Authentication Methods in Internet-of-Things Platform: A Comprehensive Review

Gholam Reza Zargar[1], Hamid Barati[1], Ali Barati[1]
1- Department of Computer Engineering, Dezful Branch, Islamic Azad University, Dezful, Iran.
Email: gh.zargar@iaud.ac.ir, hamid.barati@iau.ac.ir (Corresponding author), alibarati@iau.ac.ir

ABSTRACT:
Authentication is a critical aspect of securing Internet-of-Things (IoT) platforms, ensuring only authorized devices and user's access sensitive data and services. One critical aspect of IoT is ensuring secure and anonymous authentication protocols to safeguard sensitive data. This paper presents a comprehensive review of authentication methods specifically tailored for IoT environments. Through an extensive analysis of existing literature, various authentication techniques in IoT environments are explored. The review covers key aspects such as security mechanisms, privacy preservation techniques, scalability, and usability of these protocols. Furthermore, the paper discusses challenges unique to IoT authentication, such as resource constraints, scalability, and resilience against diverse cyber threats. Various authentication protocols and frameworks applicable to IoT ecosystems are analyzed, highlighting their strengths, weaknesses, and suitability for different IoT use cases. Additionally, the review examines recent advancements in authentication technologies like blockchain in the context of IoT security. Insights from this review aim to provide researchers and practitioners with a deeper understanding of IoT authentication methods and inform the development of robust, efficient, and scalable authentication solutions for IoT platforms.

KEYWORDS: Authentication, Internet of Things, Security, Privacy Preservation.

1. INTRODUCTION

The Internet of Things refers to a network of interconnected physical objects or "things" embedded with sensors, software, and other technologies that enable them to collect and exchange data with other devices and systems over the internet [1]. These objects can range from everyday items such as household appliances, wearable devices, and vehicles to more specialized equipment used in industrial settings, healthcare, agriculture, and beyond [2-3]. The core concept behind the IoT is to create a seamless ecosystem where devices can communicate with each other, share information, and perform tasks autonomously without requiring human intervention [4-5]. This interconnectedness allows for the creation of smart environments where data collected from various sensors can be analyzed and utilized to improve efficiency, enhance decision-making processes, and enable new services and applications [6].

The IoT ecosystem comprises several key components essential for its operation and functionality [7]. Firstly, sensors and actuators are integral devices embedded within physical objects. Sensors collect data from the surrounding environment, while actuators execute actions based on received instructions [7-8]. Connectivity is another vital component, as IoT devices rely on various communication technologies such as Wi-Fi, Bluetooth, cellular networks, and low-power wide-area networks (LPWAN) to transmit data to other devices or centralized systems. Data processing and analytics play a crucial role in deriving insights from the collected data [9]. This involves real-time processing and analysis using cloud computing platforms or edge computing devices to extract meaningful information for decision-making. Applications and services form the next key component, utilizing the data and insights generated by IoT devices to develop a wide range of applications across industries [10]. These applications include smart home automation, remote healthcare monitoring, predictive maintenance in manufacturing, precision agriculture, and smart city initiatives

Paper type: Research paper
https:// 10.71822/mjtd.2024.1123260
Received: 20 June 2024; revised: 8 August 2024; accepted: 29 October 2024; published: 1 December 2024
How to cite this paper: Gh. R. Zargar, H. Barati, A. Barati, **"Authentication Methods in Internet-of-Things Platform: A Comprehensive Review"**, *Majlesi Journal of Telecommunication Devices*, Vol. 13, No. 4, pp. 239-258, 2024.

[11-13]. Finally, security and privacy are paramount considerations in the IoT ecosystem. Given the sensitive nature of the transmitted and stored data, robust security measures and privacy protection mechanisms are essential to prevent unauthorized access, data breaches, and misuse of personal information [14]. This ensures the integrity and confidentiality of the data exchanged within the IoT network. Overall, the IoT holds immense potential to revolutionize various aspects of our lives, offering unprecedented levels of connectivity, efficiency, and convenience [15]. However, it also presents challenges related to interoperability, security, privacy, and ethical considerations that need to be addressed as the IoT continues to evolve and expand [16].

Security in the IoT is critical due to the vast network of connected devices vulnerable to cyber threats [17]. Ensuring IoT security involves several key measures. First, device authentication and authorization protocols are essential to verify the identity and permissions of devices. Secondly, data encryption is crucial to protect the confidentiality and integrity of information transmitted between devices and servers [18].. Additionally, robust security updates and patch management are needed to address vulnerabilities promptly. IoT devices should also implement secure communication protocols like TLS/SSL to safeguard data in transit. Furthermore, network segmentation can limit the impact of breaches by isolating critical systems from potentially compromised devices. Finally, user awareness and privacy protection are vital considerations. Implementing these measures comprehensively is crucial for building trust in IoT systems and safeguarding against evolving cyber threats [19].

Authentication in IoT involves verifying the identity of devices, users, or applications before allowing access to IoT networks or services [20]. Cryptographic techniques such as digital certificates and secure tokens are commonly used for device authentication, ensuring only trusted devices can interact within IoT ecosystems. Biometric authentication, like fingerprint or facial recognition, adds another layer of security for user access to IoT devices [21]. Multi-factor authentication (MFA) is also vital, requiring multiple credentials for verification, enhancing security against unauthorized access. Secure communication protocols like TLS/SSL are integrated into IoT authentication processes to encrypt data during transmission, safeguarding against eavesdropping and tampering. Strong authentication mechanisms are crucial in IoT to mitigate cyber threats, protect privacy, and maintain the integrity of interconnected systems in increasingly complex and dynamic IoT environments [22].

This paper offers a comprehensive examination of security challenges and prerequisites within the IoT framework, employing a layer-oriented strategy. It subsequently conducts a current assessment of diverse authentication methods employed in IoT systems. Employing a multi-faceted classification approach, it evaluates and contrasts existing authentication protocols, elucidating their strengths and weaknesses.

