits. - Stays away from risky or poorly configured software by outside providers
Policymakers / Regulators	- Make sure your IoT security is clearly defined. - Regulations and meeting the right requirements	- Creates standards used in the entire profession - When a minimum-security prison is required

6. Conclusion

6.1. Summary of Findings

6.1.1. Recap of Key Insights

Focusing on IoT security, this study addresses important weaknesses. Among these are issues linked to easy authentication, not encrypting data, and missing firmware updates [66]. According to the survey, because of a lack of firm security standards and less than-ideal resources, many IoT devices have weak security and are at risk of cyber-attacks [59]. Looking closer at the network activity showed that some crooks might be able to get to sensitive data [44]. Chiefly, it is clear that better security policies, regular use of best practices, and stricter action by regulators can help improve the security of IoT networks. New cyber threats can be prevented by beefing up device security, installing network protection, and teaching people what to do [71, 72].

6.1.2. Impact of Research

This study significantly changes the IoT industry and the people who use it, and it seeks to push forward research. The study advises the industry to use advanced measures like encryption and multi-layer security and always work with the latest software to avoid cyberattacks. According to the study, users can increase security in their network by modifying their default passwords and updating the firmware. Also, findings from this research can help write and establish clear security rules and laws [59]. Studies can widen the areas above by dealing with threat detection based on AI, blockchain-based security, and security systems designed for specific IoT applications [66, 71].

6.1.3. Suggestions for Future Work

Other studies can be carried out in different fields to go further than the ones reported here. A chance is to design AI systems that can quickly identify and block any cyber threats from the IoT network [44]. Experts might use blockchain technology to ensure decentralized verification and reliable security while data is exchanged between devices in IoT setups [73]. It is also vital to review and evaluate encryption algorithms for IoT devices that do not use much power so security remains high even if the system is fast [66]. Also, studies in the future might work towards having a single set of rules for countries so IoT security measures remain the same everywhere [59, 66]. Gaining long-term insights into how security solutions work with IoT devices in real life could be helpful for companies and those setting regulations [73]. Table 9 summarizes the main points of this paper and explains what is expected shortly.

Table 9. Summary of key contribution and future directions

Category Key Contributions	Description
Theoretical framework	Combine all necessary information about IoT, its weaknesses, and how to protect them into a workable model.
Comparative Analysis	Describe today's protocols' bright and dark sides, such as TLS or Blockchain.
Security Assessment	Researchers designed ways to access data about the risks in IoT systems.
Policy Relevance Future Directions	Gave clear guidelines to policymakers, system users, and developer
Empirical validation	Try out the suggested framework in real-life IoT conditions.
AI-Driven Solutions	Check out machine learning-related intrusion detection systems.
Standardization Efforts	Back efforts to create standard rules and safety measures for IoT around the globe.

References

[1] What is the Internet of Things (IoT)? , IBM, 2025. [Online]. Available: https://www.ibm.com/think/topics/internet-of-things.

[2] Dimitris Gkoulis, "Creating Interpretable Synthetic Time Series for Enhancing the Design and Implementation of Internet of Things (IoT) Solutions," *Internet of Things*, vol. 30, pp. 1-32, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[3] What is IoT? - Internet of Things Explained - AWS, 2025. [Online]. Available: https://aws.amazon.com/what-is/iot/

[4] The Applications of IoT in Business, Tulane University, 2025. [Online]. Available: https://online.sse.tulane.edu/articles/internet-of-things/

[5] Mrutyunjay Padhiary, Pankaj Roy, and Dipak Roy, "The Future of Urban Connectivity: AI and IoT in Smart Cities," pp. 33-66, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[6] "Internet of Things (IoT) - Key Business Insights Gartner, 2025. [Online]. Available: https://www.gartner.com/en/information-technology/insights/internet-of-things.

[7] Hossein Omrany et al., "IoT-Enabled Smart Cities: A Hybrid Systematic Analysis of Key Research Areas, Challenges, and Recommendations for Future Direction," *Discover Cities*, vol. 1, no. 1, pp. 1-34, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[8] Ebenezer Esenogho, Karim Djouani, and Anish M. Kurien, "Integrating Artificial Intelligence Internet of Things and 5G for Next-Generation Smartgrid: A Survey of Trends Challenges and Prospect," *IEEE Access*, vol. 10, pp. 4794-4831, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Qurra tul Aain, Irshad Ahmed Sumra, and Mariam Khan, "Security Challenges and Attacks in IoT: A Survey," *Journal of Computing and Biomedical Informatics*, vol. 8 no. 1, pp. 1-10, 2024. [Google Scholar] [Publisher Link]

