A Review: Internet of Things (IoT) Security Challenges

Abdulrahman Aminu Ghali[1], Mohd Hafizul Afifi Abdullah[2], Abdul Ghafar Jaafar[3], Noureen Talpur [4], Zainab Hassan[5], Ashikin Ali[6]

[1,2,5,6] *Faculty of Information and Communication Technology (FICT), Universiti Tunku Abdul Rahman, 31900 Kampar, Malaysia.*

[3]*Faculty of Artificial Intelligence, Universiti Teknologi Malaysia, Kuala Lumpur, Malaysia.*

[4]*Centre for Research in Data Science, Universiti Teknologi PETRONAS, 32610 Seri Iskandar, Malaysia.*

[1]*aminu@utar.edu.my,* [2]*hafizulafifi@utar.edu.my,* [3]*abdulghafar@utm.my,* [4]*noureen.talpur@utp.edu.my,* zainabscuzzy16@1utar.my[5]*, ashikin@utar.edu.my*[6]

Article history

Received:
3 Mac 2026

Received in revised form:
12 Mac 2026

Accepted:
4 April 2026

Published online:
15 June 2026

*Corresponding author
aminu@utar.edu.my

Abstract

The Internet of Things (IoT) has achieved widespread adoption among millions of individuals today, driven by the growing use of smart devices, including smartphones, smart cars, lighting, air conditioning, and high-speed networks. IoT is applied in various areas, including industries, healthcare, homes, agriculture, oil and gas, and education, to name a few. However, due to the many connections of IoT devices, there is no exact method or algorithm for overseeing communications and security concerns, such as Mirai-based botnet Attacks, AI-powered IoT Attacks (Emerging Threats), Satellite & Space IoT attacks, heterogeneity challenges, and Distributed Denial of Service (DDoS) attacks, which have led to enormous challenges in the IoT environment. The paper divides the challenges into three categories: recent IoT attacks, general security challenges, and existing attacks in IoT. Besides, this paper aims to review and investigate the security challenges in the IoT environment and propose various solutions to mitigate these challenges. Based on the analysis of recent IoT attacks, satellite and space attacks account for a 70% share, while in the broader security challenge, heterogeneity accounts for 80%. In existing IoT attacks, the DDoS attack poses a 90% risk.

Keywords: *IoT, AI security, threats, security challenges, IoT environment, architecture layers*

* *Corresponding author. aminu@utar.edu.my*

1. Introduction

The Internet of Things (IoT) has garnered significant attention from individuals worldwide. For this reason, it is anticipated that the IoT device market size in Europe will reach approximately $500 billion by 2030 [1]. Currently, there are over 18 billion IoT-connected devices worldwide, with an estimated total of 39.6 billion device connections expected by 2033 [2]. The basic idea of IoT is centered on linking uniquely identifiable smart devices to communicate with each other through the Internet for the purpose of cooperating to perform complex tasks. As such, these devices require the ability to collect, process, and transmit data through various channels [3].

The advent of IoT has provided numerous solutions for various industries, including healthcare, homes, agriculture, oil and gas, and education, with new and innovative solutions to handle complex task operations. [4-6]. On the other hand, implementing algorithms in the IoT environment is challenging due to the difficulties associated with multiple devices and distributed computing [7], which include a lack of clarity on how the algorithms work [8]. With the IoT, not only do devices or "things" send and receive data from one another when connected to the Internet, but they can now also remotely control the operations of other devices. [9, 10]. Therefore, due to the feasibility of advanced technology like artificial intelligence (AI), security concerns have become more prevalent than ever, and no exact algorithms to oversee communications, security challenges such as Mirai-based botnet Attacks, AI-powered IoT Attacks (Emerging Threats), Satellite and space IoT Attacks, and Distributed Denial of service (DDoS) attacks. Becomes critical in the IoT environment [11][38].

Therefore, ensuring the security of IoT is of paramount importance in the IoT environment. As such, this paper reviews the most significant attacks and provides a reliable solution for resolving the challenges. This paper is organized as follows: Section 2 describes the IoT application areas, and Section 3 explores the related works. Section 4 discusses the IoT architecture layers. Section 5 describes the general security challenges in the IoT environment, while Section 6 outlines the existing attacks in this context. Section 7 explains the methodology that has been used to achieve the results. Lastly, Section 8 shows the results of the study. Section 9 concludes the paper.

2. Application Area of IoT

2.1 Healthcare

The implementation of IoT has significantly improved the healthcare system within a very short timeframe. For instance, IoT in healthcare is evident in the use of IoT sensors worn by patients to collect and record data in real-time, as well as in monitoring systems for analysis and diagnosis. These devices enable patients and older individuals to monitor their health status regularly through a dedicated mobile application. [12]. Similarly, it enables doctors to confer on complex cases worldwide by remotely monitoring chronic diseases. Applications of IoT in the healthcare sector are receiving remarkable acceptance, such as e-health, connected health, or mobile health [12], enabling the remote monitoring of a patient's health. Adopting mobile health enhances patient clinical outcomes, while simultaneously decreasing costs and improving the productivity of healthcare personnel. [12]. Due

to its significance, over 50% of US patients are not monitored by telemetry, and the invention of IoT applications has helped doctors respond faster in emergency cases.

However, patient data are generally considered highly sensitive due to their high-dimensional and complex features, which can be used to profile an individual [13]. Therefore, such data must be securely protected against unauthorized access. Despite the numerous benefits of IoT applications in the healthcare system, it still faces some setbacks due to security challenges, as noted by Zingbox [14]. For instance, if an IoT device used for administering and reminding users to take a specific medication [12] is attacked, it can prevent the device from prompting a reminder alert, causing a catastrophic and negative impact on the person's health. Hence, security in this aspect is of paramount importance. To address the issue, a security model focusing on confidentiality and authentication is needed.

2.2 Education

IoT technology has significantly transformed the education sector in various institutions worldwide, enabling easy access to learning and education [15]. For instance, smartboards and digital highlighters enable the transfer of printed texts via phone, and the smartboard can receive and display the information to students. Additionally, textbooks feature a quick response (QR) code and augmented reality (AR) capabilities that can be easily scanned to provide instant access to learning materials. IoT also enhances security in the education sector [16] by utilizing components such as Radio Frequency Identification (RFID) to capture data from smart devices ("things"), allowing parents to monitor their children while they are away or at school. Nevertheless, IoT devices are vulnerable to DoS attacks, necessitating robust authentication mechanisms to mitigate these issues.

2.3 Homes

Many individuals have accepted and adopted the use of IoT in their workplaces and homes due to its varied functionalities, making homes more unique than ever. Smart homes comprise many types of devices that are networked together to provide services for human usage. Connected devices in a smart home include televisions, speakers, CCTVs, fridges, bulbs, locks, water controls, smart doors, gas controls, and air conditioners [9]. These devices enable real-time monitoring, safety, and security measures to prevent intruders [9]. To achieve an IoT-enabled smart home, six distinct layers are applied, including the middle layer, application layer, coding layer, perception layer, network layer, and business layer. [17].

