# IoT Authentication Protocols: Challenges, and Comparative Analysis

AMAR N.ALSHEAVI, School of Computer Science and Technology, University of Science and Technology of China, China and Sana'a University, Yemen

AMMAR HAWBANI*, School of Computer Science, Shenyang Aerospace University, China

WAJDY OTHMAN†, Xinchuang Haihe Laboratory (Advanced Computing and Key Software Haihe Lab), and jointly with the School of Cyber Science, Nankai University, China

XINGFU WANG, School of Computer Science and Technology, University of Science and Technology of China, China

GAMIL R. S. QAID, Department of Computer Engineering, Computer Science and Engineering Faculty, Hodeidah University, Al-Hudaydah, Yemen

LIANG ZHAO, School of Computer Science, Shenyang Aerospace University, China

AHMED AL-DUBAI, School of Computing, Edinburgh Napier University, United Kingdom

ZHI LIU, Department of Computer and Network Engineering, The University of Electro-Communications, Japan

A.S. ISMAIL, Faculty of Science, Zagazig University, Egypt

RUTVIJ H. JHAVERI, School of Technology, Pandit Deendayal Energy University, India

SAEED H. ALSAMHI, Technological University of the Shannon Midlands Midwest, Ireland

MOHAMMED A. A. AL-QANESS, College of Physics and Electronic Information Engineering, Zhejiang Normal University, China

*Corresponding author
†Corresponding author

Authors' addresses: Amar N.Alsheavi, ammarnabil23050@gmail.com, School of Computer Science and Technology, University of Science and Technology of China, JinZhai, Hefei, China, 230026 and Sana'a University, Yemen, ; Ammar Hawbani, anmande@ustc.edu.cn, School of Computer Science, Shenyang Aerospace University, Daoyinandajie Road, Shenyang, China, 230026; Wajdy Othman, wajdy@mail.ustc.edu.cn, Xinchuang Haihe Laboratory (Advanced Computing and Key Software Haihe Lab), and jointly with the School of Cyber Science, Nankai University, Binhai New Area, Tianjin, China, 300450; Xingfu Wang, wangxfu@ustc.edu.cn, School of Computer Science and Technology, University of Science and Technology of China, JinZhai, Hefei, China, 230026; Gamil R. S. Qaid, dr.g_qaid@hoduniv.net.ye, Department of Computer Engineering, Computer Science and Engineering Faculty, Hodeidah University, Al-Hudaydah, , Hodeidah, Yemen, 230026; Liang Zhao, lzhao@sau.edu.cn, School of Computer Science, Shenyang Aerospace University, Daoyinandajie Road, Shenyang, China, 110136; Ahmed Al-Dubai, School of Computing, Edinburgh Napier University, New York, United Kingdom, a.al-dubai@napier.ac.uk; Zhi Liu, Department of Computer and Network Engineering, The University of Electro-Communications, Tokyo, Japan, , liu@ieee.org; A.S. Ismail, Faculty of Science, Zagazig University, JinZhai, Hefei, Egypt, 44519, a.sami@zu.edu.eg; Rutvij H. Jhaveri, School of Technology, Pandit Deendayal Energy University, , Gandhinagar, India,, rutvij.jhaveri@sot.pdpu.ac.in; Saeed H. Alsamhi, Technological University of the Shannon Midlands Midwest, Ireland, salsamhi@ait.ie; Mohammed A. A. Al-qaness, alqaness@zjnu.edu.cn, College of Physics and Electronic Information Engineering, Zhejiang Normal University, Jinhua, Zhejiang, China, 321004.



Manuscript submitted to ACM

In the ever-evolving information technology landscape, the Internet of Things (IoT) is a groundbreaking concept that bridges the physical and digital worlds. It is the backbone of an increasingly sophisticated interactive environment, yet it is a subject of intricate security challenges spawned by its multifaceted manifestations. Central to securing IoT infrastructures is the crucial aspect of authentication, necessitating a comprehensive examination of its nuances, including benefits, challenges, opportunities, trends, and societal implications. In this paper, we thoroughly review the IoT authentication protocols, addressing the main challenges such as privacy protection, scalability, and human factors that may impact security. Through exacting analysis, we evaluate the strengths and weaknesses of existing authentication protocols and conduct a comparative performance analysis to evaluate their effectiveness and scalability in securing IoT environments and devices. At the end of this study, we summarize the main findings and suggest ways to improve the security of IoT devices in the future.

CCS Concepts: • **General and reference → Surveys and overviews**; • **IoT → Authentication protocols;Security and privacy;Attacks in IoT Authentication;Challenges in IoT authentication**.

Additional Key Words and Phrases: Authentication Protocols, Key Agreement, Security, Privacy Concerns, Blockchain, Machine learning, Cyber Threats in IoT, Scalability in Authentication, Internet of Things.

**ACM Reference Format:**
Amar N.Alsheavi, Ammar Hawbani, Wajdy Othman, Xingfu Wang, Gamil R. S. Qaid, Liang Zhao, Ahmed Al-Dubai, Zhi Liu, A.S. Ismail, Rutvij H. Jhaveri, Saeed H. Alsamhi, and Mohammed A. A. Al-qaness. 2024. IoT Authentication Protocols: Challenges, and Comparative Analysis. 1, 1 (October 2024), 35 pages. https://doi.org/10.1145/nnnnnnn.nnnnnnn

## 1 INTRODUCTION

The Internet of Things (IoT) is a magical technology that interconnects objects and technology in a way that resembles the imagination of science fiction. This amazing world offers a marvelous blend of interactions, data, and communication between things, creating an innovative and marvelous environment. With this tremendous progress come new challenges, the most significant of which is how to ensure security and trust in this connected universe.

IoT links living and nonliving entities with inanimate objects to create ecological systems and stands as one of the most recent and advanced computing paradigms developed in the twenty-first century. Integrated into the IoT are technologies such as Wireless Sensor Networks (WSNs), which have been around since the 1980s. An integral part of IoT is the WSN technology, which consists of wirelessly interconnected sensor nodes that connect to real-world entities through digital interfaces.

IoT has rapidly emerged as a comprehensive concept for enabling the integration of the physical and digital worlds. Although IoT offers numerous benefits, such as enhanced efficiency and convenience, it poses significant security challenges due to its distributed, diverse, and resource-constrained nature. Among these challenges, authentication plays a critical role in protecting IoT devices and services against various threats, including unauthorized access and data tampering [49].

In recent years, the IoT has seen widespread adoption across various sectors, leading to a transformative shift in how smart devices interact with each other and with users. As IoT usage expands rapidly, the issues related to security and data protection have become increasingly complex and urgent. Securing communications between connected devices within the IoT network presents a major challenge, particularly with the growing number of cyber-attacks targeting these systems.

IoT technology integrates physical and digital entities through interconnected platforms and networks, enabling the delivery of new and diverse services. However, this deep integration requires advanced security measures to ensure data integrity and protect privacy. Authentication emerges as a fundamental pillar in this context, ensuring that connected devices within the network are trustworthy and that the communications between them are secure. As the number of connected devices grows and applications diversify into areas such as healthcare, transportation, agriculture, and smart homes, the biggest challenge lies maintaining a reliable and secure environment amidst the increasing complexity of these networks. This requires the development of robust and innovative authentication solutions that can meet the increasing cyber threat, thus improving the security and trust of users in these systems[132], [40], [74].

Table 1. List of important abbreviations

| Abbreviation | Description | Abbreviation | Description |
|---|---|---|---|
| 2FA | Two-Factor Authentication | MITM | Man-in-the-Middle |
| AI | Artificial Intelligence | MQTT | Message Queuing Telemetry Transport |
| AP | Authentication Protocol | OTPs | One-time Passwords |
| APIs | Application Programming Interfaces | OCSP | Online Certificate Status Protocol |
| CRL | Certificate Revocation Lists | PIN | Personal Identification Number |
| CA | Certificate Authority | PKI | Public Key Infrastructure |
| CoAP | Constrained Application Protocol | PUF | Physically Unclonable Functions |
| D2D | Device-to-Device | QR | Quick Response Code |
| DDoS | Distributed Denial of Service | RFID | Radio-Frequency Identification Authentication |
| DoS | Denial-of-Service | SMS | Short Message Service |
| HMAC | Hash-based Message Authentication Code | SSL | Secure Sockets Layer |
| HOTP | HMAC-based One-Time Password | TLS | Transport Layer Security |
| HTTPS | Hypertext Transfer Protocol Secure | TOCTOU | Time-of-Check to Time-of-Use |
| IIoT | Industrial Internet of Things | TOTP | Time-based One-Time Password |
| IoT | Internet of Things | USB | Universal Serial Bus |
| IoV | Internet of Vehicles | VPNs | Virtual Private Networks |
| MFA | Multi-factor Authentication | WSN | Wireless Sensor Networks |

The cloud is the setting or location where intelligent and powerful apps are present and have the capacity to gather and combine data from IoT devices with data from other sources, perform data analysis to find issues, forecast the future and spot trends. Consumer applications give users access to remote IoT devices and let them monitor the data processed in the cloud [15]. These devices connect to each other to collect and exchange data and information [64]. As a result, security and data response time are subject to extremely high demands due to the sheer volume of devices and information [59].

In the world of IoT, authentication is a fundamental and vital process. This process is one of the key factors that contribute to the security and protection of devices and data in this interconnected world. As time progresses, the importance of authentication in the IoT domain grows due to the increasing cyber threats. It plays a critical role in protecting devices and data from breaches and ensuring trust in communication between devices and users. IoT has evolved beyond being just a modern technology; it has become an integral part of our daily lives. It is used in various sectors, such as healthcare, transportation, agriculture, and smart homes. This broad integration underscores the importance of securing devices and data to prevent unauthorized access and protect privacy and safety. In this context, authentication appears as the security process that helps verify the identity of devices and users within the IoT environment. Strong authentication is the key to building a trusted IoT environment and significantly contributes to securing communication processes and providing protection against growing cyber threats.

### 1.1 Research Questions

This survey aims to answer the following three fundamental questions:

- **RQ1. Authentication in IoT:** How do advanced authentication methods like password-based, certificate-based, biometric, two-factor, and multi-factor protocols enhance security and efficiency to balance high security with a user-friendly experience in IoT environments, considering their unique challenges and proposed solutions? (This question aligns with the content detailed in Sections 2, 3, and 4).
- **RQ2. Tackling IoT Security:** What key security risks, such as man-in-the-middle, denial-of-service, replay, and brute-force attacks, does IoT authentication face, along with concerns around data privacy and scalability? How can multi-layered security solutions effectively address these challenges while ensuring scalability and efficiency? (This question corresponds to discussions presented in Sections 2, 3, and 4).
- **RQ3. Optimizing IoT Authentication:** How do various authentication protocols, including password-based, certificate-based, biometric, two-factor, multi-factor and single-factor authentication, perform against criteria such as security, privacy, scalability, usability, and cost-effectiveness? This question aims to analyze and evaluate the strengths and limitations of each approach through a comprehensive comparative analysis, shedding light on the most effective strategies to improve security in IoT environments. (This question relates to the insights highlighted in Sections 2, 3, and 4).

### 1.2 Contributions

The main contributions of this work are as follows:

(1) **Exploring IoT Authentication Protocols**: We conduct a thorough review of various IoT APs, including password-based, certificate-based, biometric, two-factor, and multifactor methods. We evaluated the efficacy of each protocol, emphasizing their unique features and roles in securing IoT devices.
(2) **Unraveling Challenges in IoT Security**: We review key challenges in IoT authentication, including security risks, privacy concerns, and scalability issues. We navigate the complexities of implementing robust authentication methods in diverse IoT environments and propose potential strategies to overcome these challenges effectively.
(3) **Assessing and Comparing IoT Security Protocols**: We perform a thorough comparative analysis of different IoT APs based on various evaluation criteria; we highlight the strengths and weaknesses of each protocol, offering a detailed perspective on their overall performance. Our analysis aims to inform the selection of suitable authentication methods tailored to the needs of various IoT applications.

### 1.3 Related Surveys

Table 2 presents the comprehensive classification and flow of papers; IoT presents multiple challenges when it comes to security and authentication issues. Trust in an IoT environment is based on the effectiveness and security of the protocols used for authentication and protection. Therefore, understanding and reviewing relevant research and work is of paramount importance to enhance security and privacy in this evolving context. The objectives of this research are to review and analyze a set of related research papers that discuss authentication issues in IoT, with a focus on aspects such as privacy, security, and performance. This study differentiates itself from previous surveys by offering a detailed comparison of IoT authentication protocols, focusing specifically on their effectiveness in improving security within IoT frameworks. It contributes a unique perspective by examining how different protocols address emerging security challenges, providing valuable information on the evolution of IoT security measures. In addition, this paper introduces new methodologies and technologies that have recently been adopted in the security of the IoT, marking a significant advancement over previous reviews.

This is done by reviewing research conducted on IoT in recent years, as shown in Table 2, which includes, in the context of IoT APs, a variety of studies exploring significant challenges and trends in this advanced IoT. This table serves as a valuable source for understanding recent authentication developments in the context of IoT. It highlights a diverse set of references that address topics such as security, privacy, challenges associated with IoT devices, and the use of modern technologies such as encryption and IoT protocols to achieve appropriate security. Furthermore, the table reflects ongoing efforts to strike a balance between security and privacy protection, particularly in sensitive areas such as healthcare-related IoT systems. This diversity in research topics reflects the complexity of authentication in the IoT and provides the reader with a comprehensive overview of future challenges and potential research trends in this evolving domain.

Table 2 illustrates that while many studies have addressed APs in IoT, most of them have focused on specific aspects such as privacy or security without providing a comprehensive analysis that integrates the various dimensions of these protocols. For example, the study by Nishant et al. [36] focused on privacy and security issues in IoT, examining solutions like encryption and statistical analysis. Another study by Pham et al. [110] explored lightweight APs, aiming to balance security with resource efficiency, which is crucial in resource-constrained systems. On the other hand, Shariq et al. [134] utilized machine learning techniques to analyze behavioral patterns and enhance authentication accuracy.

Some studies have investigated the use of digital signatures and encryption to protect data, while others have focused on techniques like machine learning to analyze behavioral patterns in systems. However, there remains a gap in the literature in terms of the provision of a comprehensive and in-depth comparison of various APs, with a focus on their effectiveness in addressing the diverse security challenges facing IoT.

This survey distinguishes itself from previous studies by offering a thorough analysis of IoT APs. Not only reviews existing protocols, it also goes beyond that by providing a detailed comparative analysis that covers a wide range of critical criteria such as

Table 2. A galaxy of related studies: exploring IoT authentication protocols

| Reference (Year) | Applications | Challenges | Enabling Technologies |
|---|---|---|---|
| [21] (2020) | - A secure and scalable IoT system - Utilizes multi-factor authentication and lightweight encryption - Provides secure data sharing - Applicable for traffic monitoring | - System efficiency to reduce user burden - Protection against electronic attacks - Scalability to meet application requirements | - Multi-factor authentication for identity verification - Lightweight encryption for data security - Utilizing big data for analysis and discovery |
| [134] (2021) | - A new AP in IoT - Relies on vector space - Ensures privacy and security - Provides secure authentication for users | - Efficiency and compatibility with limited resources - Privacy during user identity verification - Security and protection against internet attacks | - Using machine learning to create user models - Employing artificial intelligence to make data-driven decisions - Using encryption to secure data transmission |
| [105] (2021) | - Blockchain authentication for secure participation in cloud IoT - Provides a secure and private way for sensitive data - Applicable for data sharing between organizations | - Blockchain authentication in a cloud IoT environment - Secure data distribution - Ensuring security and privacy | - Blockchain technology for security and authentication - IoT: Enabling device communication and data sharing - Emphasis on security and privacy |
| [110] (2021) | - Lightweight AP for IoT - Preserving privacy in D2D communication - Secure communication among IoT devices - Various applications of the protocol | - Efficiency and application in resource-limited systems - Preserving user privacy - Providing security against electronic attacks | - Encryption for securing data during transmission - Digital signature for verifying data integrity - Identity verification to determine the user's identity |
| [9] (2022) | - Fingerprint authentication Systems - Face and voice recognition authentication systems - Review of strengths and weaknesses | - Cost of modern systems - Compatibility with various devices - User acceptance of these systems | - Facial recognition for identity verification - Voice recognition for identity verification - Fingerprint recognition for identity verification |
| [19] (2022) | - Security and privacy concerns in IoT - Addresses concerns such as phishing attacks, denial of service, and hacking - Review of proposed solutions for these concerns | - Addressing weaknesses in diverse IoT systems - Deployment: Challenges in responding to attacks in globally deployed IoT systems Rapid evolution: The need for continuous security solution updates | - Statistical analysis: Used to discover data patterns - Machine learning: Employed for predicting future behavior - AI: Contributes to data-driven decision making |
| [73] (2023) | - Hybrid centralized and blockchain-based authentication structure - Secure data sharing in IoT - Multiple applications such as manufacturing and transportation | - Centralized architecture and blockchain in IoT - Achieving a balance between security and efficiency - Seamless compatibility and integration | - Blockchain technology: Used to achieve a high level of security and authentication through integration with centralized architectural structures, IoT: Enables communication and integration between diverse devices in an IoT environment - Security and Integration: Encourage achieving a balance between security and efficiency in a diverse IoT environment |
| [117] (2023) | - Authentication and key management in IoT - Providing a solution for security challenges in IoT | - Key size and management - Diversity in IoT devices - Global deployment of IoT systems | - Data encryption for protection - Digital signature for verification - Secure key management for storage and administration |
| [36] (2023) | - Privacy and security issues in IoT - Diverse topics addressed: data security, user privacy, infrastructure protection - Review of proposed solutions | - Large and diverse IoT device volume - Global proliferation of IoT systems | - Statistical analysis of IoT data - Machine learning for behavior prediction - Using AI in decision making |
| [147] (2023) | - A blockchain-based authentication scheme is presented for the IoT-based healthcare system - It provides a secure means for users to access their health data - It can be applied in various fields | - Authentication and keys in healthcare IoT - Security and sensitive data challenges - Secure integration of blockchain technology | - Blockchain technology: for security and authentication - IoT for data monitoring and interaction - Security: for data protection and confidentiality |
| This Paper (2024) | - Investigate IoT APs - Focus on the information network between devices - Explore verification and security patterns | - Enhancing security against threats - Addressing potential attacks on IoT - Diversity and scale of IoT devices: Designing secure APs for various IoT devices is challenging. Security and privacy concerns: Protection from attacks and ensuring legitimate access are essential - Scalability: The research discusses the scalability of APs - AI and machine learning: They can be exploited in complex attacks - Increasing cyber threats: The research tackles the growing threats in IoT - Rapid growth of IoT systems: highlighting challenges related to rapid expansion | - Utilizing AI and blockchain - Implementing MFA techniques - Enhancing security and trust in the IoT environment - Advanced encryption for data protection |

security, privacy, scalability, and usability. The study also explores the complex challenges in IoT authentication, presenting innovative strategies to overcome these challenges, which have not been fully covered in previous studies. Furthermore, this survey aims to fill a clear gap in the literature by integrating modern technologies such as AI and blockchain to enhance IoT security, offering new insights and practical guidance for professionals in selecting the most effective protocols. This comprehensive and analytical approach sets this research apart from others and strengthens its ability to offer practical and sustainable solutions to IoT security challenges, making it a valuable and distinguished contribution to the current literature in this field.

