Journal on
Artificial Intelligence

Tech Science Press

Doi:10.32604/jai.2025.067361

REVIEW

A Survey on Token Transmission Attacks, Effects, and Mitigation Strategies in IoT Devices

Michael Juma Ayuma[1], **Shem Mbandu Angolo**[1,*] **and Philemon Nthenge Kasyoka**[2,*]

[1]Department of Computer Science and Information Technology, School of Computing and Mathematics, The Co-operative University of Kenya, Karen, Nairobi, P.O. Box 24814-00502, Kenya
[2]School of Science and Computing, South Eastern Kenya University, Kitui, P.O. Box 170-90200, Kenya

*Corresponding Authors: Shem Mbandu Angolo. Email: asmbandu@cuk.ac.ke;
Philemon Nthenge Kasyoka. Email: pkasyoka@gmail.com

Received: 01 May 2025; Accepted: 14 July 2025; Published: 19 August 2025

ABSTRACT: The exponential growth of Internet of Things (IoT) devices has introduced significant security challenges, particularly in securing token-based communication protocols used for authentication and authorization. This survey systematically reviews the vulnerabilities in token transmission within IoT environments, focusing on various sophisticated attack vectors such as replay attacks, token hijacking, man-in-the-middle (MITM) attacks, token injection, and eavesdropping among others. These attacks exploit the inherent weaknesses of token-based mechanisms like OAuth, JSON Web Tokens (JWT), and bearer tokens, which are widely used in IoT ecosystems for managing device interactions and access control. The impact of such attacks is profound, leading to unauthorized access, data exfiltration, and control over IoT devices, posing significant threats to privacy, safety, and the operational integrity of critical IoT applications in sectors like healthcare, smart cities, and industrial automation. This paper categorizes these attack vectors, explores real-world case studies, and analyzes their effects on resource-constrained IoT devices that have limited processing power and memory, rendering them more susceptible to such exploits. Furthermore, this survey presents a comprehensive evaluation of existing mitigation techniques, including cryptographic protocols, lightweight secure transmission frameworks, secure token management practices, and network-layer defenses such as Transport Layer Security (TLS) and multi-factor authentication (MFA). The study also highlights the trade-offs between security and performance in IoT systems and identifies key gaps in current research, emphasizing the need for more scalable, energy-efficient, and robust security frameworks to address the evolving landscape of token transmission attacks in IoT devices.

KEYWORDS: Token transmission; IoT attacks; IoT authentication; cryptography; encryption

1 Introduction

IoT has changed many industries in varying ways and leveled up the idea of connected devices that can send information to one another. Starting from interconnected homes and hospitals to industries and factories, IoT has revolutionized humans' interface with machines, resulting in a quintessential enhancement of proactivity. But at the same time, a large number of IoT devices caused new security threats, firstly, regarding authentication and authorization procedures of devices for secure communication.

One of the significant open security issues that we identify in IoT systems involves token transmission during the authentication processes. Token-based authentication has emerged as a standard practice in making communications between IoT devices and the server secure and also to authenticate the identity of

the device. However, these tokens can be easily attacked if an unauthorized party acquires them to perform a token replay attack where the token is duplicated and used to impersonate the legal device. Such attacks may lead to violation of privacy, penetration and infringement of privacy of users among other things. Ideally, to secure IoT devices, it is possible to set up profound secure procedures but this is difficult since IoT devices have restricted computational power and memory. Source of Funding: [1,2]. This is especially because IoT devices interact with unsophisticated networks and thus are likely to experience insecure multi-hop networks making token transmission crucial [3].

Recent research highlights the critical vulnerabilities associated with token-based authentication in IoT systems. For instance, Al-Refai and Alawneh propose an enhanced security framework that incorporates token authentication technology, aiming to address the shortcomings of existing frameworks [1]. This is particularly important as IoT devices are frequently targeted due to their wireless communication capabilities, which expand the attack surface beyond local networks [4].

Fig. 1 shows how data privacy emerges as the most pressing concern, accounting for 28% of the total, underscoring the critical need to protect sensitive information within IoT ecosystems. Increased security threats represent the second largest issue at 17%, reflecting the growing vulnerability of IoT systems to cyberattacks. Both identity and access management and attacks against connected devices constitute 9% each, emphasizing the challenges of securing authentication protocols and mitigating malicious activities targeting IoT devices. Compliance requirements, comprising 7%, illustrate the complexities of adhering to regulatory and legal standards, while the others category (10%) captures additional concerns not explicitly categorized. Collectively, these issues underscore the multifaceted risks associated with IoT adoption, necessitating comprehensive and strategic interventions to enhance security, privacy, and regulatory compliance in IoT networks [4].

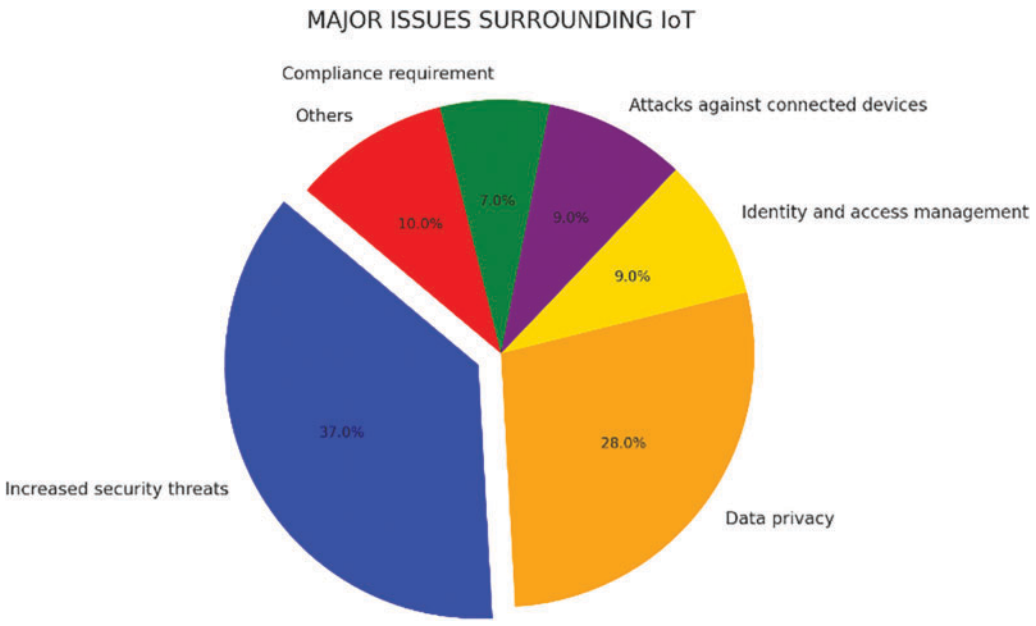

Figure 1: Major issues surrounding IoT

The implications of token transmission attacks extend beyond mere data breaches; they can lead to significant operational disruptions, particularly in critical sectors such as healthcare and industrial control systems. For example, the unauthorized manipulation of data transmitted by IoT devices can result in

erroneous outputs that affect decision-making processes. The need for robust authentication mechanisms is further emphasized by the potential for attacks that exploit the unique characteristics of IoT devices, such as their resource constraints and varying levels of security capabilities [2,5].

2 Research Methodology

This study uses a comprehensive qualitative method to analyze information system security in token transmission in the Internet of Things (IoT). A qualitative method was adopted to provide a thorough understanding of many security elements of IoT, token transfer, and authentication in IoT devices, including difficulties, solutions, and best practices. This research approach was developed in the stages listed below: Data will be gathered by an in-depth literature review of primary and secondary sources related to information systems security and IoT. The material to be examined will comprise scientific journals, books, research papers, and technical documentation. The collected data will be examined qualitatively. This entails detecting trends, critical results, and correlations among various aspects of information system security in the IoT context. The data's validity will be checked by referring to certified and trusted sources. In addition, the analysis will be verified and validated by specialists in information security and IoT. The analytic results will be evaluated to yield useful insights into information system security in the IoT era. These findings will be linked to the theoretical framework under discussion to gain a better understanding. Based on the study, research conclusions will be developed, outlining the key results, consequences, and recommendations for developing successful security methods in the IoT context. Following this methodology, it is believed that this research will contribute significantly to the knowledge and implementation of best practices for safeguarding information systems via secure token transfer in the Internet of Things age.

3 Role of Tokens in Securing IoT Communications

The role of tokens in securing IoT communications is pivotal, particularly as the number of IoT devices continues to rise and their applications expand across various sectors. Tokens serve as digital keys that facilitate secure access control, authentication, and authorization within IoT ecosystems. For authentication purposes, Tokens are frequently used to verify the identity of IoT devices when they communicate with servers or other devices. In a typical scenario, when an IoT device attempts to connect to a server, the server generates a token that uniquely identifies the device. The device stores this token and presents it in subsequent interactions, allowing the server to recognize the device without requiring the full credentials to be transmitted repeatedly. This reduces the risk of exposing sensitive information over the network [1,6]. Beyond authentication, tokens also serve as a means of defining and enforcing access control in IoT communications. Each token may contain encoded information about the permissions and privileges of the device or user in the network. This ensures that the device can only access the resources and services it is authorized to use, helping prevent unauthorized actions. Tokens are especially useful in large-scale IoT networks where different devices have varying levels of access to the system [7]. In addition, Tokens can be used to manage communication sessions between IoT devices and servers. Once a device is authenticated, a session token is generated to maintain the connection over some time without repeatedly verifying the device's credentials. This is particularly valuable for maintaining ongoing communication in environments where IoT devices need to exchange data regularly, such as in smart homes or industrial IoT applications [8]. Tokens can also help to protect the integrity of data exchanged between IoT devices and servers. The CIA triangle of security goals—confidentiality, integrity, and availability—may be impacted by these attacks. NIST's publication FIPS 199 describes the likely consequences of losing one of these three security goals.

In two scenarios—Smart Home Heating Control and Smart Health Monitor systems—the table contrasts a large number of simulated cyberattacks with their potential effects on the three security principles of

confidentiality, integrity, and availability of user information. There are three categories for the impact levels: low, moderate, and high.

Low: has minimal impact on operations, assets, or personnel.

Moderate (Mod): Severe impact on business, assets, or personnel.

High: Has a severe or catastrophic impact on business, assets, or individuals.

Non-applicable: only pertains to confidentiality.

Depending on the specifics of an attack, the possible consequences could vary. Based on the basic type of device to which they are addressed, the table illustrates the potential effects of several attacks on the CIA triad for user information. The intensity of the impact may vary depending on the application; in one case, the attacks target a smart lightbulb, while in the other, they target a smart health monitor [9].

By using cryptographically signed tokens, it becomes possible to detect if data has been tampered with during transmission. If the token is altered, the server can reject the communication, ensuring that only valid and unaltered data is accepted. In large-scale IoT networks, where thousands of devices may be communicating simultaneously, tokens offer a scalable and efficient solution for securing communications. Traditional security methods often require extensive computational resources that IoT devices may not possess. In distributed IoT networks, tokens support decentralized security models, where authentication can be performed at the edge of the network without needing constant communication with a central server. This is particularly important in edge computing environments, where IoT devices process data locally and only send essential information back to the cloud. Tokens enable these devices to authenticate locally, increasing efficiency and reducing latency. The integration of blockchain with token systems further enhances security. This not only secures communication but also enables devices to maintain a verifiable identity, which is essential for trust in IoT ecosystems [9].

Security tokens can encapsulate user credentials and establish secure sessions through encryption, while API tokens facilitate secure interactions between software applications and services [10]. Additionally, hardware tokens, which may utilize physical unclonable functions (PUFs) for authentication, provide unique identifiers for devices that contribute to ensuring secure communications in IoT environments [11]. The IoT provides a large number of applications to enhance people's daily lives and activities. Fig. 2 shows potential examples of IoT applications.

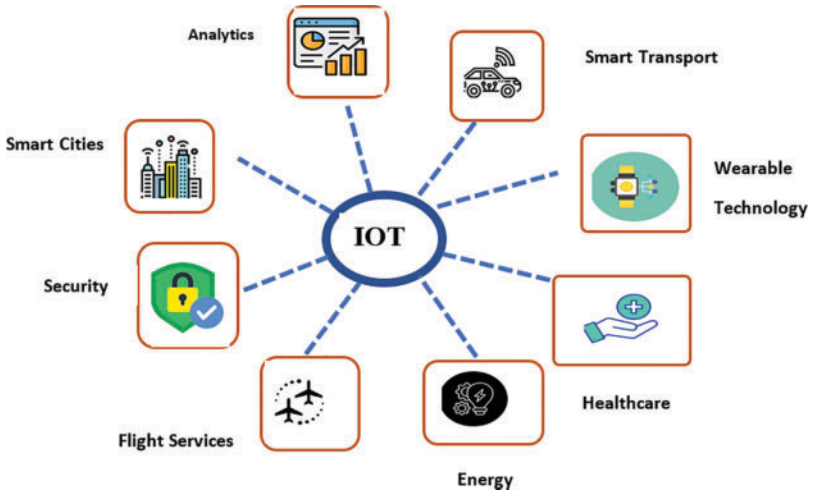

Figure 2: Overview of IoT applications

4 Types of Tokens Used in IoT Devices/Communication Protocols

Tokens are used for authentication, authorization, and sometimes even for ensuring the integrity of the data being exchanged. Depending on the specific IoT network and communication protocol, different types of tokens are employed to maintain secure, efficient, and reliable connections. This section explores the types of tokens commonly used in IoT devices and communication protocols, highlighting their functions and significance in preventing unauthorized access and mitigating potential transmission attacks.

4.1 Bearer Tokens

A bearer token is a security token that grants access to resources based on possession. Any entity holding a valid bearer token can gain access to the specified resource without requiring additional credentials or authentication. They are commonly used in RESTful communication protocols in IoT, where devices authenticate once and then use the token for subsequent interactions with cloud services or IoT platforms. These tokens are often included in HTTP request headers [12]. Table 1 shows a comparison of similarities and differences among tokens commonly used in IoT devices and communication protocols.

Table 1: Comparison table showing the similarities and differences among tokens commonly used in IoT devices and communication protocols

Feature	Bearer tokens	JWT (JSON Web Tokens)	OAuth access tokens	Refresh tokens
Definition	A simple token granting access to resources	A self-contained token with payload and signature	A token for accessing protected resources	A token to obtain new access tokens
Structure	Opaque string	Structured: header.payload.signature (Base64)	Opaque or JWT format	Opaque (usually)
Self-Contained?	No	Yes	Sometimes (depends on implementation)	No
Used for	Basic authentication and authorization	Authentication and authorization	Authorization via delegated access	Renewing access tokens
Expiration	Yes	Yes	Yes	Yes (usually long-lived)
Can be renewed?	No (new one needed)	No (new one needed)	Yes (using refresh token)	No (used to obtain new access token)
Security mechanism	Relies on HTTPS for confidentiality	Signed (with secret or private key)	Varies (can be signed JWT or opaque token)	Used securely alongside access tokens
Storage on IoT devices	Lightweight storage	May require more space (due to size)	Lightweight (varies by format)	May require secure storage
Used in protocols	HTTP, MQTT, CoAP	HTTP, MQTT, CoAP	OAuth 2.0 flows over HTTP	OAuth 2.0 token refresh flow
Validation location	Server-side lookup	Can be validated on device or server	Usually validated by authorization server	Validated only by auth server

(Continued)

Table 1 (continued)

Feature	Bearer tokens	JWT (JSON Web Tokens)	OAuth access tokens	Refresh tokens
Common in IoT for	Basic API access between devices/cloud	Secure device-to-cloud auth (e.g., Google IoT)	Smart home/user-authorized device communication	Long-lived sessions in constrained devices

4.2 JSON Web Tokens (JWT)

JSON Web Tokens (JWT) are a URL-safe, JSON-based format used to securely convey claims between parties. These tokens are made up of three parts: a header, a payload (which contains claims), and a signature. The signature ensures the data's integrity and authenticity. Because of their lightweight nature, ease of integration, and ability to be quickly validated, JWTs are frequently used for authentication and authorization in IoT systems, particularly in device-to-cloud and device-to-device communication. Yang et al. present a lightweight authentication technique that uses elliptic curve cryptography and trustworthy tokens (JWT) to effectively authenticate IoT devices and backend services. This solution assures that data delivered to the server comes from legitimate devices, alleviating worries about data integrity and authenticity [12]. Furthermore, the use of bearer tokens allows for stateless authentication, which is particularly advantageous in resource-constrained IoT devices, as it reduces the need for maintaining a session state on the server side [13].

4.3 OAuth Access Tokens

OAuth access tokens are short-lived credentials used to grant devices or applications access to resources on behalf of a user or service. These tokens contain specific permissions (or scopes) and are issued by an authorization server. OAuth are used in IoT environments to delegate secure access control to devices without revealing user credentials. They are commonly employed in scenarios where IoT devices interact with cloud-based services or A PIs. Some of the Associated Protocols include OAuth 2.0, CoAP, and HTTPS. The OAuth 2.0 framework allows IoT devices to obtain access tokens that can be used to authenticate requests to servers or other services. This mechanism is essential for ensuring that only authorized devices can access sensitive resources. For instance, García-Pozo et al. evaluated the integration of the OAuth 2.0 protocol within an IoT Publish/Subscribe architecture, demonstrating its feasibility and effectiveness in managing access control in resource-limited environments [14]. The study highlights how OAuth can facilitate secure interactions between devices and servers while accommodating the constraints of IoT devices.

4.4 Refresh Tokens

Refresh tokens are long-lived tokens that allow devices to request new access tokens without requiring re-authentication. These tokens are issued alongside access tokens and can be stored securely on the IoT device for subsequent use. They are essential in maintaining long-term device connections, especially for devices that need continuous or periodic access to resources without frequent re-authentication, which would consume significant resources. Moreover, the lightweight nature of refresh tokens is particularly beneficial for IoT devices, which often have limited processing power and battery life. Furtak discusses a cryptographic key-generating and renewing system that emphasizes the importance of secure key management in IoT networks [15]. This system can be integrated with refresh token mechanisms to ensure that keys

are renewed securely without excessive computational demands, thereby preserving the limited resources of IoT devices.

4.5 Security Assertion Markup Language (SAML) Tokens

SAML tokens are XML-based tokens used for exchanging authentication and authorization data between parties. These tokens contain assertions about the identity of the user or device and the permissions granted. While less commonly used in resource-constrained IoT systems due to their larger size, SAML tokens are deployed in enterprise IoT environments that require integration with existing SAML-based identity management systems. The integration of SAML tokens in IoT can enhance security by enabling mutual authentication between devices and servers. Alnahari and Quasim discuss the significance of mutual authentication in preventing unauthorized access and ensuring secure data sharing between IoT devices and servers [16].

4.6 CBOR Web Tokens (CWT)

CBOR Web Tokens (CWT) are a binary-encoded alternative to JSON Web Tokens, utilizing the Concise Binary Object Representation (CBOR) format. CWT tokens are specifically designed for constrained environments, where efficiency is critical. CWTs are particularly well-suited for resource-limited IoT devices, such as sensors and actuators, due to their smaller size and reduced computational overhead. They are often used for secure communications in constrained networks. CWTs are closely related to JWTs but offer a more efficient serialization format that reduces the overhead associated with token transmission. This compactness is crucial in IoT scenarios where bandwidth and processing power are limited, allowing devices to communicate securely without incurring significant resource costs. The use of CWTs also enhances interoperability among heterogeneous IoT devices. The ACE (Authentication and Authorization for Constrained Environments) framework, which utilizes CWTs, facilitates secure token generation and transmission across diverse IoT platforms [17]. This interoperability is essential in IoT ecosystems where devices from different manufacturers must communicate seamlessly while maintaining security.