Despite the benefits of IoT-enabled smart homes, security experts [18, 19] have cautioned that a large number of these devices will lead to security threats, which include passive and active attacks [19]. In passive attacks, the intruder can always obtain information without the permission of authorized users, such as eavesdropping. This type of attack is challenging to detect since the data is not altered or modified. The solution to this type of attack is prevention rather than detection. On the other hand, an active attack occurs when the attacker alters or modifies information using unauthorized means. A typical example of this attack includes DoS and replay attacks. A DoS attack prevents a legitimate user from accessing their smart devices, making communication between the devices unsuccessful, which further alters the information. [20]. A replay attack could also occur when the attacker decides to tamper with the communication channel by

repeatedly sending valid data, thus hogging the network for data modification. [17]. A confidentiality, integrity, and availability model will solve the problems mentioned. Table 1 further summarizes the security challenges in these sectors.

Table 1. Summary of the Security Challenges in the IoT Application and their Solutions

Application area	Security challenges	Proposed solutions
Healthcare	Insulin Pump Hacks	HIPAA-compliant encryption Algorithm embedded with AES
Education	Hacked Smart Boards, attacks, and DDoS	Natural Language Processing (NLP) Algorithms embedded with RSA
Smart Homes	Amazon Ring Camera Hacks	Local processing Edge Algorithm
Agriculture	Agri-Drones attacks	Jamming Detection Algorithm
Oil and Gas	Stuxnet-Like Malware	Based anomaly detection Algorithms

Table 1 summarizes the security challenges in IoT application areas, along with their proposed solutions. Despite research focused on providing solutions to mitigate IoT security challenges, these issues remain unsolved due to an inadequate understanding of the algorithms that prevent security attacks. This implies that an IoT security algorithm requires a clear understanding before it can be enhanced and implemented.

3. Related Works

In recent years, numerous research studies have been published in the field of IoT, advancing scientific knowledge [21]. However, many of these studies focus on general issues, while the challenges of security and privacy of IoT users are discussed only in a generic manner. The following related works discuss key observations, ideas, and challenges from the existing literature, along with studies that propose solutions and models to address IoT security issues.

In [22]the authors revealed that IoT comprises three levels: communication, identification, and interaction. Authors in [22] and [23] also focused on three key issues, such as confidentiality, privacy, and trust, while inadequate attention was given to critical challenges, including DoS attacks. Confidentiality is a fundamental issue in the IoT environment, where security is not guaranteed for legitimate users to access their data. Thus, in the IoT environment, not only do users access their data, but unauthorized objects may also gain access through cyberattacks. Therefore, preventing such incidents is critical. Privacy is another fundamental issue in the IoT environment, where the healthcare system is one of the most significant applications. Hence, the absence of a mechanism that prevents access to patients' sensitive information is undoubtedly a significant challenge in the IoT environment [24]. In contrast, the trust challenge identified is related to peer-to-peer interactions among various devices. As such, accessing data is only possible after a

successful trust negotiation is completed. Thus, establishing secure trust between devices and objects is a challenging task.

Meanwhile, the study [23] highlighted the importance of security requirements in the IoT environment, categorizing them into various categories. These categories include confidentiality, authentication, and access control. The main limitation of this study is the taxonomy of the IoT challenges, which is still not clear, and the absence of detailed explanations on the outlined security requirements.

On the other hand, the study by [8] focuses on IoT security challenges at the IoT layers. Among the security issues mentioned are access control, privacy, authorization, and storage. On the other hand, a significant drawback of this study is the lack of a detailed explanation of the mechanisms used to address the challenges mentioned. The works of [25] revealed that some of the IoT security challenges hinder the development of the IoT.

In the work of [26]the authors proposed a central cloud vision for IoT and described the enabling technologies and application domains for the future. The research problems identified were based on those reported in [27]. However, the authors did not elaborate on security issues and challenges in the IoT environment, and their discussions were limited to privacy and identity protection.

The authors in [28] described the perception of the IoT framework and provided details of the methods and techniques. Based on the classification, the research proposed several possible research directions related to IoT security issues. In this study, the authors recommend solving security and privacy issues by utilizing public key cryptography to provide adequate security for IoT users.

4. Architecture Layer and Challenges

The architecture layers play a significant role in the IoT environment, where every layer has a specific function. However, there are various opinions regarding the number of architecture layers in the IoT environment. The prominent architecture layers include the perception, network, and application layers. Table 2 summarizes the functions of each architecture layer.

Table 2. Summary of the Security Attacks in IoT Architecture Layers

IoT Architecture layers	Recent security challenges	Year
Perception layer	Side channel and Mirai botnet attack	2016
Network layer	Eclipse Attacks	2023
Application layer	Ring Camera Hacks	2024

The explanation of each architecture layer and its functions is given as follows:

4.1 Perception Layer

The perception layer is considered one of the core layers in the IoT architecture. This layer aims to collect information using sensors and actuators and then pass this information to the network layer for further processing. Furthermore, the perception layer consists of sensors, sensor gateways, RFID tags, and other components. The recent security challenges in this layer include Stuxnet and the Mirai Botnet, which make the IoT architecture layer very challenging.

4.2 Network Layer

The network layer comprises the internet gateway, cloud computing, and other components, which are operated using technologies such as routers, access points, servers, Bluetooth, 3G, LTE, and WiFi, among others. The primary goal of the network layer is to route and transmit data to various IoT devices over the Internet [51, 54]. The recent security challenges in this layer are KRACK and Eclipse attacks. While the work of [55] further identified other threats, such as bluejacking, bluesnarfing, blue bugging, file alteration, corruption, and file deletion. Alternatively, the confidentiality and privacy of IoT users are vulnerable to attacks due to the remote access and data exchange at this layer.

4.3 Application Layer

The application layer is concerned with the actual operations to be achieved by a communication instance. The recent security issues in this layer include Ring Camera Hacks and the Strava Heatmap Leak. The function of this layer is to process the connections of IoT devices using various communications ports. The IoT application layer protocols include HTTP, CoAP, WebSocket, MQTT, XMPP, DDS, and AMQP, to name a few [51]. The security challenges in this layer are also concerned with the homogeneity of the IoT devices. Figure 1 indicates the IoT architecture.