The remainder of the paper is organized as follows: Section 2 describes IoT architecture. Section 3 describes security in IoT. Section 4 presents a taxonomy of IoT authentication schemes. Section 5 reviews previous works on authentication methods in IoT, describing the advantages and disadvantages of each. Section 6 presents the evaluation and comparison of methods. Finally, the conclusion is presented in Section 7.

2. IOT ARCHITECTURE

While traditional Internet connects people to a network, IoT has a different approach in which it provides Machine-to-Machine (M2M) and Human-to-Machine (H2M) connectivity, for heterogeneous types of machines in order to support variety of applications [23-24]. Connecting a huge number of heterogeneous machines leads to a massive traffic, hence the need to deal with the storage of big data [25]. Therefore, the TCP/IP architecture, does not suit the needs of IoT regarding various aspects including privacy and security, scalability, reliability, interoperability, and quality of service [26]. Although numerous architectures were proposed for IoT, there is still a need for a reference architecture. The basic architecture model proposed in the literature is a five-layer architecture, as shown in Figure 1. The IoT layerd architecture provides a structured framework for designing and implementing IoT systems. It consists of several layers, each serving specific functions to enable the seamless integration of devices, data, and applications in IoT environments [27].

- Perception Layer: This layer comprises sensors, actuators, and other devices that interact with the physical environment to collect data. Sensors gather information such as temperature, humidity, and motion, while actuators perform actions based on received instructions.
- Network Layer: The network layer facilitates communication between devices, allowing them to transmit data to each other or to centralized systems. It includes various communication technologies such as Wi-Fi, Bluetooth, Zigbee, and cellular networks.
- Middleware Layer: The middleware layer provides services for data processing, storage, and management. It includes components such as data brokers, message queues, and protocol converters, which ensure interoperability and scalability in IoT systems.
- Application Layer: The application layer hosts IoT applications and services that utilize the data collected from devices to deliver value-added functionalities. This includes applications for smart home automation, industrial

monitoring, healthcare management, and more.

- Business Layer: The business layer encompasses the business logic, rules, and processes that govern IoT operations. It includes components for data analytics, decision-making, and business intelligence, enabling organizations to derive insights and make informed decisions based on IoT data.

By following the IoT Generic Architecture, organizations can design and deploy scalable, interoperable, and secure IoT solutions that effectively harness the power of connected devices to drive innovation and improve efficiency across various industries. Figure 1 shows the 5-layer architecture of the Internet of Things.

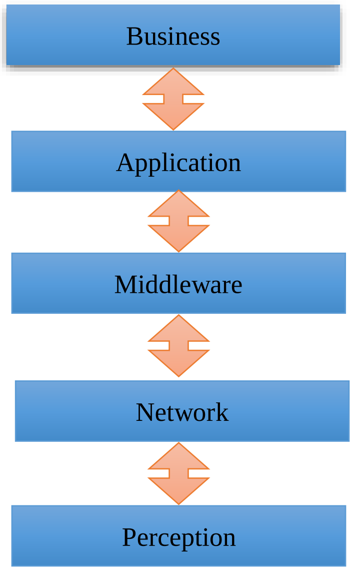

Fig. 1. Five-layer architecture.

3. SECURITY IN IOT

Security issues in the IoT pose significant challenges due to the extensive interconnectivity of devices and diverse deployment scenarios. Common concerns include weak authentication and authorization, leaving devices vulnerable to unauthorized access and control [28]. Inadequate encryption of data transmission exposes sensitive information to interception and compromise. Vulnerabilities in firmware and software, coupled with insecure communication protocols, create opportunities for exploitation by cyber attackers [29]. Physical security risks, such as tampering and theft of devices, further compound these challenges. The absence of standardized security protocols and privacy concerns regarding data collection exacerbate the situation. Addressing these issues requires a comprehensive approach involving robust authentication and encryption mechanisms, regular updates to firmware and software, secure communication protocols, enhanced physical security measures, industry-wide standardization efforts, and prioritization of user privacy and data protection. By adopting these measures, organizations can mitigate the risks associated with IoT deployments and build trust in IoT technologies [30].

3.1. Perception Layer Security Issues and Requirements

The Perception Layer in the IoT ecosystem comprises sensors, actuators, and other devices that interact with the physical environment to collect data. Security issues and requirements in the Perception Layer are critical due to the direct interaction of these devices with the physical world and the sensitive data they collect. Some common security issues and requirements in the Perception Layer include [31-32]:

- Unauthorized Access: Without proper authentication mechanisms, malicious actors may gain unauthorized access to sensors or actuators, leading to data manipulation, device tampering, or physical damage.
- Data Integrity: Ensuring the integrity of data collected by sensors is essential to prevent tampering or manipulation, which could result in inaccurate or misleading information being processed by IoT systems.
- Confidentiality: Protecting the confidentiality of sensor data is crucial, especially in applications where sensitive information such as personal health data or industrial secrets is being collected. Encryption and access control mechanisms can help safeguard sensitive data from unauthorized disclosure.

- Device Authentication: Authenticating devices within the Perception Layer is essential to ensure that data is collected from trusted sources. Strong authentication mechanisms, such as digital certificates or secure tokens, can prevent spoofing or impersonation attacks.
- Physical Security: Physical security measures are necessary to protect sensors and actuators from physical tampering, theft, or damage. Installing devices in secure locations, implementing tamper-proof enclosures, and monitoring for physical intrusions can help mitigate these risks.
- Resilience to Environmental Factors: Sensors deployed in harsh or unpredictable environments may be vulnerable to damage from environmental factors such as extreme temperatures, moisture, or electromagnetic interference. Designing sensors with robust enclosures and protective coatings can enhance their resilience to environmental hazards.

Addressing these security issues requires a multi-faceted approach, including the implementation of strong authentication mechanisms, encryption techniques, physical security measures, and resilience to environmental factors. By addressing these requirements, organizations can ensure the security and reliability of the Perception Layer in IoT deployments.