4.7 Physically Unclonable Functions

Physically Unclonable Functions (PUFs) represent an innovative type of token that leverages unique physical characteristics of hardware to enhance security. PUFs can generate cryptographic keys and serve as authentication tokens, providing a robust defense against cloning and unauthorized access. For instance, Ebrahimabadi et al. propose a PUF-based authentication protocol that is resilient to modeling attacks, showcasing the potential of PUFs in securing IoT devices [18]. This hardware-based approach is particularly advantageous in resource-constrained environments, where traditional cryptographic methods may be impractical.

Comparison table showing the similarities and differences among tokens commonly used in IoT devices and communication protocols (Table 1).

5 Privacy Concerns across IoT Architecture Layers

Token transmission attacks in IoT environments exploit vulnerabilities in token-based authentication mechanisms, leading to significant security breaches. These include replay attacks, where intercepted tokens are reused to gain unauthorized access, as well as man-in-the-middle (MitM) attacks, token hijacking, and forgery. The root causes of these vulnerabilities stem from the use of weak or non-encrypted communication channels, improper token lifecycle management (e.g., lack of expiration or renewal mechanisms), and inadequate session control. These attacks exploit vulnerabilities in token-based authentication mechanisms,

which are commonly employed to secure communications between IoT devices and servers. Al-Refai and Alawneh highlighted that such attacks could lead to unauthorized access to servers, potentially resulting in data breaches or service disruptions [1]. The use of insecure communication channels in IoT environments exacerbates this risk, as attackers can easily intercept tokens if they are not encrypted or adequately secured during transmission. The nature of these attacks can vary, but they generally involve the interception, replay, or manipulation of authentication tokens, leading to unauthorized access and potential exploitation of the devices involved. This incident underscores the critical need for robust security measures, particularly in environments where IoT devices are deployed in sensitive applications, such as healthcare and critical infrastructure [1].

Fig. 3 illustrates the interaction between users, IoT devices, and potential attackers, highlighting the dual nature of authentication processes and malicious activities targeting IoT systems.

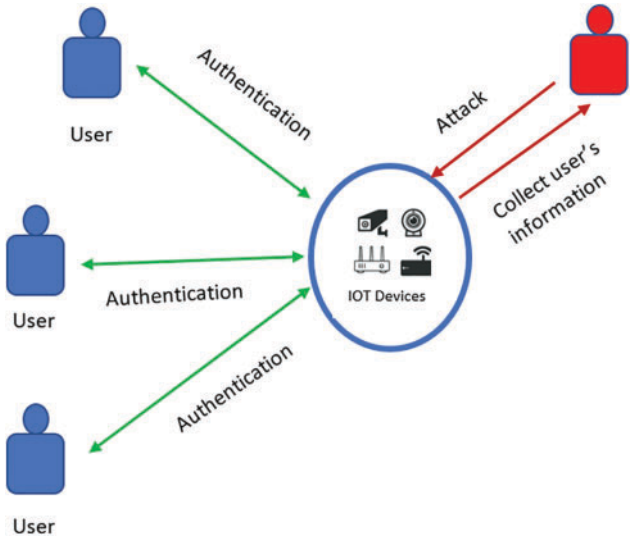

Figure 3: Attack vectors on IoT devices

By enabling devices to send tokens that verify their identity, it prevents unauthorized access to sensitive data and functions. Tokens also facilitate the enforcement of access permissions, ensure data integrity through signing or encryption, and improve scalability by simplifying the authentication process in large networks. As IoT continues to grow, the significance of secure and effective token transmission becomes increasingly vital to maintaining robust security and reliability in IoT communications [9].

Table 2 below highlights vulnerabilities in various connected devices, illustrating the risks they pose and potential exploits. For cars, vulnerabilities can allow attackers to remotely control vehicles, threatening safety. Smart home devices, prevalent in millions of homes, can be exploited for network breaches, eavesdropping, or DDoS attacks. Medical devices like insulin pumps and scanners face risks of tampering, data breaches, and ransomware, endangering patient lives. Smart TVs are vulnerable to data theft, surveillance, and malicious content injection, while embedded devices, such as routers and cameras, are often compromised through outdated software or hard-coded credentials, enabling large-scale attacks. These vulnerabilities emphasize the need for robust security practices, regular updates, and regulatory oversight to mitigate risks across all device types.

Table 2: Attacks on different IoT devices

Device type	Vulnerability possible exploits/attacks
Cars	Chrysler car firm was forced to recall 1.4 million motor vehicles after researchers showed that attackers could remotely take control of these cars.
Smart home devices	Millions of households are affected.
Medical devices	Several vulnerabilities in medical devices like insulin pumps, X-ray and CT scanners, and implantable sensors.
Smart TVs	Millions of Internet-connected televisions are vulnerable to several assaults, including click fraud, data theft, and ransomware.
Embedded devices	Everyday devices including routers, watches, cameras, and smartphones use the same hard-coded SSH and HTTPS server certificates that manufacturers leave behind, rendering millions of devices exposed to attacks such as eavesdropping and interruption.

Generally speaking, Internet of Things devices are simple and made to work with and adapt to the gadgets we use daily. Unexpected design flaws and new vulnerabilities will arise as the number of IoT devices rises, raising the likelihood of system compromise. In light of this, it is imperative to avoid sacrificing the essential safeguards of our networks' and our data's privacy, confidentiality, integrity, and availability in favor of adopting new technologies quickly [19]. A recent study by [9] found that during 2017 and 2018, there were a significant amount of assaults on IoT devices, with an average of about 5200 attacks per month. The attacks are dangerous and spreading globally. Fig. 4 shows top countries identified as the sources of most cyberattacks by adversarial actors in 2023.

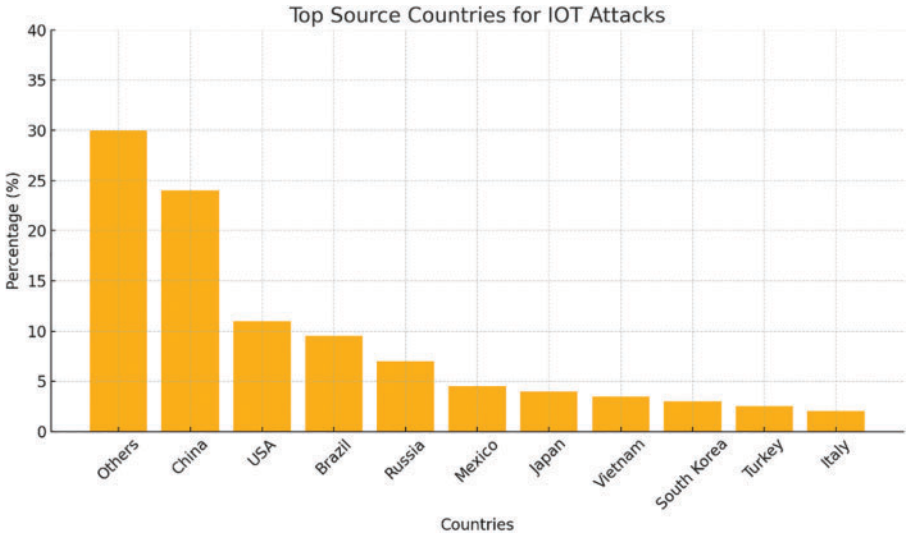

Figure 4: The figure displays the leading source nations for these IoT attacks

The necessity to protect privacy and security is typically outweighed by the ease of new technology and the desire to embrace it. But in the realm of IoT, the privacy concern is too important to overlook. The advantages of big data may cause IoT technology to be adopted before it is completely matured. The

amount and variety of data that IoT devices gather is immense. We must consider several basic security issues, including the methods used for data collection, processing, transportation, and storage.

Each layer of the Internet of Things architecture raises privacy concerns. As indicated in Table 3, efforts to reduce these security issues have resulted in the identification of security issues based on the IoT tier in which they are located.

Table 3: Privacy concerns raised in the respective layers of the IoT architecture

Layer/Function	Privacy concerns
Application	Who can access the data and information reports? How is this information used?
Transportation /Network	Data transmitted across networks, is it encrypted? Most Wireless networks and cloud services are vulnerable.
Perception/Sensor	Most devices capture personal data like name, address, and birthdate; some also invasively collect information about the user's food and music preferences, as well as health and credit card details.

Fortunately, the standard C-I-A triad (Confidentiality, Integrity, and Availability) makes it possible to organize how we tackle the problem of security [20]:

Confidentiality: It guarantees that data and information reports are only accessible to authorized individuals and only to the degree necessary.

Integrity: It guarantees that during transmission, processing, and storage, data is safe, encrypted, and strictly modified by authorized users.

Availability: While protecting data and information is crucial, we also need to ensure that it is promptly accessible to prevent it from losing its value, as in emergency and medical applications.

IoT devices are vulnerable to attacks as they are being designed as well as during the data collecting, exchange, and transmission stages, as was previously mentioned. This provides only a limited amount of assurance and confidence regarding the confidentiality, availability, and integrity of data on the Internet of Things. Our security and privacy concerns will only get worse if those problems are not fixed. IoT is still in its infancy, fortunately, despite its explosive expansion. If security is given the proper attention and increased effort during the design and development phase as well as over the product life cycle, IoT may realize its full potential and genuinely assist people without endangering anyone's security, particularly privacy [9].

6 Purpose of Study

The primary objective of this study is to conduct a comprehensive survey of token transmission attacks in Internet of Things (IoT) devices, focusing on their mechanisms, effects, and potential mitigation strategies. The research aims to systematically identify vulnerabilities in token transmission mechanisms that can be exploited by malicious actors, assess the ramifications of such attacks on IoT systems, and investigate both existing and emerging mitigation strategies, including encryption and token expiration policies. Additionally, the study seeks to promote awareness among IoT stakeholders about the risks associated with token transmission attacks and contribute to policy formulation regarding IoT security. Ultimately, this research aspires to enhance the understanding of token transmission attacks and improve the overall security practices within IoT ecosystems.

7 The General Architecture of IoT and Communication Patterns

The Internet of Things (IoT) general architecture is made up of several layers: The three main levels of the Internet of Things architecture are the perception layer, the network layer, and the application layer. The perception layer is made up of Internet of Things devices that have sensors and actuators that gather information from the surroundings and take appropriate action. The network layer uses a variety of communication protocols and technologies to send the data that the devices have collected to the cloud or other processing units. The software programs that evaluate the data and offer services to end users, enabling features like automation, control, and monitoring, are a final component of the application layer [21].

7.1 General Architecture of IoT

7.1.1 Perception Layer (Sensor Layer)

The Perception Layer, also known as the sensor layer, includes all the IoT devices, such as sensors and actuators, that gather data from the physical world. Sensors measure various environmental parameters, including temperature, humidity, motion, or light. Actuators then use this data to perform actions, such as turning on a fan or adjusting the temperature. The perception layer is composed of sensors and actuators that collect and transmit data, while the network layer enables connectivity and transport of data using communication protocols like Wi-Fi and Zigbee [22,23]. For instance, a smart thermostat collects data on the room's temperature and sends this information to higher layers of the system. When the temperature reaches a predefined threshold, the thermostat triggers an actuator to adjust the heating or cooling system.

7.1.2 Network Layer (Connectivity Layer)

The Network Layer handles the communication of data between IoT devices and other systems, such as the cloud or central servers. It is responsible for selecting and utilizing appropriate communication protocols such as Wi-Fi, Bluetooth, ZigBee, LoRaWAN, and cellular networks like LTE and 5G. This layer ensures that devices can exchange data over both short and long distances. For example, smart home devices like light bulbs, locks, and thermostats may use Wi-Fi or ZigBee to communicate with a central hub or cloud service, enabling remote management and control of the devices.

7.1.3 Data Processing Layer (Middleware Layer)

The Data Processing Layer, or Middleware Layer, processes the raw data collected by IoT devices. This layer often utilizes cloud computing or edge computing systems to aggregate, analyze, and store data. In an industrial setting, sensors attached to machinery may monitor temperature, vibration, and pressure. The data from these sensors is processed either in the cloud or on an edge server, enabling real-time analysis and decision-making. This layer is vital for converting raw sensor data into valuable insights that drive automated actions, such as predictive maintenance or system optimization.

7.1.4 Application Layer

The Application Layer is where IoT services are delivered to end-users. It includes software applications that enable users to interact with IoT devices and access the insights derived from processed data. This layer provides user interfaces, dashboards, and control mechanisms. The application layer utilizes this data to provide useful services across various fields such as healthcare, smart homes, and industrial automation [24,25]. For instance, a smart home app allows users to remotely control devices like thermostats, security cameras, and lights. The application layer ensures that users can take action based on the data from IoT devices, such as adjusting the temperature or viewing security footage.

7.1.5 Security Layer

The Security Layer is designed to protect the integrity, confidentiality, and availability of data within the IoT system. Given the vast number of connected devices, this layer incorporates various security mechanisms, including encryption, authentication, access control, and threat detection. For example, a smart home security system may require multi-factor authentication (MFA) to ensure that only authorized users can access surveillance footage. It also ensures secure communication between devices and cloud services, preventing unauthorized access and ensuring the confidentiality of sensitive data. The use of lightweight frameworks and collaborative intrusion detection systems attempts to address these vulnerabilities while maintaining the integrity and reliability of IoT networks [26]. Security concerns dictate that IoT architectures must not only support large-scale connectivity but also adapt to dynamic threats and ensure user data privacy. These structures improve resource allocation and data processing capabilities while prioritizing security measures such as encryption and access control [27]. As illustrated in the in Fig. 5, authentication and verification plays a major role in IOT security by bridging the gap to the gateway such as a router or server, to send data to the cloud or another device using relevant protocols like http or MQTTP-Message Queuing Telemetry Transport.

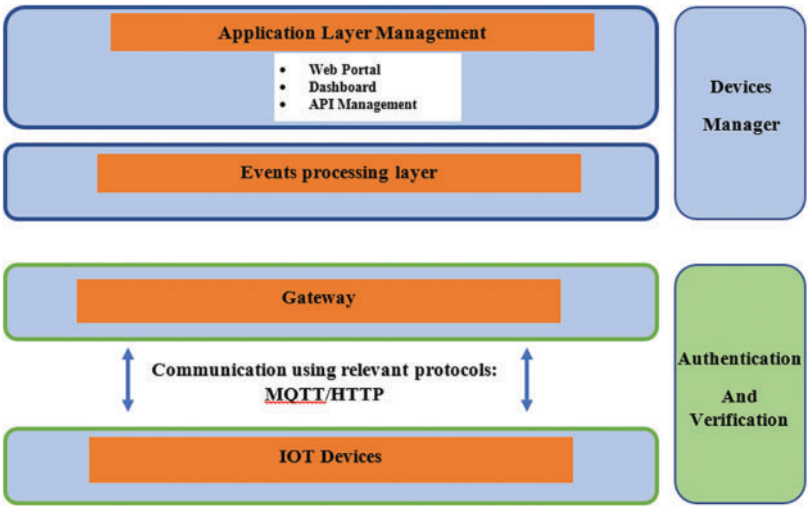

Figure 5: IoT device architecture

7.2 Communication Patterns

7.2.1 Communication Patterns in IoT

Communication patterns in IoT refer to the manner devices interact and exchange data. These patterns are crucial for ensuring efficient, reliable, and secure data transfer across IoT systems. Communication patterns within IoT systems are also vital for understanding how devices interact. Various protocols like HTTP, MQTT, and CoAP are commonly used to facilitate data exchanges between devices, allowing for real-time communication and control [27].

7.2.2 Device-to-Device (D2D)

In Device-to-Device (D2D) communication, IoT devices communicate directly with each other without the need for an intermediary, such as a central server or cloud. This communication pattern is particularly useful for real-time applications that require low latency. For example, in a smart home, a motion sensor

may detect movement and communicate directly with a light bulb to turn on. The direct communication minimizes delays and allows for immediate action, making it ideal for applications that demand rapid response times.

7.2.3 Device-to-Cloud (D2C)

Device-to-Cloud (D2C) communication involves IoT devices sending data to a cloud platform for storage, processing, and analysis. This communication pattern is often used when centralized data management and processing power are required. A common example is wearable fitness trackers that upload data, such as steps or heart rate, to a cloud service. The cloud platform processes the data and provides feedback to the user, often through a mobile app. This pattern is beneficial when large-scale data analysis, integration with other services, or long-term data storage is necessary.

7.2.4 Device-to-Gateway (D2G)

Device-to-Gateway (D2G) communication occurs when IoT devices send their data to a local gateway device, which then forwards the information to the cloud or other systems. This is especially useful for devices with limited resources, such as low-power IoT sensors that cannot directly connect to the cloud. In industrial IoT, for example, multiple sensors in a factory might send their data to a gateway, which aggregates the information before sending it to the cloud for further processing. This reduces bandwidth and computing requirements for individual devices and enables more efficient data management.

7.2.5 Machine-to-Machine (M2M)

Machine-to-Machine (M2M) communication refers to the autonomous exchange of data between machines or devices. It is often used in industrial and commercial settings where devices need to operate independently of human intervention. For instance, a manufacturing robot may communicate with a central controller to report operational status and request maintenance when needed. M2M is typically used in environments that require automation, continuous monitoring, and system optimization without human input [28].

7.2.6 Cloud-to-Device (C2D)

In Cloud-to-Device (C2D) communication, the cloud sends data, updates, or instructions to IoT devices. This pattern is commonly used when the cloud needs to control or update the operation of IoT devices. For example, a smart thermostat may receive a temperature adjustment instruction from the cloud based on weather predictions or user preferences. C2D communication ensures that devices can be managed remotely, allowing for dynamic changes to device behavior based on external conditions.

7.2.7 Broadcast Communication

Broadcast Communication is used when one device needs to send data to multiple devices at once. This is particularly useful in scenarios where many devices need to receive the same information simultaneously. For example, in a smart city application, traffic management systems might broadcast traffic alerts to all connected vehicles in a region. Broadcast communication helps disseminate critical information efficiently across a large number of devices, ensuring timely and synchronized responses.

These communication patterns are fundamental to the design and operation of IoT systems, determining how data is exchanged and processed. The choice of communication model depends on the specific needs of the IoT application, such as latency requirements, power constraints, and data volume.