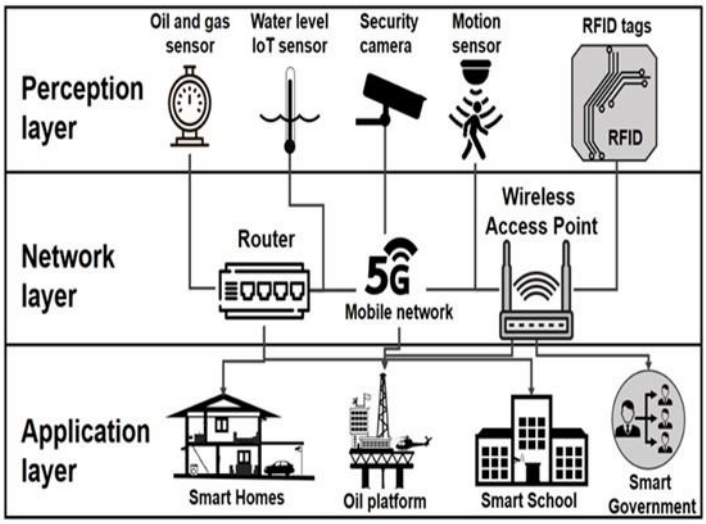

Figure 1. IoT Architecture Layer

5. General Security Challenges in IoT

The primary goal of IoT security is to secure all connected devices. However, IoT components and devices often face limitations related to computational resources and power consumption. As a result, security challenges are closely tied to the principles and functionalities needed to protect the entire IoT environment. These challenges also stem from the need to ensure security across diverse aspects such as device heterogeneity, mobility, and end-user devices.

5.1 Heterogeneity

Heterogeneity poses a significant challenge in the IoT environment, as devices often have varying capabilities and are interconnected with multiple other devices. Thus, each communication protocol must support a wide range of devices, regardless of their algorithms. Additionally, the dynamic nature of IoT devices further complicates this issue. Therefore, securing end-to-end communication remains a critical challenge, and an algorithm has been proposed to address this challenge [34].

5.2 Mobility

Another distressing factor affecting IoT is the mobility challenge, as many IoT devices are attached to moving objects, such as smart cars. Therefore, ensuring a robust algorithm and implementing an authentication algorithm to secure the communication is of paramount importance [35].

5.3 End Point Devices

An IoT environment enables devices to communicate with one another. These physical devices are connected to the Internet, enabling them to transmit real-time data. Endpoint devices encompass a wide range of items, including actuators, sensors, mobile phones, computers, cameras, chips, controllers, drivers, and more. Typically, end devices are battery-powered to allow mobility and long-distance communication [36]. However, limited battery life remains an important setback from the perspective of IoT device mobility. For instance, as everyone who carries a mobile phone has no doubt already learned the hard way, even the most sophisticated end devices in industries also suffer from the limitation of power due to DoS attacks. Therefore, limited power issues hinder the reliability and availability of these devices in the IoT ecosystem, where various IoT end devices spend most of their time reaching locations with limited power sources. As such, an algorithm is required to address the issues.

6. Existing Attack in the IoT Environment

The following section will provide an overview of the various common attacks in the IoT environment.

6.1 Replay Attacks

In this attacker captures communication packets in between communication and then send those packets with malicious content. The hacker sends a message to the recipient after looking into the system. When the transmitter stops sending data, it begins sending signals as the original sender. The intruder's primary goal in this attack is to increase network trust. A message that is primarily used in the access procedure is sent to the recipient by the attacker [39] . A replay attack is defined as a security breach wherein some data is kept without authorization and then sent again to the recipient with the intention of trapping them in an unauthorized situation, such as a duplicate transaction or false recognition or verification A few lines of python code is sufficient to perform replay attack on IoT devices that operates by Bluetooth pairing, he highlighted some recommendation for this type of attack , For example, every packet sent between the master and peripheral devices should have a password for each transaction.

6.2 Device Cloning

Device cloning attacks involve the perpetrator deceiving the victim by posing as a trusted device. If the patient unwittingly connects, the attackers can steal the patient's data and inflict significant damage on their devices. This article examines MAC spoofing and forces repair, two forms of device cloning attacks in which the attacker obtains the MAC and GATT characteristics. Inadequate built-in security, including compromised authentication, out-of-date firmware, and deployment settings like an unattended industrial wireless network, can lead to cloning attacks on IoT devices. Attackers used cloning attacks to launch different attacks like DoS attacks, data injection attacks, black hole attacks which put vital infrastructures powered by IoT at risk. Cloning IoT devices is a serious security risk and very harmful, especially in critical infrastructures enabled by IoT. To protect IoT-enabled critical infrastructures from cloning threats, it is crucial to detect IoT device cloning early. The main technological problem with IoT device detection is that cloned devices frequently behave just like the real ones and have legitimate security credentials. Furthermore, standard cryptographic-based solutions are inappropriate for IoT devices due to their restricted resources and capacities for security operations.

6.3 Routing Attack

Data routing is very crucial for health care-based systems because it enables remote information distribution and promotes network adaptability in large institutions. However, there are several problems with routing, mostly due to wireless systems open nature. The information being routed between the sensors in a wireless sensor network is the target of this attack. This is because the most important prerequisite for wireless health care systems is the secure transmission of patient data to the receiving end, which may be a hospital or a doctor.

6.4 Simulation of IoT Routing Attacks

Different routing attack scenarios are sinkhole attack, wormhole attack, version attack and flooding attack and selective forward attack are described below.

6.4.1 Sinkhole Attack

Sinkhole attacks occur when a malicious node strategically positions itself to appear more appealing to neighboring nodes as a routing choice, thereby diverting network traffic through itself instead of legitimate nodes. Sinkhole attacks are very difficult to detect because it exploits the trust between network nodes and proactive security measures are required to mitigate them.

6.4.2 Wormhole Attack

A wormhole attack involves two external malicious nodes establishing a direct connection between themselves. These nodes collaborate to forward packets faster than the legitimate network paths, making themselves appear more attractive to neighboring nodes (victims). The primary goal of this attack is to manipulate and gain control over the routing traffic flow within the network.

6.4.3 Version Attack

A version attack takes place when a malicious node broadcasts a higher version number for a DODAG (Destination-Oriented Directed Acyclic Graph) tree in a network. Upon receiving these altered DIO (DODAG Information Object) messages with the updated version number, other nodes in the network begin restructuring the DODAG tree based on the new version. This unnecessary restructuring leads to inefficiencies in the network topology, disrupting its normal operation.

6.4.4 Selective forward Attack

A selective forwarding attack occurs when malicious nodes intentionally forward only RPL control packets to manipulate routing paths while dropping the remaining data traffic packets. These nodes maintain their appeal to neighboring nodes by consistently forwarding control packets, ensuring their presence in the routing topology. By doing so, they disrupt data transmission without raising immediate suspicion, effectively compromising the reliability and efficiency of the network.

6.5 Sensor Attack

Sensors in the wireless network regularly departed or joined the network due to unintentional sensor failures and harmful actions by outside intruders. A wireless network sensor may die from a lack of power. In this scenario, a clever attacker can quickly enter the network, swap out the sensor for the genuine one, and carry out malicious actions. As a result, if patient data is not properly stored among several sensors, an attacker may alter it to their own will. Additionally, because there is no authentication structure, fraudulent data may be added or presented as legitimate. The attacker interferes with the raw data collected by the sensors, such as heart rate, body temperature, or step count. For example, they may inject false signals or modify sensor readings, leading to inaccurate data being reported to healthcare providers or fitness tracking applications.