3.2. Network Layer Security Issues and Requirements

The network layer of IoT systems faces several security issues due to the distributed nature of devices and the diverse communication protocols used. Here are some common security issues and requirements for the network layer of IoT [33-34]:

- Data Confidentiality: Ensuring that data transmitted over the network is encrypted and only accessible to authorized parties. This prevents eavesdropping and data interception by malicious actors.
- Data Integrity: Guaranteeing that data remains unchanged during transmission and reception. This prevents tampering with data in transit, which could lead to unauthorized modifications or disruptions to IoT operations.
- Authentication and Access Control: Implementing mechanisms to authenticate devices and users before granting access to IoT networks and resources. This prevents unauthorized devices from joining the network and unauthorized users from accessing sensitive data or controlling devices.
- Device Identity Management: Managing and securely storing unique identities for IoT devices to prevent spoofing and impersonation attacks. This ensures that only legitimate devices can communicate with each other and with backend systems.
- Network Segmentation: Partitioning IoT networks into separate segments or VLANs to isolate traffic and limit the potential impact of security breaches. This prevents lateral movement by attackers and contains security incidents to specific parts of the network.
- Firewalls and Intrusion Detection/Prevention Systems (IDS/IPS): Deploying firewalls and IDS/IPS solutions to monitor and filter network traffic for signs of malicious activity. This helps detect and block unauthorized access attempts, malware, and other network-based threats.
- Secure Communication Protocols: Using secure communication protocols such as Transport Layer Security (TLS), Datagram Transport Layer Security (DTLS), and Message Queuing Telemetry Transport (MQTT) with appropriate encryption and authentication mechanisms.
- Network Traffic Encryption: Encrypting all network traffic, including data exchanged between IoT devices, gateways, and backend servers. This prevents unauthorized interception and ensures the confidentiality of sensitive information.
- Secure Remote Management: Implementing secure methods for remotely managing and updating IoT devices, such as over-the-air (OTA) firmware updates and secure device management protocols. This reduces the risk of vulnerabilities being exploited due to outdated software or misconfigurations.
- Resilience and Redundancy: Building resilience into IoT networks through redundancy, failover mechanisms, and disaster recovery plans. This helps mitigate the impact of network outages, DDoS attacks, and other disruptions to IoT operations.

3.3. Middleware Layer Security Issues and Requirements

The middleware layer in IoT systems plays a crucial role in processing, aggregating, and managing data collected from the perception layer before it's sent to the application layer. Ensuring security at this layer is essential for protecting sensitive data, maintaining system integrity, and preventing unauthorized access. Here are some common security issues and requirements for the middleware layer in IoT [35-36]:

- Data Encryption and Secure Data Handling: Data processed and stored within the middleware layer should be encrypted to protect against unauthorized access and interception. Encryption mechanisms such as Advanced Encryption Standard (AES) should be employed to ensure data confidentiality.
- Access Control and Authentication: Implementing robust access control mechanisms to regulate access to middleware components and data. User authentication and authorization mechanisms should be in place to ensure that only authorized individuals or systems can interact with the middleware layer.
- Secure APIs and Communication Protocols: Ensuring that APIs and communication protocols used within the middleware layer are secure and resistant to attacks such as injection, tampering, and eavesdropping. Secure protocols like HTTPS and Message Queuing Telemetry Transport (MQTT) with TLS encryption should be used for communication between middleware components.
- Integrity Checking and Validation: Implementing mechanisms to verify the integrity of data processed within the middleware layer. Data integrity checks, digital signatures, and message authentication codes (MACs) can be used to ensure that data has not been altered or tampered with during processing.
- Secure Configuration and Management: Ensuring that middleware components are configured securely and kept up-to-date with security patches and updates. Secure configuration management practices should be followed to minimize the risk of misconfiguration-related security incidents.
- Auditing and Logging: Implementing logging and auditing mechanisms to track and monitor activities within the middleware layer. This helps detect and investigate security incidents, unauthorized access attempts, and other suspicious activities.
- Secure Integration with External Systems: When integrating with external systems or third-party services, ensuring that secure integration practices are followed. Secure authentication, data encryption, and secure API endpoints should be used to protect data exchanged between middleware components and external systems.
- Secure Data Storage: If the middleware layer stores data temporarily or persistently, ensuring that data is stored securely with appropriate access controls, encryption, and data retention policies. Secure storage mechanisms should be used to protect sensitive data from unauthorized access or disclosure.
- Resilience and Fault Tolerance: Building resilience and fault tolerance into the middleware layer to ensure continued operation in the event of system failures, disruptions, or cyberattacks. Redundancy, failover mechanisms, and disaster recovery plans should be in place to minimize downtime and data loss.
- Security Monitoring and Incident Response: Implementing security monitoring tools and incident response procedures to detect and respond to security threats and breaches in real-time. Security events should be logged, analyzed, and acted upon promptly to mitigate risks and minimize the impact of security incidents.

3.4. Application Layer Security Issues and Requirements

The Application Layer in the IoT ecosystem is responsible for processing and analyzing data collected from sensors and actuators to derive meaningful insights and enable various applications and services. Security issues and requirements at the Application Layer are crucial to safeguard sensitive data and ensure the integrity and availability of IoT systems. Some common security issues and requirements in the Application Layer include [37-38]:

- Secure Data Storage and Processing: Ensuring the secure storage and processing of data within IoT applications is essential to prevent unauthorized access, data breaches, and tampering. Encryption techniques and access control mechanisms should be employed to protect sensitive data stored in databases or processed by applications.
- Authentication and Authorization: Implementing robust authentication and authorization mechanisms within IoT applications is vital to verify the identity of users and devices and control their access to sensitive resources. Strong authentication methods, such as multi-factor authentication or biometric authentication, can help prevent unauthorized access to IoT applications.
- Secure Communication Protocols: Utilizing secure communication protocols, such as HTTPS or MQTT with TLS/SSL, is essential to encrypt data transmission between IoT devices and backend systems. Secure protocols help protect data from interception and eavesdropping by malicious actors and ensure its confidentiality and integrity during transmission.
- Vulnerability Management: Regularly updating and patching IoT applications to address known security vulnerabilities is crucial for maintaining their security posture. Vulnerability management processes should be implemented to identify, prioritize, and remediate security flaws in IoT applications in a timely manner.
- Secure APIs and Interfaces: Securing APIs and interfaces used by IoT applications to interact with external systems or services is essential to prevent unauthorized access or manipulation of data. Implementing authentication, access control, and encryption mechanisms for APIs and interfaces helps protect sensitive data and prevent security breaches.