### 1.4 Organization of the Paper

The outline of this paper is shown in Fig. 1. The remainder of this work is organized as follows. The review of IoT authentication protocols is given, where a wide range of methods are examined and analyzed with a discussion on the benefits and challenges associated with each type in Section 2. In Section 3 the challenges and issues of IoT authentications are illustrated. After that, the comparative analysis of IoT APs is given in Section 4. Following that, Section 5 highlights the learned lessons, offering valuable lessons for the future development of IoT authentication protocols. Finally, the conclusion of this paper is given in Section 6. Note that this

work includes a supplementary file, available online, which contains additional tables and detailed information. Tables and sections with underlined labels in the manuscript are cross-referenced from the supplementary file.

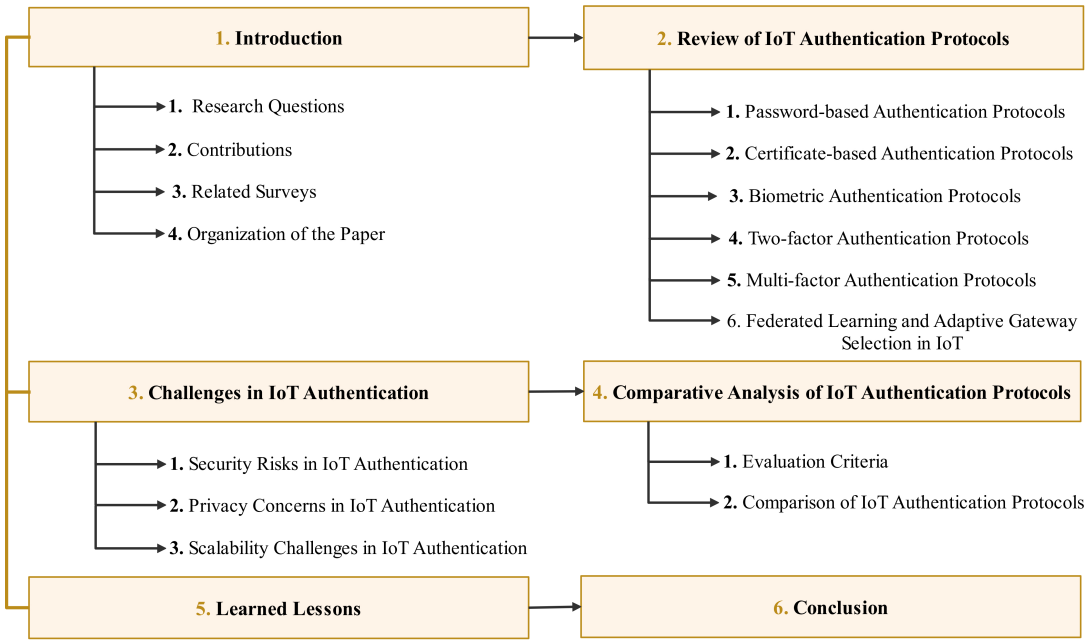


Fig. 1. The organization of the paper

Due to the comprehensive nature of this survey, we have carefully organized our analysis into a series of structured tables, which make it easier for readers to engage with the extensive data related to IoT authentication. The tables are categorized as follows: We began with Table 1, which includes a list of key abbreviations used to understand the terms in the research. Next, Table 2 provides an overview of studies on IoT authentication, highlighting the challenges and technologies used in various protocols. Table 3 compares APs such as HOTP and TOTP in terms of application suitability, adaptability, security, and cost-efficiency, offering recommendations for future improvements. Table 4 outlines the challenges and proposed solutions for managing X.509 certificates, focusing on practical measures to enhance security. Table 5 compares the Public Key Infrastructure (PKI) and X.509 certificate-based authentication in terms of security and usability. The table (available as Table 1 in the supplementary material), discusses biometric security models by comparing "Fuzzy Vault" techniques with cancelable biometrics, emphasizing recent innovations in this field. The table (available as Table 2 in the supplementary material), reviews developments in IoT security technologies, with a focus on strategies to protect against MITM attacks. The table (available as Table 3 in the supplementary material), details the impact of Denial-of-Service (DoS) attacks on IoT, highlighting the negative effects across different sectors. Table 6 addresses strategies to combat replay attacks in IoT, providing solutions to mitigate their impact. Table 7 analyzes the effects of brute-force attacks and discusses strategies to enhance security against these threats. Table 8 categorizes types of cyber-attacks and the tools used in IoT, aiding in understanding the associated security risks. Table 9 offers a comprehensive analysis of various security attacks, including their impacts, challenges, and possible solutions. Table 10 examines privacy concerns and their expected impact levels within the IoT context. Table 11 highlights the scalability challenges in IoT authentication, discussing related research challenges. Table 12 provides a detailed comparison of different APs, focusing on security and privacy standards. Table 13 compares the security and usability of password-based versus digital certificate-based authentication. Table 14 presents a comparison between biometric and two-factor authentication in terms of effectiveness and security. Lastly, Table 15 compares multi-factor authentication with single-factor authentication in terms of security and usability.

## 2 REVIEW OF IOT AUTHENTICATION PROTOCOLS

Authentication protocols verify identities, protect data, prevent cyberattacks, and establish trust. A diverse range of authentication methods have been employed in the IoT. In 2.1, we discuss password-based authentication methods and their use to verify user and device identities. We cover certificate-based authentication methods and their importance in enhancing the security of the IoT in 2.2. The challenges and solutions related to biometric data, such as fingerprints and voice recognition, are explored in 2.3. The two-factor authentication methods are explored in 2.4. Finally, in 2.5, we discuss the multifactor authentication methods.

### 2.1 Password-based Authentication Protocols

The IoT paradigm is expanding and undergoing constant development, with devices and items being linked to the Internet to exchange data and improve functionality. In this scenario, ensuring the security and privacy of devices and users through authentication plays a crucial role. Numerous IoT applications utilize password-based APs, which aid in confirming the identity of both users and connected devices. In the upcoming section, we will focus our attention on three significant APs, outlined as follows:

*2.1.1 HMAC-based One-Time Password (HOTP):* This AP relies on HMAC to generate OTPs based on time using a shared key. It is used in various settings that require increased security and safeguarding of accounts [62], [158]. Furthermore, it serves as a template for multifactor authentication, often applied to add an additional layer of security in various contexts, including IoT environments and other applications.

The HOTP implementation involves synchronization between the server and client, relying on two factors: the shared secret and the counter. This process yields a single use password (OTP) based on the shared secret and counter, valid for a brief duration before expiration [158]. HOTP stands out due to its relatively elevated security level, generating hashed passwords through HMAC using the shared key, thus making them less easily discernible [142]. Furthermore, HOTP is cost-effective and easy to implement in contrast to certain other MFA methods [80].

HOTP is also versatile, finding utility in various scenarios such as banking, e-commerce, and devices connected to the Internet [130]. It functions by generating a sequence of 6 to 8 digits, comprising random numbers derived from the shared key between the user and the server [62].

HOTP offers supplementary protection when employing temporary passwords with limited lifetimes. It operates autonomously without the need for an internet connection, making it suitable for offline situations [56]. However, sharing the shared key between the user and the server increases the complexity of key management. Consequently, the concept of an incrementing counter might be less utilized compared to the current time in specific scenarios. Caution should be exercised when reusing or tracking temporary passwords. Integrating with existing authentication systems could also pose challenges [156]. Addressing these hurdles requires safeguarding the shared key and ensuring authorized access. Regular key renewal is recommended to prevent electronic breaches and improve security. It is also essential to avoid tracking or storing temporary passwords during transmission [45], [133]. OTPs are vulnerable to brute-force attacks in which attackers attempt various passwords until they successfully log in. Counteracting this involves increasing the size of the token for greater complexity and setting expiration periods for OTP [130], [78], [69].

Network-based attacks intercept data sent between the client and the server, with the aim of infiltrating and manipulating data across the network. Encrypted communication (HTTPS) is employed to encrypt data transmitted over the network to counteract these attacks. Mechanisms for server authentication can also be applied to verify the server's identity before communication [62], [142], [78].

In summary, Authentication technologies are in a continuous state of evolution, with the potential for more robust and efficient methods to emerge in the future. These advancements could encompass 2FA, biometric recognition, and facial recognition.

*2.1.2 Time-based One-Time Password (TOTP):* This authentication mechanism relies on generating temporary passwords based on the current time of the user. The protocol employs an algorithm that uses a shared secret key, date, and current time to create these temporary passwords, making them short-lived and hard to reproduce.

TOTP represents another form of a password-based AP, expanding upon HOTP but relying on current time to generate OTPs. TOTP offers higher security compared to HOTP by setting a specific time window (e.g., 30 seconds) for each password. Once this time

window elapses, a fresh password is generated, reducing the risk of using an old password in potential attacks. TOTP serves as an effective security measure by ensuring that passwords remain valid for a designated period. Passwords are regularly renewed over time, reducing the chances of unauthorized access and breaches [1], [78].

TOTP finds extensive application across various industries, including:

a) Healthcare: Gain access to patient records electronic and sensitive health apps.
b) Transportation: Securing access to smart traffic systems and road networks.
c) Banking and Finance: Protecting online banking accounts and secure payment procedures [158], [78].

TOTP stands out with a robust authentication mechanism, adding an extra layer of security through the creation of temporary passwords. Users can conveniently generate temporary passwords through a trusted application, ensuring a user-friendly process. The versatility of TOTP extends to various applications and systems [56]. However, generating temporary passwords requires a generating device, which might cause inconvenience to certain users. Furthermore, the algorithms employed in TOTP could be susceptible to attacks such as brute-force and organized attacks [78], [8].

The security aspects within the TOTP mechanism require careful consideration, including verifying that the application generating temporary passwords remains resistant to attacks and ensuring synchronization between the application's timing and the server's timing during password verification.

Numerous research studies have put forth suggestions to enhance the security of the secret key, driven by users' strong desire to protect the key utilized for generating temporary passwords and to steer clear of sharing it with others. These studies stress the importance of using authorized devices to ensure consistent software updates. In addition, they place high priority on raising awareness about deceptive attacks, urging users to understand the risks associated with fraudulent activities and to maintain vigilance against suspicious behaviors [74].

Certain studies propose to validate the legitimacy of websites and applications where temporary passwords are entered to thwart phishing attempts. They also underscore the potential reduction of brute force attacks through the intricate refinement of algorithms utilized in TOTP, accompanied by meticulous adjustments of security parameters [56], [81].

As technology continues to progress, the researcher suggests directing efforts toward refining TOTP mechanisms to elevate authentication to a more sophisticated and secure level. In addition, the use of biometric fingerprint and facial recognition technologies is encouraged as part of the authentication process.

Table 3

provides a comparative analysis of two widely-used authentication protocols: HOTP and TOTP, it outlines their usage rates, security, and efficiency, along with recommendations for future security improvements. HOTP is rated as "Good" in terms of security and efficiency, indicating that it delivers a solid level of security while maintaining satisfactory performance under various network conditions. TOTP, on the other hand, is rated as "Higher", reflecting its enhanced security due to its time-based approach, which offers additional protection against attacks such as replay attacks.

The terms "Good" and "Higher" distinguish the relative effectiveness of these protocols based on key factors such as resistance to common attacks, performance in dynamic environments and resource demands on IoT devices. "Good" indicates that security measures are strong but could be improved without sacrificing too much efficiency. In contrast, "Higher" signifies that the protocol achieves superior security while still maintaining high efficiency. These ratings are crucial to understanding the balance between security and performance, especially when selecting authentication protocols for resource-constrained IoT environments.

Table 3. Comparison of authentication protocols: HOTP and TOTP

| **Name of Protocols ⇓** | **Usage Rate ⇓** | **Security and Efficiency ⇓** | **Recommendations for Future Security Enhancement ⇓** | **References ⇓** |
|---|---|---|---|---|
| HMAC-based one-time password (HOTP) | High | Good | Increase token size, adjust expiration intervals | [158], [130], [1], [78] |
| Time-based one-time password (TOTP) | High | Higher | Increase token size, adjust expiration intervals | [158], [130], [56], [81] |

Fig.2 presents a comparative analysis of the HOTP and TOTP authentication protocols, focusing on their application suitability, adaptability, security, and cost-efficiency. The analysis shows that while HOTP is better suited for devices that are not consistently connected to the network and offers a cost-effective solution, it lacks flexibility in dynamic and time-sensitive environments and is more vulnerable to replay attacks. In contrast, TOTP provides greater adaptability and improved security against replay attacks due to its time-based approach, making it more suitable for devices that are always connected. However, TOTP may involve higher costs due to the need for time synchronization. This comparison highlights the importance of choosing the right protocol based on the specific needs of the IoT environment, taking into account factors such as connectivity, security, and cost.

In summary, password-centric APs play a vital role in the IoT, helping to improve security and confidentiality. It is crucial to update these protocols with cutting-edge technologies and security norms to guarantee their efficient functioning. Using suitable APs can play a role in improving the security and dependability of the IoT.

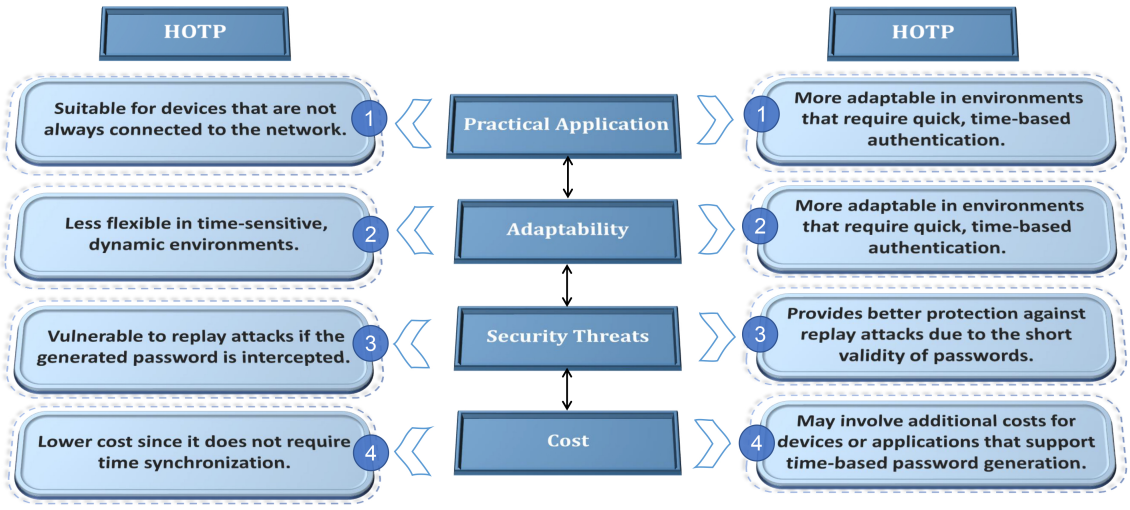


Fig. 2. Authentication methods: a comparative analysis of security protocols

### 2.2 Certificate-based Authentication Protocols

In the age of the IoT, ensuring security and authentication is of the utmost importance. X.509 certificate of authorization emerges as a vital cornerstone to achieve these goals. Such certificates bolster the validation of the identity and trustworthiness of interconnected devices, enabling them to engage in secure and reliable interactions throughout the network. We will explore the facets of this notion within the IoT, illuminating its execution and significance in safeguarding a perpetually evolving interconnected ecosystem.

*2.2.1 Public Key Infrastructure (PKI):* It functions as a structure designed to manage and distribute digital certificates together with their corresponding public and private keys. The primary goal of PKI is to establish a secure mechanism for the distribution and administration of keys within the IoT ecosystem, facilitating the realization of authentication, encryption, and security [35]. Within the domain of IoT, PKI assumes a crucial role in safeguarding security through:

a) Identity Verification.
b) Data Encryption.
c) Electronic Signatures.

In a similar context, PKI encompasses the certificate authorities responsible for issuing certificates and is utilized to confirm device identities and certifying signatures. This scope also includes CRL, key and certificate issuance, as well as the administration of key

pairs (public and private, refer to Fig. 6 and the associated issuance, management, distribution and generation of digital certificates [35].

Numerous studies have effectively applied PKI across diverse applications. For example, PKI has been used to establish secure communication between IoT devices in technologies such as connected cars, smart cities, and remote healthcare [98]. Thanks to PKI, devices in these contexts can securely and efficiently achieve authentication, encryption, and digital signing [109]. Consequently, employing methods such as PUF (physically unclonable function) can contribute to enhancing device security [35].

Fig. 3 show illustrates the client and server striving for robust encryption to ensure confidentiality and message integrity. When using encryption techniques such as SSL/TLS to secure data, the process starts with data exchange between the client (such as a Web browser) and the server. To ensure that these data remain confidential and unaltered, symmetric encryption is applied, which works like locking the information so that only the two parties involved (the client and the server) can unlock it using a shared secret key.

Before the client and server can use this "lock" (symmetric encryption), they need a secure way to exchange the secret key. This is where asymmetric encryption comes into play, which is similar to sending a locked box to the other party while keeping the key yourself. This ensures that only the intended recipient can open the box.

To verify that the other party is who they claim to be, a CA is used, acting like a trusted entity that signs the box to confirm the sender's identity. When the client sees the CA's signature on the certificate, they can trust that the key they receive is secure and that the connection is protected.

Finally, the shared secret key is used to encrypt the data that is transmitted between the client and the server, ensuring the confidentiality and integrity of the information, which means that the data has not been tampered with by any unauthorized party. This hinges on the essential components (server-client -CA) forming the PKI, as depicted in Fig. 4. Here, the client ensures a secure connection and verifies the identity, while the server establishes its own identity.