6.6 Data Tempering

Data can be changed or stole by unauthorized access to IoT devices. Patient's data is managed by third party such as cloud storage devices which stores personal data extracted from sensors. Breaches in these systems results in stealing of data. Attackers could insert malicious files which could alter the sensitive data and grant them unauthorized access to private data. The acknowledgement of falsified information by wearable devices may transfer misleading information to customers. The entire IoT infrastructure may become dysfunctional by an enemy manipulating the data value. Altering the database may cause smart devices to make biased decisions, which could interfere with users' ability to live smart lives. Login credentials are used by most databases to authenticate users.

6.7 Personal Data

The use of wearables to continuously monitor health metrics has the potential to create health data profiles. This data could be used by advertisers and third parties for the implementation of targeted marketing strategies raises significant concerns regarding user privacy. Wearable technological devices equipped with GPS or location tracking capabilities may inadvertently reveal the real-time geographical positions of users. Unauthorized entry to this data could lead to the potential hazards to personal privacy, encompassing behaviors such as stalking or harassment, are of significant concern.

Healthcare IoT devices gather sensitive patient data, and vulnerabilities in these devices can lead to data breaches that expose health records, personal information, and medical histories. Inaccurate data from healthcare IoT devices can significantly impact patient care, potentially resulting in misdiagnosis or inappropriate treatment. The summary of the attacks in IoT wearable health devices is shown in Figure 3.

6.8 DDoS Attack

DoS attacks remain a significant issue in the IoT environment to this day, as they are challenging to neutralize for IoT end users. Thus, such an attack requires a quick solution. There are various types of DDoS attacks in the IoT environment, including denial-of-service (DoS) attacks, path-based DDoS attacks, jamming, wormholes, vampire attacks, carousel attacks, and stretch attacks [37, 38]. In essence, the primary objective of DDoS attacks in the IoT environment is to render devices or networks inaccessible to users or prevent communication between devices [15]. This attack undermines the trustworthiness of IoT data.

6.9 Brute-Force Password Attacks

The recent escalation of attacks on IoT devices using brute force password attacks is becoming increasingly concerning in the IoT environment. Rather than using intelligent or complex algorithms, brute-force attacks exploit weak and commonly used passwords, which are prevalent in many IoT devices. The attack relies on trial-and-error methods using automated programs to repeatedly guess passwords until the correct one is found [40]. As a result, attackers can gain unauthorized access to these devices through persistent and exhaustive attempts [41].

7. Research Methodology

This study adopts a structured literature review methodology to systematically identify, analyze, and synthesize existing research on security challenges in the Internet of Things (IoT) environment. The review process was designed to ensure transparency, reproducibility, and comprehensive coverage of relevant studies.

7.1 Literature Search Strategy

A comprehensive literature search was conducted using major academic databases to collect relevant peer-reviewed publications related to IoT security challenges and attacks. The primary databases used for the literature search include:

- IEEE Xplore
- Scopus
- ScienceDirect
- ACM Digital Library
- SpringerLink

These databases were selected because they contain high-quality peer-reviewed journals and conference proceedings widely used in cybersecurity and IoT research.

To retrieve relevant studies, several search keywords and combinations of keywords were used, including:

- “Internet of Things security”
- “IoT cyber attacks”
- “IoT botnet attacks”
- “Distributed Denial of Service in IoT”
- “IoT intrusion detection systems”
- “AI-based IoT security”
- “IoT network vulnerabilities”

Boolean operators such as AND and OR were applied to refine the search results and identify the most relevant studies.

To ensure the inclusion of recent developments in IoT security, the literature search focused on studies published between 2018 and 2025. However, a limited number of earlier seminal studies were also included to provide foundational context for well-known IoT attacks such as botnet-based and DDoS attacks.

7.2 Inclusion and Exclusion Criteria

To maintain the quality and relevance of the reviewed literature, specific inclusion and exclusion criteria were applied during the selection process. The inclusion and exclusion criteria mentioned below in Table 3 is used to carefully examine the selection of included papers.

Table 3. Inclusion and Exclusion Criteria

Inclusion Criteria	Exclusion Criteria
Peer-reviewed journal articles and conference papers	Blog posts, commercial websites, and non-academic reports
Studies focusing on IoT security threats, vulnerabilities, and defense mechanisms	Non-peer-reviewed manuscripts and unpublished preprints
Research addressing IoT attack detection, mitigation, or security frameworks	Studies not directly related to IoT security
Articles written in English	Duplicate publications retrieved from multiple databases

7.3 Study Selection Process

The study selection process was conducted in multiple stages. Initially, a broad search across the selected databases yielded approximately 100 research papers. After removing duplicate entries and screening titles and abstracts for relevance, 50 papers remained. A full-text review was then conducted to evaluate the suitability of each study based on the defined inclusion and exclusion criteria.

Finally, 41 high-quality studies were selected for detailed analysis in this review. These studies form the basis for identifying IoT security challenges, attack categories, and emerging defense mechanisms.

7.4 Analysis Framework

The selected studies were systematically analyzed and categorized based on the following aspects:

- Types of IoT cyber attacks (e.g., botnet attacks, DDoS attacks, malware-based attacks)
- Security challenges associated with IoT environments (e.g., device heterogeneity, scalability, resource constraints)
- Detection and mitigation techniques proposed in existing research
- Emerging security paradigms such as AI-based threat detection, edge intelligence security, and zero-trust architectures.

This analytical framework enabled the identification of major research trends, limitations in existing approaches, and potential future research directions in IoT

security. The study adopts a quantitative approach to develop a multistage classification model. The methodology consists of following steps:

7.5 Systematic Search

The research begins with a structure search to identify recent developments in IoT security. Academic databases such as IEEE Xplore, Scopus, ScienceDirect, and SpringerLink were explored using keywords including: IoT security attacks, DDoS in IoT and IoT security challenges. Figure 2 outlines the proposed research methodology.