- Data Privacy and Compliance: Ensuring compliance with data privacy regulations and standards, such as GDPR or HIPAA, is essential for protecting the privacy of user data collected and processed by IoT applications. Implementing privacy-by-design principles, data anonymization techniques, and data access controls can help ensure compliance with regulatory requirements and protect user privacy.

Addressing these security issues requires a comprehensive approach, including the implementation of secure data storage and processing practices, robust authentication and authorization mechanisms, secure communication protocols, vulnerability management processes, secure APIs and interfaces, and adherence to data privacy and compliance requirements. By addressing these requirements, organizations can enhance the security and trustworthiness of IoT applications and protect sensitive data from unauthorized access or manipulation.

3.5. Business Layer Security Issues and Requirements

The Business Layer in the IoT ecosystem is responsible for managing business logic, workflows, and interactions between different components of the IoT system. Security issues and requirements at the Business Layer are crucial to safeguard sensitive business data, ensure the integrity of business processes, and protect against various cyber threats. Some common security issues and requirements in the Business Layer include [39]:

- Access Control and Authentication: Implementing robust access control mechanisms and authentication protocols helps control access to business-critical resources and ensures that only authorized users or devices can interact with the business layer. Role-based access control (RBAC), multi-factor authentication, and strong authentication mechanisms help enforce access policies and prevent unauthorized access to sensitive business data and functionalities.
- Secure Business Logic: Ensuring the security of business logic and workflows is essential to prevent exploitation by malicious actors seeking to compromise the IoT system. Implementing secure coding practices, input validation, and output encoding techniques helps mitigate the risk of injection attacks, such as SQL injection or code injection, which can lead to unauthorized access or manipulation of business data and processes.
- Data Privacy and Compliance: Ensuring compliance with data privacy regulations and standards, such as GDPR or HIPAA, is essential for protecting the privacy of user data collected and processed by IoT applications. Implementing privacy-by-design principles, data anonymization techniques, and data access controls helps ensure compliance with regulatory requirements and protect user privacy.
- Secure Integration with External Systems: Integrating IoT systems with external business applications, cloud services, or third-party platforms introduces security risks, such as data breaches or unauthorized access. Implementing secure communication protocols, encryption techniques, and access controls for data exchanged between IoT systems and external systems helps mitigate these risks and ensure the confidentiality and integrity of data transmissions.
- Business Continuity and Disaster Recovery: Planning for business continuity and disaster recovery helps mitigate the impact of security incidents or system failures on business operations. Implementing backup and recovery procedures, redundant systems, and failover mechanisms ensures the availability and resilience of critical business functions in the event of disruptions or security breaches.
- Risk Management and Governance: Implementing risk management processes and governance frameworks helps identify, assess, and mitigate security risks in the IoT ecosystem. Conducting regular security assessments, vulnerability scans, and compliance audits helps proactively identify and address security vulnerabilities and ensure ongoing compliance with security policies and regulations.

Addressing these security issues requires a comprehensive approach, including the implementation of access control mechanisms, secure business logic, data privacy measures, secure integration practices, business continuity planning, risk management processes, and governance frameworks. By addressing these requirements, organizations can enhance the security and resilience of the Business Layer in IoT deployments, safeguarding sensitive business data and ensuring the integrity of business processes and operations. Table 1 shows the security requirements at each layer of the IoT.

Table 1. Security requirements in each layer

Layer	Security Requirements
Perception	Device authentication
	Data integrity
	Privacy protection
	Firmware/software security
	Physical security
Network	Secure communication protocols
	Access control
	Encryption
	Intrusion detection and prevention
	Traffic monitoring and analysis
Middleware	Data confidentiality
	Data integrity
	Authentication and authorization mechanisms
	Protection against middleware vulnerabilities
	Secure data transmission and storage
Application	User data protection
	Secure authentication and authorization
	Encrypted communication channels
	Protection against application-level vulnerabilities
	Secure application programming interfaces (APIs)
Business	Protection of sensitive business data
	Compliance with regulations (e.g., GDPR, HIPAA)
	Access controls and role-based permissions
	Secure financial transactions
	Business continuity planning and risk management

4. A TAXONOMY OF IOT AUTHENTICATION SCHEMES

Authentication is the process of verifying the identity of an individual or entity attempting to access a system, network, application, or resource [40]. In other words, it confirms that the person or entity is who they claim to be. Authentication mechanisms typically involve presenting credentials, such as usernames, passwords, biometric data (like fingerprints or facial recognition), security tokens, or cryptographic keys [41]. Authentication is the process of verifying the identity of an individual or entity attempting to access a system, network, application, or resource. Authentication helps ensure that only authorized users gain access to sensitive information or resources, thereby protecting against unauthorized access, data breaches, and security threats [42]. It is a fundamental aspect of cyber security that helps ensure that only authorized users gain access to sensitive information or resources, thereby protecting against unauthorized access, data breaches, and security threats. Authentication is crucial for maintaining the integrity, confidentiality, and availability of information systems and resources. It is used extensively in various domains, including computer systems, networks, websites, mobile devices, and cloud services, to protect against unauthorized access and safeguard sensitive data.

IoT authentication refers to the process of verifying the identity of IoT devices or users interacting with IoT systems, networks, or applications. Given the distributed and heterogeneous nature of IoT environments, authentication becomes crucial for ensuring the security and integrity of IoT deployments. Here are some key aspects of IoT authentication [43]:

- Device Authentication: IoT devices need to authenticate themselves to the network or cloud services they interact with. This can involve the use of unique identifiers, such as MAC addresses or cryptographic keys, to establish trust and ensure that only authorized devices can access IoT resources.
- User Authentication: In scenarios where users interact with IoT systems through applications or interfaces, user authentication is necessary to verify the identity of individuals accessing the system. This may involve traditional methods like usernames and passwords or more advanced techniques such as biometric authentication.
- Mutual Authentication: In some cases, both the IoT device and the server or gateway it communicates with need to authenticate each other to establish a secure connection. This ensures that both parties are legitimate and prevents unauthorized devices or malicious actors from gaining access to sensitive data or control over IoT devices.