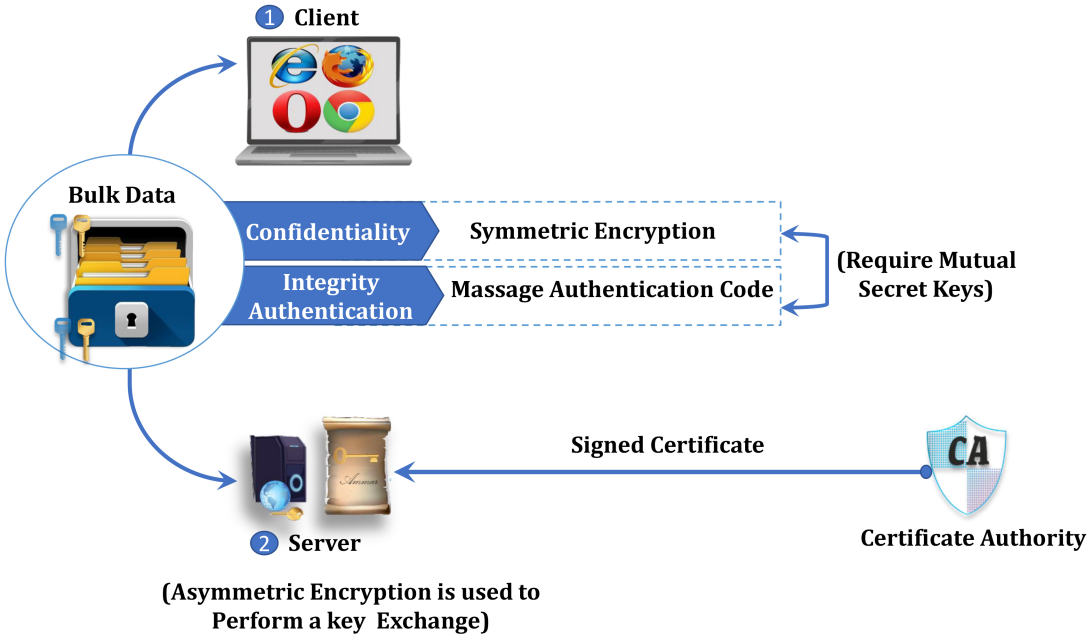


Fig. 3. Secure data exchange process between client and server using symmetric and asymmetric encryption in SSL/TLS

Additionally, in cases where the client encounters difficulty connecting to the CA, it is compelled to make a decision, and both options are suboptimal: 1) The client might opt to proceed with the connection despite the issue, thereby undermining the purpose of

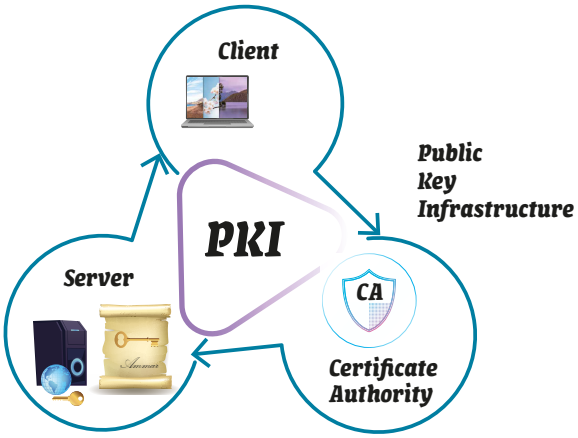


Fig. 4. Components of public key infrastructure (PKI)

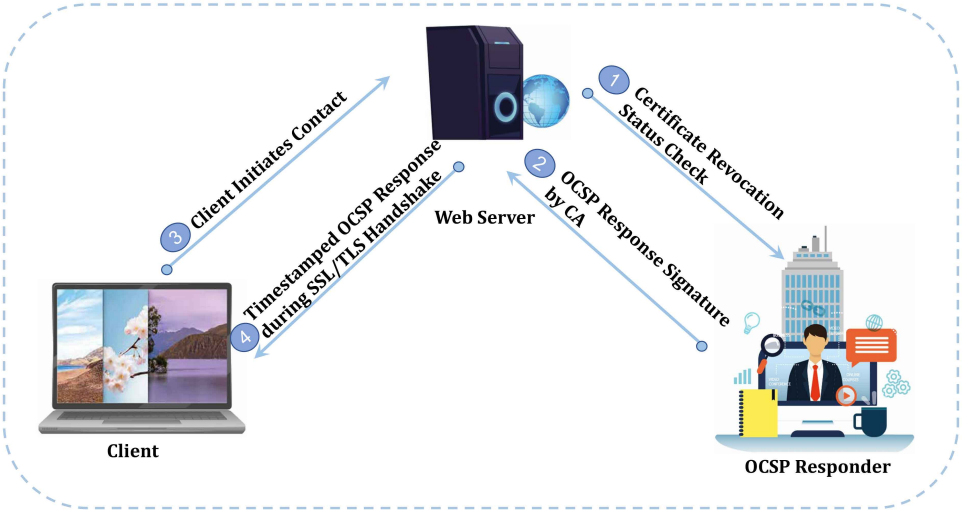


Fig. 5. Streamlining certificate revocation status checks with OCSP stapling in SSL/TLS handshake

certificate status verification. 2) Alternatively, it may choose to terminate the connection, assuming a certificate problem (resulting in false alarms). Both CRL and OCSP impose a significant burden on the client.

Fig. 5 illustrates an improved approach to the OCSP. This protocol enables real-time verification of the revocation status of a certificate. OCSP stapling shifts the responsibility from the client to the web server, where the server checks the status of all its clients. In Fig. 5, the web server contacts the OCSP responder to verify the revocation status of a certificate. The responder sends back a timestamped OCSP response signed by the CA. When the client seeks to connect to the web server, the server sends the timestamped OCSP response stapled with the certificate during the SSL/TLS handshake (provided the endorsement). The client can trust the stapled response due to its digitally signed timestamp, eliminating the need for an additional round trip to the CA. The web server can issue a single request to the CA and staple the identical response to all client requests. This approach also minimizes the volume of

requests directed to the OCSP responder. The advantages of OCSP stapling include accelerated connections for all visitors and minimal overhead on the web client, web server, and CA.

Finally, the CA is the governing body responsible for verifying identities and issuing certificates.

The future trajectory of PKI within the IoT domain might encompass a deeper integration of AI techniques, fortifying security through binary authentication approaches, and blockchain technology. In addition, the incorporation of advances in quantum key technology and identity verification using biometrics and other inventive measures could also be explored [128]. Ultimately, PKI remains a critical area for research and innovation, aiming to increase the security and effectiveness of network-connected IoT technology.

*2.2.2 X.509 Certificate-based Authentication:* This standard defines the structure of digital certificates used for authentication and security procedures, these certificates encompass details such as the recipient, the issuer, the public key, and a digital signature generated by the CA, which plays an essential role within the PKI. This norm serves to harmonize the setup, arrangement, and storage of digital certificates. The X.509 standard encompasses a collection of details that pinpoint the possessor of the certificate and its linked public key, alongside the digital endorsement from the CA [23], [129], [165]. Notable aspects of the X.509 standard include: 1) Verification of the identity of the entity. 2) Certification Authorization. 3) Data Signing and Encryption.

PKI serves as the framework governing the issuance and supervision of digital certificates, while the X.509 standard delineates the pattern and substance of the digital certificates employed in this context [23], [129], [165]. X.509 certificates encompass various attributes, including: 1) Recipient: Identifies the intended recipients of the certificate. 2) Issuer: Indicates the body responsible for issuing the certificate. 3) Validity Periods: Specifies the start and end dates of the certificate validity. 4) Public key details and digital signature [129], [165]. The authenticity of X.509 certificates is validated by verifying the digital signature using the public key from the CA, which issues and signs digital certificates, as shown in Fig. 6, which illustrates the concept of PKI and certifcate-based authentication, facilitating the distribution and identifcation of public encryption keys.

X.509 certificates face security hurdles, including challenges such as trust chain attacks and effective key management. These issues are given in Table 4, which outlines these obstacles and suggests remedies. To improve security, it is recommended to expand the use of dual authentication methods and adopt encrypted blockchain technology for key management. Numerous researchers, such as those noted in [23], [129], [165], foresee a continued evolution within the realm of X.509 certificates as technology progresses. The future may encompass improvements in key management, the adoption of biometric identification techniques, and a transition to leveraging encrypted blockchain technology for greater security. Several scientific studies have effectively showcased the application of X.509 certificates in practical scenarios, including scenarios involving digital identity, digital signatures, and institutional authentication. These studies underscore how X.509 certificates are harnessed to ensure secure communications and authentication in real world contexts [124], [85], [102], [75].

In summary, understanding the disparities and parallels between PKI and X.509 certificate-based authentication is of pivotal importance in determining the most effective approach to authenticating and protecting communications and data. Table 5 offers a comparative perspective by highlighting key aspects of each technology, assessing their practical application, and providing suggestions for the advancement and innovation in IoT. Delving into this comparison fosters a more comprehensive understanding of the roles played by both PKI and X.509 Certificate-based Authentication in augmenting security and authentication in the digital era.

Table 4. Challenges and proposed solutions in X.509 certificate-based authentication

| Challenges | Proposed Solutions | References |
|---|---|---|
| Efficient certificate management and renewal | Develop centralized management systems to facilitate renewal and administration | [140], [35], [33], [4], [60] |
| Data protection from threats and attacks | Implement multiple security measures such as multifactor authentication and encryption | [103], [102], [23], [75], [26], [74] |
| Compliance with laws and regulations | Establish policies and framework for compliance with laws and regulations | [23], [71], [128], [93], [4], [60] |
| Balancing security and usability | Provide user-friendly interfaces and train users in security practices | [35], [118], [2], [129], [38], [60] |
| Developing alternative authentication and authorization solutions | Explore innovative technologies like biometrics and AI | [124], [157], [44], [75] |

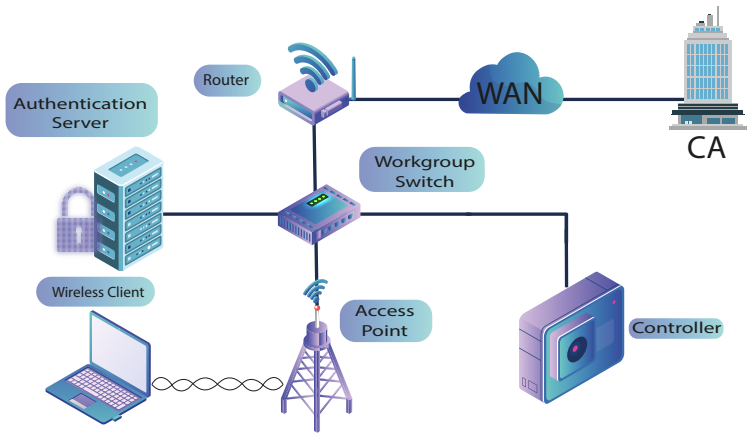


Fig. 6. Illustration of PKI and certificate-based authentication workflow in a networked environment

Table 5. Comparison: PKI vs. X.509 certificates for security & authentication

| **Aspect ⇓** | **Public Key Infrastructure (PKI)⇓ →** | **X.509 Certificate-based Authentication ⇓ ←** | **References⇓** |
|---|---|---|---|
| Concept and purpose | A comprehensive system managing and distributing public and private keys along with their certificates | A model for ensuring authentication and security based on X.509 certificates | [140], [86], [6] |
| Key components | Involves certificate authorities, key repository, and certificate revocation lists | Utilizes X.509 certificates and a key repository | [35], [37], [103] |
| Primary use cases | Used for authentication, encryption, digital signatures, and secure communications | Applied to authentication and automated authentication within secure communications | [144], [102], [118] |
| Certificate structure | Supports various types of certificates, including X.509 | Mainly relies on the use of X.509 certificates | [124], [85], [23] |
| Certificate validation and revocation | Certificate validity is verified using certificate authorities and revocation lists | Verification of certificate validity through certificate validation and updates to revocation records | [2], [83], [157] |
| Security and enhancements | Security improvement options include techniques like key fragmentation and biometrics | Enhancing security through methods like server enhancement and 2FA | [44], [151], [72] |
| Training and awareness | Training should target both PKI management and end users | Education should emphasize the proper utilization of X.509 certificates | [66], [71], [33] |
| Innovations and future | Possibilities for advancement include technologies such as blockchain and AI | Future developments can incorporate AI and facial recognition | [129], [38], [128] |
| Practical studies and illustrations | Numerous practical applications and studies exist for PKI systems | Many examples and studies showcase authentication using X.509 certificates | [160], [93], [75] |

Certificate-based authentication provides numerous advantages, including the recognition and widespread acceptance of certificates in various applications and protocols, such as SSL/TLS, email, and cloud applications [137], [150]. The certificate-based authentication system can be extended to support a large number of users, devices, and applications [9].

Fig. 7 illustrates the asymmetric encryption of user data involving a public encryption key and a private decryption key. The public key is shared in the encryption process, while the private key remains secret for decryption. These related keys mathematically allow for both encryption and decryption in both directions, preventing another key from encrypting or decrypting it. Usually, users keep their private keys. To verify with the server, the client requests a certificate from a trusted authority. Communication begins with the exchange of public keys through the server, where the client encrypts information using the server's public key and sends it in plain text. The encrypted result is encrypted by the server's public key and decrypted using the server's private key. This method allows for secure communication without exchanging private keys. Asymmetric encryption is used in digital signatures, party identity verification, and to secure network communications. However, certificate-based authentication also faces certain challenges:

i) Infrastructure cost [164].
ii) Dependency on certificate authorities [152].
iii) Complexity of certificate management [137].

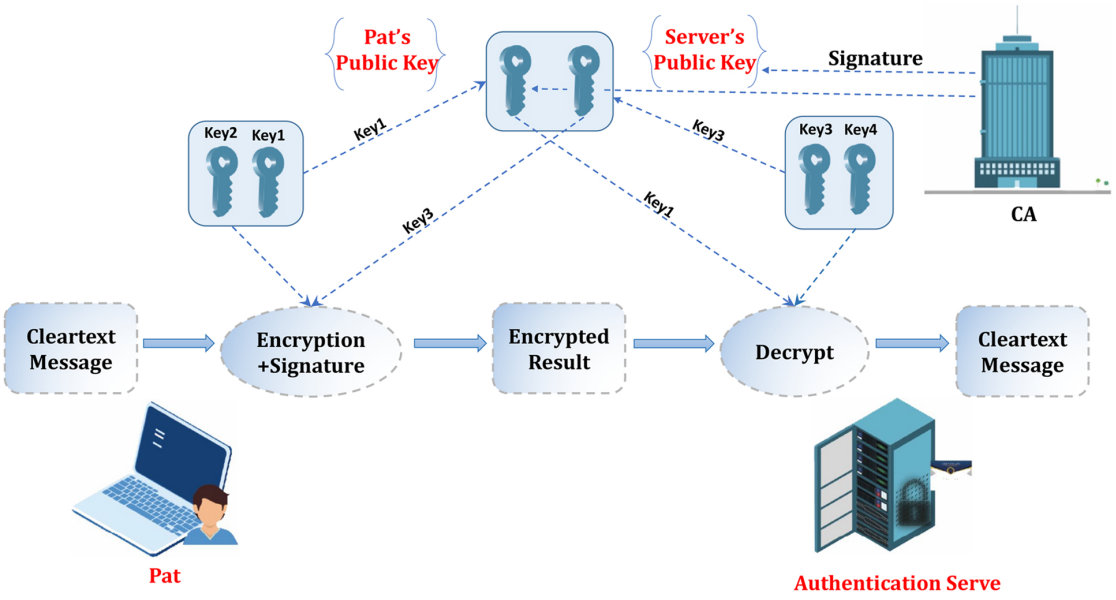


Fig. 7. Process of asymmetric encryption for securing user credentials with public and private Keys

iv) Dealing with expired certificates [50].
v) Certificate validation [131].
vi) Integration complexity [150].

To overcome these challenges, researchers have proposed various improvements to certificate-based authentication. These techniques include efficient methods for creating and managing certificates and mitigating risks associated with TOCTOU attacks and integrating certificate-based authentication with other security measures such as blockchain technology [152], [164]. In conclusion, certificate-based authentication offers significant advantages in security and reliability in digital communications. It is widely used in various areas, including IoT applications, e-commerce, online banking services, secure information exchange, and secure communication between institutions and individuals. This ensures secure communication and protection against unauthorized access.

### 2.3 Biometric Authentication Protocols

We face significant challenges in the protection of biometric data such as fingerprints and voice disguises, highlighting the need for innovative solutions. Researchers have developed advanced techniques, "Fuzzy Vault" and "Cancelable Biometrics" for security and authentication. We explore these techniques and their applications, addressing challenges and suggestions to improve their security and efficiency in modern technology [155].

*2.3.1 Fuzzy Vault:* This biometric protection model integrates biometric and randomized data to establish a secure mechanism for verification and recognition of identity. Scholars like Masoud Moradi [101] have suggested the utilization of "Fuzzy Logic" methods to construct a real-time biometric encryption system for IoT devices based on this concept. The Fuzzy Vault operates during user enrollment, employing biometric data that can be converted into mathematical points, as demonstrated by researchers such as Rakesh Kumar Mahendran [90]. These points are then combined with randomized data to create a complex and indistinct structure. Based on the investigations conducted by Fan Wu and others [153], this structure allows users to input precise biometric data alongside compatible randomized data for access and verification. Further details on the fuzzy vault can be found in the supplementary material available online.

*2.3.2 Cancelable Biometrics:* Encryption and processing techniques are utilized to convert biometric data into templates that can be easily canceled. Cancelable biometrics operates during the registration process, where biometric details are transformed into templates that can be canceled using encryption. These templates are securely stored and can be used for authentication purposes [28]. "Cancelable Biometrics" has found application in multi-server protocols for the IoV [67]. It can also be used to ensure secure identification for cloud services [27] and enhance robust authentication of wearable devices [94], [27]. More details about cancelable biometrics are provided in the supplementary file, available online.

### 2.4 Two-factor Authentication Protocols

IoT presents considerable opportunities for innovation and progress in various domains. As device connectivity grows, ensuring data and information security through authentication becomes imperative. This article delves into a pair of critical protocols for dual-factor authentication within the IoT field: 'SMS-based One-Time Password (SMS-OTP)' and 'Hardware Token-Based Authentication.' We will furnish an outline of both methods and their practical implementations.

*2.4.1 SMS-based One-Time Password (SMS-OTP):* The technology known as SMS-based one-time password is widely utilized to improve security in the authentication process within the IoT domain. This method consists of sending a temporary code by SMS to the mobile device of a previously registered user. When trying to log in or gain access to a specific service, individuals are asked to enter this code to validate their identity [89], [61]. Further details on the SMS-OTP can be found in the supplementary material available online.

*2.4.2 Hardware Token-based Authentication:* The "Hardware Token-Based Authentication" technique relies on the use of a hardware token device to create and present temporary codes. This portable device is specifically designed to generate temporary codes to improve security. When a user requires an account or identity verification, they simply press a button on the device to reveal the temporary code [95], [154]. More details about Hardware Token-Based Authentication are provided in the supplementary file, available online.

### 2.5 Multi-factor Authentication Protocols

In the era of IoT connectivity, ensuring the security and verification process is of utmost importance to protect data and information. Multifactor authentication technologies provide a strong and effective method of bolstering security within the IoT ecosystem. Smart Card-based Authentication and Mobile-based Authentication are two examples of multifactor APs that combine two or more authentication factors to increase the security and reliability of authentication.

*2.5.1 Smart Card-based Authentication:* Utilizing smart cards to improve security during system login or access characterizes the authentication technology based on smart cards. These cards embed sophisticated microchips with encrypted data and security attributes, enabling verification of user identity through a PIN or digital signature [97]. These cards introduce an added level of protection and verification. More details about Smart Card-based Authentication are provided in the supplementary file, available online.

*2.5.2 Mobile-based Authentication:* These methods utilize mobile devices to enhance security and protection. Authentication procedures can be performed through various approaches, including sending temporary codes by SMS or employing specialized authentication applications (2FA) [24]. In addition, biometric identification attributes such as fingerprints or facial recognition may also be utilized to attain higher verification levels. Furthermore, the geographical location of the phone can serve as an additional factor in confirming user identity [24].