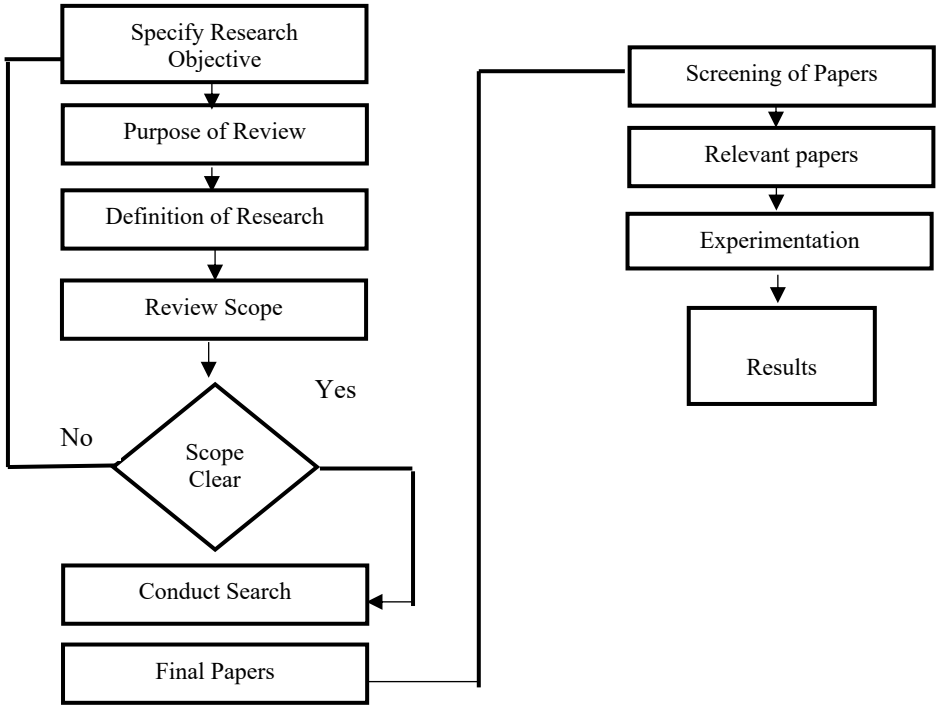

Figure 2. Proposed Research Methodology

Figure 14 clarifies the steps taken from the initial research question to the results, illustrating the logical flow and relationship between different components. It typically includes elements such as specify research objectives, purpose of review, definition of research, review scope, screening of papers, experimentation of machine learning algorithms, results and systematic map. The process begins with a systematic literature review, followed by study selection and data extraction. Identified IoT attacks and security challenges were categorized and analyzed through, and severity levels were determined. The classified risks were then mapped to the solutions that have been used to counter these attacks.

7.6 Screening and Selection of Relevant Studies

After collecting relevant publications, a screening process was conducted to ensure research quality and relevance.

7.7 Dataset

The IoT-23 dataset is a publicly available collection of labeled network traffic captures designed for research on malware detection and analysis in Internet of Things (IoT) environments. IoT-23 contains 20 labeled captures of malicious IoT network traffic and 3 of benign activity. Each capture represents a different scenario involving various IoT devices such as security cameras and smart home gadgets.

The dataset includes both packet capture (PCAP) files and metadata in CSV format, describing communication flows and labeling them as benign or malicious.

7.8 Risk-Based Categorization Model

The Risk-Based Categorization Mode classifies IoT attacks and security challenges according to their calculated risk severity levels. This model ensures that threats are not treated uniformly but are prioritized based on their percentage occurrence and impact within the IoT environment. The model is derived from the percentage-based risk computation performed during the frequency analysis stage.

To ensure a systematic and evidence-based evaluation of IoT security threats, this study employs a weighted risk assessment model using the IoT-23 Dataset to quantify the relative severity of different attacks.

Mathematical Formulation

$$\text{Risk Score} = \alpha(\text{Frequency}) + \beta(\text{Impact}) + \gamma(\text{Severity})$$
$$\alpha + \beta + \gamma = 1$$

Parameter Definitions

- **Frequency (F):** Represents the occurrence rate of each attack type derived from the IoT-23 dataset based on traffic distribution and attack instances.
- **Impact (I):** Indicates the level of damage caused by the attack, such as service disruption, resource exhaustion, or data compromise.
- **Severity (S):** Reflects the sophistication and strength of the attack, including scalability, automation, and difficulty of detection.
- **α, β, γ:** Weighting factors assigned to each parameter (e.g., $\alpha = 0.4$, $\beta = 0.3$, $\gamma = 0.3$), where their sum equals 1.

The proposed model integrates dataset-driven insights with security impact analysis to compute a composite risk score for each IoT attack. The values are then normalized to a 0–100 scale to enable consistent comparison across different attack categories. By grounding the frequency component in the IoT-23 dataset, the model ensures that the reported risk levels are data-driven and evidence-based**,** while impact and severity dimensions provide contextual understanding of attack behavior. This approach eliminates subjectivity and enhances the scientific credibility and reproducibility of the analysis.

7.9 Attack Categorization

After extraction, attacks were categorized according to recent challenges such as DDoS, brute force and replay attacks.

7.10 Percentage of Risk Calculation and Comparative Analysis

The severity percentage is calculated according to attacks appeared in recent studies. These percentages show emphasis and impact in IoT environment.

8. Result

This section provides the summary results of the paper for further understanding. Table 4 illustrates the recent general security challenges and existing attacks in the IoT environment, along with their corresponding solutions.

Table 4. Summary of the Recent Attacks in IoT

Attack	Explanation	Proposed Solution	Limitation of Existing Work
Mirai-based Botnet Attacks	Identified large-scale IoT botnets using traffic pattern analysis	Zero Trust Architecture (ZTA)	Focused on detection, lacks continuous authentication and prevention
AI-powered IoT Attacks	Used deep learning for anomaly detection in intelligent attacks	Tiny ML-based detection at edge	High computational cost, not suitable for resource-constrained IoT
Satellite & Space IoT Attacks	Studied secure communication in distributed and space-based networks	Post-Quantum Cryptography (PQC)	Traditional encryption vulnerable to future quantum threats
Device Cloning Attack	Introduced Physical Unclonable Functions (PUFs) for hardware security	Device Fingerprinting + PUF	Hardware dependency and implementation complexity
IoT Routing Attacks	Proposed RPL protocol for secure routing in IoT networks	Secure RPL with IDS integration	Vulnerable to insider and rank attacks
Data Tampering	Introduced blockchain for data integrity and immutability	Blockchain + End-to-End Encryption	High energy and computational overhead
Brute-Force Password Attacks	Established secure authentication principles	Multi-Factor Authentication (MFA)	User inconvenience and usability challenges

Table 4 above summarizes the most recent risks of attacks in the IoT environment. Figure 3 shows the attack analysis results.

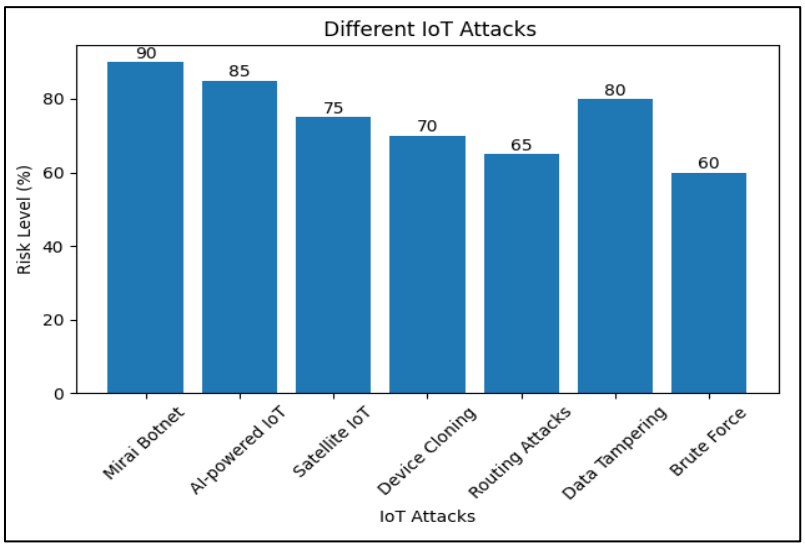

Figure 3. IoT Recent Attacks

The results in Figure 3 indicate that Mirai-based botnet attacks pose the highest risk in the IoT environment, with an approximate risk level of 90%**,** highlighting their widespread exploitation of vulnerable IoT devices. This is followed by AI-powered IoT attacks, which demonstrate a high risk level of around 85%**,** reflecting the growing sophistication and adaptability of intelligent attack mechanisms. Data tampering attacks also show a significant impact with an estimated risk of 80%**,** emphasizing concerns related to data integrity in IoT systems.