- Secure Communication Protocols: IoT authentication often relies on secure communication protocols such as Transport Layer Security (TLS) or DTLS to encrypt data exchanged between devices and servers, protecting against eavesdropping and tampering.
- Role-based Access Control: Access to IoT resources may be restricted based on the roles or permissions assigned to users or devices. Role-based access control (RBAC) mechanisms can enforce authorization policies and ensure that only authorized entities can perform specific actions within the IoT ecosystem.
- Lifecycle Management: Proper authentication in IoT requires managing the lifecycle of devices, including provisioning, registration, deprovisioning, and revocation of credentials. This ensures that only valid and up-to-date devices are allowed to participate in IoT networks.
- Integration with Identity and Access Management (IAM) Systems: IoT authentication mechanisms often need to integrate with existing identity and access management systems to centralize user authentication, enforce security policies, and streamline access control across the entire IoT infrastructure.

The key aspects of IoT authentication are shown in Figure 2.

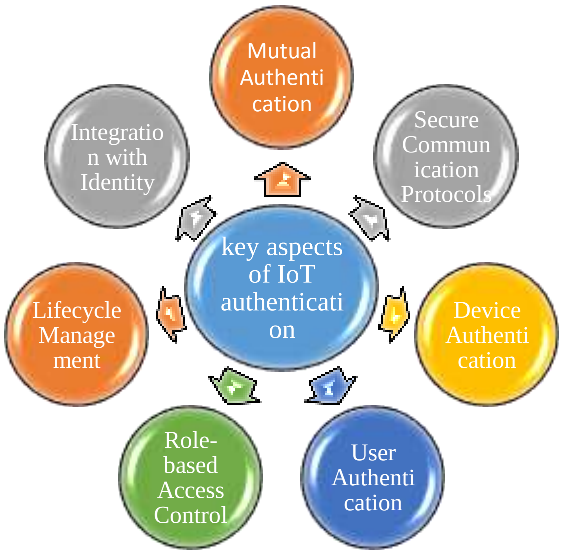
Mutual Authenti cation
Secure Commun ication Protocols
Device Authenti cation
User Authenti cation
Role-based Access Control
Lifecycle Manage ment
Integratio n with Identity
key aspects of IoT authenticati on

Fig. 2. Key aspects of IoT authentication.

Overall, IoT authentication is essential for establishing trust, preventing unauthorized access, and safeguarding sensitive data in IoT ecosystems. By implementing robust authentication mechanisms, organizations can mitigate security risks and ensure the integrity and reliability of their IoT deployments.

A taxonomy of IoT authentication schemes is a systematic classification framework that categorizes different methods and approaches used for authenticating devices and users within Internet of Things environments. This taxonomy aims to organize the various authentication mechanisms based on their characteristics, functionalities, and deployment models. A taxonomy of IoT authentication schemes categorizes these schemes based on various criteria such as authentication mechanisms, deployment models, security features, and communication protocols. Typically, a taxonomy of IoT authentication schemes includes several categories or dimensions, such as [44]:

- Authentication Mechanisms: Authentication mechanisms in information technology encompass a range of methods to verify the identity of users, devices, or applications. One common approach is password-based authentication, where users provide a secret password to access a system. Biometric authentication uses unique physical characteristics like fingerprints or facial recognition for identity verification, offering a more secure and user-friendly method. Token-based authentication involves the use of physical or virtual tokens, like security keys or one-time password (OTP) tokens, to grant access. Multi-factor authentication combines two or more authentication factors, such as passwords, biometrics, or tokens, to enhance security. Device-based authentication verifies the identity of IoT devices using digital certificates or secure tokens.
- Deployment Models: Authentication deployment models in IT encompass various approaches to how authentication is managed and implemented within systems. Centralized authentication involves a single, central server responsible for verifying user credentials and granting access to resources. This model streamlines management but can be a single point of failure if not properly secured. Distributed authentication spreads the authentication process across

multiple entities or servers, enhancing scalability and resilience. Federated authentication extends authentication across multiple domains or services, allowing users to access resources across different organizations using a single set of credentials. Each deployment model has its advantages and challenges, balancing factors like security, scalability, and ease of use.

- Security Features: Security features play a crucial role in ensuring the effectiveness and integrity of authentication schemes in IT environments. Data encryption is fundamental for securely transmitting authentication data over networks, preventing unauthorized access to sensitive information. Mutual authentication enhances security by requiring both parties (user and system) to verify each other's identities before granting access. Key management involves secure storage and distribution of cryptographic keys used for encryption, decryption, and authentication processes, safeguarding against key compromise. Secure communication protocols such as TLS/SSL establish encrypted and authenticated connections between entities, protecting data from interception and manipulation during transmission. Implementing these security features strengthens authentication mechanisms, mitigates risks associated with unauthorized access or data breaches, and fosters trust in the overall security posture of IT systems and services.
- Communication Protocols: In the realm of IoT, communication protocols are fundamental for facilitating secure and efficient interactions between IoT devices and authentication servers. Commonly employed protocols include HTTP/HTTPS, which are well-suited for web-based communications with the added security of HTTPS encryption. MQTT is lightweight and efficient, enabling publish-subscribe messaging and supporting secure communication via MQTT over TLS (MQTT-Secure). Constrained Application Protocol (CoAP) is designed specifically for resource-constrained IoT devices, offering low overhead and built-in security features like DTLS for secure data exchange. Advanced Message Queuing Protocol (AMQP) ensures reliable and secure message delivery, making it suitable for industrial IoT applications. Extensible Messaging and Presence Protocol (XMPP) facilitates real-time communication and is ideal for human-to-device interactions in IoT scenarios. DTLS provides security enhancements for UDP-based communication, ensuring confidentiality, integrity, and authentication of data exchanged between IoT devices and authentication servers.