[10] Youakim Badr, Xiaoyang Zhu, and Mansour Naser Alraja, "Security and privacy in the Internet of Things: Threats and Challenges," *Service Oriented Computing and Applications*, vol. 15, no. 4, pp. 257-271, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[11] Sri Ramya Siraparapu, and S.M.A.K. Azad, "Securing the IoT Landscape: A Comprehensive Review of Secure Systems in the Digital Era," *e-Prime - Advances in Electrical Engineering, Electronics and Energy*, vol. 10, pp. 1-18, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[12] Petar Radanliev et al., "AI Security and Cyber Risk in IoT Systems," *Frontiers in Big Data*, vol. 7, pp. 1-26, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[13] Yimin Guo et al., "Deeper Insight Into Why Authentication Schemes in IoT Environments Fail to Achieve the Desired Security," *IEEE Transactions on Information Forensics and Security*, vol. 19, pp. 4615-4627, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[14] Koohang et al., "Internet of Things (IoT): Users' Concerns about Privacy and Security," *Issues in Information Systems*, vol. 24, no. 2, pp. 191-202, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[15] Wen Fei, Hiroyuki Ohno, and Srinivas Sampalli, "A Systematic Review of IoT Security: Research Potential, Challenges, and Future Directions," *ACM Computing Surveys*, vol. 56, no. 5, pp. 1-40, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[16] Amir Djenna, Saad Harous, and Djamel Eddine Saidouni, "Internet of Things Meet the Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure," *Applied Sciences*, vol. 11, no. 10, pp. 1-30, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[17] Katerina Megas et al., "NIST Cybersecurity for IoT Program," *Computer*, vol. 57, no. 12, pp. 144-148, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[18] Calvin Lee, and Gouher Ahmed, "Improving IoT Privacy, Data Protection and Security Concerns," *International Journal of Technology Innovation and Management (IJTIM)*, vol. 1, no. 1, pp. 18-33, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[19] Ashwin Karale, "The Challenges of IoT Addressing Security, Ethics, Privacy, and Laws," *Internet of Things*, vol. 15, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[20] Katerina Svandova, and Zdenek Smutny, "Internet of Medical Things Security Frameworks for Risk Assessment and Management: A Scoping Review," *Journal of Multidisciplinary Healthcare*, vol. 17, pp. 2281-2301, 2024. [Google Scholar] [Publisher Link]

[21] P. Muralidhara Rao, and B.D. Deebak, "Security and Privacy Issues in Smart Cities/Industries: Technologies, Applications, and Challenges," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 8, pp. 10517-10553, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[22] Arif Ali Mughal, "Cybersecurity Hygiene in the Era of Internet of Things (IoT): Best Practices and Challenges", *Applied Research in Artificial Intelligence and Cloud Computing*, vol. 2, no. 1, pp. 1-31, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[23] Tianqi Bu et al., "Task Scheduling in the Internet of Things: Challenges, Solutions, and Future Trends," *Cluster Computing*, vol. 27, no. 1, pp. 1017-1046, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[24] Konstantinos Tsiknas et al., "Cyber Threats to Industrial IoT: A Survey on Attacks and Countermeasures," *IoT*, vol. 2, no. 1, pp. 163-186, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[25] S. Harihara Gopalan et al., "Enhancing IoT Security: A Blockchain-Based Mitigation Framework for Deauthentication Attacks," *International Journal of Networked and Distributed Computing*, vol. 12, no. 2, pp. 237-249, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[26] M. Sidharth Sharma, AI-Driven Anomaly Detection for Advanced Threat Detection, 2023. [Online]. Available: https://philpapers.org/rec/SIDAAD

[27] Isil Cetintav, and Mehmet Tahir Sandikkaya, "A Review of Lightweight IoT Authentication Protocols from the Perspective of Security Requirements, Computation, Communication, and Hardware Costs," *IEEE Access*, vol. 13, pp. 37703-37723, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[28] Mamoona Humayun et al., "Corrections to "Securing the Internet of Things in Artificial Intelligence Era: A Comprehensive Survey"," *IEEE Access*, vol. 12, pp. 162421, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[29] Brandon Langenberg, Hai Pham, and Rainer Steinwandt "Reducing the Cost of Implementing the Advanced Encryption Standard as a Quantum Circuit," *IEEE Transactions on Quantum Engineering*, vol. 1, pp. 1-12, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[30] Michal Kaššaj, and Tomáš Peráček, "Synergies and Potential of Industry 4.0 and Automated Vehicles in Smart City Infrastructure," *Applied Sciences*, vol. 14, no. 9, pp. 1-30, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[31] Keshav Kaushik, Susheela Dahiya, and Rewa Sharma, "*Internet of Things Advancements in Healthcare," Internet of Things: Energy, Industry, and Healthcare,* 1st ed., CRC Press, pp. 19-32, 2021. [Google Scholar] [Publisher Link]