Furthermore, satellite and space IoT attacks present a considerable risk at approximately 75%, indicating emerging vulnerabilities in extended IoT infrastructures. Device cloning attacks account for around 70%, while IoT routing attacks exhibit a moderate risk level of about 65%**.** Lastly**,** brute-force password attacks, although still relevant, show a comparatively lower risk level of approximately 60%. These values represent relative risk estimates derived from observed attack trends and literature, providing a comparative understanding of the severity of different IoT threats rather than exact statistical measurements. Figure 4 shows the IoT attacks growth across the years.

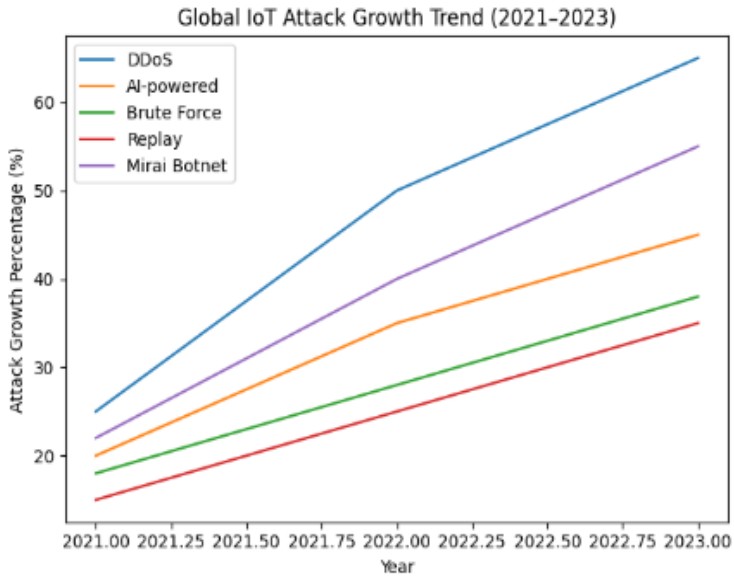

Figure 4. IoT Attack Growth Trend

Figure 4 shows all types of IoT attacks are increasing globally, with DDoS and Mirai botnet attacks showing the steepest growth, which highlights the increasing security risks in IoT networks. The trend underscores the urgent need for enhanced IoT security measures, especially for attacks that scale quickly like DDoS and botnet attacks. Table 6 provides the general IoT security challenges.

Table 6. Summary of the General IoT Security Challenge

Challenges	Solutions to the attacks
Heterogeneity	Quantum-Secure Middleware algorithm
Mobility	6G-Integrated Mobility and Quantum-Resistant Handover Algorithms
End Point Devices	Genetic algorithm for healing devices

Table 6 presents a summary of the general IoT security challenge, along with a possible solution algorithm to address the security challenge. Figure 5 illustrates the challenge analysis.

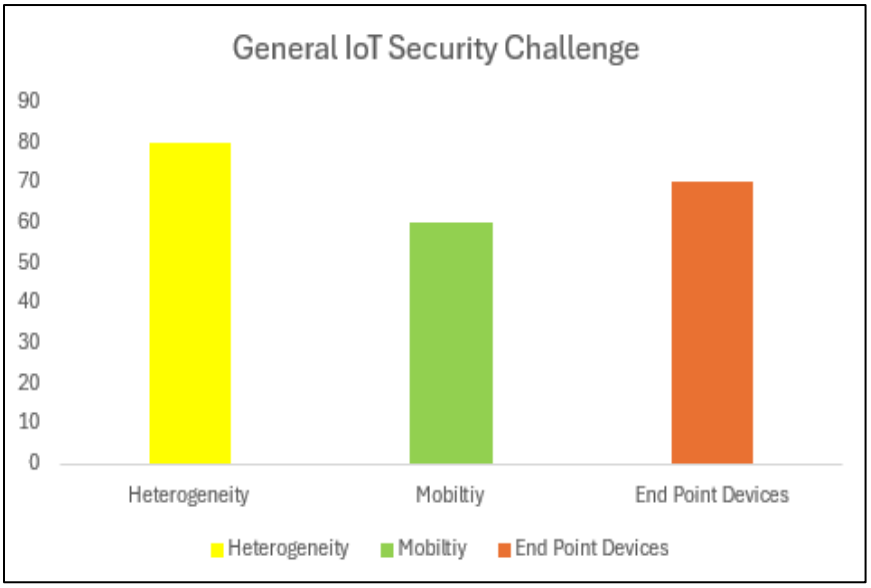

Figure 5. IoT Challenges

Figure 5 illustrates the general security challenge in IoT. Based on the analysis results, the heterogeneity challenge can be considered one of the highest challenges in IoT general security. Additionally, the analysis reveals that heterogeneity poses an 80% risk. While mobility with endpoint devices carries a 70% risk, mobility with about 60% is also a concern. Table 7 will describe the existing attacks in the IoT environment.

Table 7. Summary of the Existing Attacks in the IoT Environment

Attacks	Solutions to the attacks
DDoS attack	Implementation of a Quantum-resistant DDoS algorithm
Replay attack	Implementation of a nonce cryptographic algorithm
Brute force password attack	Implementation of the Bcrypt algorithm
Device cloning attack	Device identity verification
IoT routing attacks	Secure routing protocols
Data tampering	Data integrity verification

Table 7 identifies suggested research algorithms that can be used to address the attacks in the IoT environment. Figure 6 will describe the attack analysis based on risk percentage Table 5.