As shown in Figure 3, this taxonomy helps in organizing and understanding the various authentication schemes used in IoT systems, facilitating comparison, selection, and implementation based on specific requirements and constraints. By considering these criteria, a taxonomy of IoT authentication schemes can provide a structured framework for understanding and evaluating the diverse range of authentication methods used in IoT systems.

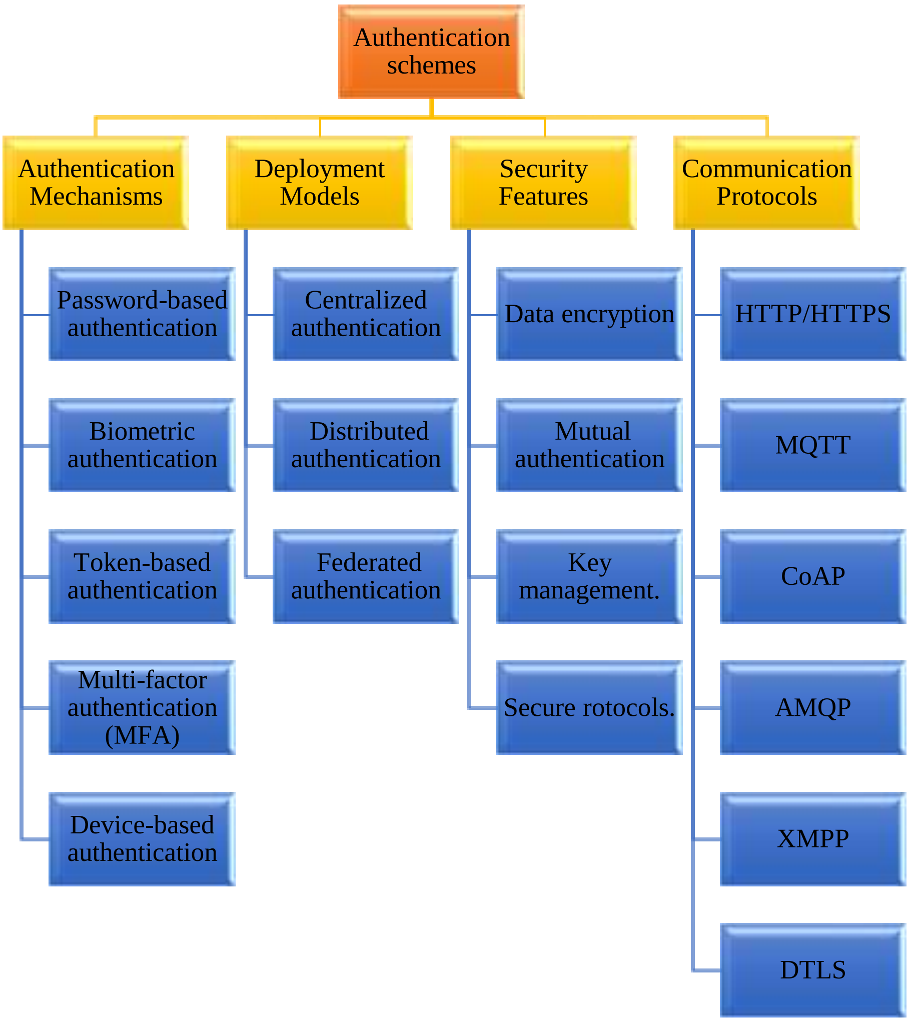

Fig.3. Taxonomy of IoT authentication schemes.

5. AUTHENTICATION METHODS

In [45], a lightweight anonymous mutual authentication and key agreement scheme is proposed for two-hop blockchain-based Wireless Body Area Networks (WBANs) to ensure secure message transmission. The scheme enables mutual authentication and key agreement between sensor nodes on patients and various hub nodes across regions, addressing security and lightweight requirements. The protocol is evaluated using the AVISPA tool for security. It consists of Initialization, Registration, and Authentication phases, conducted over secure and public channels. The approach uses XOR operations and a cryptographic hash function for mutual authentication and key agreement. Security analysis confirms robustness. Comparative analysis with related schemes shows improved energy efficiency and security, making it suitable for WBAN implementation.

In [46], two lightweight authentication and key agreement schemes are proposed for IoT device authentication. The first scheme uses ECQV implicit certificates for efficient authentication but lacks public key signature protection. The second scheme enhances security by incorporating Schnorr signatures within CL-PKC, ensuring public key verification. Both schemes leverage identity-based PKC, with the first focusing on implicit authentication and the second integrating signature information into the public user key. These schemes address security concerns like replay attacks and key leakage by minimizing transmitted data and improving communication speed, although the second scheme sacrifices speed for enhanced security.

In [47], a privacy-aware authentication protocol for multi-server CE-IoT systems is proposed, integrating Physical Unclonable Functions (PUFs) and blockchain technology. The protocol encodes real correlations of Challenge-Response Pairs (CRPs) into Mapping Correlations (MCs) using a one-time physical identity and keyed-hash function. Blockchain is employed to store and efficiently synchronize MCs, ensuring secure sharing of physical identities through multi-receiver encryption. The protocol's security is formally proven using a random oracle model, and its resilience against various attacks is discussed. In the system setup, the Responsible Center (RC) generates public parameters, initializes the Multi-Receiver Encryption (MRE) algorithm, and launches the blockchain system. Authorized verifiers join the blockchain network, and a smart contract is deployed in both the RC and verifiers to manage MCs and CRPs during the registration and authentication phases.