Concerning user authentication using mobile phones, the study by Hathaliya et al. [58] presents a model based on facial authentication via mobile phones. The research aims to improve the security of electronic health records using this biometric method, addressing the application of this model to achieve a balance between security and convenience in online healthcare. The adoption of facial authentication through mobile phones introduces an advanced security measure for electronic health records. However, privacy

concerns and potential impacts on device performance should be considered. Further details on the Mobile-based Authentication can be found in the supplementary material available online.

### 2.6 Federated Learning and Adaptive Gateway Selection in IoT

In the context of IIoT within 6G networks, federated learning has emerged as a key technology for enhancing security and scalability. Federated learning enables decentralized data processing, ensuring that sensitive data remain local on devices while only model updates are shared across the network. This approach significantly reduces the risk of data leakage and improves the scalability of IIoT systems by minimizing the need for centralized data storage and processing. This is especially critical in a 6G environment, where data volumes are enormous and the demand for real-time processing is high. Furthermore, integrating federated learning into IIoT can lead to the development of more adaptive and resilient authentication protocols, allowing models to continuously learn and improve from distributed data while maintaining privacy and security standards [113].

On the other hand, in 5G networks, adaptive gateway selection is a crucial mechanism to ensure efficient communication and data security in IoT applications. Gateway selection is vital in MANETs integrated with IoT, where network conditions can change rapidly. An adaptive gateway selection system allows the network to choose the most suitable gateway based on real-time conditions such as network load, signal strength, and latency. This flexibility not only enhances network efficiency but also contributes to the security of IoT applications by reducing risks associated with static gateway configurations that could be vulnerable to targeted attacks [112].

These recent developments highlight the importance of incorporating technologies like federated learning and adaptive gateway selection into IoT authentication protocols, particularly in advanced 5G and 6G network environments. These technologies provide robust frameworks to meet the increasing demands for security, scalability, and efficiency in modern IoT systems.

## 3 CHALLENGES IN IOT AUTHENTICATION

This section explores the multifaceted challenges and concerns that surround authentication within the IoT ecosystem. The security risks in IoT authentication are covered in 3.1, highlighting the security risks that IoT authentication mechanisms must contend with. In 3.2, data privacy and user consent are covered within the authentication of the IoT, highlighting the handling of sensitive information in the interconnected world of the IoT. The scalability hurdles faced in managing authentication across the vast network of IoT devices are covered in 3.3.

### 3.1 Security Risks in IoT Authentication

IoT authentication faces a range of security threats, including MITM attacks, DoS attacks, replay attacks, brute-force attacks, and social engineering attacks, which can compromise the integrity and confidentiality of data and services.

*3.1.1 Man-in-the-Middle (MITM) Attacks:* MITM attacks are a prevalent form of network and online communication attacks, particularly targeting IoT systems and smart devices. In MITM attacks, the attacker seeks to infiltrate the communication between two interacting parties, secretly manipulating and intercepting their messages. Several researchers have provided an overview of MITM attacks, highlighting their threat as the attacker positions himself as an intermediary between the victim and the resources with which they intend to connect. This enables the attacker to eavesdrop, record and modify sensitive data exchanged between the victim and the targeted resources. MITM attacks pose a significant risk to IoT devices, as highlighted in research articles such as [117], [36]. These articles discuss various techniques, such as transport security, cryptographic security, and spatial security, to prevent or minimize the impact of these attacks. Specific mitigation methods for MITM attacks have been studied in different contexts, as explored in [99], which introduces a lightweight AP using parameters to reduce the risk of MITM attacks. MITM attacks require special attention due to their potentially severe implications for overall system security. To further enhance our understanding of how multilayered security solutions can address these pervasive security challenges while ensuring scalability and efficiency, we have expanded our discussion in this section. This includes a deeper analysis of existing security frameworks and their effectiveness in the dynamic IoT environment, considering both technological advances and emerging security threats. This comprehensive approach ensures a robust defense mechanism that addresses current vulnerabilities and is also adaptable to future security challenges in IoT systems. Further

details and technical discussions on MITM attacks, including mitigation strategies and examples, are provided in the supplementary material available online.

*3.1.2 Denial-of-Service (DoS) Attacks:* DoS attacks are carried out to render a specific online service inoperable or significantly slow it down. This is achieved by overwhelming the service with a high volume of traffic or by depleting system resources. The primary objective is to frustrate legitimate users and hinder their access to or use of the service normally [127]. In IoT, DoS attacks are widely recognized as highly dangerous and prevalent. They involve inundating the targeted system with excessive invalid or unnecessary requests that exceed the system's capacity to handle, resulting in degraded performance or, in severe cases, complete failure. Recent studies have explored various examples of DoS attacks and notable associated developments, including the following:

a) Distributed Denial-of-Service (DDoS) attacks: These attacks are executed by networks of compromised devices, commonly referred to as "botnets." The attackers increase the traffic volume and direct it towards the target. DDoS attacks exploit thousands or even millions of compromised devices, such as personal computers and IoT devices, making detection and mitigation of the attack complex and challenging [100], [68].
b) Evasive attacks: These attacks are a specific type of DoS attack that aims to conceal the true nature of the attack, making it difficult to identify and detect.

These attacks involve altering attack patterns and using techniques such as obfuscation and traffic manipulation to confuse mitigation efforts [100], [31]. It is crucial to raise general awareness regarding electronic attacks, including DoS attacks, and to increase vigilance. Organizations and users should take the necessary precautions to protect themselves and their systems against harmful attacks. Several studies have addressed the nature of these attacks and the challenges they present. Additional examples, discussions, and detailed analysis of the impact of DoS attacks, along with mitigation strategies, can be found in the supplementary material available online.

*3.1.3 Replay Attacks:* These attacks present a significant security risk in the IoT. These attacks involve capturing and replaying data or information exchanged between devices to cause undesirable consequences or breach security measures. The attackers exploit the repetitive communication process without proper verification, allowing them to replay or reexecute operations illegitimately.

Researchers have focused on improving authentication security on smartphones and IoT devices. They stress the importance of mitigating such attacks by employing techniques such as key regeneration and generating unique tokens for each transaction [9]. In addition, there is an emphasis on authentication and secure key management in the IoT, highlighting the importance of using technologies such as timestamping and session management to prevent replay attacks [117]. Some studies explore the use of PUF to counter replay attacks and establish secure mutual authentication [88]. Ensuring security in healthcare networks for IoT is also essential by examining a bidirectional AP that relies on random keys and token generation to thwart replay attacks.

Table 6 provides information on various studies discussing replay attacks in the IoT, addressing different aspects of combating these threats. These points offer a comprehensive understanding of the importance of countering replay attacks in the IoT context and propose measures to safeguard systems and data.

Table 6. Insights and countermeasures for combatting replay attacks in IoT

| Category | Placement | Method of Protection / Suggested Approaches |
|---|---|---|
| Safeguarding data [117] | Within the IoT | The research analyzed encryption methods, message signing, and the verification of unique codes as preventive measures against this category of attacks |
| Verification methods [9] | Integration with smartphones and IoT devices | The investigation investigated potent authentication techniques like digital signatures and the implementation of digital certificates to thwart replay attacks |
| Countermeasures against IoT attacks [51] | Implementation of intelligent agricultural applications | The research delved into techniques involving timestamp signatures in messages and the utilization of trusted servers to minimize the consequences of such attacks |
| IoT communications and information [148] | The concept of (IoT) | The research encompassed strategies for data security, such as strong encryption and the use of timestamp signatures, to counter this type of attack |

Researchers are committed to exploring future studies to combat Replay attacks in the IoT, proposing enhancements to enhance the security of devices and systems against these threats. Replay attacks pose a severe threat to the safety and integrity of IoT systems, since they involve duplicating recorded actions or messages to manipulate systems and access sensitive information. Researchers

recommend future efforts to strengthen security by improving APs and implementing suitable security frameworks for IoT. In addition, they propose exploring alternative techniques, such as behavioral analysis and machine learning, to detect abnormal patterns and verify message authenticity. Improvements in authentication and key management protocols will further enhance data security and device control.

The construction and updating of systems and security protocols is imperative to keep up with technological advancements and current threats. Collaborative efforts between academia and industry are essential to sustain research and innovation in IoT security, developing effective technologies to detect and prevent such attacks in the future.

*3.1.4 Brute-force Attacks:* These attacks are a prevalent concern in IoT, involving exhaustive attempts to access protected information, such as passwords or secret keys, without prior knowledge [9]. These attacks pose a significant security threat to IoT devices and systems. The deep integration of devices with the Internet, coupled with inadequate security measures in many cases [77], makes smart home devices, sensors, surveillance cameras, and connected medical devices particularly vulnerable to brute-force attacks [77], [121]. Various methods can be utilized to execute these attacks in the context of the IoT. However, their primary goal remains to gain control of the device and use it for DDoS attacks or accessing personal or corporate data [159], [25].

Numerous studies have provided extensive information on the impact of brute-force attacks, as well as the technologies and strategies used within the IoT context. Table 7 elucidates the effect of brute-force attacks on IoT and suggests countermeasures.

Table 7. Impact and countermeasures of brute-force attacks in IoT

| Types of Attacks | Impact | Proposed Countermeasure |
|---|---|---|
| Brute-force attacks [117], [79] | Exploitation of devices without authorization | Establishing robust authentication and key management practices |
| Password attacks [63], [13] | Unauthorized hacking and access | Deploying encryption methods and efficient key management protocols |
| Privacy breaches [43], [7] | Breaches of privacy and security | Leveraging AI technologies to detect and thwart these attacks |
| Illegitimate attacks [120] | Illegitimate access to systems | Strengthening security measures and conducting awareness campaigns |
| Attacks on smart devices [9] | Unauthorized exploitation of devices | Integrating contemporary authentication systems into smart devices and IoT devices |

Table 8. Types of cyber-attacks and associated tools in IoT

| Attacks ⇓ | Description ⇓ | Used equipment ⇓ |
|---|---|---|
| MITM attacks | Infiltration attacks where the attacker gains access to sensitive information or manipulates it within the communication | Tools like ettercap, bettercap, and MITM are used for man-in-the-middle attacks [9] |
| Denial-of-service (DoS) attacks | Attacks aimed at disrupting a specific service by sending a large volume of data or fake requests | Hping, LOIC, and Slowloris are tools associated with denial-of-service attacks [117] |
| Replay attacks | Replaying previous events to manipulate or deceive (fraudulent) actions | Wireshark, Scapy, and Burp Suite are tools used for network analysis and security testing [51] |
| Brute-force attacks | Password hacking attacks involve trying out various possible combinations | Hydra, Medusa, and John the Ripper are tools utilized for password cracking [88] |

Brute-force attacks present a significant challenge for IoT due to their reliance on limited resources and devices connected to untrusted networks. Scientific research has extensively examined various strategies to combat and mitigate brute-force attacks, offering future-oriented solutions. For example, a study [79] by Taylor et al. Focused on secure APs and key management for IoT devices, along with improving passwords and mechanisms for detecting brute-force attacks to minimize their impact.

Furthermore, another study [104] by Ali Hassan et. al, explored the role of AI techniques in identifying brute-force attacks in IoT environments, providing examples of using neural networks and deep learning to detect and prevent such attacks.

Ultimately, implementing advanced protection measures, including encryption and MFA, can effectively protect the Internet of IoT from brute-force attacks. Researchers recommend adopting robust authentication and key management strategies, improving password strength, and utilizing robust encryption algorithms and early attack detection mechanisms. Continuous updates, monitoring security developments, and exploring innovative technologies and strategies in this domain are strongly advised. Within the interconnected world of IoT, security vulnerabilities pose significant risks. Table 8 highlights various types of attack, including MITM, DoS, Replay, and brute force attacks, along with their descriptions and the tools used. By understanding these threats, we can proactively implement preventive measures to ensure the integrity and resilience of IoT networks.

Refer to Table 8 for more information. It presents a comprehensive overview of different types of cyber attack in the IoT, together with their corresponding descriptions and the tools used [117]. By analyzing this table, we can gain valuable knowledge about potential threats and recommended countermeasures to enhance IoT security [9].

Table 9 presents a comparative analysis of four categories of electronic attacks, evaluating their strengths, vulnerabilities, and potential consequences. MITM attacks are robust, allowing intruders to infiltrate and control communications. However, they become vulnerable when dealing with systems with weak authentication of parties, which could lead to the theft of sensitive information and data manipulation [9].

Table 9. Analysis of well-known security attacks in terms of impact, challenges and solutions

| **Evaluation criteria** | **Attacks** | | | |
|---|---|---|---|---|
| | **Man-in-the-Middle (MITM) Attacks [9]** | **Denial-of-Service (DoS) Attacks [117]** | **Replay Attacks [51]** | **Brute-force Attacks [88]** |
| Strength | Allows the attacker to infiltrate and control communication | Disrupt the targeted service and denies legitimate access | Exploits unauthorized repetition of previous events | Breaks weak passwords or gains control over user accounts |
| Weakness | Countering the attack in some systems with weak party authentication | Attacking well-protected systems and may require significant resource consumption | The targeted system's ability to identify and prevent replays | Strong password complexity and enforced security measures |
| Damage | Lead to the theft of sensitive information and data manipulation | Result in service disruption and loss of productivity | Lead to data manipulation and account compromise | Result in compromised accounts and data theft. |
| Challenges and complexity | Weaknesses in authentication systems, ineffective prevention of attacks | Service attacks, resource exhaustion | Weak identity verification and protection against repeated attacks | Password cracking through trial and error, weak password complexity |
| Solutions | Use of modern authentication techniques, implementation of strong encryption measures | Implementation of attack detection and prevention systems | Use of digital signatures, implementation of message replay verification frameworks | Enhance password complexity, Implement account security policies |
| Recommendations | Improve key management, provide regular security updates | Increase network capacity, develop early attack detection systems | Application of digital signatures in targeted systems | Increase password length and complexity, use automatic lockout mechanisms |
| Future work | Study the impact of new communication technologies such as 5G and cloud computing | Study the impact of cloud computing and improvements in 5G networks | Study advanced verification mechanisms, enhance protection against repeated attacks | Provide 2FA techniques, implement biometric authentication methods |

DoS attacks are highly effective in disrupting targeted services and denying legitimate access. However, their potency decreases against well-protected systems, requiring substantial resource consumption, resulting in service disruptions and loss of productivity [117].

Regarding other attack types, “Replay Attacks” demonstrate strength in exploiting unauthorized event repetition. However, their effectiveness may wane against systems lacking identification and prevention mechanisms, which can lead to data manipulation and compromise user accounts [51].

Similarly, "Brute-force Attacks" are potent in breaking weak passwords and seizing user account control. However, their efficacy weakens against strong password complexity and enforced security measures, potentially leading to compromised accounts and data theft [88].

In conclusion, a comprehensive study and understanding of these types of attack is essential for organizations and individuals to improve digital security and implement vital preventive measures, safeguarding data and services against various electronic threats.

### 3.2 Privacy Concerns in IoT Authentication

IoT authentication refers to the procedure of confirming the identity of devices connected to the Internet and the individuals who interact with them. This involves gathering sensitive personal information solely to verify users' identities. However, there are notable privacy concerns associated with IoT authentication, particularly when it involves sensitive data such as biometrics and location details [115]. Several privacy concerns are linked to IoT authentication, including:

(1) Gathering and utilizing personal data: IoT authentication necessitates the collection of personal and sensitive information to establish users' identities, giving rise to concerns about proper handling and the risk of unauthorized data disclosure [134], [115].
(2) Biometric data and geographic information: Authentication data, such as biometrics (e.g., fingerprints), and location details, are highly sensitive and require extra security measures to safeguard against misuse and leakage [19], [115].
(3) Hacking and security threats: IoT authentication systems may be susceptible to cyber-attacks and breaches, compromising users' privacy and exposing their data to potential risks [115].

(4) Tracking and monitoring: Location information and authentication data could be exploited for tracking users' movements and behavior, raising privacy concerns and conflicting with individuals right to privacy [19], [115].
(5) Insufficient privacy policies: Some IoT authentication systems may lack stringent privacy policies and data protection mechanisms, thereby increasing the possibility of privacy violations [115], [134].

Fig. 8 shows a pie chart as a powerful visual tool used to display the distribution of various privacy concerns as percentages. Each privacy concern is represented in its own section, indicating its percentage contribution to the total concerns. Note that these percentages are approximates based on the data cited in the previous references and may vary depending on information from reliable sources.

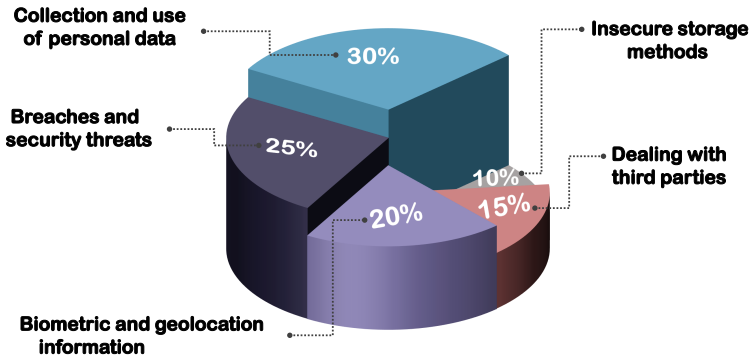


Fig. 8. A pie chart depicting the distribution of privacy-related concerns

Likewise, Table 10 categorizes privacy concerns and security challenges associated with IoT authentication based on their expected impact levels, classified as weak, moderate, moderate-high, high, and critical. The chart offers an overview of various concerns and their expected impact levels, along with the projected impact levels for each security challenge, supported by relevant references.

Using the data presented in Table 10, the bar graph in Fig. 9 presents privacy concerns versus security challenges and their respective expected impact levels. This graphical representation enables readers or researchers to prioritize and assess potential risks by identifying concerns and challenges with more significant impacts, thereby focusing efforts on addressing and improving security based on these data. The researcher proposes additional privacy concerns related to IoT authentication, including the recognition of user personal traits and behaviors, which could lead to precise profiling and potential privacy and personal discrimination breaches. Furthermore, mandatory data sharing in IoT authentication, prompted by legal requirements or pressure from relevant authorities, may conflict with users' desire to safeguard their privacy. Furthermore, IoT authentication processes may involve interactions with third-party entities, such as external authentication service providers, raising concerns about the privacy of shared information with these external parties.

### 3.3 Scalability Challenges in IoT Authentication

The rapid expansion of IoT has facilitated seamless connectivity among various online devices, enabling efficient data exchange. A crucial aspect of IoT security involves ensuring secure authentication for these interconnected devices. As the number of connected devices and services in IoT environments grows, scalability becomes a critical issue for APs, which need to handle large volumes of traffic and support various hardware and software platforms.