8 Resource-Constrained Nature of IoT

The resource-constrained nature of Internet of Things (IoT) devices significantly influences their design and functionality. Many IoT devices utilize low-power microcontrollers with limited processing capabilities, restricting their ability to perform complex calculations or run resource-intensive applications. This constraint, coupled with minimal memory and storage capacity, necessitates the use of lightweight protocols and data formats for efficient communication and data handling, often relying on cloud-based solutions for extensive processing and storage. Additionally, power efficiency is a critical concern, especially for battery-operated devices, leading to trade-offs in performance and reduced data transmission frequency. Network connectivity challenges further complicate matters, as devices may operate in environments with variable network reliability, requiring robust protocols capable of functioning in low-bandwidth scenarios. Consequently, IoT devices face difficulties in managing high-bandwidth data transmissions, especially in environments requiring real-time data processing [29,30]. The lack of computational power exacerbates issues related to data transmission efficiency, as devices must optimize data packets to fit within the constraints of their bandwidth—the narrower the bandwidth, the more critical data minimization becomes [31]. These limitations necessitate the development of lightweight protocols and algorithms that can operate efficiently within the confines of these resources. For instance, Lian et al. discuss the importance of self-triggered control mechanisms that minimize unnecessary resource consumption, thereby extending the operational life of IoT devices. This method is mostly relevant in scenarios where IoT gadgets must balance responsiveness with energy efficiency. Traditional resource management strategies, which often rely on fixed rules and predefined policies, may not be effective in such dynamic environments. Instead, adaptive and context-aware resource management techniques are necessary to optimize performance across varied device capabilities and operational contexts. Lightweight cryptographic algorithms and scalable consensus mechanisms are being explored to enhance security without imposing significant computational burdens on devices. This is particularly important in applications such as the Internet of Medical Things (IoMT), where security and privacy are paramount [31,32]. IoT devices are often designed to operate under strict resource limitations, which can hinder their ability to implement traditional security measures. Limited resources available in IoT environments complicate the implementation of robust security protocols, leading to vulnerabilities during data aggregation and transport encryption [33], this is particularly concerning as IoT devices frequently handle sensitive information, making them lucrative targets to attackers. The resource-starved nature of many IoT devices makes it challenging to maintain reliable systems, as these devices are prone to errors and security issues. Efficient resource management is critical in addressing the challenges posed by the resource-constrained nature of IoT devices. Techniques such as data aggregation and in-network processing can significantly reduce the amount of data transmitted, thereby conserving bandwidth and energy [34].

9 Common Token Transmission Attacks in IoT Devices

Adversarial attacks mostly target the process of token exchange, especially when devices exchange tokens to verify their identities and grant access to resources. Due to the often-constrained nature of IoT devices—such as limited processing power, memory, and network security, attackers can exploit vulnerabilities in token transmission protocols. This section will explore these prevalent attack types, their potential impact on IoT ecosystems, and the challenges involved in safeguarding token exchanges in these resource-limited environments.

9.1 Replay Attacks

A replay attack is a network attack where a valid transaction in a network is maliciously or fraudulently repeated. A common target in these attacks is token transmission, where tokens are used to authenticate devices to servers or other systems. In a replay attack on token transmission, the attacker captures a legitimate token sent by an IoT device during communication with a server. This token could represent a digital signature, an authentication code, or a session identifier. Once captured, the attacker replays this token, often to impersonate the original device. Since many IoT systems do not have strong mechanisms to differentiate between new and replayed tokens, the server may accept the replayed token as valid, granting the attacker access to sensitive systems or data. For example, an attacker might intercept the token used to unlock a smart home device and reuse it to gain unauthorized access to the property. This can lead to unauthorized access, data forgery, and various other malicious activities, particularly in resource-constrained environments typical of IoT systems. The vulnerability of IoT devices to replay attacks is underscored by the fact that many systems transmit data in plaintext, making them susceptible to interception and misuse. For instance, Hwang and Lee highlight that unprotected communications in large network systems, such as Industrial IoT (IIoT), can result in substantial financial losses due to data forgery and replay attacks [35]. The implications of such attacks are particularly concerning in the context of IoT, where devices often operate with limited computational resources and may lack robust security mechanisms.

9.2 Token Hijacking

Token hijacking typically occurs when an attacker intercepts a token during its transmission between the IoT device and a server or other device. This can happen due to weak security protocols or unencrypted communications, which are common vulnerabilities in IoT systems because of their limited computing power and energy constraints. Many IoT devices rely on lightweight protocols, making them easier targets for attackers. The reliance on token-based authentication in IoT systems makes them vulnerable to various attacks, including session hijacking and unauthorized access. When an attacker successfully hijacks a token, they can impersonate legitimate devices, leading to unauthorized operations and data breaches [1,2]. This vulnerability is exacerbated by the resource-constrained nature of many IoT devices, which often lack robust security measures [2]. The implications of token hijacking extend beyond individual devices to the broader IoT ecosystem. For instance, compromised devices can be integrated into botnets, facilitating large-scale Distributed Denial of Service (DDoS) attacks that disrupt services and compromise network integrity [36]. These attacks can leverage hijacked devices, such as routers and cameras, to amplify their impact, making it crucial to develop effective countermeasures. The interconnectedness of IoT devices means that the failure of one device can lead to cascading failures across the network, highlighting the need for comprehensive security strategies.

Conventional devices are usually secure as compared to IoT devices because of traditional security practices as indicated in Table 4. This specifies the reason behind the drastic increase in IoT attack surface.

Table 4: A detailed analysis indicating why IoT is preferred over other devices for DDoS attacks

Parameter	Other devices	IoT devices
Maintenance	Servers require maintenance from the handler.	Minimal to no maintenance is required for IoT devices.

(Continued)

Table 4 (continued)

Parameter	Other devices	IoT devices
Security	Servers, laptops, and other similar devices are usually challenging to infect because of user awareness of security.	IoT devices may not be so user friendly and people tend to neglect the security of these devices because of ignorance making them more vulnerable to attacks.
Updates	Servers and similar devices are updated regularly and follow security protocols.	Firmware updates are rarely provided for IoT devices and also mostly these updates do not follow secure protocols resulting in insecure IoT devices.
Access	Power and internet services to these devices are limited: subsequently, access gained by the attacker also gets affected.	Often IoT devices work on very low power and remain connected to the internet for example CCTV, refrigerators, etc. This provides uninterrupted access to the attacker.

When an attacker gains access to these devices, they may transform them into bots; this group of devices is known as a botnet [37].

9.3 Man in the Middle Attacks

These attacks allow attackers to intercept, modify, or impersonate messages between devices without detection. MitM attacks are particularly concerning in IoT environments due to the reliance on wireless communication protocols, which are inherently susceptible to eavesdropping and interception. Research indicates that various types of attacks, including MitM, replay, and impersonation attacks, are prevalent in IoT systems, especially in applications such as e-commerce, healthcare, and data transmission [38]. The use of software-enabled access points (SoftAP) has further increased the risk of MitM attacks, as attackers can easily position themselves between the IoT devices and their intended communication endpoints [39]. The MQTT protocol, commonly used in IoT communications, is also vulnerable to MitM attacks. Attackers often target central communication devices, such as brokers, to intercept messages. This vulnerability is compounded by the fact that many IoT devices utilize outdated or inconsistent encryption standards, which can facilitate downgrade attacks and further expose the system to MitM threats [40]. Many IoT devices utilize protocols that are not designed with robust security features, such as the Modbus Transmission Control Protocol, which is commonly used in smart grids and industrial IoT applications. These protocols can be vulnerable to various kinds of cyber attacks, including IP spoofing and ARP poisoning, which facilitate MITM attacks [41].

9.4 Token Injection

Token injection attacks on token transmission in IoT (Internet of Things) devices refer to security vulnerabilities where malicious actors insert unauthorized tokens or manipulate legitimate tokens during communication between IoT devices and their network. As highlighted by Xiao, the use of access tokens can lead to token compromise attacks, where attackers can steal tokens and impersonate devices to perform malicious operations [2]. This vulnerability is exacerbated by the resource-deprived nature of many IoT gadgets, which limits their ability to implement complex security measures. Furthermore, the study by Purnama emphasizes the importance of secure access control mechanisms, noting that encrypted token theft

remains a critical concern in IoT environments [42]. As highlighted by Muzammil et al., these attacks can effectively sever the original communication line and establish a new one, enabling the attacker to overhear sensitive conversations, including the transmission of access tokens [43]. The critical nature of the attack stems from its ability to compromise the integrity and confidentiality of the transmission, potentially allowing the attacker to impersonate the legitimate user or device.

In the context of emerging technologies such as the Internet of Things (IoT), the risks associated with MitM attacks are pronounced. Fereidouni et al. point out that IoT systems are particularly vulnerable to such threats, where devices often use insecure protocols for token transmission. Their research confirms that weaknesses in IoT infrastructure can be exploited by MitM attacks, making these systems especially precarious [44].

9.5 Crossing Requests in IoT

Crossing request attacks on token transmission in IoT devices involve manipulating or exploiting concurrent requests to mislead or compromise the system's handling of tokens. It is often related to Cross-Site Request Forgery (CSRF) or Cross-Site Scripting (XSS) in web applications but adapted for IoT contexts. In a crossing request attack, the attacker manipulates two or more concurrent token transmission processes. This could involve sending unauthorized requests alongside legitimate ones or exploiting how a system processes multiple requests simultaneously. The goal is to either inject a malicious token while a legitimate one is being processed or confuse the system into treating an unauthorized request as legitimate by leveraging a valid session or token or both. This type of attack can lead to unauthorized access and data breaches [45].

9.6 Eves Dropping

Eavesdropping attacks on token transmission in IoT devices involve interception between IoT devices and their network or backend servers to steal or monitor tokens being transmitted. These attacks take advantage of unencrypted or poorly secured communication channels to gain access to the tokens in transmission, which are often used for authentication, session management, or authorization. This can allow the attacker to gain unauthorized access to the system. The literature highlights that IoT devices, often operating with limited computational resources, are particularly susceptible to such attacks, as they may lack robust security protocols to protect against eavesdropping and other forms of intrusion [46]. The Mirai malware incident exemplifies the risks associated with eavesdropping in IoT environments, where compromised devices were used to launch distributed denial-of-service (DDoS) attacks, illustrating how attackers can exploit vulnerabilities in token transmission to gain unauthorized access to networks [46]. Furthermore, the physical accessibility of many IoT devices allows attackers to easily intercept communications, thereby facilitating eavesdropping attacks that can compromise the integrity and confidentiality of data being transmitted [47]. The research by Yang et al. emphasizes that when attackers infiltrate factory networks, they can manipulate data transmission, thereby compromising the entire operational environment [12].

9.7 Brute Force

Brute force attacks on token transmission in IoT devices involve attackers systematically attempting to guess or compute valid tokens used for authentication, session management, or access control. It involves systematically attempting all possible combinations of passwords or tokens until the correct one is found [48]. This type of attack targets weak token generation methods, such as predictable or short tokens, allowing attackers to flood the system with multiple token guesses in hopes of finding a valid one. IoT devices frequently utilize various communication protocols, including File Transfer Protocol (FTP), which may be improperly configured, thereby exposing them to brute-force attacks. Moreover, the reliance on SMS-based

authentication for IoT devices has been criticized for its inherent vulnerabilities. Research indicates that such systems can be easily manipulated, allowing attackers to gain control over devices without needing to analyze firmware directly [1]. For instance, the integration of two-factor authentication schemes has been proposed as a viable solution to enhance security in IoT environments. These schemes can greatly reduce the risk of unauthorized intrusion by requiring additional verification steps beyond simple password entry.

The communication between IoT devices and their companion applications is often inadequately secured, which can facilitate token transmission attacks in IoT devices [1]. Many companion apps do not implement proper encryption or authentication measures, allowing attackers to intercept and manipulate data transmissions. Fig. 6 displays a clustered bar chart displaying the Privacy and Security Publication Statistics on IoT from IEEE, Springer, and Elsevier. Each document type (Books, Journals, Series, Web Pages) is represented by the number of publications related to both privacy and security concerns in IoT, categorized by publisher.

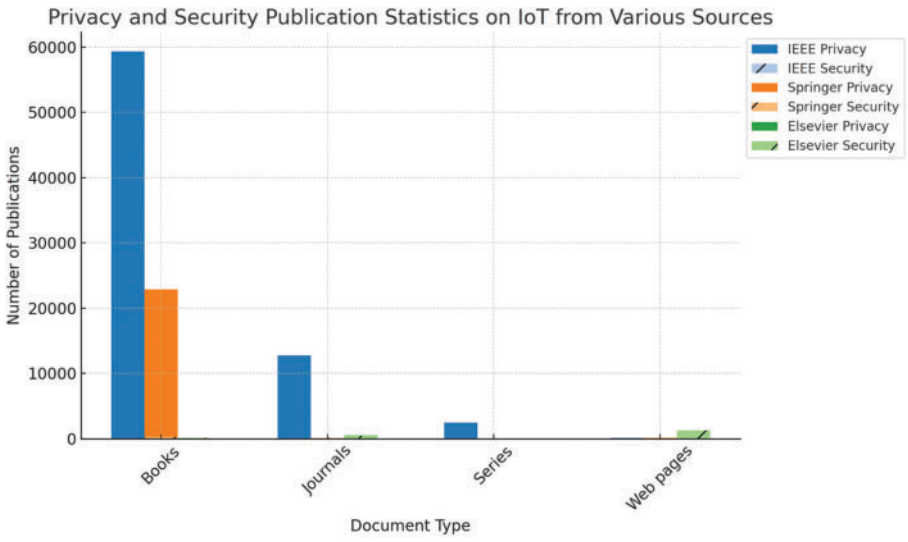

Figure 6: Privacy and security publication statistics on IoT from various sources

Key Observations:

Books have the highest publication count, especially under IEEE and Springer, with privacy concerns dominating.

Journals show moderate publications for privacy with smaller counts in security, mainly from Elsevier.

Web pages (for Elsevier) show a balanced interest in both privacy and security concerns [49]. In addition, Table 5 below illustrates a summary of other contributions and insights drawn from other research papers that have contributed to this survey.

Table 5: Contributions and insights drawn from other research papers

Journal article	Results	Applications	conclusions	Methods used	Contributions
1. IoT: Internet of Threats? A Survey of Practical Security Vulnerabilities in Real IoT Devices [50]-IEEE Internet of Things Journal	Overview of security risks in the IoT sector	Personal health care Environmental monitoring.	Low-end IoT devices lack strong security mechanisms.	Overview of security risks in the IoT sector.	Overview of security risks in the IoT sector.

(Continued)

Table 5 (continued)

Journal article	Results	Applications	conclusions	Methods used	Contributions
	Analysis of attacks against real IoT devices	Home automation Smart mobility Industry 4.0.	Security should be integral in IoT system design.	Analysis of attacks against real IoT devices Save.	Analysis of attacks against real IoT devices.
2. Security of Wireless Embedded Devices in the Real World [51].	Cryptographic keys can be recovered from various tokens.	Access control and identification applications.	Key extraction from cryptographic tokens is feasible.	Analysis of commercial products for cryptographic key recovery.	• Analyzes security of various wireless embedded devices. • Demonstrates feasibility of recovering secret cryptographic keys.
	Key extraction impacts security of contactless applications.	Contactless payments and public transport systems.	Security implications for contactless applications are significant.	Examination of implications of key extraction on security.	The paper illustrates key extraction attacks on electronic passports, KeeLoq systems, and Mifare-based applications, demonstrating significant vulnerabilities that compromise the security of contactless applications in real-world scenarios.
3. Analysis of IoT Networks Security: Threats, Risks, ESP8266 based Penetration Testing Device and Defense Framework for IoT Infrastructure [52].	Introduces ESP8266 NodeMCU for IoT penetration testing.	ESP8266 NodeMCU prototype for penetration testing.	IoT networks require comprehensive security measures against vulnerabilities.	Deauthentication attacks on IoT devices.	• Introduces ESP8266 NodeMCU prototype for penetration testing. • Highlights de-authentication attacks as a security measure.
	Highlights the need for comprehensive IoT security measures.	Deauthentication attacks on IoT devices.	ESP8266 prototype aids in penetration testing for IoT devices.	Passive scanning methods for penetration testing.	
4. Anatomy of attacks on IoT systems: a review of attacks, impacts, and countermeasures [53]. 01 January 2022-Journal of surveillance, security and safety.	Identified and categorized IoT attacks and assets.		Describes IoT components and attack anatomy clearly.	Review of IoT layered representation and functional components.	• Review of IoT attacks and their impacts. • Evaluation of countermeasures against IoT security threats.
	Evaluated counter measures' effectiveness against IoT threats.		Evaluate counter measures' effectiveness against IoT assets and attacks.	Categorization of at tacks and mapping against targeted assets.	
5. Security threats in IoT [54].	Discusses vulnerabilities and security challenges in IoT devices.		IoT devices vulnerable to cyber-attacks due to security deficiencies.	Vulnerabilities and security challenges of IoT devices are discussed.	• Discusses vulnerabilities and security challenges of IoT devices. • Provides implementation and analysis of IoT-oriented attacks and security solutions.
	Analyzes IoT attacks and proposes security solutions.		Lightweight security models are needed for resource-constrained IoT devices.	Implementation, analysis of IoT attacks, and security solutions presented.	
6. Lightweight Authentication Mechanism for Industrial IoT Environment Combining Elliptic Curve Cryptography and Trusted Token [12].	73% efficiency improvement with lightweight elliptic curve cryptography.	Authentication mechanism for terminal IoT devices and backend servers.	The proposed mechanism combines elliptic curve cryptography and tokens for identity authentication.	Authentication mechanism based on elliptic curve cryptography and trusted tokens.	• Authentication mechanism using elliptic curve cryptography and trusted tokens. • Ensures data transmission from legitimate devices, preventing false data transmission.
	Effective protection against various network attacks with mutual authentication support.	Data transmission security in industrial IoT environments.	The mechanism provides mutual authentication and enhanced protection for overall identity verification.	Packet encryption using the TLS protocol to ensure data confidentiality.	