In [48], a secure authentication protocol is presented for a cloud-assisted Telemedicine Information System (TMIS) with access control, integrating blockchain for data integrity. It employs ciphertext-policy attribute-based encryption (CP-ABE) for access control and blockchain to ensure data integrity. The protocol's robustness is demonstrated through informal and Burrows-Adabi-Needham (BAN) logic analyses, along with formal validation using AVISPA, highlighting its security and efficiency advantages over existing methods. Key protocol stages include initialization, registration, key generation, authentication, data upload, treatment, and checkup, defined with corresponding notations in Table 1. To prevent replay attacks, random numbers (secrets) and synchronized timestamps from TMIS entities are used. This comprehensive approach addresses security concerns, affirming the protocol's readiness for practical deployment in cloud-assisted TMIS environments.

In [49], a lightweight mutual two-factor authentication mechanism is proposed for IoT devices and servers, leveraging PUFs and a hashing algorithm. The mechanism ensures secure authentication and session key agreement without storing cryptographic keys in non-volatile memory, thus addressing vulnerability concerns. The protocol is validated through formal analysis, demonstrating resilience against various attack scenarios while maintaining efficiency in terms of memory, server capacity, and energy consumption. By utilizing SRAM PUFs and an Arbiter PUF, the proposed mechanism achieves reliable two-factor mutual authentication without encryption, which can drain IoT device batteries quickly. Unlike existing methods requiring encryption, this approach relies solely on a hashing algorithm for mutual authentication, making it lightweight and suitable for power-constrained IoT networks.

In [50], a blockchain-assisted highly secure system for medical IoT devices is proposed using Lamport Merkle Digital Signature (LMDS). The Lamport Merkle Digital Signature Generation (LMDSG) model initially authenticates IoT devices by constructing a tree where leaves represent the hash function of sensitive patient medical data. A Centralized Healthcare Controller (CHC) determines the root of the LMDSG using Lamport Merkle Digital Signature Verification (LMDSV). In this verification, if the hash of the public key '$pb'key$' matches the leaf '$P\ gn$', the signature is valid. This LMDS technique efficiently detects malicious user behavior with minimal Computational Overhead (CO) and Computational Time (CT). Performance analysis considers CO, CT, and authentication accuracy, demonstrating higher security and lower CT and CO compared to existing methods in medical IoT systems.

In [51], a novel blockchain-based authentication scheme is designed to address IoT challenges. This framework leverages the modular square root algorithm integrated with blockchain technology to ensure an efficient authentication process. The security and effectiveness of the proposed scheme are demonstrated through comprehensive security analysis and detailed experiments. The proposed authentication scheme for IoT consists of four phases: system initialization, registration, authentication, and update/revocation. This scheme offers secure and lightweight authentication by combining blockchain with the MSR cryptographic algorithm, emphasizing decentralization, privacy preservation, and efficiency. A thorough security analysis evaluates the performance of the proposed scheme using Remix, comparing computation and communication costs with alternative methods to validate its effectiveness.

In [52], a blockchain-based decentralized authentication structure is proposed for IoT devices, organizing them into clusters based on computational capability, energy reserve, and location. Each cluster implements authentication through interconnected blockchains in a hierarchical manner. To reduce processing load, a consensus protocol verifies identity-based encryption key signatures of devices and their associated clusters. The proposed framework introduces a novel approach to authenticate IoT devices by grouping them into hierarchical clusters, each with its own blockchain for authentication. Clusters connect to a larger blockchain via a hash from the upper-level blockchain. A lightweight consensus algorithm validates nodes based on their public and cluster head key values, ensuring fast and efficient block validation within each cluster. This method maintains blockchain immutability while achieving speed and efficiency.

In [53], a lightweight authentication scheme using a consortium blockchain and a cryptocurrency-like digital token (LiIDCoin) is proposed to establish and manage trust among entities. LiIDCoin amounts manipulate the trust lifecycle. The scheme proves resilient against common attacks and is more efficient than competitors in terms of storage, communication, and authentication costs. It introduces cross-domain IoT authentication using a consortium blockchain and a novel data structure based on unspent transaction outputs (UTXO) with coin operations (issuance, transfer, query, revocation) for authentication and lifecycle management. LiIDCoin represents entity trust, demonstrated by transaction evidence on the blockchain, with the lifecycle managed by adjusting LiIDCoin amounts. Comprehensive security requirements are analyzed, and the scheme is implemented on the HLF platform, demonstrating superiority over competitors.

In [54], a three-factor authentication and key agreement protocol is introduced for Industrial Internet of Things (IIoT) systems, leveraging Elliptic-Curve Cryptography (ECC). The protocol is designed to ensure both forward and backward secrecy by addressing the elliptic curve Diffie-Hellman problem. It can be applied to single-gateway scenarios and has also been extended to support multigateway environments. The proposed scheme incorporates three factors for authentication and utilizes ECC. It is specifically tailored for IIoT settings. The protocol's security is formally analyzed and proven to meet the required standards. By employing the computationally infeasible elliptic curve discrete logarithm problem, the proposed scheme achieves both forward and backward secrecy.

In [55], a three-factor authentication scheme called defense-in-depth is proposed for IoT environments on the blockchain. It employs mutual authentication and user authorization through smart card registration on a private blockchain, eliminating the need for a trusted server. The scheme integrates ECC for enhanced security. Security analysis, including assessments using the AVISPA tool, demonstrates the protocol's efficiency in terms of computational and communication costs. The protocol addresses vulnerabilities in IoT network authentication by implementing three-factor and mutual authentication, utilizing lightweight ECC cryptography to safeguard user privacy and enhance network resilience against security threats. Built on the blockchain platform, the protocol ensures data protection, decentralized management, transparency, and tamper-proof smart card creation for each user.

In [56], a three-factor authentication framework suitable for critical IoT applications is proposed. The framework incorporates identity, password, and a digital signature scheme. It utilizes a publish-subscribe pattern and leverages ECC and computationally low hash chains. The key features of the framework include mutual authentication of the Gateway node with both the remote user and sensor node, as well as the generation of dynamic session keys. Upon reviewing and analyzing relevant papers, it was found that none of the proposed protocols supported the user access level determination feature, which is a crucial security requirement in authentication protocols.