[32] Hao Kong et al., "A Survey of mmWave Radar-Based Sensing in Autonomous Vehicles, Smart Homes and Industry," *IEEE Communications Surveys and Tutorials*, vol. 27, no. 1, pp. 463-508, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[33] Mohsen Soori, Behrooz Arezoo, and Roza Dastres, "Internet of Things for Smart Factories in Industry 4.0, A Review," *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 192-204, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[34] Shams Forruque Ahmed et al., "Erratum: Toward a Secure 5G-Enabled Internet of Things: A Survey on Requirements, Privacy, Security, Challenges, and Opportunities," *IEEE Access*, vol. 12, pp. 13125-13145, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[35] Astha Srivastava et al., "Future IoT-Enabled Threats and Vulnerabilities: State of the Art, Challenges, and Future Prospects," *International Journal of Communication Systems*, vol. 33, no. 12, pp. 1-41, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[36] Qasem Abu Al-Haija, and Ayat Droos, "A Comprehensive Survey on Deep Learning-Based Intrusion Detection Systems in Internet of Things (IoT)," *Expert Systems*, vol. 42, no. 2, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[37] Abdinasir Hirsi et al., "Comprehensive Analysis of DDoS Anomaly Detection in Software-Defined Networks," *IEEE Access*, vol. 13, pp. 23013 - 23071, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[38] Jing Qiu et al., "A Survey on Access Control in the Age of the Internet of Things," *IEEE Internet of Things Journal*, vol. 7, no. 6, pp. 4682-4696, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[39] Chen Wang, Travis Atkison, and Hana Park, "Dynamic Adaptive Vehicle Re-Routing Strategy for Traffic Congestion Mitigation of Grid Network," *International Journal of Transportation Science and Technology*, vol. 14, pp. 120-136, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[40] Ons Aouedi et al., "A Survey on Intelligent Internet of Things: Applications, Security, Privacy, and Future Directions," *IEEE Communications Surveys and Tutorials*, vol. 27, no. 2, pp. 1238 - 1292, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[41] Ala Hamarsheh, "An Adaptive Security Framework for Internet of Things Networks Leveraging SDN and Machine Learning," *Applied Sciences*, vol. 14, no. 11, pp. 1-28, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[42] Elias Dritsas, and Maria Trigka, "Academic Editors: Muhammad A Survey on the Applications of Cloud Computing in the Industrial Internet of Things," *Big Data and Cognitive Computing, Basel*, vol. 9, no. 2, pp. 1-32, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[43] Tianyu Zhang et al., "A Survey on Industrial Internet of Things (IIoT) Testbeds for Connectivity Research," arXiv Preprint, 2024. [Google Scholar] [Publisher Link]

[44] Anca Jurcut et al., "Security Considerations for Internet of Things: A Survey," *SN Computer Science*, vol. 1, no. 4, pp. 1-19, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[45] Arwa Alrawais et al., "Fog Computing for the Internet of Things: Security and Privacy Issues," *IEEE Internet Computing*, vol. 21, no. 2, pp. 34-42, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[46] Sanjeet Singh et al., "Empowering Connectivity: Exploring the Internet of Things," pp. 89-116, 2025. [CrossRef] [Google Scholar] [Publisher Link]

[47] Muhammad Sohaib J. Solaija, Hanadi Salman, and Hüseyin Arslan, "Towards a Unified Framework for Physical Layer Security in 5G and Beyond Networks," *IEEE Journals and Magazine*, vol. 3, pp. 321-343, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[48] Meenu Vijarania, Swati Gupta, and Akshat Agarwal, "*A Review on Security Frameworks and Protocols in the Internet of Things*," Internet of Things and Cyber Physical Systems, 1st ed., CRC Press, pp. 71-82, 2022. [Google Scholar] [Publisher Link]

[49] Anna Kalyashina et al., "Enhancing IoT Systems through Cloud-Fog-Edge Architectures Challenges and Opportunities," *E3S Web of Conferences*, vol. 583, pp. 1-11, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[50] Brittany D. Davis, Janelle C. Mason, and Mohd Anwar, "Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study," *IEEE Internet of Things Journal*, vol. 7, no. 10, pp. 10102-10110, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[51] Badis Hammi et al., "Survey on Smart Homes: Vulnerabilities, Risks, and Countermeasures," *Computers and Security*, vol. 117, pp.1-13, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[52] S.C. Vetrivel, R. Maheswari, and T.P. Saravanan, "Industrial IOT: Security Threats and Counter Measures," *Communication Technologies and Security Challenges in IoT*, Springer, Singapore, pp. 403-425, 2024. [CrossRef] [Google Scholar] [Publisher Link]