(Continued)

Table 5 (continued)

Journal article	Results	Applications	conclusions	Methods used	Contributions
7. A First Step Towards Understanding Real-world Attacks on IoT Devices [55].	Real-world attackers target IoT devices specifically. Captured activities include direct human interaction.	Building a honeypot ecosystem for IoT devices. Developing Honeycamera for IoT camera interactions.	Real-world attackers target IoT devices specifically. The honeypot ecosystem aids in understanding attack behaviors.	Building a honeypot ecosystem for IoT devices. Deploying low-interaction honeypots to attract attackers.	• Developed a honeypot ecosystem for IoT attack data. • Created Honeycamera for simulating real video interactions. • Building a comprehensive honeypot ecosystem for IoT devices. • Understanding attacker behaviors targeting IoT systems.
8. Security Attacks on IoT [55].	Identified common IoT security attacks and their implications. Suggested precautions across IoT layers to enhance security.	IoT applications monitor, control, and track object states. Applications enable interaction between users and IoT devices.	IoT lacks a complete layer structure; three layers are accepted. Common security attacks include Botnet, Man in the Middle, and Denial of Service.	Examples and analyses of common IoT security attacks. Recommendations for precautions in IoT layers. Save	• Application of security measures in IoT layers. • Methods for implementing IoT security precautions.
9. Security Analysis and Prevention of Attacks on IoT Devices [56].	The proposed system prevents common IoT attacks using MAC addresses. Focus on preventing DoS and DDoS attacks.	Prevention of DoS and DDoS attacks on IoT devices. Security enhancement using MAC address-based protection.	The proposed system prevents attacks targeting IoT devices. Future research work can be done.	Prevention of attacks using MAC addresses. Focus on DoS and DDoS attack prevention. Save	
10. Internet of Things (IoT): Taxonomy of security attacks [57].	Taxonomy of IoT security attacks constructed. Aids developers in understanding security risks.	Smart home applications Healthcare and transportation domains	Security in IoT is vital for sensitive operations. Taxonomy assists developers in understanding security risks.	Studies network security in smart homes, health care, and transportation. Constructs taxonomy of security attacks for IoT networks. Save	• Studies network security in smart home, healthcare, and transportation domains. • Constructs taxonomy of security attacks for IoT developers. • Security aspects in smart homes, health care, transportation. • Enhancing protections against IoT security flaws.
11. SmartPatch: Verifying the Authenticity of the Trigger Event in the IoT Platform [58].	Faked 7 events, and impacted 138 SmartApps. Developed SmartPatch to secure SmartThings systems.	Developed tool SmartPatch to automatically patch vulnerable SmartApps and Device Handlers.	Proposed authenticity-verification-based scheme to deny fake events.		Authenticity-verification-based scheme to deny fake events. SmartPatch tool for patching vulnerable SmartApps and Device Handlers. Save

(Continued)

Table 5 (continued)

Journal article	Results	Applications	conclusions	Methods used	Contributions
12. TTAS: Trusted Token Authentication Service for Securing SCADA Networks in Energy Management Systems for Industrial Internet of Things [59].	SCADA system using Modbus protocol has security vulnerabilities.	Trusted Token Authentication Service for SCADA systems.	Proposed Encryption and verification mechanism based on trusted token authen tication service and TLS protocol.		Trusted token authentication service
	Encryption and verification mechanism effectively protects against vulnerabilities.	Security and authentication in Industrial Internet of Things.	Mechanism effectively improves SCADA network security.		Transport Layer Security (TLS) protocol
13. Lightweight ECC and token-based authentication mechanism for WSN-IoT [60].	Lightweight ECC enhances security in WSN-IoT communication.	Wireless Sensor Networks in specific IoT applications.	Lightweight ECC and token-based authentication mechanism proposed		Elliptic Curve Cryptography (ECC) for secure communication.
	The token-based mechanism prevents unauthorized network access.	Secured and authenticated communication for network access.	Elliptic curve cryptography used to remove malicious nodes.		Token-based Security Scheme for authentication.
14. IoT-Based Smart City: Security Issues and Tokenization, Pseudonymization, Tunneling Techniques used for Data Protection [61].	Highlights challenges and solutions of applying IoT in a Smart City.	Smart healthcare, parking, waste management, water supply.	IoT-based smart cities can improve the quality of life.		The paper discusses the challenges and solutions of applying IoT technologies in smart cities.
International Journal of Trend in Scientific Research and Development	Addresses security issues and data protection techniques in Smart City.	Enhancing urban life quality in smart cities through IoT applications.	Security and privacy concerns need to be addressed.		It highlights the benefits and applications of IoT in healthcare, parking, waste management, and water supply.
15. Enhancing IoT Security Through Experimental Methods and Blockchain Integration [62].	Explored denial-of-service attacks on smart home networks.	Healthcare.	IoT requires enhanced connectivity and robust data security.		Experimental attack simulations.
	Investigated mining, transaction processing, and blockchain chaining in cryptocurrencies.	Smart cities.	Comprehensive strategies are essential for secure IoT deployment.		Integration of blockchain technology Save.

9.8 Side-Channel Attack

In a side-channel attack, the attacker monitors physical or behavioral aspects of the IoT device or its communication environment while tokens are being generated, transmitted, or validated. These attacks often exploit vulnerabilities in hardware or software implementations of cryptographic processes, where devices unintentionally emit signals that reveal partial or full information about the token or cryptographic keys.

1. Timing Attacks: An attacker measures the time it takes for an IoT device to process a token or cryptographic operation. By carefully observing how long different operations take, they can deduce parts of the cryptographic key or token being transmitted.

2. Power Analysis Attacks: By measuring the power consumption of an IoT device while it processes tokens, an attacker can extract patterns that correspond to specific operations, helping to reconstruct cryptographic keys or other sensitive data.
3. Electromagnetic Emissions: Some IoT devices emit electromagnetic signals while performing computations, including token generation or validation. Attackers with the right equipment can capture these emissions and use them to infer the token or cryptographic operations.
4. Fault Injection Attacks: Attackers deliberately introduce small faults (such as voltage spikes, electromagnetic pulses, or laser pulses) into the IoT device to cause it to behave abnormally. This may cause the device to leak critical information about tokens or cryptographic processes.

One of the primary concerns regarding Side-Channel Attacks (SCAs) is their ability to compromise token-based authentication mechanisms. Myridakis et al. highlight that SCAs can be employed to analyze power dissipation patterns, which can reveal critical information about the cryptographic operations performed by IoT devices [63]. This risk is compounded in IoT environments where devices often communicate over insecure channels, making them susceptible to interception and manipulation. The vulnerabilities inherent in IoT devices, often due to their limited computational resources and simplistic designs, make them particularly susceptible to such attacks [63,64].

The mechanisms of side-channel attacks can be broadly categorized into two types: those targeting symmetric key algorithms and those targeting asymmetric key algorithms. In both cases, attackers analyze variations in power consumption or electromagnetic emissions while the device processes cryptographic operations. For instance, power analysis attacks can reveal the encryption keys by observing the power fluctuations during the encryption process [65]. This highlights the necessity for robust countermeasures, such as randomized voltage regulation systems that can obscure the power consumption patterns of IoT devices, thereby complicating the attacker's ability to glean sensitive information [66].

A comparison table that outlines the similarities and differences among common token transmission attacks in IoT devices (Table 6):

Table 6: A comparison table that outlines the similarities and differences among common token transmission attacks in IoT devices

Attack type	Description	Goal	Method	Common targets	Similarities	Differences
Replay attack	Malicious actor captures and replays a valid token to gain unauthorized access.	Reusing a captured token to authenticate without detection.	Intercepting token transmission and sending it later.	IoT devices, communication channels	All attacks involve unauthorized access or disruption of token transmission.	Relies on capturing and reusing tokens without modification, unlike other attacks.
Token hijacking	Attacker steals a valid token from a legitimate user or device.	Stealing tokens to impersonate legitimate devices.	Gaining access to tokens through vulnerabilities in communication or storage.	IoT devices, communication protocols	All attacks manipulate or interfere with token transmission.	Focuses on stealing a token in use, while others may focus on creating fake tokens or intercepting data.

(Continued)

Table 6 (continued)

Attack type	Description	Goal	Method	Common targets	Similarities	Differences
Man-in-the-Middle (MITM)	Attacker intercepts and potentially alters communication between two parties.	Intercepting and modifying token exchanges.	Intercepting, reading, and/or modifying messages between devices to steal or alter tokens.	IoT devices, network connections	Involves unauthorized interception of communication, common with many attacks.	Involves both interception and modification of token data.
Token injection	Attacker sends a malicious token or fake token to a target.	Injecting a fraudulent token to gain unauthorized access.	Inserting a fake or modified token into the system to authenticate as a legitimate user/device.	IoT devices, API servers	All attacks aim to compromise the authenticity of tokens.	Focuses on injecting new or altered tokens, while others hijack or reuse existing tokens.
Cross-Site Request Forgery (CSRF)	Attacker forces a user to send an unwanted request that includes an authentication token.	Use of a user's credentials without consent.	Trick a user into sending requests, often with malicious tokens embedded in the request.	Web-based IoT interfaces, user authentication processes	All exploit vulnerabilities in token-based authentication systems.	Relies on user interaction, unlike other attacks that exploit communication or token interception.
Eavesdropping	Attacker listens in on unsecured communications to capture tokens.	Collecting sensitive token data during transmission.	Intercepting communication (e.g., unencrypted traffic) to extract tokens.	IoT devices, insecure communication channels	All attacks involve unauthorized observation or manipulation of tokens.	Primarily focuses on listening to token transmission rather than manipulating or reusing them.
Brute force	Attacker systematically guesses tokens or passwords to gain access.	Exhausting possible token combinations until the correct one is found.	Attempting many possible token values until successful authentication is achieved.	IoT devices, weak token/password systems	All attacks involve attempting to bypass authentication.	Requires guessing tokens or credentials, while others manipulate token transmission directly.
Side-channel attack	Attacker gathers information from indirect sources, like power or timing data.	Extracting secret information (tokens, keys) from indirect channels.	Analyzing side-channel information (e.g., power consumption, electromagnetic leaks) to retrieve tokens.	Encrypted devices, IoT sensors	All attacks aim to compromise authentication mechanisms.	Involves indirect data extraction, unlike other attacks that focus directly on token transmission.

Token transmission attacks in IoT systems—such as replay attacks, token hijacking, man-in-the-middle (MITM) attacks, token injection, crossing requests, eavesdropping, brute force, and side-channel attacks—share a common goal: compromising the security of authentication and authorization mechanisms as depicted in Table 6. These attacks typically target the confidentiality, integrity, or validity of tokens transmitted between IoT devices and services. Most of them exploit weak or unencrypted communication channels, poor token management, or insufficient validation practices. They often result in unauthorized access, data leakage, or disruption of services. Despite these similarities, they differ in method and complexity. For instance, replay and token injection attacks are relatively simple and focus on reusing or manipulating valid tokens, whereas MITM and side-channel attacks are more sophisticated, involving interception or physical analysis. Some attacks, like brute force and token hijacking, operate over networks without requiring direct device access, while side-channel attacks often demand physical proximity to the device. Passive attacks like eavesdropping contrast with active ones like brute force or injection, highlighting the diverse nature of threats in IoT environments.

10 Other Security Challenges in IoT

One of the primary security challenges in IoT devices is the management of privacy and access control. As noted by Dodson et al., manufacturers must adhere to best practices in security throughout the lifecycle of their devices, which includes understanding the security and privacy risks associated with their products [67]. This is echoed by Gebresilassie et al., who highlight the inadequacies of existing identity management systems that rely on centralized authorities, which can lead to identity theft and other security breaches [68]. The dynamic nature of IoT environments complicates these challenges, as devices often operate in unstandardized and diverse ecosystems, making consistent security enforcement difficult [69]. Ahmed points out that various communication protocols used in IoT networks, such as Wi-Fi and Bluetooth, are susceptible to attacks. The vulnerability is further exacerbated by the lack of robust security features in many low-end IoT devices, as highlighted by the findings of the ASM project, which indicates that many commercial devices fail to provide even basic security services [70]. Many IoT devices are designed with minimal processing power and memory, which restricts their ability to implement robust security measures. This often leads to poor security practices, such as the use of default passwords and lack of firmware updates, making them susceptible to various attacks [71]. The rapid proliferation of IoT devices has exacerbated these vulnerabilities; for instance, it was reported that over 8.4 billion IoT devices were connected to the internet as of 2017, creating a vast attack surface for cybercriminals [72]. Further, the "functionality first, security second" mentality prevalent in IoT device development contributes to the introduction of insecure devices into networks, which has been linked to significant denial-of-service (DoS) attacks [72]. In addition to device-level vulnerabilities, the IoT ecosystem faces significant challenges related to data security and privacy. The interconnected nature of IoT devices means that a breach in one device can compromise the entire network, leading to unauthorized access to sensitive data and disruption of services [73]. The lack of standardized security protocols further complicates the situation, as different devices may employ varying levels of security, making it difficult to establish a cohesive security framework. Table 7 shows a summary of other common security attack types with their descriptions of IoT devices.

Relationship between other security challenges and token transmission attacks.

Table 7: Summary of other common security attack types with their descriptions of IoT devices

Attack type	Main goal	Method of attack	Focus	Impact on token transmission	Similarities	Differences
Sinkhole attack	Claim significant resources and mislead the network.	Redirect network traffic to a malicious node.	Misleading the network by rerouting traffic.	Indirectly impacts token transmission by misdirecting traffic.	Disrupts network traffic and potentially intercepts token data.	Focuses on network disruption, not directly on token manipulation.
Black hole attack	Send replay messages to the source node.	Replay previously intercepted data to the source.	Intercept and replay network messages.	Directly impacts token transmission by replaying intercepted tokens.	Both involve intercepting and manipulating messages.	Focuses on replaying intercepted messages, unlike others that may inject or modify tokens.
Wormhole attack	Create a fake tunnel between two malicious nodes.	Establish a fake tunnel between two locations to forward data.	Malicious nodes intercept and forward messages.	Directly impacts token transmission by altering communication paths.	Both involve network manipulation that can intercept or modify token communication.	Focuses on creating an artificial communication path, different from direct token hijacking or injection.
Sybil attack	Pretend the identities of multiple IoT devices.	Generate fake identities (nodes) within the network.	Masquerading as multiple devices to manipulate the network.	Directly impacts token transmission by impersonating legitimate devices.	Both impersonate legitimate devices to gain access, similar to token hijacking.	Focuses on identity theft, unlike attacks that focus on stealing or modifying tokens.
DoS attack	Disrupt the availability of network services.	Overwhelm the target node with excessive traffic.	Prevent normal communication by overwhelming resources.	Indirectly impacts token transmission by causing network congestion.	Both focus on disrupting normal communication flow.	Focuses on denial of service, rather than direct interception or manipulation of tokens.
Node capture attack	Capture a node and gain full control over it.	Physically or virtually capture a node to steal information.	Capture a device to manipulate or extract data.	Directly impacts token transmission if tokens are stored in the captured device.	Both attack device control to steal or manipulate data.	Focuses on gaining control of a device, unlike attacks that intercept data during transmission.
Node injection attack	Deploy malicious nodes into the network.	Inject rogue nodes into the network to manipulate communication.	Add malicious nodes that affect data or token integrity.	Directly impacts token transmission by injecting fake tokens.	Both involve adding malicious entities to the network to disrupt token transmission.	Focuses on inserting fake nodes, while others may target existing communication channels.
RFID spoofing attack	Imitate valid RFID tag information.	Fake an RFID tag to impersonate a legitimate device.	Steal or spoof RFID identity information.	Directly impacts token transmission by impersonating an RFID tag.	Both involve impersonating legitimate devices or users to gain access.	Specific to RFID systems, whereas other attacks may be more general in scope (IoT or network-wide).

(Continued)

Table 7 (continued)

Attack type	Main goal	Method of attack	Focus	Impact on token transmission	Similarities	Differences
RFID cloning attack	Clone valid RFID tag information.	Duplicate an existing RFID tag to impersonate it.	Duplicate a valid RFID tag to impersonate its identity.	Directly impacts token transmission by cloning an RFID tag.	Both involve impersonating RFID devices to bypass security.	Focuses on duplicating tags, whereas other attacks may involve impersonation or interception.
RFID sniffing attack	Intercept data transfer in RFID networks.	Capture RFID communication signals and decode data.	Listen to communication between devices to capture information.	Directly impacts token transmission by capturing tokens.	Both involve intercepting data in transit.	Specific to RFID systems, unlike others which focus on IoT or network-wide communications.
MITM attack	Intercept and modify the communication between two parties.	Intercept, read, and alter communication messages.	Intercept and possibly alter messages between two parties.	Directly impacts token transmission by modifying or stealing tokens.	Both intercept communication between parties to steal or modify data.	Focuses on altering communication between two entities, unlike others that focus on impersonation.
Code/Fragment injection	Inject malicious code or fake fragments into the network.	Insert malicious code or packets to disrupt communication.	Inject harmful data fragments to compromise network communication.	Directly impacts token transmission by injecting fake or malicious data.	Both manipulate the communication stream to affect token integrity.	Focuses on injecting malicious fragments or code into communication, unlike other attacks targeting tokens.
Eavesdropping attack	Secretly intercept communication to capture data.	Listen to and intercept data being transmitted without detection.	Capture network traffic to extract sensitive data.	Directly impacts token transmission by intercepting and capturing tokens.	Both intercept and capture communication to steal data.	Focuses on passive listening without altering or injecting data.
Brute force attack	Attempt to guess or crack the correct key or token.	Try multiple combinations to guess the correct key/token.	Exhaustive attempts to guess passwords or tokens.	Indirectly impacts token transmission by attempting to guess valid tokens.	Both target authentication systems, seeking to bypass them.	Focuses on guessing tokens through trial and error, unlike others that intercept or impersonate tokens.
Encryption key attack	Extract the key used for encrypting/decrypting data.	Extract or guess the encryption key to decrypt data.	Attempt to retrieve the encryption key to access protected data.	Indirectly impacts token transmission by decrypting protected tokens.	Both attack security measures protecting token transmission.	Focuses on breaking encryption to access tokens, unlike others which manipulate tokens directly.

The attacks discussed share several commonalities, primarily their goal of gaining unauthorized access to data, credentials, or devices. Many exploit vulnerabilities in communication channels, aiming to intercept, redirect, or modify tokens or other sensitive information. Attacks like Sybil, RFID Spoofing, and Node Injection often focus on impersonating devices or users, while MITM, Eavesdropping, and Brute Force

attacks target the token or authentication mechanisms themselves. These attacks can either disrupt network infrastructure (e.g., DoS, Sinkhole) or compromise the security measures protecting token transmission (e.g., Encryption Key Attacks). The direct impact on token transmission is seen in attacks like MITM and Eavesdropping, where tokens are intercepted or modified, while others such as DoS or Brute Force exert indirect influence by blocking legitimate communication or attempting to crack credentials. In summary, while these attacks may target different layers of the network or communication process, they all ultimately aim to undermine the security of token-based authentication systems in IoT networks. Wireless IoT technologies are crucial for enabling communication in the Internet of Things ecosystem, offering low-power, wide-area, and short-range connectivity options. These technologies include ZigBee, Bluetooth Low Energy (BLE), 6LoWPAN, and LoRaWAN, each designed for specific IoT applications like home automation, industrial monitoring, and smart cities. Despite their advantages, they are vulnerable to various security threats. Common attacks on these wireless protocols include Denial of Service (DoS), Man-in-the-Middle (MITM) attacks, eavesdropping, encryption key vulnerabilities, and code injection, among others as illustrated in Table 8.

Table 8: Summary of common security threats towards IoT common communication protocols

Wireless technology	Security attacks
ZigBee	sinkhole, Encryption key, code injection, DoS
BLE (Bluetooth Low Energy)	MTM, DoS, brute force, Eavesdropping
6LoWPAN (IPv6 over Low Power Wireless Personal Area Networks)	Fragment injection, sinkhole, blackhole, Sybil, DoS
LoRaWAN (Long Range Wide Area Network)	Encryption key, DoS, MTM (Man-in-the-Middle)

11 Real-World Examples of Token Attacks in IoT

Real-world token attacks in IoT devices have emerged as a critical concern, where malicious actors exploit vulnerabilities to intercept, replicate, or manipulate tokens, gaining unauthorized access to sensitive data and control over connected devices. This subtopic explores prominent instances of token-related attacks in IoT environments, highlighting the methods employed by attackers and the consequences of such breaches.

11.1 Carna Botnet

One notable instance is the Carna botnet, discovered in 2012 and highlighted the widespread issue of default and weak passwords in IoT devices. This botnet scanned the internet and identified over 1.2 million devices that allowed logins with empty or default credentials, effectively demonstrating how attackers can exploit token-based authentication systems that lack robust security measures. The implications of such vulnerabilities are profound, as they enable attackers to gain unauthorized access to a vast array of IoT devices, leading to potential data theft and manipulation. In addition to these examples, the Denial-of-Sleep attack represents a specific type of token attack where adversaries exploit wake-up tokens used by energy-constrained IoT nodes. By continuously sending wake-up tokens, attackers can deplete the device's battery, rendering it inoperative

11.2 The Mirai Botnet Attack

In 2016, the Mirai botnet launched a huge Distributed Denial of Service (DDoS) attack against Dyn, a significant DNS provider, using compromised IoT devices. Twitter, Netflix, Reddit, and many other well-known websites were unavailable due to this attack.