This section presents a comprehensive review of the scalability challenges related to IoT authentication, drawing insights from multiple research studies. The focus will be on analyzing challenges, exploring preventive measures, and identifying future directions

Table 10. Privacy concerns and expected impact level

| | Points | Expected Impact Level | | | | | References |
|---|---|---|---|---|---|---|---|
| | | Weak | Moderate | Moderate-High | High | Critical | |
| Privacy Concerns | Privacy breach | - | - | - | √ | - | [36] |
| | Unauthorized data usage | - | - | √ | - | - | [36] |
| | Phishing attacks | - | - | - | - | √ | [110] |
| | Facial recognition privacy concerns | - | - | - | √ | - | [134] |
| | Location data collection and usage | - | - | √ | - | - | [22] |
| | Movement and activity data usage | - | √ | - | - | - | [29] |
| | Communication security threats | - | - | - | - | √ | [11] |
| | Tracking personal activities and behavior | - | - | √ | - | - | [29] |
| | Data used for targeted advertising | - | - | √ | - | - | [110] |
| | Breaches and espionage | - | - | - | √ | - | [41] |
| | Non-compliance with privacy standards and security recommendations | - | √ | - | - | - | [36] |
| Security Challenges | Secure authentication for IoT devices | - | - | - | - | √ | [147] |
| | IoT communication and data protection | - | - | - | - | √ | [18] |
| | Cyberattacks and hacking mitigation | - | - | - | √ | - | [34] |
| | Securing keys and authentication mechanisms | - | - | - | √ | - | [110] |
| | Ensuring device and software integrity | - | - | √ | - | - | [108] |
| | Compliance with security standards and regulations | - | √ | - | - | - | [87] |
| | Secure identity and access management | - | - | - | - | √ | [70] |
| | Improving endpoint security | - | - | - | √ | - | [134] |
| | Securing IoT networks | - | - | - | √ | - | [14] |
| | Secure authentication and authorization management | - | - | - | √ | - | [34] |
| | Detecting new attacks and identifying attack patterns | - | √ | - | - | - | [22] |

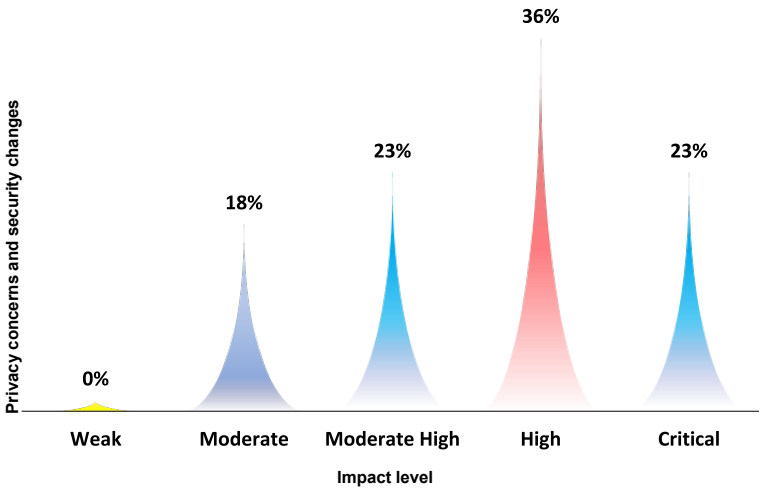


Fig. 9. Privacy concerns and expected impact level in IoT authentication

in IoT authentication. Security and authentication in the IoT are becoming increasingly challenging. To achieve scalability in IoT authentication, a holistic approach is essential to cater to the diverse requirements and resource limitations of various IoT devices. Researchers have carried out numerous studies to address these challenges and propose solutions that enhance the security and scalability of IoT systems.

Table 11 provides a detailed overview of some of the most significant research and studies on scalability challenges in IoT authentication. The data were compiled from reliable scientific articles and references in this domain. The table presents key details for each study, including its reference, research area, summary of contributions, and future implications. By reviewing the table, readers can gain comprehensive insight into the latest developments and challenges in IoT authentication, including the technologies utilized

Table 11. Comprehensive references on scalability challenges in IoT authentication

| Reference | Research Area | Overview | Contributions | Features |
|---|---|---|---|---|
| [9] | Blockchain applicability for IoT | Identifies modern challenges of authentication schemes in smartphones and IoT devices, emphasizing performance and scalability issues | Evaluation of the performance and scalability of authentication schemes in smartphones and IoT devices | Evaluation of performance and scalability for authentication schemes in smartphones and IoT devices |
| [53] | An Expandable protocol-Level strategy for mitigating machine learning breaches on authentication methods using PUF for the Internet of Medical Things | Addresses machine learning attacks on authentication systems within IoT medical devices using PUF | Suggests an adaptable protocol-level approach to prevent machine learning attacks on authentication mechanisms in IoT medical devices, verified through experimental validation | Proposal of a flexible protocol-level strategy to avoid machine learning attacks on authentication mechanisms in medical IoT devices |
| [119] | IoT authentication and authorization security framework utilizing blockchain technology | Enhances authentication and authorization in IoT using blockchain technology | Creation of a security framework for authentication and authorization in IoT through the utilization of blockchain technology, with theoretical analysis of the proposed framework | Establishment of a security framework for authentication and authorization in IoT using blockchain technology |
| [138] | Access management of IoT devices using decentralized authentication: A review | Reviews the use of decentralized authentication for access management in IoT devices | Summarizes the findings of various studies related to access management using decentralized authentication | Summarization of findings from multiple studies on access management using centralized and decentralized authentication |
| [114] | IoT device authentication and authorization scheme utilizing lightweight DAG blockchain | Introduces a lightweight authentication and authorization system for IoT devices using blockchain technology | Presents a lightweight and scalable model for authentication and authorization in IoT devices using blockchain technology | Introducing a lightweight system for authentication and authorization for IoT devices using blockchain technology |
| [32] | Blockchain scalability | Identifies challenges to achieve scalability in blockchain systems | Literature review on challenges in achieving scalability in blockchain systems | Identifying challenges in achieving scalability in blockchain systems |
| [73] | Authentication architecture for heterogeneous IoT systems: A hybrid approach combining centralized and blockchain methods | Presents an efficient authentication model for heterogeneous IoT systems using a distributed structure and blockchain technology | Theoretical analysis of the proposed model for the evaluation of its effectiveness | Presenting an efficient model for authentication in various IoT systems using a distributed structure and blockchain technology |
| [55] | Improved scalability of blockchain for smart IoT devices: Development of a generalized model | Aims to enhance the scalability of blockchain for smart IoT devices | Literature review on enhancing blockchain scalability for smart IoT devices | Striving to enhance the scalability of blockchain for smart IoT devices |
| [161] | Expandable authenticated encryption scheme for IoT using PUF technology | Presents a model for expanding the authenticated encryption using PUF technology in IoT | Experimental validation of the effectiveness of the proposed model | Introducing a model to expand the authenticated encryption system using PUF technology |
| [91] | Modeling a lightweight and scalable integrated blockchain framework (LightBlock) for IoT use cases | Introduces a lightweight and scalable integrated blockchain model tailored for IoT applications | Experimental validation of the proposed model's effectiveness | Presenting a lightweight and scalable model for an integrated blockchain framework for IoT applications |
| [76] | Scalable lightweight protocol for interoperable public blockchain-based supply chain ownership management | Proposes a scalable and lightweight protocol for managing supply chain ownership using public blockchain | Experimental verification of the proposed protocol's effectiveness | Proposing a lightweight and scalable protocol for managing ownership in the supply chain using public blockchain |
| [21] | Developing a secure and expandable IoT system for big data, utilizing multifactor authentication and lightweight cryptography | Develops a secure and scalable IoT system using multifactor authentication and lightweight cryptography | Experimental verification of the scalable and secure IoT system | Developing a secure and scalable IoT system using multifactor authentication and lightweight encryption |
| [135] | Blockchain-based secure energy trading using vehicle-to-grid Mutual authentication in smart transportation | Implements secure energy trading using blockchain technology and mutual authentication between the vehicle and the grid | Experimental verification of the effectiveness of secure energy trading using blockchain technology | Implementing secure energy trading using blockchain technology and mutual authentication between the vehicle and the grid |
| [136] | Towards an optimal security using multifactor scalable lightweight cryptography for IoT | Aims to achieve optimal security using scalable lightweight and multifactor cryptography in IoT | Experimental verification of achieving optimal security using lightweight and multifactor cryptography | Achieving optimal security using scalable lightweight cryptography and multifactor authentication in IoT |
| [126] | Secured decentralized marketplace for virtual payments in IoT environment utilizing blockchain technology | Develops a secure virtual payment system using blockchain technology in the IoT environment | Literary review of the secure payment system in the decentralized market using blockchain technology | Developing a secured virtual payment system using blockchain technology in the IoT environment |

and the importance of diverse research and studies in this context. This valuable information can guide future research efforts aimed at developing scalable security solutions for IoT systems and protecting data and devices connected to the Internet effectively. The contribution of Table 11 lies in the direction of future research, identifying strengths, and addressing weaknesses in IoT authentication, thus increasing the security and efficiency of IoT systems and optimally harnessing the potential of this cutting edge technology in the coming times.

Table 11 reveals that IoT authentication faces scalability challenges from device diversity, limited resources, network connectivity, deployment complexities, and security concerns. Solutions include lightweight protocols, blockchain-based approaches, and access control mechanisms. Energy efficiency, device mobility, multiservice utilization, and real-time data processing are also crucial to scalable solutions. Continued research and innovation are vital to address the evolving challenges of the IoT while maintaining security

and scalability. Key factors include detecting fraud, managing errors, ensuring compliance, and fortifying defenses against forgery attacks. Balancing scalability and security is essential in the dynamic IoT landscape.

Lastly, the researcher presents some recommendations and proposals based on the referenced and discussed literature in this study, summarized as follows:

(1) Develop lightweight protocols for better integration with resource-constrained IoT devices, enhancing performance and reducing power consumption.
(2) Machine Learning and AI-Based Authentication: We highly recommend exploring machine learning and AI for adaptive authentication in dynamic IoT environments, detecting anomalies, and identifying unauthorized access.
(3) Leverage blockchain technology to improve scalability, ensuring security, transparency, anticounterfeiting, and secure key management.
(4) Implement a multilayered authentication approach to achieve scalability and security, accommodating different levels of security and device capabilities.
(5) Conduct rigorous security and performance tests to identify vulnerabilities and enhance the system's reliability.
(6) Integration of AI in device authentication: Using deep learning and AI techniques to improve the patterns recognition capabilities of devices, enabling faster and more effective identity verification through autonomous authentication.
(7) Embracing the zero trust concept: considering the zero trust concept in IoT authentication, emphasizing continuous identity verification during device interactions with networks and applications.

In conclusion, the researcher asserts that focusing on these recommendations and proposals can increase scalability in IoT authentication and fortify the security of this dynamic and expanding ecosystem. Continuous efforts in research and innovation are essential to ensure that IoT technology stays up-to-date with modern advancements, ensuring reliability and ever-increasing security for the future.

## 4 COMPARATIVE ANALYSIS OF IOT AUTHENTICATION PROTOCOLS

Comparative analysis of IoT authentication protocols is essential to make informed decisions about the security, compatibility, efficiency, and overall effectiveness of authentication mechanisms in IoT deployments. We use a wide range of standards and evaluation criteria to evaluate these protocols as explained in 4.1. The comparative evaluation of IoT APs is provided in 4.2. To make it more user-friendly, Table 12 summarizes a comprehensive comparison of APs from recent years.

### 4.1 Evaluation Criteria

Integrated APs in the IoT are important because they find a careful balance. This allows for safer and more efficient applications. Furthermore, it highlights the potential role of emerging technologies like AI and big data analytics in enhancing these protocols and ensuring the security and confidentiality of interconnected devices and networks in the IoT landscape. The evaluation criteria collectively contribute to the assessment of IoT APs, helping decision makers choose the most suitable mechanisms for their specific IoT deployments. The evaluation of protocols based on the criteria ensures that security, privacy, scalability, usability, and cost effectiveness are considered in the selection process.

*4.1.1 Security:* A paramount criterion in evaluating IoT authentication protocols is the cornerstone of safeguarding the interconnected world of the IoT. In this context, security is a multifaceted approach to fortifying the protection, integrity, and confidentiality of IoT devices, data, and communications [49]. A fundamental security component is the incorporation of robust encryption mechanisms [143]. The mechanisms encode data in a manner that makes it exceptionally challenging for unauthorized parties to decipher, ensuring the confidentiality of transmitted information. Furthermore, authentication methods play a pivotal role in security. Developing protocols capable of surviving various attacks, including hacking attempts, malware, and DoS attacks, is imperative to ensure the resilience of IoT systems. Moreover, these security measures must remain adaptive to the evolving threat landscape, staying one step ahead of emerging vulnerabilities.

The overarching security goals of the IoT authentication protocols are to protect sensitive data from unauthorized access and tampering. Confidentiality is maintained and data integrity is preserved. Access control is another pivotal goal, limiting interaction with IoT devices and networks exclusively to authorized entities [146]. Robust security measures inherently contribute to protecting user privacy by thwarting unauthorized access to personal information. Therefore, security is a fundamental element in the design and implementation of IoT authentication systems, as any compromise in this domain can lead to dire consequences, including data breaches, device manipulation, and network disruptions [52].

*4.1.2 Privacy:* As an essential evaluation criterion for IoT authentication protocols, privacy protects sensitive user information, personal data, and communication exchanges from unauthorized access, misuse, or disclosure. Privacy involves implementing encryption techniques to secure data during transmission, user-controlled data sharing mechanisms that allow people to manage access to their information, and secure data handling practices that ensure data privacy throughout its lifecycle [65]. Privacy measures are vital to ensure data security and foster trust and confidence among users in the IoT ecosystem, ensuring that their private information is treated with the utmost care and respect.

*4.1.3 Scalability:* A pivotal criterion in evaluating IoT authentication protocols addresses the capacity of protocols to adapt and manage effectively the growing demands of IoT networks as the number of connected devices and users continues to increase. The criterion ensures that IoT systems have the flexibility to accommodate a substantial volume of devices and users while maintaining efficient service delivery and network performance. The achievement of scalability involves using emerging technologies such as D2D communication and fog computing, which allows APs to handle the growing ecosystem efficiently [53] [110]. The overarching objectives of scalability in IoT authentication protocols include enabling seamless growth, maintaining efficient service delivery to minimize latency, adapting to dynamic network conditions, and controlling costs associated with protocol implementation as the IoT ecosystem evolves [84], [122]. In essence, scalability is imperative to ensure that IoT systems can easily scale to meet the evolving demands of the interconnected IoT ecosystem while preserving performance and efficiency.

*4.1.4 Usability:* A critical evaluation criterion for IoT authentication protocols revolves around the design and implementation of the protocols to provide a user-friendly experience for device users and administrators. The criterion emphasizes the creation of intuitive user interfaces and provides clear and comprehensible guidelines to streamline the authentication process and ensure that the interaction with IoT services becomes a straightforward and easily understandable endeavor. Usability encompasses the design of user interfaces that are intuitive and easy to navigate, presenting authentication options and prompts in a clear and user-friendly manner. The overarching usability objectives within IoT authentication protocols encompass simplifying the user experience by minimizing complexity, improving authentication efficiency while maintaining security, reducing the occurrence of user errors that can lead to vulnerabilities or disruptions, and ultimately fostering user trust in IoT systems [59]. By prioritizing usability, IoT authentication protocols aim to make IoT services accessible and user-friendly, significantly contributing to user confidence and the overall success of IoT deployments [47].

*4.1.5 Cost-effectiveness:* A pivotal evaluation criterion for IoT authentication protocols focuses on a comprehensive evaluation of the general expenses related to the deployment and maintenance of these protocols for a long period of time. It carefully evaluates various costs, including initial setup expenses, hardware and software investments, ongoing maintenance, and operational outlays. Gleichzeitig, cost-effectiveness efforts emphasize the establishment of a harmonious equilibrium between the advantages and benefits of a specific AP to the IoT ecosystem and the associated costs. The overarching objective is to ensure that the economic viability of the deployment of the IoT remains intact, safeguarding against situations where high costs hinder sustainability [20]. Specific inquiries delve into the use of blockchain and cloud computing methods to optimize efficiency and reduce expenses while executing APs. While prioritizing cost-effectiveness, maintaining the AP's quality and security is essential, including optimizing resource utilization, exploring cost-saving technologies such as blockchain and cloud computing, and achieving an optimal balance between cost-efficiency and robust security.

Moreover, it is crucial to anticipate and address upcoming risks, such as quantum attacks. Protocols should be recognized for their user-friendly nature and scalability to accommodate an ever-expanding array of devices and users. This inevitably calls for

the innovative deployment of methods such as blockchain to achieve cost-effectiveness. The true strength lies in offering holistic authentication solutions that carefully balance security, privacy, scalability, user-friendliness, and cost-effectiveness within the IoT.

By perusing Table 12, we navigate a lucid path toward security and privacy. The table illuminates ingenious concepts that seamlessly meld safeguarding with scalability, bestowing user-friendliness upon interconnected devices. Some references dive into specific hurdles and privacy quandaries, while others probe innovative methodologies.

This security study aims to flexibly assess and classify APs in the IoT, according to a modern standard based on security levels. In Table 12, a comparative analysis of 27 different research references was carried out. The purpose of this explanation is to clarify the results and conclusions drawn from this comparison.

The results revealed variations in the strength of the protocols, underscoring the importance of precise analysis to identify strengths and weaknesses. Labels of "poor," "medium" and "high" were assigned based on the number of attacks each protocol can withstand. Security-related information was deduced for the APs used in the IoT domain, considering the listed references. The attacks include MITM, Replay attack, DoS attack, and brute-force attack.

Using specific criteria, the security level of each protocol in Table 12 was classified as "poor" if it could withstand two or fewer attacks, "Medium" if it could withstand three attacks, and "High" if it could withstand four or five attacks. Protocols labeled as "poor" demonstrated a weak ability to resist attacks, highlighting the need for improvement to ensure device security. Although "medium" protocols showed some improvement, they still required enhancement. In contrast, "high" protocols exhibited high effectiveness against attacks, making them crucial in the IoT environment.

This effort contributes to providing accurate security standards that serve as valuable guidance for researchers and stakeholders. Table 12 serves as a source of inspiration for innovation, offering a comprehensive assessment of the security and privacy levels. The research highlights the importance of striking a balance between security and privacy in designing APs in the evolving IoT world.

### 4.2 Comparison of IoT Authentication Protocols

*4.2.1 Password-based vs. Certificate-based Authentication.* In the age of digitalization and constant connectivity, authentication systems stand out as significant instruments that ensure the safeguarding of data and personal information. As technology advances rapidly, the need to understand and evaluate the various systems used in this context is increasing. Although some may perceive traditional passwords as easy and efficient, the emergence of contemporary authentication methods such as digital certificates has expanded our array of choices, each offering different levels of security. In Table 13, we will thoroughly and impartially examine both authentication systems reliant on passwords and digital certificates. This meticulous comparison will be based on multiple pivotal criteria. Our aspiration is that this comparative analysis deepens and broadens the reader's grasp of these technologies, specifically focusing on their significance and roles in upholding data security in today's technology-centric society.

In the field of digital authentication, the challenge involves selecting the best-suited approach based on the unique requirements and contexts of each application. Password-centric and digital certificate authentication systems constitute the primary alternatives within this domain. Upon evaluating diverse criteria, it becomes apparent that each option has its own merits and drawbacks. For example, for ease and expense, passwords may be preferable. However, in the domains of security and dependability, digital certificates could present themselves as the prime selection. Ultimately, the decision hinges on achieving an equilibrium between security prerequisites, financial considerations, and user convenience.