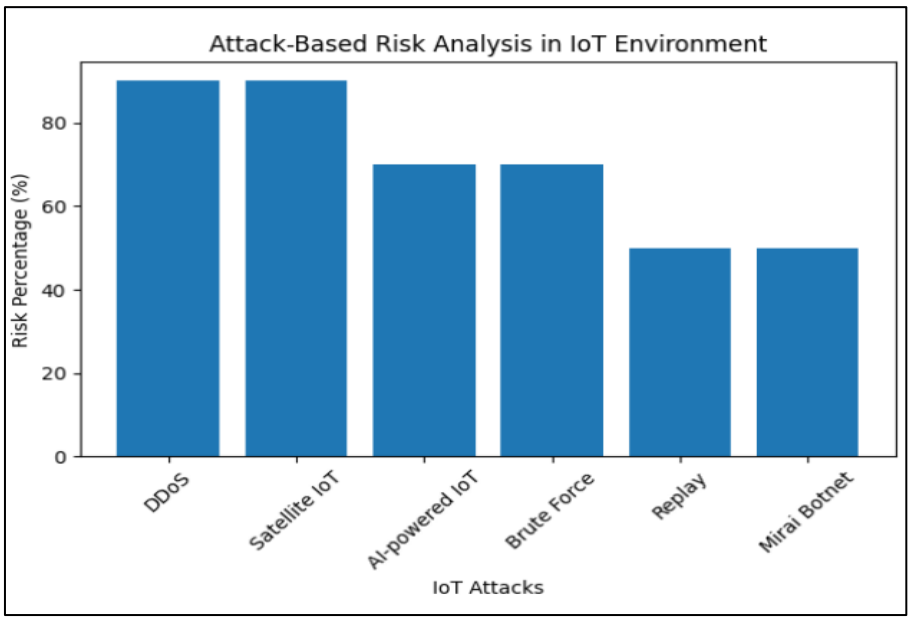

Figure 6. Existing Attacks in the IoT Environment

Figure 6 describes the analysis of the existing attacks in the IoT environment. Hence, the analysis results reveal that DDoS attacks pose the highest risk among existing attacks in the IoT environment, accounting for 90% of the total risk. In contrast, brute force password attacks account for 70% of the risk, while replay attacks account for 50%. This shows that the DDoS attack needs the utmost attention in the IoT environment.

9. Conclusion

This paper reviews and investigates recent IoT attacks, general security challenges, and existing threats in the IoT environment, and proposes various solutions for mitigating these attacks. The IoT security attacks mentioned in this study should be addressed from both technical and adoption perspectives. The main contribution of this paper is to provide current information about security attacks and threats in the IoT environment. In addition, this paper will suggest future directions for future researchers. To conclude, the paper suggests that if Post-Quantum Cryptography (PQC) algorithms are implemented in different ways, the risk of attacks will be minimal.

Acknowledgments

The research was fully supported by Universiti Tunku Abdul Rahman (UTAR) for financial support, which made this research possible.

References

[1] X. Li, S. Ma, and Z. Zhang, "Friends or Foes? The Effect of IoT Platform Entry Into Smart Device Market Under Quantity Discount Pricing Contract," IEEE Transactions on Engineering Management, vol. 71, pp. 10984-10997, 2024, doi: 10.1109/TEM.2024.3402733.

[2] Statista, "Number of Internet of Things (IoT) connections worldwide from 2022 to 2023, with forecasts from 2024 to 2033," ed, 2024.

[3] K. A. Cooper, "Security for the Internet of Things," Master's Degree Master's Thesis], 2015. [Online]. Available: http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-172526

[4] A. S. Petrenko, S. A. Petrenko, K. A. Makoveichuk, and P. V. Chetyrbok, "The IIoT/IoT device control model based on narrow-band IoT (NB-IoT)," in 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), Moscow and St. Petersburg, Russia, 2018: IEEE, pp. 950-953, doi: 10.1109/EIConRus.2018.8317246.

[5] A. A. Ghali, R. Ahmad, and H. Alhussian, "A Framework for Mitigating DDoS and DOS Attacks in IoT Environment Using Hybrid Approach," Electronics, vol. 10, no. 11, p. 1282, 2021, doi: 10.3390/electronics10111282.

[6] M. Othman, M. Arif, M. H. A. Abdullah, M. M. Yusof, and R. Mohamed, "Human resource management on cloud," JOIV: International Journal on Informatics Visualization, vol. 1, no. 4-2, pp. 260-263, 2017.

[7] N. Talpur, N. C. G. Alier, H. Matsom, M. H. A. Abdullah, and S. Khatoon, "Predicting Employee Performance using Machine Learning to Enhance Workforce Efficiency," in 2024 8th International Conference on Computing, Communication, Control and Automation (ICCUBEA), Pune, India, 2024: IEEE, pp. 1-4, doi: 10.1109/ICCUBEA61740.2024.10774749.

[8] M. Ammar, G. Russello, and B. Crispo, "Internet of Things: A survey on the security of IoT frameworks," Journal of Information Security and Applications, vol. 38, pp. 8-27, 2018, doi: 10.1016/j.jisa.2017.11.002.

[9] S. Rajput, N. Talpur, R. Boudville, G. M. E. Abro, B. Talpur, and F. Zahid, "Modernizing Home Protection: An IoT-Driven Approach with Smart Lock and Android Application," in 2024 IEEE 14th International Conference on Control System, Computing and Engineering (ICCSCE), Penang, Malaysia, 2024: IEEE, pp. 82-87, doi: 10.1109/ICCSCE61582.2024.10696484.

[10] N. Aziz, M. H. A. Abdullah, N. A. Osman, M. N. Musa, and E. A. P. Akhir, "Predictive Analytics for Oil and Gas Asset Maintenance Using XGBoost Algorithm," in Proceedings of the 2nd International Conference on Emerging Technologies and Intelligent Systems, Cham, M. A. Al-Sharafi, M. Al-Emran, M. N. Al-Kabi, and K. Shaalan, Eds., 2023: Springer International Publishing, pp. 108-117.

[11] Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," Wireless Networks, vol. 20, no. 8, pp. 2481-2501, 2014/11/01 2014, doi: 10.1007/s11276-014-0761-7.

[12] M. Othman, N. M. Halil, M. M. Yusof, R. Mohamed, and M. H. A. Abdullah, "Empowering Self-Management through M-Health Applications," MATEC Web of Conferences, vol. 150, p. 05018, 2018, doi: 10.1051/matecconf/201815005018.

[13] N. Talpur, S. J. Abdulkadir, M. H. Hasan, H. Alhussian, and A. Alwadain, "A novel wrapper-based optimization algorithm for the feature selection and classification," Computers, Materials & Continua, vol. 74, no. 3, pp. 5799-5820, 2023.

[14] N. N. Thilakarathne, M. K. Kagita, and T. R. Gadekallu, "The Role of the Internet of Things in Health Care: A Systematic and Comprehensive Study," SSRN Electronic Journal, 2020, doi: 10.2139/ssrn.3690815.

[15] P. Sharma, "Digital revolution of education 4.0," International Journal of Engineering and Advanced Technology, vol. 9, no. 2, pp. 3558-3564, 2019, doi: 10.35940/ijeat.A1293.129219.

[16] M. Abdel-Basset, G. Manogaran, M. Mohamed, and E. Rushdy, "Internet of things in smart education environment: Supportive framework in the decision-making process," Concurrency and Computation: Practice and Experience, vol. 31, no. 10, p. e4515, 2019, doi: 10.1002/cpe.4515.