By taking advantage of IoT devices' weak default passwords, the Mirai software transformed them into a remotely controllable botnet. This attack demonstrated the flaws in IoT devices and the possibility of token-related attacks once attackers take control of them, even if its main goal was to interfere with services rather than steal tokens. The malware's operational model involves scanning the internet for devices with default usernames and passwords, enabling easy compromise. Once compromised, these devices can be orchestrated to perform coordinated actions that contribute to massive DDoS attacks, such as the one launched against Dyn [74].

One may argue that the Mirai bot is the ancestor of the IoT bots that are currently in use. This is because the majority of bots are disseminated following the publication of the Mirai bot's source code. The Mirai bot targets any Internet of Things device with an exposed Telnet port and a Linux operating system. The Mirai bot first used the Linux OS to infiltrate Internet of Things devices. But since then, it has broadened the scope of its operations to encompass other operating systems, indicating the possibility of extensive cyberattacks utilizing Internet of Things devices [75]. The first step uses D3FEND's detection technique to check if a pre-mapped log is generated. If the log is generated, the second step in the protection process is to isolate the IoT device that generated it to a different network. Using the log collected during the observation, the third stage determines if the device has been infected by the Mirai bot. To eliminate the malware and lift the network isolate, continue to the fourth step if an infection has been verified. Lastly, fortify the account using the log found in the first step to eradicate the root cause of the malware problem. Response to a Mirai bot is made possible by this defense mechanism. In smart cities, security guards can identify tactics at specific times—and when to exchange defense strategies with other infrastructure. To counter the Mirai bot, the defense procedure is created with elements used at each stage, as shown in Table 9 below.

Table 9: Example of application of Mirai bot defense technique through the defense process

Defense process	Mirai botnet phase	Sysmon log	MITRE ATT&CK techniques	DEFEND tactics	DEFEND technique
1	Intrusion	Event ID 3	Brute force	Detection	Script Execution Analysis, etc.
2	C&C propagation attack	Event ID 1, Event ID 3	Ingress tool transfer, Exploitation of remote services, Network denial of service	Isolate	DNS allow listing, DNS denylisting, broadcast domain isolation, etc.
3	C&C propagation	Event ID 1, Event ID 3, Event ID 11, Event ID 22	Brute force, Exploit public-facing application	Deceive	Connected honeypot, Decoy file, Decoy network resource, etc.
4	C&C propagation attack	Event ID 1, Event ID 3	Brute force, Exploit public-facing application	Evict	Process termination, Account locking

(Continued)

Table 9 (continued)

Defense process	Mirai botnet phase	Sysmon log	MITRE ATT&CK techniques	DEFEND tactics	DEFEND technique
5	–	Event ID 3	Brute force, Exploit public-facing application	Harden	Strong password policy software

The following are the Mirai botnet formation phases:

1. Target Scan: Use ports 23 and 2323 to generate a random IP address and look for running Telnet services.
2. Intrusion: Using pre-set default credentials, launch a dictionary attack against the Telnet service.
3. C&C: Use information about IoT device architecture to download and execute more malware.
4. Propagation: The IoT devices scan the network for susceptible IoT devices and spread the malware appropriately after sending the infection status to the reporting server.
5. DDoS attack: Use the received attack option to launch a DDoS attack after receiving an attack command via C&C.

11.3 Mozi Botnet Case Study

Network gateways and digital video recorders are among the IoT devices infected by the Mozi bot, a botnet that exploits networks like BitTorrent. Mozi repurposed the Gafgyt bot's source code that had been previously distributed. A P2P botnet made up of nodes that traverse a Distributed Hash Table (DHT) is the Mozi bot. Because it passes through DHT disguised as regular traffic, it becomes challenging to track. Furthermore, there are two categories into which Mozi bot's IoT device penetration technique can be separated. A dictionary attack is carried out if the remote port on Telnet is open, and if it is unsuccessful, it uses an IoT device's weakness to gain access. Malicious activities like DDoS attacks and token data leaks will be carried out if the intrusion is successful [75].

The Mozi botnet's formation phases are as follows:

1. Target Scan: Determine the attack target (an Internet of Things device) by using the Transmission Control Protocol (TCP) Synchronization (SYN) Reply.
2. Intrusion: Use HTTP command injection or launch a dictionary attack on the telnet port to get access to the IoT device.
3. Load: Makes a connection to a pre-designated server, after which malware is downloaded and run to carry out actual malicious operations.
4. C&C: After the P2P network has been registered, check it periodically to update the configuration file and the list of nearby nodes.
5. Propagation: Constant spread via intrusion detection and device scanning tools.
6. Attack: Get a command from an attacker and carry out an attack using that command.

The first step uses D3FEND's detection technique to see if a pre-mapped log is generated. The defense process advances to the second step, when the IoT device that produced the log is isolated to a different network, depending on whether the log is generated. The third phase is reached if quarantine is implemented, and the resulting log is used to determine whether the Mozi bot is infected. Proceed to the fourth step to eliminate the virus and release the isolate of the IoT device if it is found that the Mozi bot has infected it. Lastly, fortify the account using the log found in the first step to eliminate the root source of the malware invasion.

In contrast to a centralized framework, the Mozi bot's P2P structure allows it to communicate with numerous devices and carry out malevolent tasks like DDoS attacks and radio waves. By completing an isolation step right after gathering logs, botnets that use this P2P framework can also be stopped from spreading. In smart cities, security guards can identify tactics at specific times—and when to exchange defense strategies with other infrastructure. Examples of logs used to counter the Mozi bot using the D3FEND defense tactics, MITRE ATT&CK attack techniques, and the developed defense procedure are displayed in Table 10 below.

Table 10: An illustration of how to use the Mozi bot defense approach via the defensive procedure

Defense process	Mozi botnet phase	Sysmon log	MITRE ATT&CK technique	D3FEND tactic	D3FEND technique
1	Intrusion	Event ID 3	The exploitation of remote services via Brute force	Detection	Detection of remote terminal sessions, etc.
2	Load C&C propagation	Event ID 1, Event ID 3	Transmission of ingress tools, remote service exploitation, and network denial of service	Isolate	Broadcast domain isolation, DNS allow listing, DNS denylisting, etc.
3	Load C&C propagation	Event ID 1, Event ID 3, Event ID 8, Event ID 11, Event ID 22	Exploit public-facing applications via Brute force	Deceive	Decoy file, Decoy network resource, connected honeypot, etc.
4	C&C propagation attack	Event ID 1, Event ID 3	Brute Force, Exploit public-facing application	Evict	Process termination, Account locking
5	–	Event ID 3	Brute force, Exploit public-facing application	Harden	Strong password policy software, Software update

The attack on smart home devices serves as another illustration. In this instance, hackers gained illegal access to home networks by taking advantage of flaws in the token authentication procedure. The communication between a smart thermostat and its related mobile application was intercepted and manipulated by a hacker in one documented instance. Potential privacy violations and unapproved energy use could result from the attacker controlling the thermostat remotely by taking advantage of flaws in the token exchange procedure [2].

Moreover, in healthcare IoT applications, there have been instances where attackers targeted medical devices that utilized token-based authentication for access control. For example, vulnerabilities in the token management of insulin pumps allowed attackers to gain unauthorized access, potentially endangering patients' lives by altering dosage settings remotely. Such attacks not only compromise patient safety but also raise significant ethical and legal concerns regarding the security of medical IoT devices [76].

There have also been reports of token transmission attacks in industrial IoT environments. To obtain sensitive operational data, for example, attackers can take advantage of flaws in industrial IoT devices' authentication systems. Significant threats to operational integrity and safety may arise from data manipulation or illegal influence over vital systems. Yang et al.'s research demonstrates how attackers might influence

data transmission in industrial settings by exploiting token vulnerabilities, which can have detrimental effects on operational effectiveness and security [12].

12 Trends in Token-Based Attacks Targeting IoT Devices (Emerging Threats)

One prominent trend is the increasing sophistication of attacks leveraging machine learning and artificial intelligence. Adversaries are now employing advanced techniques to target the machine learning algorithms used in IoT communications. For instance, adversaries can conduct poisoning attacks on federated learning-based intrusion detection systems, implanting backdoors that allow them to misclassify malicious traffic as [77]. This trend emphasizes how important it is to have strong security systems that can evolve with the threats.

Another significant trend is the exploitation of weak token management practices in IoT devices. Many devices utilize token-based authentication, which can be vulnerable to compromise due to hard-coded credentials or insufficient encryption. For example, the use of hardware fingerprints has been proposed as a means to enhance the security of token-based authentication, mitigating the risks associated with token theft [2]. However, the widespread adoption of insecure token practices continues to expose IoT devices to attacks, emphasizing the need for improved security protocols and practices.

Moreover, the rise of botnets specifically targeting IoT devices has become a critical concern. The Bot-IoT dataset illustrates how attackers exploit the vulnerabilities of interconnected devices to create large-scale botnets capable of executing DDoS attacks and other malicious activities. This tendency can jeopardize entire networks in addition to affecting individual devices, resulting in serious disruptions and data breaches. Blockchain technology, with its inherent decentralized and immutable characteristics, offers a promising solution to enhance the security of token authentication systems [78]. It operates as a decentralized ledger that records transactions across multiple nodes in a network. The tamper-resistant nature of blockchain ensures that once a token is recorded, it cannot be altered or deleted, significantly mitigating risks associated with unauthorized changes [79,80]. In integration with access control protocols, blockchain enables secure token issuance and verification processes that uphold the integrity of access tokens throughout their lifecycle [2,81]. To provide a more secure framework for IoT authentication, this strategy seeks to solve the flaws in conventional token management techniques.

Furthermore, the emergence of adversarial deep learning techniques poses new challenges for IoT security. Attackers can directly target the algorithms used for spectrum sensing in IoT communications, manipulating the outcomes of transmissions and potentially leading to unauthorized access. This trend underscores the necessity for IoT systems to incorporate robust defenses against adversarial attacks, ensuring integrity for both data and authentication processes. The increase of file-less attacks is another emerging threat in the IoT landscape. According to Raman and Varadharajan, these attacks do not rely on traditional malware but instead exploit existing vulnerabilities in IoT devices, making them harder to detect [82]. This trend indicates a shift in attack strategies, where adversaries leverage legitimate functionalities of devices to execute malicious actions without the need for external malware, complicating the detection and prevention of such attacks.

The vulnerability of federated learning-based IoT intrusion detection systems to poisoning attacks is another emerging threat. Nguyen et al. demonstrate how attackers can manipulate the training data used in these systems to implant backdoors, allowing them to misclassify malicious traffic as benign [77]. This highlights the risks associated with relying on machine learning models for security, particularly when the integrity of the training data can be compromised.

13 Mitigation Strategies on Token Transmission Attacks in IoT Devices

Adversarial attacks can lead to data breaches, unauthorized device control, and security compromises within IoT ecosystems. To address these risks, effective mitigation strategies are critical in ensuring secure token transmission. These strategies aim to safeguard the confidentiality, integrity, and availability of tokens, preventing malicious actors from exploiting vulnerabilities in IoT networks. This section will explore various mitigation techniques designed to enhance the security of token transmission, focusing on their effectiveness in IoT environments.

13.1 Strong Encryption Standards

The implementation of robust encryption mechanisms is essential to safeguard the integrity and confidentiality of tokens during transmission. One effective approach to enhance security is the use of hybrid signcryption schemes, which combine encryption and signature processes into a single operation. This method not only improves computational efficiency but also provides better security for data transmission in resource-constrained IoT environments. For instance, Wu et al. propose a certificateless hybrid signcryption mechanism that significantly reduces resource consumption while enhancing security, making it particularly suitable for IoT applications [83]. Similarly, the LiSP-XK signcryption method has been shown to be efficient and effective in resource-limited settings, achieving better performance compared to traditional methods [75].

In addition to encryption and hardware-based solutions, the implementation of comprehensive authentication frameworks is crucial. Al-Refai and Alawneh propose an enhanced authentication and authorization framework that incorporates identity verification and sender verification mechanisms to protect IoT protocols from various attack vectors [1]. When considering authentication, encryption, and device integrity all at once, this framework emphasizes the value of a comprehensive approach to security.

The integration of advanced cryptographic techniques, such as Elliptic Curve Cryptography (ECC), has been shown to advance authentication and encryption processes in IoT systems [12], highlight a lightweight authentication mechanism that combines ECC with trusted tokens, ensuring that only authenticated devices can communicate, thus mitigating the risk of token theft and impersonation. This is further supported by the work of Zhao and Ding [84], who propose a dual-server identity-based encryption scheme that allows for secure data transmission and authorized equality testing without exposing sensitive information.

13.2 Hash-Based Message Authentication Codes (HMAC) for Integrity

Hash-based message Authentication Codes (HMACs) serve as a critical mitigation strategy against token transmission attacks in Internet of Things (IoT) devices. The inherent vulnerabilities of token-based authentication systems, particularly in resource-constrained environments typical of IoT, necessitate robust security measures. HMACs provide a mechanism to ensure both the integrity and authenticity of messages transmitted between devices, thereby mitigating risks associated with token compromise. HMACs utilize a cryptographic hash function combined with a secret key to produce a unique message digest that can be appended to the original message. This process ensures that any alteration of the message during transmission can be detected, as the hash value will not match if the message is tampered with [85]. The National Institute of Standards and Technology (NIST) endorses the use of HMACs, particularly with hash functions from the SHA-2 family, to guarantee message integrity and authentication [86].

This endorsement provides a standardized approach to implementing HMACs across various IoT applications. In the context of IoT, where devices mostly communicate over insecure channels, the implementation of HMACs can significantly enhance security. NIST's statistical test suite (NIST SP 800-22) is

crucial for assessing the randomness of cryptographic systems, including the hash functions employed in HMACs. This suite serves as a measure to evaluate the security of generated hash values against potential vulnerabilities [87].

Further, NIST has recognized the SHA-2 family, particularly SHA-256 and SHA-512, as robust hash functions suitable for constructing HMACs. These functions exhibit properties such as collision resistance and pre-image resistance, which are essential for maintaining the integrity of data. The work of Lahraoui et al. underscores the necessity of evaluating hash functions through rigorous frameworks like NIST's statistical tests to ensure their resistance against various attack vectors [88].

By leveraging the efficiency and speed of hash functions, HMAC provides a mechanism that allows devices to authenticate data with minimal computational overhead, which is crucial for battery-operated IoT devices (Mansour et al., 2024). The underlying robustness of HMAC demonstrates high level security when paired with secure hash functions, particularly SHA-256, making it suitable for applications requiring stringent confidentiality and integrity measures [89].

This is particularly relevant in scenarios where devices must operate continuously and securely, such as in smart home systems or industrial IoT applications. The implementation of such methods is critical in addressing the vulnerabilities associated with traditional token-based authentication, which can be susceptible to replay and impersonation attacks.

13.3 Lightweight Security Protocols for IoT

In the context of mitigating token transmission attacks in Internet of Things (IoT) devices, lightweight security protocols play a crucial role. These protocols are designed to operate efficiently within the constraints of IoT devices, which often have insufficient computational power and memory. Token transmission attacks, which can involve interception or unauthorized access to communication tokens, necessitate robust yet lightweight security measures to ensure the integrity and confidentiality of data.

Mutual authentication frameworks tailored for RFID devices are vital for instance, the research by Alhasan et al. proposes an ultra-lightweight mutual authentication protocol to prevent replay attacks in low-cost RFID tags. Their protocol employs secret key rotation, T-functions, and timestamps to ensure that authentication remains robust against various attack vectors [90]. The performance of such protocols demonstrates the feasibility of maintaining security while operating within the resource constraints typical of IoT devices.

Similarly, Fathy and Ali introduce a lightweight cryptographic framework that encompasses encryption, authentication, and key management, specifically tailored for IoT applications. Their comparative analysis with IPsec highlights the efficiency and security advantages of their proposed protocols, making them suitable for resource-constrained environments [91]. The use of Physical Unclonable Functions (PUFs) has emerged as a promising solution for lightweight security in constrained IoT devices. Idriss et al. discuss a PUF-based authentication protocol that leverages challenge-response mechanisms to enhance security. However, they also note that many existing PUF solutions lack essential features such as mutual authentication and message encryption, which are critical in defending against various attack vectors [92]. This highlights the need for continuous improvement and adaptation of lightweight protocols to address emerging threats effectively. The integration of lightweight digital signatures has also been explored as a means to secure communication in wireless sensor networks.

13.4 Multi-Factor Authentication (MFA) and Contextual Authentication

Multi-Factor Authentication (MFA) and contextual authentication are increasingly recognized as effective mitigation strategies against token transmission attacks in IoT devices. Token transmission attacks exploit vulnerabilities in the authentication process, particularly in systems relying solely on single-factor authentication methods. IoT device security can be significantly increased by using MFA, which asks users to give several forms of verification. By requiring the usage of at least two distinct authentication factors—which could be something the user knows (like a password), something they own (like a smart card or mobile device), or something they are (like biometric data)—MFA contributes to improving security [13,93]. This layered approach makes it considerably more difficult for attackers to gain unauthorized access, as they would need to compromise multiple factors simultaneously. For instance, the use of One-Time Passwords (OTPs) in conjunction with traditional passwords has been shown to bolster security in cloud computing environments, which is analogous to IoT applications [94]. Contextual authentication adds another layer of security by analyzing various contextual factors such as user location, device type, and historical access patterns to assess the risk associated with a login attempt [95]. This approach allows for dynamic adjustments in authentication requirements based on the perceived risk level. For instance, if the user attempts to access a system from an unusual location or device, the system can trigger additional authentication steps, thereby mitigating the risk of token theft or misuse [95]. The combination of MFA and contextual authentication not only enhances security but also improves usability by reducing friction in low-risk scenarios while maintaining robust defenses in high-risk situations.

13.5 CoAP (Constrained Application Protocol) with DTLS

Constrained Application Protocol (CoAP) is a thin application layer protocol created especially for Internet of Things (IoT) devices with limited resources. It is appropriate for applications including industrial automation, smart home devices, and environmental monitoring because of its architecture, which is tuned for low-power and low-bandwidth networks [96].

The integrity and confidentiality of sensitive data transferred between devices may be jeopardized by token transmission attacks, which raise serious concerns about the security of CoAP connections. It is often advised to combine Datagram Transport Layer Security (DTLS) with CoAP in order to reduce token transfer threats. This protocol employs encryption methods that safeguard the data transmitted between devices, reducing the risk of unauthorized access and eavesdropping, thereby ensuring the confidentiality of sensitive information exchanged within IoT networks [97,98].

The lightweight nature of DTLS makes it a fitting choice for CoAP, as it can operate effectively within the constraints of low-power devices while still providing robust security measures. Moreover, the combination of CoAP and DTLS allows for secure data transmission while maintaining the efficiency required by resource-constrained environments. Recent advancements have led to the development of energy-efficient variants of DTLS, such as the Energy-Efficient DTLS (eeDTLS), which optimizes the handshake process and reduces message overhead. This is particularly beneficial for IoT devices that rely on battery power, as it minimizes energy consumption during secure communications.