[53] Jason R.C. Nurse, Sadie Creese, and David De Roure, "Security Risk Assessment in the Internet of Things Systems," *IT Professional*, vol. 19, no. 5, pp. 20-26, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[54] Rahul Johari et al., "Penetration Testing in IoT Network," *2020 5th International Conference on Computing, Communication and Security (ICCCS)*, Patna, India, pp. 1-17, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[55] Pooja Anand et al., "Iot Vulnerability Assessment for Sustainable Computing: Threats, Current Solutions, and Open Challenges," *IEEE Access*, vol. 8, pp. 168825-168853, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[56] Seyyed Keyvan Mousavi et al., "Security of Internet of Things Based on Cryptographic Algorithms: A Survey," *Wireless Networks*, vol. 27, no. 2, pp. 1515-1555, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[57] Inayat Ali, Sonia Sabir, and Zahid Ullah, "Internet of Things Security, Device Authentication and Access Control: A Review," 2019. [Google Scholar] [Publisher Link]

[58] Tuhin Borgohain et al., "Authentication Systems in the Internet of Things," 2015. [Google Scholar] [Publisher Link]

[59] Nickson M. Karie et al., "A Review of Security Standards and Frameworks for IoT-Based Smart Environments," *IEEE Access*, vol. 9, pp. 121975-121995, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[60] Tarak Nandy et al., "Review on Security of Internet of Things Authentication Mechanism," *IEEE Access*, vol. 7, pp. 151054-151089, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[61] K.V.V.N.L. Sai Kiran et al., "Building an Intrusion Detection System for IoT Environment using Machine Learning Techniques," *Procedia Computer Science*, vol. 171, pp. 2372-2379, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[62] Ansam Khraisat, and Ammar Alazab, "A Critical Review of Intrusion Detection Systems in the Internet of Things: Techniques, Deployment Strategy, Validation Strategy, Attacks, Public Datasets and Challenges," *Cybersecurity*, vol. 4, no. 1, pp. 1-27, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[63] Yusuf Perwej et al., "A Systematic Literature Review on the Cyber Security," *International Journal of Scientific Research and Management*, vol. 9, no. 12, pp. 669-710, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[64] David Barrera et al., "Security Best Practices: A Critical Analysis Using IoT as a Case Study," *ACM Transactions on Privacy and Security*, vol. 26, no. 2, pp. 1-30, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[65] Sumit Singh Dhanda, Brahmjit Singh, and Poonam Jindal, "Lightweight Cryptography: A Solution to Secure IoT," *Wireless Personal Communications*, vol. 112, no. 3, pp. 1947-1980, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[66] Hanan 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. [CrossRef] [Google Scholar] [Publisher Link]

[67] M. Al-Kuwaiti, N. Kyriakopoulos, and S. Hussein, "A Comparative Analysis of Network Dependability, Fault-Tolerance, Reliability, Security, and Survivability," *IEEE Communications Surveys and Tutorials*, vol. 11, no. 2, pp. 106-124, 2009. [CrossRef] [Google Scholar] [Publisher Link]

[68] Gregory B. White, and Natalie Sjelin, "The NIST Cybersecurity Framework vol. 61, no. 1-2, pp. 39-5, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[69] Constant Kohler, "The Eu Cybersecurity Act and European Standards: an Introduction to the Role of European Standardization," *International Cybersecurity Law Review*, vol. 1, no. 1-2, pp. 7-12, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[70] Kevin Macnish, and Jeroen van der Ham "Ethics in Cybersecurity Research and Practice," *Technology in Society*, vol. 63, pp. 1-10, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[71] Abhishek Khanna, and Sanmeet Kaur, "Internet of Things (IoT), Applications and Challenges: A Comprehensive Review," *Wireless Personal Communications*, vol. 114, no. 2, pp. 1687-1762, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[72] Dener Ottolini, Ivan Zyrianoff, and Carlos Kamienski, "Interoperability and Scalability Trade-offs in Open IoT Platforms," *2022 IEEE 19th Annual Consumer Communications and Networking Conference (CCNC)*, Las Vegas, NV, USA, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[73] S. Hemavathy, Kokila Jagadeesh, and V.S. Kanchana Bhaaskaran, "Unified Security Framework using Device-Specific Fingerprint: Mitigating Hardware Trojans and Authenticating Firmware Updates," *IEEE Access*, vol. 13, pp. 26897-26914, 2025. [CrossRef] [Google Scholar] [Publisher Link]