[17] Z. Shouran, A. Ashari, and T. Priyambodo, "Internet of things (IoT) of smart home: privacy and security," International Journal of Computer Applications, vol. 182, no. 39, pp. 3-8, 2019.

[18] B. Ur, J. Jung, and S. Schechter, "The current state of access control for smart devices in homes," in Workshop on home usable privacy and security (HUPS), Newcastle, United Kingdom, 2013, vol. 29, pp. 209-218.

[19] V. Sivaraman, H. H. Gharakheili, A. Vishwanath, R. Boreli, and O. Mehani, "Network-level security and privacy control for smart-home IoT devices," in 2015 IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), Abu Dhabi, United Arab Emirates, 2015: IEEE, pp. 163-167, doi: 10.1109/WiMOB.2015.7347956.

[20] Y. Javed, A. S. Khan, A. Qahar, and J. Abdullah, "Preventing DoS Attacks in IoT Using AES," Journal of Telecommunication, Electronic and Computer Engineering (JTEC), vol. 9, no. 3-11, pp. 55-60, 2017.

[21] A. Riahi Sfar, E. Natalizio, Y. Challal, and Z. Chtourou, "A roadmap for security challenges in the Internet of Things," Digital Communications and Networks, vol. 4, no. 2, pp. 118-137, 2018, doi: 10.1016/j.dcan.2017.04.003.

[22] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," Ad Hoc Networks, vol. 10, no. 7, pp. 1497-1516, 2012, doi: 10.1016/j.adhoc.2012.02.016.

[23] M. Abomhara and G. M. Køien, "Security and privacy in the Internet of Things: Current status and open issues," in 2014 International Conference on Privacy and Security in Mobile Systems (PRISMS), Aalborg, Denmark, 2014: IEEE, pp. 1-8, doi: 10.1109/PRISMS.2014.6970594.

[24] A. A. Ghali, S. Jamel, K. M. Mohamad, S. K. A. Khalid, Z. A. Pindar, and M. M. Deris, "An Improved Low Contrast Image in Normalization Process for Iris Recognition System," in Recent Advances on Soft Computing and Data Mining, Cham, R. Ghazali, M. M. Deris, N. M. Nawi, and J. H. Abawajy, Eds., 2018: Springer International Publishing, pp. 495-505, doi: 10.1007/978-3-319-72550-5_47.

[25]D. E. Kouicem, A. Bouabdallah, and H. Lakhlef, "Internet of things security: A top-down survey," Computer Networks, vol. 141, pp. 199-221, 2018/08/04/ 2018, doi: 10.1016/j.comnet.2018.03.012.

[26]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, doi: 10.1016/j.future.2013.01.010.

[27]O. Vermesan et al., "Internet of things strategic research roadmap," in Internet of things-global technological and societal trends from smart environments and spaces to green ICT: River Publishers, 2022, pp. 9-52.

[28]R. Hodgson, "Solving the security challenges of IoT with public key cryptography," Network Security, vol. 2019, no. 1, pp. 17-19, 2019, doi: 10.1016/s1353-4858(19)30011-x.

[29]R. Mahmoud, T. Yousuf, F. Aloul, and I. Zualkernan, "Internet of things (IoT) security: Current status, challenges and prospective measures," in 2015 10th International Conference for Internet Technology and Secured Transactions (ICITST), London, United Kingdom, 2015, pp. 336-341, doi: 10.1109/ICITST.2015.7412116.

[30]C. Bekara, "Security Issues and Challenges for the IoT-based Smart Grid," Procedia Computer Science, vol. 34, pp. 532-537, 2014, doi: 10.1016/j.procs.2014.07.064.

[31]M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 82, pp. 395-411, 2018, doi: 10.1016/j.future.2017.11.022.

[32]L. Atzori, A. Iera, G. Morabito, and M. Nitti, "The Social Internet of Things (SIoT) – When social networks meet the Internet of Things: Concept, architecture and network characterization," Computer Networks, vol. 56, no. 16, pp. 3594-3608, 2012, doi: 10.1016/j.comnet.2012.07.010.

[33]A. A. Ghali, R. Ahmad, and H. Alhussian, "A Framework for Enhancing Network Lifetime in Internet of Things Environment Using Clustering Formation," in International Conference on Artificial Intelligence for Smart Community, Singapore, R. Ibrahim, K. Porkumaran, R. Kannan, N. Mohd Nor, and S. Prabakar, Eds., 2022: Springer Nature Singapore, pp. 401-407, doi: 10.1007/978-981-16-2183-3_39.

[34]R. Roman, J. Zhou, and J. Lopez, "On the features and challenges of security and privacy in distributed internet of things," Computer Networks, vol. 57, no. 10, pp. 2266-2279, 2013, doi: 10.1016/j.comnet.2012.12.018.

[35]P. N. Mahalle, B. Anggorojati, N. R. Prasad, and R. Prasad, "Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things," Journal of Cyber Security and Mobility, vol. 1, no. 4, pp. 309-348, 2013.

[36]D. Minoli, K. Sohraby, and B. Occhiogrosso, "IoT Security (IoTSec) Mechanisms for e-Health and Ambient Assisted Living Applications," in 2017 IEEE/ACM International Conference on Connected Health: Applications, Systems and Engineering Technologies (CHASE), Philadelphia, PA, USA, 2017: IEEE, pp. 13-18, doi: 10.1109/CHASE.2017.53.

[37]A. Patil and R. Gaikwad, "Comparative Analysis of the Prevention Techniques of Denial of Service Attacks in Wireless Sensor Network," Procedia Computer Science, vol. 48, pp. 387-393, 2015, doi: 10.1016/j.procs.2015.04.198.

[38]A. Aminu Ghali, R. Ahmad, and H. S. A. Alhussian, "Comparative Analysis of DoS and DDoS Attacks in Internet of Things Environment," in Artificial Intelligence and Bioinspired Computational Methods, Cham, R. Silhavy, Ed., 2020: Springer International Publishing, pp. 183-194, doi: 10.1007/978-3-030-51971-1_15.

[39]N. SeungJae, H. DongYeop, S. WoonSeob, and K. Ki-Hyung, "Scenario and countermeasure for replay attack using join request messages in LoRaWAN," in 2017 International Conference on Information Networking (ICOIN), Da Nang, Vietnam, 2017: IEEE, pp. 718-720, doi: 10.1109/ICOIN.2017.7899580.

[40]C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and Other Botnets," Computer, vol. 50, no. 7, pp. 80-84, 2017, doi: 10.1109/MC.2017.201.

[41]M. Nedbal. "IoT Insecurity: 6 Common Attacks and How to Protect Customers." Channel Futures. https://www.channelfutures.com/regulation-compliance/iot-insecurity-6-common-attacks-and-how-to-protect-customers (accessed 11 February 2025).