Additionally, the Lithe protocol, which combines CoAP with DTLS features, exemplifies how lightweight security can be achieved without sacrificing performance. Research indicates that conventional security mechanisms often fail under resource constraints, making protocols like Lithe crucial for IoT applications [99]. For instance, lightweight cryptographic techniques integrated into Lithe ensure that even devices with limited computational power can perform secure exchanges without succumbing to vulnerabilities associated with heavyweight security protocols [100]. The successful application of Lithe achieves a crucial balance: it satisfies the need for robust security against threats, such as man-in-the-middle

attacks and eavesdropping, while simultaneously respecting the operational limitations of the underlying hardware [101].

This approach not only enhances security against token transmission attacks but also improves overall system efficiency. Furthermore, the implementation of intrusion detection systems (IDS) can complement the security measures provided by DTLS. By monitoring network traffic for unusual patterns indicative of token transmission attacks, these systems can provide an additional layer of protection. The integration of machine learning techniques into IDS can further enhance their effectiveness by enabling them to adapt to evolving attack vectors [96]. This multifaceted approach not only addresses the immediate security concerns but also aligns with the operational constraints typical of IoT environments.

13.6 Secure Token Management

Many researchers have explored mechanisms such as attribute-based encryption and blockchain technology to enhance the security and management of tokens. One promising approach is the use of ciphertext policy attribute-based encryption (CP-ABE), which allows for fine-grained access control by encrypting tokens based on user attributes [42]. This method not only secures the tokens but also facilitates streamlined management through one-to-many encryption, enabling a single token to grant access to multiple subjects. Such an approach mitigates the need for issuing separate tokens for each user, thus simplifying token management. Furthermore, the integration of blockchain technology into token management has been shown to enhance security by implementing token operations as blockchain transactions, which can provide an immutable record of token usage and enhance accountability [102]. In addition to encryption and blockchain, the incorporation of hardware fingerprints into the authentication process has emerged as a viable strategy to bolster token security. By binding tokens to unique hardware identifiers, the risk of token compromise can be significantly reduced, as attackers would need to replicate the hardware fingerprint to successfully impersonate a device [2]. This method complements traditional token management by adding an additional layer of security that is particularly beneficial for resource-constrained IoT devices. Moreover, frameworks that combine enhanced token authentication with identity verification mechanisms have been proposed to further protect against various attacks, including man-in-the-middle and replay attacks [1]. Such frameworks often utilize timestamps and sender verification methods to ensure that tokens are only valid for a limited time and are issued by authenticated devices. This dynamic approach to token management not only improves security but also addresses the challenges posed by the static nature of traditional token systems.

13.7 Token Expiration and Revocation Strategies

Token expiration serves as a proactive measure to limit the window of opportunity for attackers who may compromise tokens. By implementing short-lived tokens, the potential damage from a stolen token is minimized, as the token becomes invalid after a specified period.

Zhang et al. propose a cryptographic accumulator technique for managing the issuance and revocation of verifiable credentials, which ensures user privacy during the revocation process [103]. This approach allows institutions to maintain secure records of credential status without compromising user anonymity. Utilizing similar mechanisms in broader token management strategies can facilitate effective revocation while upholding privacy rights and considering the energy constraints of IoT devices. This approach not only addresses security concerns but also optimizes the energy consumption of IoT devices, which is crucial for their operational longevity. Revocation strategies are equally important, particularly in scenarios where a token is compromised or when a user's access rights change. The challenge of effectively propagating credential revocation in shared IoT ecosystems has been highlighted by Janes et al., who found that many devices fail to revoke access properly, allowing unauthorized access even after credential changes [104]. This

underscores the necessity for robust revocation mechanisms that can promptly and effectively update access controls across devices. Techniques such as verifier-local revocation (VLR) have been proposed, which allow for efficient member revocation in group signature schemes, although they may rely on weaker security notions [105]. Moreover, blockchain technology offers promising solutions for token management, including revocation. For example, the BlendCAC framework utilizes smart contracts to manage token registration, propagation, and revocation, thus decentralizing control and enhancing security. More robust access control systems in IoT contexts are made possible by this decentralized method, which also reduces the dangers connected with a single point of failure.

13.8 Token Binding to Prevent Reuse and Hijacking

Token binding enhances security by associating a token with a specific session or request, thereby preventing its reuse and reducing the risk of hijacking. Gupta and Narayan proposed a key-based mutual authentication framework that binds tokens to specific point-of-sale (POS) machines, thereby preventing unauthorized access and token reuse during mobile transactions [106]. This concept can be extended to IoT devices, where binding tokens to specific devices or sessions ensures that even if a token is intercepted, it cannot be reused by an attacker on a different device. Moreover, continuous authentication protocols can further strengthen token-binding strategies. Badhib et al. highlight the necessity of continuous authentication to prevent session hijacking, which is particularly relevant in IoT scenarios where devices may operate in untrusted environments [107]. By continuously verifying the legitimacy of devices during a session, the risk of token misuse is significantly reduced.

Mondal et al. highlight how lightweight cryptographic algorithms, such as elliptic curve cryptography (ECC), can be utilized alongside dynamic key generation to provide a robust security framework suitable for the unique constraints of IoT devices [108]. In addition, the integration of time-sensitive protocols can further benefit from utilizing hybrid cryptographic approaches as seen in the work of Munshi and Alshawi, a three-phase authentication protocol that combines ECC with Advanced Encryption Standard (AES). Here, dynamic key generation is coupled with an optimization strategy, allowing the system to effectively manage key lifecycles while ensuring secure token exchanges [109]. This combination strikes a balance between security and efficiency, particularly in resource-limited scenarios typical of IoT applications.

13.9 Network-Level Security Approaches

Network-level security approaches are critical for mitigating token transmission attacks in Internet of Things (IoT) devices. By implementing robust network security strategies, companies can improve the resilience of their IoT environment against such threats. One effective strategy is the deployment of Intrusion Detection Systems (IDS). Ferrag et al. emphasize the necessity of purpose-built cybersecurity solutions, such as IDS, which can monitor network traffic for malicious behavior and provide real-time alerts [110]. These systems can detect anomalies in token transmission patterns, enabling prompt responses to potential attacks. Moreover, IDS can be integrated with machine learning algorithms to improve detection accuracy and adapt to evolving threats, as highlighted by Vutukuru, who discusses the application of advanced machine learning techniques for IoT security [111].

Network segmentation can also be used to separate IoT devices from other network segments. By keeping a token transmission attack inside a designated section, this tactic reduces its possible impact. The attack surface can be decreased by companies limiting communication between IoT devices and external networks through the use of firewalls and access controls. Employing intrusion detection systems (IDS), encryption protocols, network segmentation, secure authentication frameworks, and ongoing monitoring can help enterprises improve the security of their IoT ecosystems and guard against unwanted access and

control. The work of Lahraoui et al. underscores the necessity of evaluating hash functions through rigorous frameworks like NIST's statistical tests to ensure their resistance against various attack vectors [88]. Their study emphasizes that employing strong hash functions within HMAC can lead to enhanced security for message transmission.

13.10 Incorporate the Use of More Secure Communication Protocols (e.g., TLS, HTTPS)

To prevent token transmission attacks in Internet of Things (IoT) devices, it is essential to employ secure communication protocols. Enforcing strong communication protocols can prevent such problems and greatly improve token transmission security. IPsec, which offers a framework for protecting Internet Protocol (IP) communications via encryption and authentication, is one practical method.

While traditional IPsec utilizes the Internet Key Exchange (IKE) for establishing security associations, Othmen et al. advocate for enhanced key management approaches that improve security in low-power, lossy network environments [112]. Their work emphasizes the necessity of optimized routing protocols that prioritize secure data transmission while integrating with IPsec's framework. Additionally, configurations employing group key management can streamline the secure transmission of tokens between multiple devices, minimizing delays and maintaining efficiency [112]. Combinations of IPsec with application-layer security protocols can provide comprehensive protection, especially for sensitive token transmission scenarios within IoT settings [98]. This layered approach aids in defending against a broader array of threats, including eavesdropping and man-in-the-middle attacks.

Tokens sent between devices are shielded from interception and manipulation thanks to DTLS, which in particular offers a secure channel for datagram-based applications. Attacks involving tokens can be considerably decreased by putting these protocols into place. IoT applications frequently use the Message Queuing Telemetry Transport (MQTT) protocol because of its portability. Due to the necessity for attackers to get around several security mechanisms, this can greatly lower the chance that token transmission attacks would be successful. To prevent token transmission attacks in Internet of Things devices, it is essential to adopt appropriate secure communication protocols. Lightweight authentication techniques, MFA, and protocols like IPsec, DTLS, and TLS can all greatly improve the security of token transfer. These tactics can be used to improve the security of IoT systems against unwanted access and guarantee the integrity of communications. Secure communication will become increasingly important as the IoT environment develops to protect user data and preserve the integrity of IoT devices.

13.11 AI-Powered Strategies for Countering Cyberattacks

Scientists have recently proposed several ways that use AI techniques to identify domains generated by domain generation algorithms (DGAs), detect or classify malware, and detect network intrusions, phishing, and spam attacks on IoT devices. The literature is divided into four major categories in this section: malware identification, network intrusion detection, phishing and SPAM identification, and others, which include recognizing DGAs and thwarting APT.

Fig. 7 illustrates crucial areas in AI can be used in anomaly detection to prevent attacks [113].

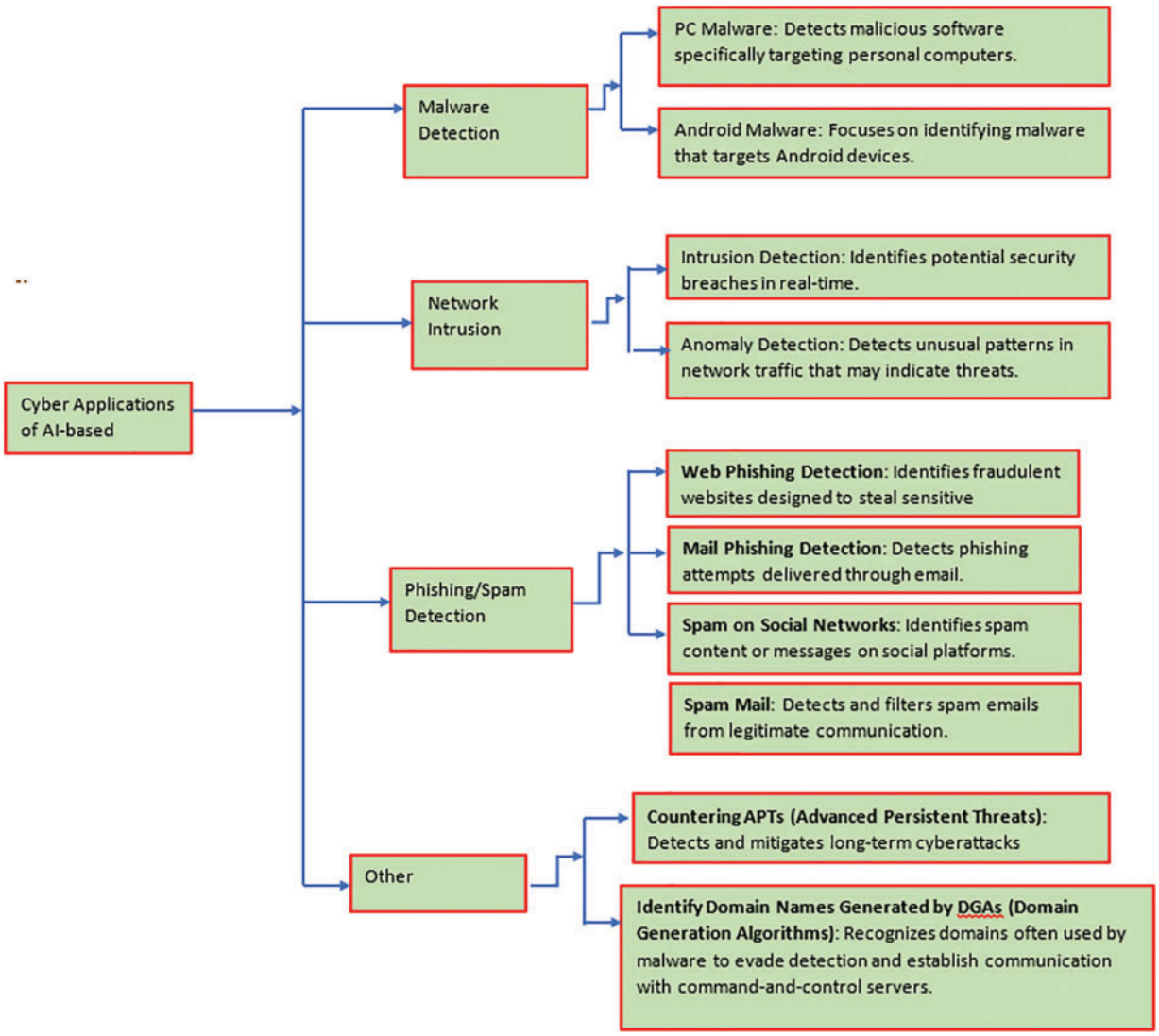

Figure 7: Areas AI can be used in anomaly detection to prevent attacks

13.12 Applying Appropriate Cybersecurity Framework

The use and selection of an appropriate cybersecurity framework is critical for mitigating risks associated with token-based authentication, which is prevalent in IoT environments. Table 11 highlights critical cybersecurity frameworks and standards and their applications across various industries. Each framework serves a specific purpose in protecting digital assets, ensuring regulatory compliance, and mitigating cyber risks. These frameworks are tailored to address the unique challenges of specific sectors while maintaining flexibility for broader organizational adoption.

Table 11: Illustrates common cybersecurity frameworks that can be incorporated to prevent attacks

Framework	Industry	Purpose	Key focus
ISO 27001 (Information Security Management System-ISMS)	Finance, healthcare, IT, and government sectors to secure critical data and mitigate risks	Establishes requirements for an ISMS to manage sensitive information.	Risk assessment, incident response, and continuous improvement in security practices.
NIST framework	Critical infrastructure sectors like energy, healthcare, finance, transportation	Provides guidelines to identify, protect, detect, respond, and recover from cybersecurity threats.	Flexibility in implementation to fit organizations of all sizes.
HIPAA (Health Insurance Portability and Accountability Act)	Healthcare providers, health plans, healthcare clearinghouses	Regulates the protection of sensitive patient healthcare data.	Privacy and security rules to safeguard Protected Health Information (PHI)
PCI DSS (Payment Card Industry Data Security Standard)	Merchants, financial institutions, payment processors	Sets security requirements to protect cardholder data during payment processing.	Secure transaction processes and prevent fraud.
GDPR (General Data Protection Regulation)	Businesses, government agencies, non-profits	Governs data privacy for individuals within the European Union (EU).	Consent, data protection, and rights for data subjects.
CIS Controls (Center for Internet Security Controls)	Organizations of all sizes and sectors	A set of best practices to protect systems against known cyber threats.	Basic and advanced cyber hygiene.
HITRUST CSF (Common Security Framework)	Healthcare organizations and business associates	Integrates multiple standards like HIPAA, PCI DSS, and ISO 27001 for healthcare security.	Simplifies compliance with multiple regulations.
COBIT (Control Objectives for Information and Related Technologies)	Organizations of all sizes and industries	Provides a framework for IT governance and management.	Aligning IT with business goals and ensuring effective management of IT risks.
NERC-CIP (North American Electric Reliability Corporation-Critical Infrastructure Protection)	Electric utilities, power generation companies	Ensures the reliability and protection of the electric power system.	Securing critical infrastructure against cyber and physical threats.
FISMA (Federal Information Security Management Act)	U.S. federal government agencies and contractors	Requires federal agencies to develop, document, and implement an information security program.	Protecting government information and IT systems.
SOC 2 (Service Organization Control 2)	Service providers such as data centers, SaaS companies, managed service providers, cloud computing providers	Assesses service providers' security, availability, processing integrity,	Security for third-party services.
IAB CCPA (Interactive Advertising Bureau-California Consumer Privacy Act)	Businesses collecting personal information from California residents	Ensures privacy rights and consumer protections for California residents	Transparency and consumer control over personal data.
CISA telecoms framework	Telecom providers operating in the US	Provides guidelines to secure telecommunications infrastructure.	Risk management and threat detection for telecom networks.
NIST special publication 800-53	US federal agencies and organizations	800-53: Focuses on security controls for federal information systems and organizations.	Compliance with US government data security requirements.

(Continued)

Table 11 (continued)

Framework	Industry	Purpose	Key focus
NIST special publication 800-171	Non-federal organizations handling controlled unclassified information for the US government	800-171: Designed for non-federal organizations handling Controlled Unclassified Information (CUI).	Compliance with US government data security requirements.
UK telecoms (Security) Act 2021	Telecommunication companies operating in the United Kingdom	Establishes legal requirements to secure telecom networks in the UK.	Resilience against security threats, supply chain risks, and operational failures.

13.13 Context-Aware Authentication in Dynamic IoT Environments

Context-aware authentication in dynamic IoT environments is a promising approach to mitigate token transmission attacks, which are prevalent due to the vulnerabilities inherent in token-based authentication mechanisms. Context-aware authentication uses contextual data, including user behavior, device attributes, and ambient conditions, to improve security and lower the possibility of unwanted access. This framework addresses the limitations of traditional authentication techniques by continuously validating user identities based on their context, thereby reducing the likelihood of token theft or misuse. The continuous nature of this authentication process ensures that even if a token is compromised, the system can detect anomalies in user behavior and respond accordingly. In addition, Fard et al. discuss the application of machine learning for dynamic authentication, emphasizing how contextual data, such as surrounding MAC addresses, can be utilized to establish a secure authentication process for IoT devices [114]. This method not only ensures better security but also allows for a more adaptive response to potential threats, making it more difficult for attackers to exploit token vulnerabilities. By understanding the mobility patterns and contextual factors affecting device interactions, systems can implement more robust authentication measures that adapt to changing conditions, thereby mitigating risks associated with token transmission attacks. Sylla et al. propose a blockchain-based context-aware authorization management system, which extends traditional authentication frameworks by incorporating context-awareness capabilities [17]. This decentralized approach improves security by ensuring that authentication tokens are contextualized, making it harder for attackers to exploit static tokens that may be intercepted during transmission. This capability can be leveraged to enhance authentication processes, ensuring that only trusted devices are allowed to communicate, thus reducing the risk of token-related attacks. Context-aware authentication strategies offer a robust framework for mitigating token transmission attacks in IoT devices. By leveraging contextual information, continuous monitoring, and adaptive responses, these strategies can significantly improve the security of IoT environments.

A summary of mitigation strategies on token transmission attacks in IoT devices is shown in Table 12:

Table 12: Summary of mitigation strategies on token transmission attacks in IoT devices

Mitigation strategy	Description	Focus	Impact on token transmission	Similarities	Differences
Strong encryption standards	Uses encryption methods to secure token data during transmission.	Protects data confidentiality.	Secures tokens during transmission, preventing interception.	All strategies aim to prevent unauthorized access or manipulation of tokens.	Focuses on encrypting data, whereas others may focus on authentication or token management.