*4.2.2 Biometric vs. Two-factor Authentication.* In a world infused with technology marked by rapid digital progress, the importance of protecting privacy and safeguarding data integrity emerges as a central cornerstone of any digital framework. As a result, there is a pressing need to advance authentication and identity verification techniques. Within this range of methods, we encounter biometric authentication and 2FA. The former hinges on the innate distinctions that define humans, whether these attributes are physical or behavioral. The latter relies on providing users with a code or additional verification mode along with the conventional password. However, which of these options boasts greater security and efficacy? And how can we objectively compare them? These are the inquiries that we aim to tackle in Table 14. We invite readers to dig deeper, distinguishing the core disparities between these methods and understanding how each approach can address security demands in the digital era.

Table 12. Exploring authentication protocols: a comprehensive comparison

| References | Research Reference | Publication Year | Evaluation Criteria | | | | |
|---|---|---|---|---|---|---|---|
| | | | Security | Privacy | Scalability | Usability | Cost-effectiveness |
| [139] | Multi-level authentication protocol for enabling secure communication in IoT | 2021 | M | × | ✓ | ✓ | × |
| [110] | A lightweight authentication protocol for D2D-enabled IoT systems with privacy | 2021 | P | ✓ | ✓ | ✓ | × |
| [158] | A lightweight authentication protocol for IoT-based cloud environment | 2021 | P | ✓ | ✓ | × | × |
| [134] | A novel vector-space-based lightweight privacy-preserving RFID authentication protocol for IoT environment | 2021 | M | ✓ | ✓ | × | ✓ |
| [116] | A robust provable-secure privacy-preserving authentication protocol for Industrial IoT | 2021 | P | ✓ | ✓ | ✓ | × |
| [9] | Modern authentication schemes in smartphones and IoT devices | 2021 | H | ✓ | × | ✓ | × |
| [149] | A new mutual authentication and key agreement protocol for mobile client–server environment | 2021 | M | ✓ | × | × | ✓ |
| [59] | A novel authentication protocol for IoT-enabled devices | 2022 | H | ✓ | ✓ | × | ✓ |
| [53] | A Scalable protocol level approach to prevent machine learning attacks on physically unclonable function based authentication mechanisms for internet of medical things | 2021 | M | × | ✓ | × | × |
| [64] | A secure and LoRaWAN compatible user authentication protocol for critical applications in IoT environment | 2021 | H | ✓ | ✓ | × | × |
| [29] | A two-stage feature transformation-based fingerprint authentication system for privacy protection in IoT | 2021 | P | ✓ | × | ✓ | × |
| [11] | Advanced digital signatures for preserving privacy and trust management in hierarchical heterogeneous IoT | 2021 | H | ✓ | ✓ | × | ✓ |
| [54] | An anti-quantum authentication protocol for space information networks based on ring learning with errors | 2021 | H | ✓ | ✓ | × | ✓ |
| [99] | An improved lightweight two-factor authentication protocol for IoT applications | 2022 | H | ✓ | ✓ | ✓ | ✓ |
| [114] | Blockchain applicability for IoT: performance and scalability challenges and solutions | 2022 | M | ✓ | ✓ | ✓ | ✓ |
| [10] | Blockchain-based privacy-preserving authentication protocol for UAV networks | 2023 | H | ✓ | ✓ | ✓ | ✓ |
| [96] | Cybersecurity for industrial IoT (IIoT): Threats, countermeasures, challenges, and future directions | 2023 | H | ✓ | ✓ | ✓ | ✓ |
| [30] | Data aggregation protocols for WSN and IoT applications | 2023 | H | ✓ | ✓ | × | ✓ |
| [92] | Detecting compromised IoT devices: existing techniques, challenges, and a way forward | 2023 | H | ✓ | × | ✓ | × |
| [161] | Old school, new primitive: Towards scalable PUF-based authenticated encryption scheme in IoT | 2023 | P | × | × | × | × |
| [82] | Healthcare internet of things (H-IoT): current trends, future prospects, applications, challenges, and security issues | 2023 | H | × | ✓ | × | × |
| [48] | Lightweight fuzzy extractor based on LPN for device and biometric authentication in IoT | 2021 | P | ✓ | × | × | × |
| [145] | LSPA-SGs: A lightweight and secure protocol for authentication and key agreement based elliptic curve cryptography in smart grids | 2022 | P | × | × | × | ✓ |
| [162] | Robust continuous authentication using cardiac biometrics from wrist-worn wearables | 2021 | P | × | × | × | × |
| [141] | Security and privacy in cloud-based E-health system | 2021 | H | ✓ | × | × | × |
| [3] | Sensor-based continuous authentication of smartphones' users using behavioral biometrics | 2020 | M | ✓ | × | ✓ | × |
| [106] | A secure and lightweight authentication protocol for IoT-based smart homes | 2021 | M | ✓ | ✓ | × | × |

H =**High**, M = **Medium**, P = **Poor**

Table 13. Authentication in the digital era: an in-depth contrast of password- and digital certificate systems-based authentication protocol

| Criterion/Aspect | **Passwords-based** (as in [39], [163]) | **Digital Certificates-based** (as in [39], [163]) |
|---|---|---|
| Overview | Most common method; relies on something the user knows | Offers higher security and relies on something the user possesses |
| Security | Vulnerable to attacks like shoulder surfing; depends on password strength | Protects against forgery attacks and relies on digital signature |
| Ease of use | Users can choose and change; can be problematic if forgotten | Requires a complex infrastructure; offers higher reliability |
| Scalability | Easier to adapt to new technologies; may face security concerns | Requires more intricate infrastructure; considered safer when scaling up |
| Cost | Generally less expensive; doesn't require costly technology | More costly due to the required infrastructure; includes renewal and maintenance costs |
| Compatibility | Widely used and generally compatible with most systems | Might require specific infrastructure or configurations for compatibility |
| User convenience | Requires users to remember passwords; can be burdensome with multiple passwords | Does not require the user to remember info; may need a physical device like USB key or smart card; |
| Nature of protection | Knowledge-based | Possession-based |
| Renewal & validity | Needs periodic change; may expire after multiple failed attempts | Requires renewal based on a validity period; can be long-term based on the policy |
| Reliability | Easily compromised by attacks; depends on user awareness | Reduces the risk of attacks; provides an additional layer of security with encryption |
| Flexibility | Can be used in nearly any system | May require a specific system for effectiveness |
| Privacy | People might share passwords | It is not advisable to share digital certificates |
| Stability | Might change frequently | Usually stable for a longer duration |
| 2FA | Can be paired with other means for 2FA | Often a part of a 2FA solution |
| Dependability | Can be affected by attacks or human errors | More dependable due to encryption and dual authentication |
| Integration with other systems | Easily integrated into most systems | Might require specific infrastructure for integration |
| Monitoring and reporting | Might offer basic reports on access attempts | Offers detailed reports on certificate usage and status |
| Updates and renewals | Might need periodic renewal based on security policies | May require periodic renewal based on validity duration |
| Required training | Users may need basic training on best practices | May require more detailed training for users and support teams |

Table 14. Examining biometric and two-factor authentication in the digital era for identity verification

| **Criterion/Aspect** | **Biometric Verification-based** (as in [123], [46], [111]) | **Two-Factor Authentication** (as in [125], [17], [5]) |
|---|---|---|
| Definition | System based on unique biological or behavioral features of an individual | System that uses two distinct pieces of information to verify identity |
| Security | Vulnerable to replication and theft | More secure than traditional methods but can be compromised if both factors are stolen |
| Convenience | Easy and quick to use | Might be considered complex for some users |
| Cost | Can be high | Mainly software-based and less costly |
| Applications | Used in financial institutions and sensitive places | Common in web applications and digital services |
| Privacy | Concerns about biometric data theft | One-time codes protect digital identity |
| Reliability | Physical conditions can affect accuracy | Might be affected if the verification device is lost |
| Integration | Requires special technologies and devices | Easy integration with various digital services |
| Flexibility | Static and biometric data cannot be changed | Authentication methods can be easily changed |
| Ease of Use | Doesn't require many steps from the user | Might require multiple steps for verification |
| Adaptability | Depends on immutable individual traits | Can be adapted based on context and requirements |
| Sustainability | Needs periodic technical updates | Relies on available software technology |
| Response speed | Immediate Response | Delays are possible due to messages or notifications |
| Complexity | Based on biological features | Uses multiple verification modes |
| Prevalence | Slowly becoming more common | Widely used in web applications and services |
| Compatibility | Might require special devices | Compatible with most apps and systems |
| Updates & maintenance | Might require costly technical updates | Updates are software-based and less expensive |
| Ability to fraud | Hard to cheat but not impossible | Can be compromised if an attacker accesses both methods |
| Reliability | Depends on the user's physical conditions | Depends on the available verification methods |
| Social acceptance | Some might see it as invasive or intrusive | Generally accepted and familiar to users |

It is worth highlighting that selecting the appropriate system is heavily dependent on the specific context and needs of each application or system.

*4.2.3 Multi-factor Authentication vs. Single-factor Authentication.* Without a doubt, secure authentication methods are essential technological elements that play an essential role in protecting digital data and information. In this era of digital advancement, it becomes apparent how important it is to analyze and compare the effectiveness and efficiency of various authentication approaches. In Table 15, we provide an elaborate overview that illuminates the contrast between multifactor authentication and single-factor authentication strategies. This detailed evaluation highlights the fundamental differences between these methods and highlights both their advantages and challenges. The purpose of this table is to offer readers a comprehensive perspective that assists in comprehending and assessing the most efficient and secure methods across a range of application scenarios. We encourage you to explore this information and apply it to enhance and refine your digital systems. By grasping these systems, we can attain elevated levels of security in an ever-more intricate and interconnected environment.

## 5 LEARNED LESSONS

After a thorough and detailed review of IoT authentication protocols, we uncovered a set of fundamental difficulties, valuable opportunities, and deep insights that can guide *the future development of this vital field*. The key insights we gained are as follows:

- IoT authentication protocols are the cornerstone of data protection and communication integrity in this connected world. These protocols enable us to build more secure and reliable systems, thereby improving confidence in the widespread use of IoT technologies.
- The rapid increase in connected devices presents a significant challenge in managing security and privacy. However, advancements in encryption technologies and secret key management offer us the opportunity to build systems that can withstand complex cyber-attacks.

Table 15. In-depth analysis: comparing multi-factor authentication and single-factor authentication in the age of digital transformation

| **Criterion/Aspect** | **Multi-factor Authentication** (as in [57], [107], [42] ) | **Single-factor Authentication** (as in [46], [12], [16] ) |
|---|---|---|
| Security level | High due to multiple protection layers | Relatively low due to reliance on a single factor |
| User convenience | Can be complex at times | Easier and faster |
| Cost | Higher due to multiple layers | Less costly |
| Reliability | High due to multiple securities | Lower in some scenarios |
| Suitable applications | Banking platforms, private networks | Basic applications |
| Supporting technologies | Biometrics, physical devices | Passwords |
| Adaptability to new threats | High | Low |
| Response time | Might be slower | Faster |
| User interaction level | Higher interaction | Lesser interaction |
| Update and maintenance | Requires more updates and maintenance | Easier to update |
| System integration | Requires greater integration | Lesser integration |
| Privacy | High due to multi-factor authentication | Might be limited |
| Dependability | High | Relatively low |
| Compatibility with other technologies | Requires greater compatibility | Lesser compatibility |
| Effectiveness in user recognition | High | Relatively low |
| Adaptability to changes | High due to multi-factor flexibility | Low |
| User experience | Might be complex at times | Easier and smoother |
| Auditing and tracking | Factors used can be clearly tracked | Lesser clarity in tracking |
| Integration with current infrastructure | Might require changes in the infrastructure | Easier integration |
| Impact on system performance | Might have an impact due to multiple verifications | Lesser impact on performance |

- The role of authentication protocols is not limited to data protection alone, but also extends to improving system efficiency and reducing resource consumption, particularly in resource-constrained environments. Protocols provide suitable for such environments; they may require additional security measures to ensure robust protection against more complex threats.
- IoT, combined with emerging technologies like artificial intelligence and blockchain, presents significant opportunities for enhancing security and scalability. These technologies will shape the future, making authentication protocols more adaptive and resilient to increasing threats.
- It is safe to say that the future of IoT will require a stronger emphasis on adopting multi-factor authentication and biometric technologies to ensure a smooth and secure user experience. Innovations in these areas will be key to ensuring security without compromising efficiency or scalability.
- Federated learning in 6G environments offers an innovative approach to improving security and privacy. By analyzing data locally on devices without transferring it to central servers, this method enhances the protection of personal data and reduces the risks associated with cyber breaches.
- Adaptive gateway selection in 5G networks improves communication efficiency and data security by identifying the most effective and least congested paths for data transmission. This increases network effectiveness and reduces data transfer delays, enhancing the performance of critical applications.

During this exciting research journey, we encountered various difficulties that provided us with valuable lessons that will benefit future researchers. The challenges we faced are:

- **Choosing the right protocol:** One of the primary difficulties we faced was selecting the appropriate authentication protocols for different IoT environments. This required a deep understanding of the technical and practical aspects of each protocol, which added considerable complexity to my analysis. However, overcoming this difficulty greatly enriched the depth of the research.
- **Balancing security and efficiency:** Striking a balance between strong security measures and maintaining high performance was particularly challenging in resource-limited environments. This difficulty required continuous evaluation of the trade-offs between security and system efficiency, which proved to be a time-consuming and complex task.
- **Managing secret keys:** Ensuring the secure storage and renewal of secret keys, particularly when dealing with protocols like HOTP and TOTP, was another significant difficulty. The challenge was to maintain system flexibility while securing key management against evolving threats.

- **Addressing complex attacks:** Dealing with complex attacks like brute-force and network-based attacks was critical, necessitating the development of advanced strategies to enhance security.
- **Integrating multi-factor authentication:** While effective in enhancing security, it added complexity in terms of user experience and system compatibility, prompting us to consider more balanced authentication solutions between security and ease of use.
- **Managing dynamic changes in network infrastructure:** Implementing federated learning requires the ability to adapt to continuous changes in network infrastructure and device distribution, which poses a difficulty in maintaining stable performance and ensuring data security under these varying conditions.
- **Handling technical complexities in adaptive gateway selection:** Despite the significant benefits of adaptive gateway selection, implementing this approach requires complex management and precise coordination among different network components to ensure optimal path selection without causing interference or performance degradation.

Through this comprehensive review, we can conclude that "IoT authentication protocols will continue to evolve, with these developments interacting like a chain reaction, where the advancement of one aspect stimulates another, leading to modern authentication systems capable of addressing challenges that we have not witnessed before."

## 6 CONCLUSION

We have conducted a comprehensive and up-to-date survey on IoT authentication protocols, highlighting the main challenges in this field. Our goal was to provide a clear and concise overview of the latest authentication algorithms for devices and services in the IoT, as well as the security threats and risks they face. We also looked at some emerging and promising technologies and techniques that can enhance the security and reliability of IoT applications, such as biometrics, certification, multifactor authentication, fuzzy vault, TOTP, and cancelable biometrics. Our survey shows that IoT authentication systems are diverse and complex, with different pros and cons. We have identified some of the common problems and dangers that IoT authentication protocols encounter, such as scalability, privacy, MITM attacks, DoS attacks, replay attacks, brute-force attacks, and hacking and security threats. We have also offered some possible solutions and countermeasures for these problems, such as adaptive APs, privacy-preserving methods, layered security measures, and secure communication channels, AI-based machine learning authentication, blockchain-based authentication, and MFA. Our findings have important implications for the current and future security of IoT systems. They show the need for authentication mechanisms that are both effective and efficient in coping with the changing and dynamic nature of IoT environments. However, our paper still has some limitations. These include limited information access, challenges with authentication technology, and access to diverse sources. Therefore, we suggest some directions for future research, such as conducting more empirical studies and experiments, developing APs that are more user-friendly and customized to individual needs, and exploring the ethical and legal issues related to IoT authentication. In summary, authentication is a crucial and challenging aspect of IoT security, requiring continuous innovation and improvement to ensure a secure and lasting IoT environment. Our work will serve as a valuable and informative guide for researchers, practitioners, and policy makers interested in or involved in IoT authentication. We also hope our work will inspire further research and development in this fascinating and essential area.

## ACKNOWLEDGMENTS

This work was supported in part by Open Fund of Anhui Engineering Research Center for Intelligent Applications and Security of Industrial Internet, under Grant IASII24-04, and in part by Shenyang Aerospace University Talent Research Start-up Fund under Grant 502/120423005. Amar N. Alsheavi is grateful for the financial support from the ANSO scholarship.

## REFERENCES

[1] Mohammad Abdussami, Ruhul Amin, and Satyanarayana Vollala. 2023. Provably secured lightweight authenticated key agreement protocol for modern health industry. *Ad Hoc Networks* 141 (2023), 103094.

[2] Mideth Abisado, Arlene Trillanes, Angelique Lacasandile, and Angelica De La Cruz. 2022. Using Low-Resourced Language in Social Media Platforms Towards Disease Surveillance for Public Health Monitoring using Artificial Intelligence. In *Proceedings of the 11th International Conference on Software and Information Engineering*. 77–85.

[3] Mohammed Abuhamad, Ahmed Abusnaina, DaeHun Nyang, and David Mohaisen. 2020. Sensor-based continuous authentication of smartphones' users using behavioral biometrics: A contemporary survey. *IEEE Internet of Things Journal* 8, 1 (2020), 65–84.

[4] Sharmistha Adhikari, Sangram Ray, Mohammad S Obaidat, and GP Biswas. 2020. Efficient and secure content dissemination architecture for content centric network using ECC-based public key infrastructure. *Computer Communications* 157 (2020), 187–203.

[5] Shreesh Kumar Agarwal and Amit M Joshi. 2022. Device authentication with FPGA based self correcting Physical Unclonable Function for Internet of Things. *Microprocessors and Microsystems* 95 (2022), 104717.

[6] Shaik Shakeel Ahamad and Al-Sakib Khan Pathan. 2021. A formally verified authentication protocol in secure framework for mobile healthcare during COVID-19-like pandemic. *Connection Science* 33, 3 (2021), 532–554.

[7] Tariq Ahamed Ahanger, Abdullah Aljumah, and Mohammed Atiquzzaman. 2022. State-of-the-art survey of artificial intelligent techniques for IoT security. *Computer Networks* 206 (2022), 108771.

[8] Adel Ali Ahmed and Waleed Ali Ahmed. 2019. An effective multifactor authentication mechanism based on combiners of hash function over internet of things. *Sensors* 19, 17 (2019), 3663.

[9] Milad Taleby Ahvanooey, Mark Xuefang Zhu, Qianmu Li, Wojciech Mazurczyk, Kim-Kwang Raymond Choo, Birij B Gupta, and Mauro Conti. 2021. Modern authentication schemes in smartphones and IoT devices: An empirical survey. *IEEE Internet of Things Journal* 9, 10 (2021), 7639–7663.