(Continued)

Table 12 (continued)

Mitigation strategy	Description	Focus	Impact on token transmission	Similarities	Differences
Hash-based message authentication codes (HMAC)	Uses a cryptographic hash to verify token integrity and authenticity.	Ensures token integrity and authenticity.	Validates the integrity of tokens and prevents modification.	Both aim to secure token authenticity and integrity.	Focuses on ensuring integrity specifically, unlike strategies focusing on overall security.
Lightweight security protocols for IoT	Implements simpler security protocols optimized for IoT devices with limited resources.	Ensures security while minimizing resource usage.	Secures communication while being resource-efficient.	Aims to secure communication without overwhelming device resources.	Focused on resource constraints in IoT devices, unlike other strategies designed for high-capacity systems.
Multi-Factor Authentication (MFA) and contextual authentication	Requires multiple forms of verification to ensure the legitimacy of token requests.	Strengthens authentication through multiple verification steps.	Reduces the likelihood of unauthorized access via token misuse.	Increases authentication strength, like other strategies aiming for robust security.	Involves user interaction and context, while others focus solely on token integrity and communication.
CoAP (Constrained application Protocol) with DTLS	Uses CoAP for efficient communication in IoT with DTLS (Datagram Transport Layer Security) for encryption.	Efficient secure communication for constrained IoT environments.	Secures token transmission in resource-constrained environments.	Both focus on optimizing communication and security for IoT devices.	Focused on specific IoT protocols (CoAP/DTLS), unlike general approaches.
Secure token management	Implements systems for securely storing, issuing, and handling tokens throughout their lifecycle.	Manages the entire lifecycle of tokens securely.	Ensures tokens are properly managed, reducing misuse.	All strategies focus on maintaining token security throughout their use.	Emphasizes the management process rather than just transmission or authentication of tokens.
Token expiration and revocation strategies	Implements token expiration and revocation to prevent the use of old or compromised tokens.	Reduces risks by ensuring tokens cannot be reused or exploited.	Ensures that old or invalid tokens cannot be reused.	Similar in goal to other strategies that limit the lifespan of tokens.	Focuses on time-based control, while others focus on real-time security measures.
Token binding to prevent reuse and Hijacking	Binds tokens to specific devices or sessions to prevent unauthorized use of stolen tokens.	Prevents reuse and hijacking of tokens.	Reduces the chances of token hijacking and replay attacks.	Similar to other strategies aimed at preventing token theft.	Specifically focuses on binding tokens to devices, while others focus on general protection methods.
Network-level security approaches	Implements security measures at the network layer, such as firewalls and intrusion detection systems.	Secures token transmission at the network level.	Protects the integrity of tokens by securing the transmission medium.	Similar in overall goal of improving security, particularly token transmission.	Focuses on network-level security rather than token-level or protocol-specific protection.

(Continued)

Table 12 (continued)

Mitigation strategy	Description	Focus	Impact on token transmission	Similarities	Differences
Incorporate the use of more secure communication protocols (e.g., TLS, HTTPS)	Implements advanced, widely-used communication protocols to ensure secure token transmission.	Strengthens the communication channel using established protocols.	Secures the transmission of tokens between devices and servers.	Similar to encryption-based strategies focusing on securing data transmission.	Relies on standard communication protocols, while other strategies focus on token management or authentication.
AI-Powered strategies for countering cyberattacks	Uses machine learning and AI algorithms to detect and mitigate cyberattacks in real-time.	Detects and responds to cyberattacks proactively.	Identifies and mitigates attacks targeting token transmission.	All strategies aim to prevent or detect attacks targeting token security.	Uses AI and machine learning, whereas others rely on traditional cryptographic methods.
Applying appropriate cybersecurity framework	Implements a holistic security framework that addresses multiple layers of security across IoT systems.	Ensures comprehensive security across IoT systems.	Integrates various security measures, including token protection.	All strategies focus on securing tokens and systems against attacks.	Provides a broader, system-wide security approach, unlike more focused strategies.
Context-aware authentication in dynamic iot environments	Adjusts authentication mechanisms based on the context of the device or user.	Provides dynamic, contextual security measures.	Ensures tokens are validated based on context, reducing misuse.	Focuses on strengthening authentication mechanisms in dynamic environments.	Incorporates contextual data, unlike other strategies that focus purely on tokens or encryption.

14 Conclusion

As the deployment of IoT devices expands across sectors such as healthcare, manufacturing, and smart homes, the risk of exploitation through token-based authentication vulnerabilities continues to rise. These vulnerabilities can lead to significant data breaches, unauthorized control over IoT networks, and exploitation of weaknesses in token management protocols. Therefore, addressing token transmission security is crucial for safeguarding IoT systems.

Several recommendations have been proposed to mitigate these risks. First, enhanced encryption mechanisms specifically designed for the resource limitations of IoT devices are essential. Lightweight encryption algorithms, such as Elliptic Curve Cryptography (ECC) and optimized Advanced Encryption Standards (AES), can effectively protect token transmission from eavesdropping and tampering. Additionally, ensuring regular firmware updates to address vulnerabilities, particularly in token management protocols, is critical for maintaining security [12].

The use of machine learning for anomaly detection based on baseline device behaviors can also be highly effective. Machine learning systems can analyze traffic patterns to detect and respond to abnormal activities in real time, enhancing the overall security posture. Moreover, the integration of Artificial Intelligence (AI) for predictive analytics can significantly improve the detection and response capabilities for token transmission attacks. AI-driven systems learn from past incidents and adapt to new threats, providing more resilient defenses for IoT networks.

Adherence to established cybersecurity guidelines, such as those from NISTIR 8228, which emphasizes cybersecurity and privacy management throughout the device lifecycle, will strengthen token security. IoT

device manufacturers should collaborate to establish common security standards, creating protocols that ensure secure communication between heterogeneous devices while safeguarding user privacy [67].

14.1 Future Directions for Improving Token Security in IoT

To further enhance token security in IoT devices and systems, several future research directions should be explored. These can be grouped into three key aspects: Emerging Technologies, Quantum Computing, and User Education and Awareness.

14.1.1 Emerging Technologies for Enhanced Security

With the continuous evolution of IoT, emerging technologies offer promising solutions for improving token security. Technologies such as Fog Computing, Edge Computing, and Blockchain have great potential. Fog and Edge Computing can support decentralized security models, which are critical for reducing the risks associated with centralized token management systems. These technologies enable token-based communication to take place closer to the devices, enhancing response times and reducing the attack surface. In addition, challenges such as trust management and fault resilience must also be addressed [115].

Blockchain technology, with its decentralized structure, can also play a pivotal role in improving token security by eliminating the reliance on vulnerable centralized servers. Blockchain-based solutions could offer enhanced authentication, access control, and trust mechanisms, though concerns related to computation complexity and privacy must be resolved. Similarly, lightweight cryptographic methods tailored to the specific needs of IoT devices will be essential, especially for managing keys in constrained environments.

14.1.2 Quantum Computing and Post-Quantum Security

The advent of Quantum Computing presents a new frontier in cryptography, which will undoubtedly impact the future security of IoT systems. As quantum computers become more powerful, traditional cryptographic techniques may become vulnerable to attacks, especially in terms of encryption key-breaking. In this context, quantum-resistant encryption algorithms are needed to future-proof IoT systems against the cryptographic threats posed by quantum computing. Research into Quantum Key Distribution (QKD) and quantum signatures offers promising solutions for ensuring secure data transmission in the post-quantum era. These quantum-based techniques could revolutionize how tokens are secured, providing new, robust methods for safeguarding communication against eavesdropping and tampering [116]. In addition to quantum computing, emerging technologies are revolutionizing various industries, but they also introduce new security challenges. Fog Computing and Edge Computing enhance data processing by bringing it closer to the source, reducing latency and minimizing risks associated with transmitting sensitive data. SDN offers flexible, dynamic control over network traffic, enabling rapid response to security threats. To secure resource-constrained IoT devices, Lightweight Cryptography provides efficient encryption solutions. Homomorphic Encryption (HE) and Secure Enclaves (SE) ensure that sensitive data remains protected even during processing, providing enhanced privacy and security. Machine Learning plays a crucial role in identifying anomalies and potential threats in real time, bolstering proactive security measures. As shown in Table 12, these emerging solutions are vital for strengthening security in increasingly complex and interconnected systems.

A summary table showing security purposes and challenges of the studied emerging technologies is shown in Table 13.

Table 13: Security purposes and challenges of the studied emerging technologies

Emerging solution	Security purpose	Security challenge
Fog computing	Authentication, confidentiality	Trust management
Edge computing	Access control, authentication, privacy-preserving	Attack and fault resilience
SDN	Key management, identity management	Scalability
Blockchain	Authentication, access control, trust	Computation complexity, privacy
Lightweight cryptography	Confidentiality, integrity, authentication	Key management
HE and SE	Privacy-preserving	Computation complexity
Machine learning	Anomaly detection, attack detection	Computation complexity, privacy

14.1.3 User Education and Awareness

One of the often-overlooked aspects of securing IoT devices is User Education and Awareness. Many IoT vulnerabilities stem from user behaviors, such as the failure to change default passwords or enable multi-factor authentication (MFA). Manufacturers must take a proactive role in educating users about the potential security risks and the best practices for securing their IoT devices. Clear guidelines should be provided for users, especially in areas such as token management, password configuration, and enabling advanced security measures like MFA. By raising awareness, users will be better equipped to secure their devices, reducing the overall attack surface for token-related vulnerabilities [117].

14.2 Conclusion and Collaboration for Future Security

Looking forward, addressing token transmission threats in IoT devices requires collaboration among cybersecurity experts, regulatory authorities, and IoT manufacturers. By exploring these future directions—leveraging emerging technologies, preparing for the quantum computing era, and prioritizing user education—we can significantly enhance the security of IoT networks and mitigate the risks associated with token-based authentication vulnerabilities. A comprehensive approach, incorporating technological advancements and best practices, is essential to ensuring the resilience and security of future IoT systems.

Acknowledgement: We sincerely thank all the individuals and the institution whose support and contributions have made this work possible.

Funding Statement: The authors received no specific funding for this study.

Author Contributions: Research work was conducted by Michael Juma Ayuma, reviewed, supervised and validated by Shem Mbandu Angolo and Philemon Nthenge Kasyoka. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The data used in this study is publicly available on papers published in the relevant journals as recorded in this manuscript.

Ethics Approval: Not applicable.

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

References

1. Mohammad A, Al-Refai H, Alawneh AA. User authentication and authorization framework in IoT protocols. Comput Sci Forthcoming. 2022. doi:10.20944/preprints202208.0188.v1.
2. Xiao Y, He Y, Zhang X, Wang Q, Xie R, Sun K, et al. From hardware fingerprint to access token: enhancing the authentication on IoT devices. In: Proceedings of the 2024 Network and Distributed System Security Symposium; 2024 Feb 26–Mar 1; San Diego, CA, USA. doi:10.14722/ndss.2024.241231.
3. Rawal D, Murugan R. Emerging threats and defensive strategies on the Internet of Things. Int Res J Mod Eng Technol Sci. 2024;6(5):2244–50. doi:10.56726/irjmets56144.
4. Sharma R, ud din Mohi S, Sharma N, Kumar A. Enhancing IoT botnet detection through machine learning-based feature selection and ensemble models. ICST Trans Scalable Inf Syst. 2023;11(2):1–6. doi:10.4108/eetsis.3971.
5. Lin IC, Tseng PC, Chen PH, Chiou SJ. Enhancing data preservation and security in industrial control systems through integrated IOTA implementation. Processes. 2024;12(5):921. doi:10.3390/pr12050921.
6. Zhang Y, Luo Y, Chen X, Tong F, Xu Y, Tao J, et al. A lightweight authentication scheme based on consortium blockchain for cross-domain IoT. Secur Commun Netw. 2022;2022(6):9686049. doi:10.1155/2022/9686049.
7. Sivaselvan N, Bhat KV, Rajarajan M, Das AK, Rodrigues JJPC. SUACC-IoT: secure unified authentication and access control system based on capability for IoT. Clust Comput. 2023;26(4):2409–28. doi:10.1007/s10586-022-03733-w.
8. Arcenegui J, Arjona R, Román R, Baturone I. Secure combination of IoT and blockchain by physically binding IoT devices to smart non-fungible tokens using PUFs. Sensors. 2021;21(9):3119. doi:10.3390/s21093119.
9. Obaidat MA, Obeidat S, Holst J, Al Hayajneh A, Brown J. A comprehensive and systematic survey on the Internet of Things: security and privacy challenges, security frameworks, enabling technologies, threats, vulnerabilities and countermeasures. Computers. 2020;9(2):44. doi:10.3390/computers9020044.
10. Deepak, Gulia P, Gill NS, Yahya M, Gupta P, Shukla PK. Exploring the potential of blockchain technology in an IoT-enabled environment: a review. IEEE Access. 2024;12(37):31197–227. doi:10.1109/access.2024.3366656.
11. Alhamarneh RA, Mahinderjit Singh M. Strengthening Internet of Things security: surveying physical unclonable functions for authentication, communication protocols, challenges, and applications. Appl Sci. 2024;14(5):1700. doi:10.3390/app14051700.
12. Yang YS, Lee SH, Wang JM, Yang CS, Huang YM, Hou TW. Lightweight authentication mechanism for industrial IoT environment combining elliptic curve cryptography and trusted token. Sensors. 2023;23(10):4970. doi:10.3390/s23104970.
13. Diaz Rivera JJ, Akbar W, Ahmed Khan T, Muhammad A, Song WC. Secure enrollment token delivery mechanism for zero trust networks using blockchain. IEICE Trans Commun. 2023;106(12):1293–301. doi:10.1587/transcom.2022tmp0005.
14. Pozo A, Alonso Á, Salvachúa J. Evaluation of an IoT application-scoped access control model over a publish/subscribe architecture based on FIWARE. Sensors. 2020;20(15):4341. doi:10.3390/s20154341.
15. Furtak J. Cryptographic keys generating and renewing system for IoT network nodes—a concept. Sensors. 2020;20(17):5012. doi:10.3390/s20175012.
16. Alnahari W, Quasim MT. Authentication of IoT device and IoT server using security key. In: Proceedings of the 2021 International Congress of Advanced Technology and Engineering (ICOTEN); 2021 Jul 4–5; Taiz, Yemen. doi:10.1109/icoten52080.2021.9493492.
17. Sylla T, Mendiboure L, Chalouf MA, Krief F. Blockchain-based context-aware authorization management as a service in IoT. Sensors. 2021;21(22):7656. doi:10.3390/s21227656.
18. Ebrahimabadi M, Younis M, Karimi N. A PUF-based modeling-attack resilient authentication protocol for IoT devices. IEEE Internet Things J. 2022;9(5):3684–703. doi:10.1109/JIOT.2021.3098496.
19. Al Hayajneh A, Bhuiyan MZA, McAndrew I. Improving Internet of Things (IoT) security with software-defined networking (SDN). Computers. 2020;9(1):8. doi:10.3390/computers9010008.
20. Singh D, Pati B, Panigrahi CR, Swagatika S. Security issues in IoT and their countermeasures in smart city applications. In: Advanced computing and intelligent engineering. Singapore: Springer Singapore; 2020. p. 301–13. doi:10.1007/978-981-15-1483-8_26.

21. Afzaal R, Jan S, Ponum M, Sana S, Adnan K, Jameel A. Efficient metrics for data recovery at perception layer: e-health case study. Forthcoming. 2022;36(1):41. doi:10.21203/rs.3.rs-2047297/v2.
22. Abdulazeez S, Nawar AK, Hassan NB, Tariq E. Internet of Things: architecture, technologies, applications, and challenges. AlKadhim J Comput Sci. 2024;2(1):36–52. doi:10.61710/kjcs.v2i1.67.
23. Nisha N, Gill NS, Gulia P. A review of intrusion detection system and security threat in Internet of Things enabled environment. Indones J Electr Eng Comput Sci. 2024;35(1):428. doi:10.11591/ijeecs.v35.i1.pp428-435.
24. Abuseta Y. Towards a generic software architecture for IoT systems. Int J Softw Eng Appl. 2024;15(6):1–16. doi:10.5121/ijsea.2024.15601.
25. Tariq U, Ahmed I, Bashir AK, Shaukat K. A critical cybersecurity analysis and future research directions for the Internet of Things: a comprehensive review. Sensors. 2023;23(8):4117. doi:10.3390/s23084117.
26. Wardana AA, Kołaczek G, Sukarno P. Lightweight, trust-managing, and privacy-preserving collaborative intrusion detection for internet of things. Appl Sci. 2024;14(10):4109. doi:10.3390/app14104109.
27. Adam M, Hammoudeh M, Alrawashdeh R, Alsulaimy B. A survey on security, privacy, trust, and architectural challenges in IoT systems. IEEE Access. 2024;12(4):57128–49. doi:10.1109/access.2024.3382709.
28. Zhao Y. Internet of things technology in smart furniture: an overview. J Electrotechnol Electr Eng Manag. 2024;7(1):107–12. doi:10.23977/jeeem.2024.070114.
29. Yuan B, Yang M, Xu Z, Chen Q, Song Z, Li Z, et al. Leakage of authorization-data in IoT device sharing: new attacks and countermeasure. IEEE Trans Dependable Secure Comput. 2024;21(4):3196–210. doi:10.1109/tdsc.2023.3323713.
30. Helmschmidt F, Hosseyni P, Küsters R, Pruiksma K, Waldmann C, Würtele T. The grant negotiation and authorization protocol: attacking, fixing, and verifying an emerging standard. In: Proceedings of the 28th European Symposium on Research in Computer Security; 2023 Sep 25–29; The Hague, The Netherlands. doi:10.1007/978-3-031-51479-1_12.
31. Ramani R, Rosline Mary A, Edwin Raja S, Arun Shunmugam D. Optimized data management and secured federated learning in the Internet of Medical Things (IoMT) with blockchain technology. Biomed Signal Process Control. 2024;93(1):106213. doi:10.1016/j.bspc.2024.106213.
32. Dhinakaran D, Srinivasan L, Udhaya Sankar SM, Selvaraj D. Quantum-based privacy-preserving techniques for secure and trustworthy Internet of Medical Things an extensive analysis. Quantum Inf Comput. 2024;24(3–4):227–66. doi:10.26421/qic24.3-4-3.
33. Alluhaidan ASD, Prabu P. End-to-end encryption in resource-constrained IoT device. IEEE Access. 2023;11:70040–51. doi:10.1109/access.2023.3292829.
34. Abhijith HV. Efficient and secure data aggregation for resource-constrained IoT environments. Int J Saf Secur Eng. 2024;14(3):999–1006. doi:10.18280/ijsse.140329.
35. Hwang YW, Lee IY. A lightweight certificate-based aggregate signature scheme providing key insulation. Comput Mater Contin. 2021;69(2):1747–64. doi:10.32604/cmc.2021.018549.
36. Khan ZA, Namin AS. A survey of DDOS attack detection techniques for IoT systems using Blockchain technology. Electronics. 2022;11(23):3892. doi:10.3390/electronics11233892.
37. Vishwakarma R, Jain AK. A survey of DDoS attacking techniques and defence mechanisms in the IoT network. Telecommun Syst. 2020;73(1):3–25. doi:10.1007/s11235-019-00599-z.
38. Mohamed NN, Mohd Yussoff Y, Ahmed Saleh M, Hashim H. Hybrid cryptographic approach for Internet ofhybrid cryptographic approach for Internet of Things applications: a review. J Inf Commun Technol. 2020;19:279–319. doi:10.32890/jict2020.19.3.1.
39. Alterazi HA, Kshirsagar PR, Manoharan H, Selvarajan S, Alhebaishi N, Srivastava G, et al. Prevention of cyber security with the internet of things using particle swarm optimization. Sensors. 2022;22(16):6117. doi:10.3390/s22166117.
40. Lau CH, Yeung KH, Yan F, Chan S. Blockchain-based authentication and secure communication in IoT networks. Secur Priv. 2023;6(6):e319. doi:10.1002/spy2.319.
41. Tertytchny G, Karbouj H, Hadjidemetriou L, Charalambous C, Michael MK, Sazos M, et al. Demonstration of man in the middle attack on a commercial photovoltaic inverter providing ancillary services. In: Proceedings of the 2020 IEEE CyberPELS (CyberPELS); 2020 Oct 13; Miami, FL, USA. doi:10.1109/cyberpels49534.2020.9311531.

42. Purnama H, Mambo M. IHIBE: a hierarchical and delegated access control mechanism for IoT environments. Sensors. 2024;24(3):979. doi:10.3390/s24030979.
43. Muzammil MB, Bilal M, Ajmal S, Shongwe SC, Ghadi YY. Unveiling vulnerabilities of web attacks considering man in the middle attack and session hijacking. IEEE Access. 2024;12(7):6365–75. doi:10.1109/access.2024.3350444.
44. Fereidouni H, Fadeitcheva O, Zalai M. IoT and man-in-the-middle attacks. Secur Priv. 2025;8(2):e70016. doi:10.1002/spy2.70016.
45. Chiadighikaobi IR, Katuk N, Osman B. DMUAS-IoT: a decentralised multi-factor user authentication scheme for IoT systems. Int J Comput. 2022;424–34. doi:10.47839/ijc.21.4.2777.
46. Alharbi IA, Almalki AJ, Alyami M, Zou C, Solihin Y. Profiling attack on WiFi-based IoT devices using an eavesdropping of an encrypted data frames. Adv Sci Technol Eng Syst J. 2022;7(6):49–57. doi:10.25046/aj070606.
47. Arpaia P, Caputo F, Cioffi A, Esposito A. The role of metrology in the cyber-security of embedded devices. Acta IMEKO. 2023;12(2):1–6. doi:10.21014/actaimeko.v12i2.1455.
48. Neto ECP, Dadkhah S, Ferreira R, Zohourian A, Lu R, Ghorbani AA. CICIoT2023: a real-time dataset and benchmark for large-scale attacks in IoT environment. Sensors. 2023;23(13):5941. doi:10.3390/s23135941.
49. Neeli J, Patil S. Insight to security paradigm, research trend & statistics in Internet of Things (IoT). Glob Transitions Proc. 2021;2(1):84–90. doi:10.1016/j.gltp.2021.01.012.
50. Meneghello F, Calore M, Zucchetto D, Polese M, Zanella A. IoT: internet of threats? A survey of practical security vulnerabilities in real IoT devices. IEEE Internet Things J. 2019;6(5):8182–201. doi:10.1109/JIOT.2019.2935189.
51. Kasper T, Oswald D, Paar C. Security of wireless embedded devices in the real world. In: Proceedings of the Information Security Solutions Europe 2011 Conference; 2011 Nov 22–23; Prague, Czech Republic. doi:10.1007/978-3-8348-8652-1_16.
52. Shailendra, Joseph KT. Analysis on IoT networks security: threats, risks, ESP8266 based penetration testing device and defense framework for IoT infrastructure. In: Proceedings of the 2023 3rd International Conference on Intelligent Technologies (CONIT); 2023 Jun 23–25; Hubli, India. doi:10.1109/CONIT59222.2023.10205679.
53. Msgna M. Anatomy of attacks on IoT systems: review of attacks, impacts and countermeasures. J Surveill Secur Saf. 2022;3(4):150–73. doi:10.20517/jsss.2022.07.
54. Georgiana Dorobantu O, Halunga S. Security threats in IoT. In: Proceedings of the 2020 International Symposium on Electronics and Telecommunications (ISETC); 2020 Nov 5–6; Timisoara, Romania. doi:10.1109/isetc50328.2020.9301127.
55. Tabari AZ, Ou X. A first step towards understanding real-world attacks on IoT devices. arXiv:2003.01218. 2020. doi:10.48550/arXiv.2003.01218.
56. Raghuprasad A, Padmanabhan S, Arjun Babu M, Binu PK. Security analysis and prevention of attacks on IoT devices. In: Proceedings of the 2020 International Conference on Communication and Signal Processing (ICCSP); 2020 Jul 28–30; Chennai, India. doi:10.1109/iccsp48568.2020.9182055.
57. Nawir M, Amir A, Yaakob N, Lynn OB. Internet of Things (IoT): taxonomy of security attacks. In: Proceedings of the 2016 3rd International Conference on Electronic Design (ICED); 2016 Aug 11–12; Phuket, Thailand. doi:10.1109/ICED.2016.7804660.
58. Yuan B, Wu Y, Yang M, Xing L, Wang X, Zou D, et al. Smartpatch: verifying the authenticity of the trigger-event in the IoT platform. IEEE Trans Dependable Secure Comput. 2023;20(2):1656–74. doi:10.1109/tdsc.2022.3162312.
59. Yang YS, Lee SH, Chen WC, Yang CS, Huang YM, Hou TW. TTAS: trusted token authentication service of securing SCADA network in energy management system for industrial Internet of Things. Sensors. 2021;21(8):2685. doi:10.3390/s21082685.
60. Sasirega L, Shanthi C. Lightweight ECC and token based authentication mechanism for WSN-IoT. Sci Tech J Inform Technol Mech Optics. 2022;22(2):332–8. doi:10.17586/2226-1494-2022-22-2-332-338.
61. Pawar CR, Mandlik RS. IoT based smart city: security issues and tokenization, pseudonymization, tunneling techniques used for data protection. Int J Trend Sci Res Dev. 2020;4(4):946–9.
62. Velamakanni RS, Patwal DPS. Enhancing IoT security through experimental methods and blockchain integration. Eatp. 2024;30(5):8859–70. doi:10.53555/kuey.v30i5.4468.

63. Myridakis D, Papafotikas S, Kalovrektis K, Kakarountas A. Enhancing security on IoT devices via machine learning on conditional power dissipation. Electronics. 2020;9(11):1799. doi:10.3390/electronics9111799.
64. Krishna RR, Priyadarshini A, Jha AV, Appasani B, Srinivasulu A, Bizon N. State-of-the-art review on IoT threats and attacks: taxonomy, challenges and solutions. Sustainability. 2021;13(16):9463. doi:10.3390/su13169463.
65. Khan M, Chen Y. A randomized switched-mode voltage regulation system for IoT edge devices to defend against power analysis based side channel attacks. In: Proceedings of the 2021 IEEE Intl Conf on Parallel & Distributed Processing with Applications, Big Data & Cloud Computing, Sustainable Computing & Communications, Social Computing & Networking (ISPA/BDCloud/SocialCom/SustainCom); 2021 Sep 30–Oct 3; New York, NY, USA. doi:10.1109/ispa-bdcloud-socialcom-sustaincom52081.2021.00238.
66. Xenofontos C, Zografopoulos I, Konstantinou C, Jolfaei A, Khan MK, Choo KR. Consumer, commercial, and industrial IoT (in)security: attack taxonomy and case studies. IEEE Internet Things J. 2022;9(1):199–221. doi:10.1109/JIOT.2021.3079916.
67. NIST SP 1800-15A. Securing small-business and home Internet of Things (IoT) devices. Gaithersburg, MD, USA: National Institute of Standards and Technology; 2021.
68. Gebresilassie SK, Rafferty J, Morrow P, Chen L, Abu-Tair M, Cui Z. Distributed, secure, self-sovereign identity for IoT devices. In: Proceedings of the 2020 IEEE 6th World Forum on Internet of Things (WF-IoT); 2020 Jun 2–16; New Orleans, LA, USA. doi:10.1109/wf-iot48130.2020.9221144.
69. Lee I. Internet of Things (IoT) cybersecurity: literature review and IoT cyber risk management. Future Internet. 2020;12(9):157. doi:10.3390/fi12090157.
70. Son H, Kim BS, Cho J, Lee B. ASM: augmented security module for commercial IoT devices. Teh Vjesn. 2024;31(1):48–55. doi:10.17559/tv-20230608000709.
71. Bakır Ç. New hybrid distributed attack detection system for IoT. Bitlis Eren Üniversitesi Fen Bilim Derg. 2024;13(1):232–46. doi:10.17798/bitlisfen.1380547.
72. Bryant B, Saiedian H. Key challenges in security of IoT devices and securing them with the blockchain technology. Secur Priv. 2022;5(5):e251. doi:10.1002/spy2.251.
73. Alkhamisi K. An analysis of security attacks on IoT applications. Int J Inf Syst Comput Technol. 2023;2(1):44–9. doi:10.58325/ijisct.002.01.0053.
74. Gelgi M, Guan Y, Arunachala S, Rao MSS, Dragoni N. Systematic literature review of IoT botnet DDOS attacks and evaluation of detection techniques. Sensors. 2024;24(11):3571. doi:10.3390/s24113571.
75. Kim D, Jeon S, Shin J, Seo JT. Design the IoT botnet defense process for cybersecurity in smart city. Intell Autom Soft Comput. 2023;37(3):2979–97. doi:10.32604/iasc.2023.040019.
76. Huraj L, Šimon M, Horák T. Resistance of IoT sensors against DDoS attack in smart home environment. Sensors. 2020;20(18):5298. doi:10.3390/s20185298.
77. Nguyen TD, Rieger P, Miettinen M, Sadeghi AR. Poisoning attacks on federated learning-based IoT intrusion detection system. In: Proceedings of the 2020 Workshop on Decentralized IoT Systems and Security; 2020 Feb 23; San Diego, CA, USA. doi:10.14722/diss.2020.23003.
78. Ahakonye LAC, Nwakanma CI, Kim DS. Tides of blockchain in IoT cybersecurity. Sensors. 2024;24(10):3111. doi:10.3390/s24103111.
79. Anitha R, Murugan M. Privacy-preserving collaboration in blockchain-enabled IoT: the synergy of modified homomorphic encryption and federated learning. Int J Commun Syst. 2024;37(18):e5955. doi:10.1002/dac.5955.
80. Al-Nbhany WANA, Zahary AT, Al-Shargabi AA. Blockchain-IoT healthcare applications and trends: a review. IEEE Access. 2024;12(3):4178–212. doi:10.1109/access.2023.3349187.
81. Sharma S, Sharma T, Tiwari A, Gupta S. Streamlining IoT-driven data using blockchain. Int Res J Adv Engg Mgt. 2024;2(5):1509–14. doi:10.47392/irjaem.2024.0204.
82. Raman JA, Varadharajan V. HoneyNetCloud investigation model, a preventive process model for IoT forensics. Ingénierie Des Systèmes D Inf. 2021;26(3):319–27. doi:10.18280/isi.260309.
83. Wu J, Zhang J, Ji Y. DCEC: D2D-enabled cost-aware cooperative caching in MEC networks. Electronics. 2023;12(9):1974. doi:10.3390/electronics12091974.

84. Zhao M, Ding Y. Dual-server identity-based encryption with authorized equality test for IoT data in clouds. Secur Commun Netw. 2022;2022(4):4905763. doi:10.1155/2022/4905763.
85. Upadhyay D, Gaikwad N, Zaman M, Sampalli S. Investigating the avalanche effect of various cryptographically secure hash functions and hash-based applications. IEEE Access. 2022;10(6):112472–86. doi:10.1109/access.2022.3215778.
86. Ngo CT, Eshraghian JK, Hong JP. An area-optimized and power-efficient CBC-PRESENT and HMAC-PHOTON. Electronics. 2022;11(15):2380. doi:10.3390/electronics11152380.
87. Kumari T, Singh D, Singh B. Multi-chaotic maps and blockchain based image encryption. Concurr Comput. 2024;36(14):e8092. doi:10.1002/cpe.8092.
88. Lahraoui Y, Lazaar S, Amal Y, Nitaj A. Securing data exchange with elliptic curve cryptography: a novel hash-based method for message mapping and integrity assurance. Cryptography. 2024;8(2):23. doi:10.3390/cryptography8020023.
89. Uriawan W, Ramadita R, Putra RD, Siregar RI, Addiva R. Authenticate and verification source files using SHA256 and HMAC algorithms. Comput Sci. Forthcoming. 2024. doi:10.20944/preprints202407.0075.v1.
90. Alhasan AQA, Rohani MF, Abu-Ali MS. Ultra-lightweight mutual authentication protocol to prevent replay attacks for low-cost RFID tags. IEEE Access. 2024;12:50925–34. doi:10.1109/access.2024.3386100.
91. Fathy C, Ali HM. A secure IoT-based irrigation system for precision agriculture using the expeditious cipher. Sensors. 2023;23(4):2091. doi:10.3390/s23042091.
92. Idriss TA, Idriss HA, Bayoumi MA. A lightweight PUF-based authentication protocol using secret pattern recognition for constrained IoT devices. IEEE Access. 2021;9:80546–58. doi:10.1109/access.2021.3084903.
93. Bamashmos S, Chilamkurti N, Shahraki AS. Two-layered multi-factor authentication using decentralized blockchain in an IoT environment. Sensors. 2024;24(11):3575. doi:10.3390/s24113575.
94. Okeke RO, Orimadike SO. Enhanced cloud computing security using application-based multi-factor authentication (MFA) for communication systems. Eur J Electr Eng Comput Sci. 2024;8(2):1–8. doi:10.24018/ejece.2024.8.2.593.
95. Preuveneers D, Joos S, Joosen W. AuthGuide: analyzing security, privacy and usability trade-offs in multi-factor authentication. In: Trust, privacy and security in digital business. Berlin/Heidelberg, Germany: Springer; 2021. p. 155–70. doi:10.1007/978-3-030-86586-3_11.
96. Almeghlef SM, AL-Ghamdi AA, Ramzan MS, Ragab M. Machine learning-based DoS amplification attack detection against constrained application protocol. Appl Sci. 2023;13(13):7391. doi:10.3390/app13137391.
97. Beniwal R, Kumar V, Sharma V. A multi-cluster security framework for healthcare IoT: the synergy of redundant Byzantine fault tolerance with extensions and coati-based network. Trans Emerg Telecommun Technol. 2025;36(3):e70098. doi:10.1002/ett.70098.
98. Hossain M, Kayas G, Hasan R, Skjellum A, Noor S, Riazul Islam SM. A holistic analysis of Internet of Things (IoT) security: principles, practices, and new perspectives. Future Internet. 2024;16(2):40. doi:10.3390/fi16020040.
99. Kim TH. A study on impact of lightweight cryptographic systems on Internet of Things-based applications. Asia Pac J Convergent Res Interchange. 2024;10(1):49–59. doi:10.47116/apjcri.2024.01.05.
100. El Hadj Youssef W, Abdelli A, Khriji L, Machhout M. Perspective chapter: lightweight ciphers for IoT data protection. In: Online identity—an essential guide. London, UK: IntechOpen; 2024. doi:10.5772/intechopen.1002608.
101. Quincozes VE, Quincozes SE, Kazienko JF, Gama S, Cheikhrouhou O, Koubaa A. A survey on IoT application layer protocols, security challenges, and the role of explainable AI in IoT (XAIoT). Int J Inf Secur. 2024;23(3):1975–2002. doi:10.1007/s10207-024-00828-w.
102. Hu T, Yang S, Wang Y, Li G, Wang Y, Wang G, et al. N-accesses: a blockchain-based access control framework for secure IoT data management. Sensors. 2023;23(20):8535. doi:10.3390/s23208535.
103. Zhang T, Wang Y, Gong B, Xu J, Wu J, Wan C. Privacy protection during the issuance and revocation of verifiable credentials in self-sovereign identity. Concurr Comput Pract Exp. 2025;37(9–11):e70084. doi:10.1002/cpe.70084.

104. Janes B, Crawford H, OConnor TJ. Never ending story: authentication and access control design flaws in shared IoT devices. In: Proceedings of the 2020 IEEE Security and Privacy Workshops (SPW); 2020 May 21; San Francisco, CA, USA. doi:10.1109/spw50608.2020.00033.
105. Perera MNS, Koshiba T. Almost fully secured lattice-based group signatures with verifier-local revocation. Cryptography. 2020;4(4):33. doi:10.3390/cryptography4040033.
106. Gupta BB, Narayan S. A key-based mutual authentication framework for mobile contactless payment system using authentication server. J Organ End User Comput. 2021;33(2):1–16. doi:10.4018/joeuc.20210301.oa1.
107. Badhib A, Alshehri S, Cherif A. A robust device-to-device continuous authentication protocol for the Internet of Things. IEEE Access. 2021;9:124768–92. doi:10.1109/access.2021.3110707.
108. Mondal B, Arif I, Barua T, Chowdhury MRI. Data security in iot devices and sensor networks for robust threat detection and privacy protection. Acad J Sci Technol Eng Math Educ. 2024;1(1):19. doi:10.69593/ajieet.v1i01.116.
109. Munshi A, Alshawi B. Hybrid encryption model for secured three-phase authentication protocol in IoT. J Sens Actuator Netw. 2024;13(4):41. doi:10.3390/jsan13040041.
110. Ferrag MA, Friha O, Hamouda D, Maglaras L, Janicke H. Edge-IIoTset: a new comprehensive realistic cyber security dataset of IoT and IIoT applications for centralized and federated learning. IEEE Access. 2022;10:40281–306. doi:10.21227/mbc1-1h68.
111. Vutukuru SR, Lade SC. SecureIoT: novel machine learning algorithms for detecting and preventing attacks on IoT devices. J Electr Syst. 2024;19(4):315–35. doi:10.52783/jes.641.
112. Othmen S, Mansouri W, Asklany S. Robust and secure routing protocol based on group key management for Internet of Things systems. Eng Technol Appl Sci Res. 2024;14(3):14402–10. doi:10.48084/etasr.7115.
113. Truong TC, Diep QB, Zelinka I. Artificial intelligence in the cyber domain: offense and defense. Symmetry. 2020;12(3):410. doi:10.3390/sym12030410.
114. Hazratifard M, Gebali F, Mamun M. Using machine learning for dynamic authentication in telehealth: a tutorial. Sensors. 2022;22(19):7655. doi:10.3390/s22197655.
115. Harbi Y, Refoufi A, Aliouat Z, Harous S. Improved bio-inspired security scheme for privacy-preserving in the Internet of Things. Peer Peer Netw Appl. 2022;15(6):2488–502. doi:10.1007/s12083-022-01372-x.
116. Liu G, Li W, Fan X, Li Z, Wang Y, Ma H. An image encryption algorithm based on discrete-time alternating quantum walk and advanced encryption standard. Entropy. 2022;24(5):608. doi:10.3390/e24050608.
117. Kolay S, Hiwarkar T. IoT security: issues, the best practices and open challenges. Int J Inf Secur Eng. 2023;1(2):7–13. doi:10.37591/ijise.v01i02.124811.