[10] Muhammad Arslan Akram, Hira Ahmad, Adnan Noor Mian, Anca Delia Jurcut, and Saru Kumari. 2023. Blockchain-based privacy-preserving authentication protocol for UAV networks. *Computer Networks* 224 (2023), 109638.

[11] Mahdi R Alagheband and Atefeh Mashatan. 2022. Advanced digital signatures for preserving privacy and trust management in hierarchical heterogeneous IoT: Taxonomy, capabilities, and objectives. *Internet of Things* 18 (2022), 100492.

[12] Reem AlHusain and Ali Alkhalifah. 2021. Evaluating fallback authentication research: a systematic literature review. *Computers & Security* 111 (2021), 102487.

[13] Nawaf Aljohani, Joseph Shelton, and Kaushik Roy. 2017. A secure one time password protocol schema. *International Journal of Information Privacy, Security and Integrity* 3, 2 (2017), 75–95.

[14] Maria Almulhim and Noor Zaman. 2018. Proposing secure and lightweight authentication scheme for IoT based E-health applications. In *2018 20th International Conference on advanced communication technology (ICACT)*. IEEE, 481–487.

[15] Ali Abdullah S. AlQahtani, Hosam Alamleh, and Baker Al Smadi. 2022. IoT Devices Proximity Authentication In Ad Hoc Network Environment. In *2022 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS)*. 1–5. https://doi.org/10.1109/IEMTRONICS55184.2022.9795787

[16] Fatima Alqubaisi, Ahmad Samer Wazan, Liza Ahmad, and David W Chadwick. 2020. Should we rush to implement password-less single factor fido2 based authentication?. In *2020 12th annual undergraduate research conference on applied computing (URC)*. IEEE, 1–6.

[17] Muhammad Naveed Aman, Mohamed Haroon Basheer, and Biplab Sikdar. 2018. Two-factor authentication for IoT with location information. *IEEE Internet of Things Journal* 6, 2 (2018), 3335–3351.

[18] Muhammad Naveed Aman, Mohammed Haroon Basheer, and Biplab Sikdar. 2019. Data provenance for IoT with light weight authentication and privacy preservation. *IEEE Internet of Things Journal* 6, 6 (2019), 10441–10457.

[19] Muhammad Aqeel, Fahad Ali, Muhammad Waseem Iqbal, Toqir A Rana, Muhammad Arif, Rabiul Auwul, et al. 2022. A Review of Security and Privacy Concerns in the Internet of Things (IoT). *Journal of Sensors* 2022 (2022).

[20] Kanneboina Ashok and S Gopikrishnan. 2023. Statistical Analysis of Remote Health Monitoring Based IoT Security Models & Deployments From a Pragmatic Perspective. *IEEE Access* 11 (2023), 2621–2651.

[21] Saleh Atiewi, Amer Al-Rahayfeh, Muder Almiani, Salman Yussof, Omar Alfandi, Ahed Abugabah, and Yaser Jararweh. 2020. Scalable and secure big data IoT system based on multifactor authentication and lightweight cryptography. *IEEE Access* 8 (2020), 113498–113511.

[22] Yahya Atwady and Mohammed Hammoudeh. 2017. A survey on authentication techniques for the internet of things. In *proceedings of the international conference on future networks and distributed systems*.

[23] Federal Bridge Certification Authority. 2023. X. 509 Certificate Policy for the Federal Bridge Certification Authority. (2023).

[24] Yucel Aydin, Gunes Karabulut Kurt, Enver Ozdemir, and Halim Yanikomeroglu. 2020. A flexible and lightweight group authentication scheme. *IEEE internet of things Journal* 7, 10 (2020), 10277–10287.

[25] Muhammad Faizan Ayub, Khalid Mahmood, Saru Kumari, Arun Kumar Sangaiah, et al. 2021. Lightweight authentication protocol for e-health clouds in IoT-based applications through 5G technology. *Digital Communications and Networks* 7, 2 (2021), 235–244.

[26] Venkata Ramana Badarla, Surya Nepal, and Rudrapatna K Shyamasundar. 2022. *Information Systems Security: 18th International Conference, ICISS 2022, Tirupati, India, December 16–20, 2022, Proceedings*. Vol. 13784. Springer Nature.

[27] Silvio Barra, Aniello Castiglione, Fabio Narducci, Maria De Marsico, and Michele Nappi. 2019. Biometric data on the edge for secure, smart and user tailored access to cloud services. *Future Generation Computer Systems* 101 (2019), 534–541.

[28] Aseel Bedari. 2022. *Minutia Modelling and Secure Fingerprint Authentication with Applications to the IoT*. Ph. D. Dissertation. La Trobe.

[29] Aseel Bedari, Song Wang, and Jucheng Yang. 2021. A two-stage feature transformation-based fingerprint authentication system for privacy protection in IoT. *IEEE Transactions on Industrial Informatics* 18, 4 (2021), 2745–2752.

[30] Beneyaz Ara Begum and Satyanarayana V Nandury. 2023. Data aggregation protocols for WSN and IoT applications–A comprehensive survey. *Journal of King Saud University-Computer and Information Sciences* (2023).

[31] Dhruba Kumar Bhattacharyya and Jugal Kumar Kalita. 2016. *DDoS attacks: evolution, detection, prevention, reaction, and tolerance.* CRC Press.

[32] Ting Cai, Wuhui Chen, Kostas E Psannis, Sotirios K Goudos, Yang Yu, Zibin Zheng, and Shaohua Wan. 2023. On-Chain and Off-Chain Scalability Techniques. In *Blockchain Scalability*. Springer, 81–96.

[33] Luka Celic and Ratko Magjarevic. 2020. Seamless connectivity architecture and methods for IoT and wearable devices. *Automatika: časopis za automatiku, mjerenje, elektroniku, računarstvo i komunikacije* 61, 1 (2020), 21–34.

[34] Poornima M Chanal and Mahabaleshwar S Kakkasageri. 2020. Security and privacy in IoT: a survey. *Wireless Personal Communications* 115, 2 (2020), 1667–1693.

[35] Susovan Chanda, Ashish Kumar Luhach, Waleed Alnumay, Indranil Sengupta, and Diptendu Sinha Roy. 2022. A lightweight device-level Public Key Infrastructure with DRAM based Physical Unclonable Function (PUF) for secure cyber physical systems. *Computer Communications* 190 (2022), 87–98.

[36] Nishant Chaurasia and Prashant Kumar. 2023. A Comprehensive Study on Issues and Challenges Related to Privacy and Security in IoT. *e-Prime-Advances in Electrical Engineering, Electronics and Energy* (2023), 100158.

[37] Chien-Ming Chen, Bin Xiang, King-Hang Wang, Yong Zhang, and Tsu-Yang Wu. 2019. An efficient and secure smart card based authentication scheme. *Journal of Internet Technology* 20, 4 (2019), 1113–1123.

[38] Joo Yeon Cho and Andrew Sergeev. 2021. Using QKD in MACsec for secure Ethernet networks. *IET Quantum Communication* 2, 3 (2021), 66–73.

[39] Jusop Choi, Junsung Cho, Hyoungshick Kim, and Sangwon Hyun. 2020. Towards secure and usable certificate-based authentication system using a secondary device for an industrial internet of things. *Applied Sciences* 10, 6 (2020), 1962.

[40] Souhayla Dargaoui, Mourade Azrour, Ahmad El Allaoui, Azidine Guezzaz, Abdulatif Alabdulatif, and Abdullah Alnajim. 2024. Internet of Things Authentication Protocols: Comparative Study. *Computers, Materials & Continua* 79, 1 (2024).

[41] Manik Lal Das, Pardeep Kumar, and Andrew Martin. 2020. Secure and privacy-preserving rfid authentication scheme for internet of things applications. *Wireless Personal Communications* 110 (2020), 339–353.

[42] Sanchari Das, Bingxing Wang, Andrew Kim, and L Jean Camp. 2020. Mfa is a necessary chore!: Exploring user mental models of multi-factor authentication technologies. (2020).

[43] Samundra Deep, Xi Zheng, Alireza Jolfaei, Dongjin Yu, Pouya Ostovari, and Ali Kashif Bashir. 2022. A survey of security and privacy issues in the Internet of Things from the layered context. *Transactions on Emerging Telecommunications Technologies* 33, 6 (2022), e3935.

[44] Daniel Diaz-Sanchez, Andrés Marín-Lopez, Florina Almenárez Mendoza, Patricia Arias Cabarcos, and R Simon Sherratt. 2019. TLS/PKI challenges and certificate pinning techniques for IoT and M2M secure communications. *IEEE Communications Surveys & Tutorials* 21, 4 (2019), 3502–3531.

[45] Jovana Dobreva, Lina Lumburovska, Hristina Mihajloska Trpcheska, Vesna Dimitrova, et al. 2021. A Comparative Analysis of HOTP and TOTP Authentication Algorithms. Which one to choose? *Security & Future* (2021).

[46] Nishant Doshi and Payal Chaudhari. 2023. Cryptanalysis of Authentication Protocol for Cloud Assisted IoT Environment. *Procedia Computer Science* 220 (2023), 886–891.

[47] Saurabh Dutta. 2017. *Striking a balance between usability and cyber-security in IoT devices.* Ph. D. Dissertation. Massachusetts Institute of Technology.

[48] Shahriar Ebrahimi and Siavash Bayat-Sarmadi. 2021. Lightweight fuzzy extractor based on LPN for device and biometric authentication in IoT. *IEEE Internet of Things Journal* 8, 13 (2021), 10706–10713.

[49] Moneer Fakroon. 2021. Secure Authentication Schemes for Internet of Things (IoT). (2021).

[50] Abba Garba, David Khoury, Patrick Balian, Samir Haddad, Jinane Sayah, Zhong Chen, Zhi Guan, Hani Hamdan, Jinan Charafeddine, and Khalid Al-Mutib. 2023. LightCert4IoTs: Blockchain-Based Lightweight Certificates Authentication for IoT Applications. *IEEE Access* 11 (2023), 28370–28383.

[51] Dimitrios Glaroudis, Athanasios Iossifides, and Periklis Chatzimisios. 2020. Survey, comparison and research challenges of IoT application protocols for smart farming. *Computer Networks* 168 (2020), 107037.

[52] Prosanta Gope. 2019. LAAP: Lightweight anonymous authentication protocol for D2D-aided fog computing paradigm. *computers & security* 86 (2019), 223–237.

[53] Prosanta Gope, Owen Millwood, and Biplab Sikdar. 2021. A scalable protocol level approach to prevent machine learning attacks on physically unclonable function based authentication mechanisms for internet of medical things. *IEEE Transactions on Industrial Informatics* 18, 3 (2021), 1971–1980.

[54] Junyan Guo, Ye Du, Xuesong Wu, and Meihong Li. 2021. An anti-quantum authentication protocol for space information networks based on ring learning with errors. *Journal of Communications and Information Networks* 6, 3 (2021), 301–311.

[55] Mathuri Gurunathan, Moamin A Mahmoud, and Faisal Hadi Faisal. 2023. Enhanced Blockchain Scalability for IoT-based Smart Devices-A Generic Model Development. In *2023 IEEE 13th Symposium on Computer Applications & Industrial Electronics (ISCAIE)*. IEEE, 320–325.

[56] Badis Hammi, Achraf Fayad, Rida Khatoun, Sherali Zeadally, and Youcef Begriche. 2020. A lightweight ECC-based authentication scheme for Internet of Things (IoT). *IEEE Systems Journal* 14, 3 (2020), 3440–3450.

[57] Md Arif Hassan and Zarina Shukur. 2021. A secure multi factor user authentication framework for electronic payment system. In *2021 3rd International Cyber Resilience Conference (CRC)*. IEEE, 1–6.

[58] Jigna J Hathaliya, Sudeep Tanwar, and Richard Evans. 2020. Securing electronic healthcare records: A mobile-based biometric authentication approach. *Journal of Information Security and Applications* 53 (2020), 102528.

[59] Daojing He, Ziming Zhao, Sammy Chan, and Mohsen Guizani. 2022. A Novel Authentication Protocol for IoT-Enabled Devices. *IEEE Internet of Things Journal* 10, 1 (2022), 867–876.

[60] Joel Höglund, Samuel Lindemer, Martin Furuhed, and Shahid Raza. 2020. PKI4IoT: Towards public key infrastructure for the Internet of Things. *Computers & Security* 89 (2020), 101658.

[61] Silke Holtmanns and Ian Oliver. 2017. SMS and one-time-password interception in LTE networks. In *2017 IEEE International Conference on Communications (ICC)*. 1–6. https://doi.org/10.1109/ICC.2017.7997246

[62] Yun Huang, Zheng Huang, Haoran Zhao, and Xuejia Lai. 2013. A new one-time password method. *IERI Procedia* 4 (2013), 32–37.

[63] Sivan Sper Ibrahim et al. 2021. *Development of data encryption algorithm for database security by using ASCII code.* Master's thesis. Sakarya Üniversitesi.

[64] Abdollah Jabbari and Jamshid Bagherzadeh Mohasefi. 2021. A secure and LoRaWAN compatible user authentication protocol for critical applications in the IoT environment. *IEEE Transactions on Industrial Informatics* 18, 1 (2021), 56–65.

[65] Priyank Jain, Manasi Gyanchandani, and Nilay Khare. 2016. Big data privacy: a technological perspective and review. *Journal of Big Data* 3 (2016), 1–25.

[66] Hua Jiang, Gang Zhang, and Jinpo Fan. 2019. Structure analysis and generation of X. 509 digital certificate based on national secret. In *Journal of Physics: Conference Series*, Vol. 1187. IOP Publishing, 042067.

[67] Qi Jiang, Xin Zhang, Ning Zhang, Youliang Tian, Xindi Ma, and Jianfeng Ma. 2021. Three-factor authentication protocol using physical unclonable function for IoV. *Computer Communications* 173 (2021), 45–55.

[68] Mattijs Jonker, Alistair King, Johannes Krupp, Christian Rossow, Anna Sperotto, and Alberto Dainotti. 2017. Millions of targets under attack: a macroscopic characterization of the DoS ecosystem. In *Proceedings of the 2017 Internet Measurement Conference*. 100–113.

[69] Changhun Jung, Jinchun Choi, Rhongho Jang, David Mohaisen, and DaeHun Nyang. 2021. A network-independent tool-based usable authentication system for Internet of Things devices. *Computers & Security* 108 (2021), 102338.

[70] Mohsin Kamal, Abdulah Aljohani, and Eisa Alanazi. 2020. IoT meets COVID-19: status, challenges, and opportunities. *arXiv preprint arXiv:2007.12268* (2020).

[71] S Karthikeyan and T Poongodi. 2022. Secured Data Compression and Data Authentication in Internet of Thing Networks Using LZW Compression Based X. 509 Certification. In *2022 IEEE International Conference on Data Science and Information System (ICDSIS)*. IEEE, 1–5.

[72] Salabat Khan, Fei Luo, Zijian Zhang, Mussadiq Abdul Rahim, Mubashir Ahmad, and Kaishun Wu. 2022. Survey on issues and recent advances in vehicular public-key infrastructure (VPKI). *IEEE Communications Surveys & Tutorials* 24, 3 (2022), 1574–1601.

[73] Osama A Khashan and Nour M Khafajah. 2023. Efficient hybrid centralized and blockchain-based authentication architecture for heterogeneous IoT systems. *Journal of King Saud University-Computer and Information Sciences* 35, 2 (2023), 726–739.

[74] Sara El-Sayed Khater, Basheer Abd Elfattah Youssef, and Salwa El-Gamal. 2022. Internet of Things (IoT) Authentication and Integrity Model using MBTSKHF One Time Password (OTP). In *Proceedings of the 11th International Conference on Software and Information Engineering*. 97–103.

[75] Rida Khatoun. 2022. *Cybersecurity in Smart Homes: Architectures, Solutions and Technologies.* John Wiley & Sons.

[76] Jing Huey Khor, Michail Sidorov, and Seri Aathira Balqis Zulqarnain. 2023. Scalable Lightweight Protocol for Interoperable Public Blockchain-Based Supply Chain Ownership Management. *Sensors* 23, 7 (2023), 3433.

[77] Constantinos Kolias, Georgios Kambourakis, Angelos Stavrou, and Jeffrey Voas. 2017. DDoS in the IoT: Mirai and other botnets. *Computer* 50, 7 (2017), 80–84.

[78] Liang Kou, Yiqi Shi, Liguo Zhang, Duo Liu, and Qing Yang. 2019. A Lightweight Three-Factor User Authentication Protocol for the Information Perception of IoT. *Computers, Materials & Continua* 58, 2 (2019).

[79] T Krishna, S Phani Praveen, Shakeel Ahmed, and Parvathaneni Naga Srinivasu. 2022. Software-driven secure framework for mobile healthcare applications in IoMT. *Intelligent Decision Technologies* Preprint (2022), 1–14.

[80] Rudra Krishnasrija, Amit Kr Mandal, and Agostino Cortesi. 2023. A lightweight mutual and transitive authentication mechanism for IoT network. *Ad Hoc Networks* 138 (2023), 103003.

[81] Yunlim Ku, Okkyung Choi, Kangseok Kim, Taeshik Shon, Manpyo Hong, Hongjin Yeh, and Jai-Hoon Kim. 2013. Two-factor authentication system based on extended OTP mechanism. *International Journal of Computer Mathematics* 90, 12 (2013), 2515–2529.

[82] Mohit Kumar, Ashwani Kumar, Sahil Verma, Pronaya Bhattacharya, Deepak Ghimire, Seong-heum Kim, and ASM Sanwar Hosen. 2023. Healthcare Internet of Things (H-IoT): Current Trends, Future Prospects, Applications, Challenges, and Security Issues. *Electronics* 12, 9 (2023), 2050.

[83] Hyuksang Kwon, Jeongseob Ahn, and JeongGil Ko. 2019. LightCert: On designing a lighter certificate for resource-limited Internet-of-Things devices. *Transactions on emerging telecommunications technologies* 30, 10 (2019), e3740.

[84] Jianhua Li, Jiong Jin, Lingjuan Lyu, Dong Yuan, Yingying Yang, Longxiang Gao, and Chao Shen. 2021. A fast and scalable authentication scheme in IOT for smart living. *Future Generation Computer Systems* 117 (2021), 125–137.

[85] Yannan Li, Yong Yu, Chunwei Lou, Nadra Guizani, and Lianhai Wang. 2020. Decentralized public key infrastructures atop blockchain. *IEEE Network* 34, 6 (2020), 133–139.

[86] Lining Liu and Yongquan Li. [n. d.]. Proceedings of 2022 11th International Conference on Software and Information Engineering ICSIE 2022. ([n. d.]).

[87] Shanhe Lou, Yixiong Feng, Guangdong Tian, Zhihan Lv, Zhiwu Li, and Jianrong Tan. 2017. A cyber-physical system for product conceptual design based on an intelligent psycho-physiological approach. *IEEE Access* 5 (2017), 5378–5387.

[88] Karim Lounis and Mohammad Zulkernine. 2021. T2T-MAP: A PUF-based thing-to-thing mutual authentication protocol for IoT. *IEEE Access* 9 (2021), 137384–137405.

[89] Siqi Ma, Runhan Feng, Juanru Li, Yang Liu, Surya Nepal, Diethelm, Elisa Bertino, Robert H Deng, Zhuo Ma, and Sanjay Jha. 2019. An empirical study of sms one-time password authentication in android apps. In *Proceedings of the 35th annual computer security applications conference*. 339–354.

[90] Rakesh Kumar Mahendran and Parthasarathy Velusamy. 2020. A secure fuzzy extractor based biometric key authentication scheme for body sensor network in Internet of Medical Things. *Computer Communications* 153 (2020), 545–552.

[91] Moamin A Mahmoud, Mathuri Gurunathan, Ramona Ramli, Kazeem Alasinrin Babatunde, and Faisal Hadi Faisal. 2023. Review and Development of a Scalable Lightweight Blockchain Integrated Model (LightBlock) for IoT Applications. *Electronics* 12, 4 (2023), 1025.

[92] Imran Makhdoom, Mehran Abolhasan, Daniel Franklin, Justin Lipman, Christian Zimmermann, Massimo Piccardi, and Negin Shariati Moghadam. 2023. Detecting compromised IoT devices: Existing techniques, challenges, and a way forward. *Computers & Security* (2023), 103384.

[93] Daniel Maldonado-Ruiz, Jenny Torres, Nour El Madhoun, and Mohamad Badra. 2022. Current trends in blockchain implementations on the paradigm of public key infrastructure: a survey. *IEEE Access* 10 (2022), 17641–17655.

[94] Anup Kumar Maurya, Ashok Kumar Das, Sajjad Shaukat Jamal, and Debasis Giri. 2021. Secure user authentication mechanism for IoT-enabled Wireless Sensor Networks based on multiple Bloom filters. *Journal of Systems Architecture* 120 (2021), 102296.

[95] Daniele Mazzei, Giacomo Baldi, Gualtiero Fantoni, Gabriele Montelisciani, Antonio Pitasi, Laura Ricci, and Lorenzo Rizzello. 2020. A Blockchain Tokenizer for Industrial IOT trustless applications. *Future Generation Computer Systems* 105 (2020), 432–445.

[96] Sri Harsha Mekala, Zubair Baig, Adnan Anwar, and Sherali Zeadally. 2023. Cybersecurity for industrial IoT (IIoT): Threats, countermeasures, challenges and future directions. *Computer Communications* (2023).

[97] Chandrashekhar Meshram, Rabha W Ibrahim, Lunzhi Deng, Shailendra W Shende, Sarita Gajbhiye Meshram, and Sharad Kumar Barve. 2021. A robust smart card and remote user password-based authentication protocol using extended chaotic maps under smart cities environment. *Soft Computing* 25, 15 (2021), 10037–10051.

[98] Shivendu Mishra, Ritika Yaduvanshi, Kumkum Dubey, and Prince Rajpoot. 2021. ESS-IBAA: Efficient, short, and secure ID-based authentication algorithm for wireless sensor network. *International Journal of Communication Systems* 34, 8 (2021), e4764.

[99] Amir Masoud Aminian Modarres and Ghazaleh Sarbishaei. 2022. An Improved Lightweight Two-Factor Authentication Protocol for IoT Applications. *IEEE Transactions on Industrial Informatics* (2022).

[100] David Moore, Colleen Shannon, Douglas J Brown, Geoffrey M Voelker, and Stefan Savage. 2006. Inferring internet denial-of-service activity. *ACM Transactions on Computer Systems (TOCS)* 24, 2 (2006), 115–139.

[101] Masoud Moradi, Masoud Moradkhani, Mohammad Bagher Tavakoli, et al. 2022. A real-time biometric encryption scheme based on fuzzy logic for IoT. *Journal of Sensors* 2022 (2022).

[102] Ahmad Mostafa. 2020. Blockchain-based distributed authentication Mechanism for internet-of-things devices. In *Proceedings of the 9th International Conference on Software and Information Engineering*. 159–164.

[103] Majid Mumtaz, Junaid Akram, and Luo Ping. 2019. An RSA based authentication system for smart IoT environment. In *2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*. IEEE, 758–765.

[104] Maryam M Najafabadi, Taghi M Khoshgoftaar, Clifford Kemp, Naeem Seliya, and Richard Zuech. 2014. Machine learning for detecting brute force attacks at the network level. In *2014 IEEE International Conference on Bioinformatics and Bioengineering*. IEEE, 379–385.

[105] Uma Narayanan, Varghese Paul, and Shelbi Joseph. 2021. Decentralized blockchain based authentication for secure data sharing in Cloud-IoT: DeBlock-Sec. *Journal of Ambient Intelligence and Humanized Computing* (2021), 1–19.

[106] JiHyeon Oh, SungJin Yu, JoonYoung Lee, SeungHwan Son, MyeongHyun Kim, and YoungHo Park. 2021. A secure and lightweight authentication protocol for IoT-based smart homes. *Sensors* 21, 4 (2021), 1488.

[107] Soumya Prakash Otta, Subhrakanta Panda, Maanak Gupta, and Chittaranjan Hota. 2023. A Systematic Survey of Multi-Factor Authentication for Cloud Infrastructure. *Future Internet* 15, 4 (2023), 146.

[108] Akash Suresh Patil, Rafik Hamza, Alzubair Hassan, Nan Jiang, Hongyang Yan, and Jin Li. 2020. Efficient privacy-preserving authentication protocol using PUFs with blockchain smart contracts. *Computers & Security* 97 (2020), 101958.

[109] Christos Patsonakis, Katerina Samari, Aggelos Kiayias, and Mema Roussopoulos. 2020. Implementing a smart contract PKI. *IEEE Transactions on Engineering Management* 67, 4 (2020), 1425–1443.

[110] Chau DM Pham and Tran Khanh Dang. 2021. A lightweight authentication protocol for D2D-enabled IoT systems with privacy. *Pervasive and Mobile Computing* 74 (2021), 101399.

[111] D Prabhu, S Vijay Bhanu, and S Suthir. 2022. Privacy preserving steganography based biometric authentication system for cloud computing environment. *Measurement: Sensors* 24 (2022), 100511.

[112] Vu Khanh Quy, Nguyen Tien Ban, Dang Van Anh, Nguyen Minh Quy, and Dinh C Nguyen. 2023. An adaptive gateway selection mechanism for MANET-IoT applications in 5G networks. *IEEE Sensors Journal* (2023).

[113] Vu Khanh Quy, Dinh C Nguyen, Dang Van Anh, and Nguyen Minh Quy. 2024. Federated learning for green and sustainable 6G IIoT applications. *Internet of Things* 25 (2024), 101061.

[114] Ziaur Rahman, Xun Yi, Sk Tanzir Mehedi, Rafiqul Islam, and Andrei Kelarev. 2022. Blockchain Applicability for the Internet of Things: Performance and Scalability Challenges and Solutions. *Electronics* 11, 9 (2022), 1416.

[115] Hritu Raj, Mohit Kumar, Prashant Kumar, Amritpal Singh, and Om Prakash Verma. 2022. Issues and challenges related to privacy and security in healthcare using iot, fog, and cloud computing. *Advanced Healthcare Systems: Empowering Physicians with IoT-Enabled Technologies* (2022), 21–32.

[116] Diksha Rangwani, Dipanwita Sadhukhan, Sangram Ray, Muhammad Khurram Khan, and Mou Dasgupta. 2021. A robust provable-secure privacy-preserving authentication protocol for Industrial Internet of Things. *Peer-to-peer Networking and Applications* 14 (2021), 1548–1571.

[117] P Muralidhara Rao and BD Deebak. 2023. A Comprehensive Survey on Authentication and Secure Key Management in Internet of Things: Challenges, Countermeasures, and Future Directions. *Ad Hoc Networks* (2023), 103159.

[118] Aqsa Rashid, Asif Masood, Haider Abbas, and Yin Zhang. 2021. Blockchain-based public key infrastructure: a transparent digital certification mechanism for secure communication. *IEEE Network* 35, 5 (2021), 220–225.

[119] Mohammed A Rashid and Houshyar Honar Pajooh. 2019. A security framework for IoT authentication and authorization based on blockchain technology. In *2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 264–271.

[120] A Mallikarjuna Reddy, K Srinivas Reddy, M Prasad, and A Obulesh. 2021. Internet of things (IoT) security threats and countermeasures. *Network Security* 5 (2021), 12–26.

[121] Rodrigo Roman, Pablo Najera, and Javier Lopez. 2011. Securing the internet of things. *Computer* 44, 9 (2011), 51–58.

[122] Kumar Sekhar Roy, Subhrajyoti Deb, and Hemanta Kumar Kalita. 2022. A novel hybrid authentication protocol utilizing lattice-based cryptography for IoT devices in fog networks. *Digital Communications and Networks* (2022).

[123] Riseul Ryu, Soonja Yeom, David Herbert, and Julian Dermoudy. 2023. The design and evaluation of adaptive biometric authentication systems: Current status, challenges and future direction. *ICT Express* (2023).

[124] Dipanwita Sadhukhan, Sangram Ray, Mou Dasgupta, and Joel JPC Rodrigues. 2023. CLAACS-IOD: Certificate-embedded lightweight authentication and access control scheme for Internet of Drones. *Software: Practice and Experience* (2023).

[125] Mohammad Javad Sadri and Maryam Rajabzadeh Asaar. 2021. An anonymous two-factor authentication protocol for IoT-based applications. *Computer Networks* 199 (2021), 108460.

[126] Sujit Sangram Sahoo and Vijay Kumar Chaurasiya. 2023. VIBE: Blockchain-based Virtual Payment in IoT Ecosystem: A Secure Decentralized Marketplace. *Multimedia Tools and Applications* (2023), 1–26.

[127] Muhammad Asad Saleem, Salman Shamshad, Shafiq Ahmed, Zahid Ghaffar, and Khalid Mahmood. 2021. Security analysis on "A secure three-factor user authentication protocol with forward secrecy for wireless medical sensor network systems". *IEEE Systems Journal* 15, 4 (2021), 5557–5559.

[128] Tania Saleem, Muhammad Umar Janjua, Muhammad Hassan, Talha Ahmad, Filza Tariq, Khadija Hafeez, Muhammad Ahsan Salal, and Muhammad Danish Bilal. 2022. ProofChain: An X. 509-compatible blockchain-based PKI framework with decentralized trust. *Computer Networks* 213 (2022), 109069.

[129] S Santesson, R Housley, T Freeman, and L Rosenthol. 2023. RFC 9399: Internet X. 509 Public Key Infrastructure: Logotypes in X. 509 Certificates.

[130] Manasha Saqib, Bhat Jasra, and Ayaz Hassan Moon. 2022. A lightweight three factor authentication framework for IoT based critical applications. *Journal of King Saud University-Computer and Information Sciences* 34, 9 (2022), 6925–6937.

[131] Trusit Shah and Subbarayan Venkatesan. 2018. Authentication of IoT device and IoT server using secure vaults. In *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*. IEEE, 819–824.

[132] Ali Shahidinejad and Jemal Abawajy. 2024. An all-inclusive taxonomy and critical review of blockchain-assisted authentication and session key generation protocols for IoT. *Comput. Surveys* 56, 7 (2024), 1–38.

[133] Salman Shamshad, Muhammad Faizan Ayub, Khalid Mahmood, Saru Kumari, Shehzad Ashraf Chaudhry, and Chien-Ming Chen. 2022. An enhanced scheme for mutual authentication for healthcare services. *Digital Communications and Networks* 8, 2 (2022), 150–161.

[134] Mohd Shariq and Karan Singh. 2021. A novel vector-space-based lightweight privacy-preserving rfid authentication protocol for iot environment. *The Journal of supercomputing* 77 (2021), 8532–8562.

[135] Giriraj Sharma, Amit M Joshi, and Saraju P Mohanty. 2023. sTrade: Blockchain based secure energy trading using vehicle-to-grid mutual authentication in smart transportation. *Sustainable Energy Technologies and Assessments* 57 (2023), 103296.

[136] S Sheeja et al. 2022. Towards an Optimal Security Using Multifactor Scalable Lightweight Cryptography for IoT. In *2022 3rd International Conference on Communication, Computing and Industry 4.0 (C2I4)*. IEEE, 1–6.

[137] Zeeshan Siddiqui, Jiechao Gao, and Muhammad Khurram Khan. 2022. An improved lightweight PUF–PKI digital certificate authentication scheme for the Internet of Things. *IEEE Internet of Things Journal* 9, 20 (2022), 19744–19756.

[138] Inderpal Singh and Balraj Singh. 2022. Access management of IoT devices using access control mechanism and decentralized authentication: A review. *Measurement: Sensors* (2022), 100591.

[139] Khushal Singh and Nanhay Singh. 2021. Multi-level authentication protocol for enabling secure communication in IoT. (2021).

[140] Priyadarshi Singh, Abdul Basit, N Chaitanya Kumar, and V Ch Venkaiah. 2019. Towards a Hybrid Public Key Infrastructure (PKI): A Review. *Cryptology ePrint Archive* (2019).

[141] Remya Sivan and Zuriati Ahmad Zukarnain. 2021. Security and privacy in cloud-based e-health system. *Symmetry* 13, 5 (2021), 742.

[142] Seunghwan Son, Yohan Park, and Youngho Park. 2021. A secure, lightweight, and anonymous user authentication protocol for IoT environments. *Sustainability* 13, 16 (2021), 9241.

[143] Hamed Taherdoost. 2023. Security and Internet of Things: Benefits, Challenges, and Future Perspectives. *Electronics* 12, 8 (2023), 1901.

[144] Dan Tao, Pengchen Ma, and Mohammad S Obaidat. 2019. Anonymous identity authentication mechanism for hybrid architecture in mobile crowd sensing networks. *International Journal of Communication Systems* 32, 14 (2019), e4099.

[145] Susan A Mohammed Taqi and Saeed Jalili. 2022. LSPA-SGs: A lightweight and secure protocol for authentication and key agreement based Elliptic Curve Cryptography in smart grids. *Energy Reports* 8 (2022), 153–164.

[146] Usman Tariq, Irfan Ahmed, Ali Kashif Bashir, and Kamran Shaukat. 2023. A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review. *Sensors* 23, 8 (2023), 4117.

[147] Ashish Tomar, Niraj Gupta, Divya Rani, and Sachin Tripathi. 2023. Blockchain-assisted authenticated key agreement scheme for IoT-based healthcare system. *Internet of Things* (2023), 100849.

[148] Jonathan Tournier, François Lesueur, Frédéric Le Mouël, Laurent Guyon, and Hicham Ben-Hassine. 2021. A survey of IoT protocols and their security issues through the lens of a generic IoT stack. *Internet of Things* 16 (2021), 100264.

[149] Loïc D Tsobdjou, Samuel Pierre, and Alejandro Quintero. 2021. A new mutual authentication and key agreement protocol for mobile client—server environment. *IEEE Transactions on Network and Service Management* 18, 2 (2021), 1275–1286.

[150] Anusha Vangala, Basudeb Bera, Sourav Saha, Ashok Kumar Das, Neeraj Kumar, and YoungHo Park. 2020. Blockchain-enabled certificate-based authentication for vehicle accident detection and notification in intelligent transportation systems. *IEEE Sensors Journal* 21, 14 (2020), 15824–15838.

[151] Jizhi Wang et al. 2019. The prediction of serial number in OpenSSL's X. 509 certificate. *Security and Communication Networks* 2019 (2019).

[152] Mohammad Wazid, Ashok Kumar Das, and Sachin Shetty. 2022. Tacas-iot: Trust aggregation certificate-based authentication scheme for edge-enabled iot systems. *IEEE Internet of Things Journal* 9, 22 (2022), 22643–22656.

[153] Fan Wu, Xiong Li, Lili Xu, Pandi Vijayakumar, and Neeraj Kumar. 2020. A novel three-factor authentication protocol for wireless sensor networks with IoT notion. *IEEE Systems Journal* 15, 1 (2020), 1120–1129.

[154] Anil Yadav, Sujata Pandey, and Rajat Singh. 2021. Lightweight capability-token for consent-based authentication protocol for smart sensor nodes. *Journal of Information Security and Applications* 63 (2021), 103024.

[155] Wencheng Yang, Song Wang, James Jin Kang, Michael N Johnstone, and Aseel Bedari. 2022. A linear convolution-based cancelable fingerprint biometric authentication system. *Computers & Security* 114 (2022), 102583.

[156] Zheng Yang, Chenglu Jin, Jianting Ning, Zengpeng Li, Anh Dinh, and Jianying Zhou. 2021. Group time-based one-time passwords and its application to efficient privacy-preserving proof of location. In *Annual Computer Security Applications Conference*. 497–512.

[157] Sergey E Yunakovsky, Maxim Kot, Nikolay Pozhar, Denis Nabokov, Mikhail Kudinov, Anton Guglya, Evgeniy O Kiktenko, Ekaterina Kolycheva, Alexander Borisov, and Aleksey K Fedorov. 2021. Towards security recommendations for public-key infrastructures for production environments in the post-quantum era. *EPJ Quantum Technology* 8, 1 (2021), 14.

[158] Sadra Zargar, Ali Shahidinejad, and Mostafa Ghobaei-Arani. 2021. A lightweight authentication protocol for IoT-based cloud environment. *International Journal of Communication Systems* 34, 11 (2021), e4849.

[159] Bruno Bogaz Zarpelão, Rodrigo Sanches Miani, Cláudio Toshio Kawakani, and Sean Carlisto de Alvarenga. 2017. A survey of intrusion detection in Internet of Things. *Journal of Network and Computer Applications* 84 (2017), 25–37.

[160] Hai Zhang and Feng Zhao. 2023. Cross-domain identity authentication scheme based on blockchain and PKI system. *High-Confidence Computing* 3, 1 (2023), 100096.

[161] Xiaolin Zhang, Dawu Gu, Tengfei Wang, and Yu Huang. 2023. Old School, New Primitive: Towards Scalable PUF-based Authenticated Encryption Scheme in IoT. *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* (2023).

[162] Tianming Zhao, Yan Wang, Jian Liu, Jerry Cheng, Yingying Chen, and Jiadi Yu. 2021. Robust continuous authentication using cardiac biometrics from wrist-worn wearables. *IEEE Internet of Things Journal* 9, 12 (2021), 9542–9556.

[163] Ma Zhaofeng, Meng Jialin, Wang Jihui, and Shan Zhiguang. 2020. Blockchain-based decentralized authentication modeling scheme in edge and IoT environment. *IEEE Internet of Things Journal* 8, 4 (2020), 2116–2123.

[164] Fei Zhu, Xun Yi, Alsharif Abuadbba, Ibrahim Khalil, Surya Nepal, Xinyi Huang, and Xingfu Yan. 2021. Certificate-based anonymous authentication with efficient aggregation for wireless medical sensor networks. *IEEE Internet of Things Journal* 9, 14 (2021), 12209–12218.

[165] Jiayu Zhu, Chengcheng Wan, Pengbo Nie, Yuting Chen, and Zhendong Su. 2020. Guided, Deep Testing of X. 509 Certificate Validation via Coverage Transfer Graphs. In *2020 IEEE International Conference on Software Maintenance and Evolution (ICSME)*. IEEE, 243–254.