In [57], a method called PUFTAP-IoT proposed, which combines physical unclonable functions (PUF) and honey list techniques with three-factor authentication to design secure protocols for IoT environments. The aim is to resist attacks such as ID/password guessing, brute-force, and capture attacks. PUFTAP-IoT is analyzed for security using formal methods like BAN logic, Real-Or-Random (ROR) model, and scyther simulation tools. PUFTAP-IoT demonstrates its ability to provide secure services in IoT environments. The method incorporates PUF and honey list technologies to enhance security for sensing devices in the IoT environment, protecting against online guessing, brute-force attacks, and sensor takeover attacks.

In [58], a lightweight authenticated key agreement and access control protocol proposed for group communication in the blockchain using elliptic curve and bi-linear pairing. The protocol's secrecy is proven in the random-oracle paradigm, and a comprehensive heuristic security assessment is conducted to ensure its protection against potential threats and adherence to required security features. The protocol is utilized to implement the linear secret sharing (LSS) method. Non-transferable, unique assets such as user biometrics are employed for effective access control. The approach incorporates a robust login and authentication step, enabling quick identification of rogue users through appropriate threshold settings. The technique supports session key creation and authentication and combines access control and authentication into a single step.

In [59], the paper focuses on designing a secure user authentication scheme for cloud-assisted IoT systems. The proposed scheme is specifically designed for cloud-assisted IoT environments, with an emphasis on lightweight computation on gateways. It ensures secure access between remote users and IoT devices, incorporating desirable features such as forward secrecy and multi-factor security. The security of the scheme is rigorously proven using methods such as the random-oracle model, heuristic analysis, the ProVerif tool, and BAN logic. Additionally, the proposed scheme improves efficiency by offloading heavy computation and storage tasks to the cloud center. Overall, this paper presents a comprehensive and secure user authentication solution tailored for cloud-assisted IoT systems.

In [60], the Authenticated Devices Configuration Protocol (ADCP) is proposed to manage authentication and establish a secure overlay network within existing IoT networks. The Authenticated Device Transmission Protocol (ADTP) ensures secure communication within the overlay network. ADCP mitigates zero-day attacks and achieves zero round-trip-time key exchange. Both protocols use a distributed blockchain database optimized for data integrity to store authentication records, ensuring integrity. They are compatible with existing communication protocols and require no software reprogramming. Formal analysis confirms resilience against various attacks. This method addresses authentication-related security issues in IoT networks using blockchain, easily integrating into current networks. Experimental results show feasibility, and formal analysis confirms resilience against attacks, supported by a stochastic model showing security enhancement.

In [61], a hybrid blockchain-based many-to-many cross-domain authentication scheme is proposed for smart agriculture IoT networks. This scheme facilitates simultaneous mutual authentication between multiple devices and data service providers from various agricultural systems. It introduces a Groupable Batch Verification (GBV) algorithm that dynamically adjusts batch sizes to enhance cross-domain batch authentication flexibility. Additionally, the scheme includes a pseudonym update mechanism to safeguard device privacy and prevent illegal access by tracking malicious devices. The proposed approach addresses certificate management and key escrow issues, offering cryptographic configuration adaptability. Security analysis and performance evaluation demonstrate practical security, efficiency, and affordability. The hybrid blockchain model reduces computational overhead and communication costs in many-to-many authentication scenarios, ensuring scalability and safety in cross-domain agricultural collaboration, unlike single-chain structures.

In [62], a novel lightweight authentication and key management scheme is proposed for IoT networks, integrating blockchain with Chebyshev chaotic maps. IoT devices undergo a registration process to obtain a temporary identity used for authentication and group key generation. During authentication, the device's temporary identity is updated and securely recorded on the blockchain, preventing exploitation by attackers. The Key Generation Center (KGC) uses Chebyshev polynomials to establish group keys without involving third parties, ensuring secure communication among group members. This approach guarantees efficient and secure group key generation and management, enhancing communication privacy within IoT networks. Formal and informal security analyses confirm the scheme's ability to meet rigorous security requirements while providing flexible key management. By integrating blockchain and Chebyshev chaotic maps, the proposed method delivers reliable and anonymous authentication alongside robust group key management for IoT devices.

In [63], an enhanced mutual authentication protocol is proposed for IoT-based Energy Internet (EI) using blockchain technology. The proposed protocol extends an existing smart grid authentication method by integrating blockchain-based security mechanisms to facilitate secure communication among IoT devices. To evaluate the protocol's performance, we conducted Caliper benchmarking and security testing using BAN logic and ProVerif. Experimental results demonstrate the protocol's achievement of both security and efficiency. Our blockchain-based solution enhances device authentication in IoT-based EI networks by utilizing a smart contract for user registration and verification. Multiple distributed registration authorities in the network improve resilience against attacks. This solution provides secure and efficient authentication for IoT devices in EI networks, validated through security analysis and performance evaluations with ProVerif, BAN logic, and the Caliper benchmark.

In [64], an authentication framework is proposed for an edge computing-enabled Internet of Things environment to establish secure communication between devices and edge servers, as well as among devices themselves. The protocol, named Device-Edge Authentication and Key Agreement (DEAKA), comprehensively addresses communication security. Additionally, a protocol called Device-Device Authentication and Key Agreement (DDAKA) is proposed for mutual authentication and key agreement among devices. The framework involves three entities: IoT devices, edge servers (ESs), and a trusted registration center (RC). Formal and informal security analyses demonstrate that the protocols meet a wide range of security requirements and can resist various security threats. Computational and transmission costs of the protocols are analyzed and compared, ensuring efficiency in resource utilization. This work extends existing authentication methods to cover inter-device communication in edge computing IoT environments, enhancing overall network security and reliability.

In [65], a blockchain-based secure remote authentication protocol (BSRA) proposed for fog-enabled Internet of Things systems. The protocol utilizes lightweight cryptographic primitives, including PUFs and cryptographic hash functions, to design an efficient authentication scheme. It incorporates temporary identities and authentication-piggybacking-synchronization techniques to ensure anonymity and effectiveness. The proposed protocol enables mutual authentication between users and IoT devices with the assistance of fog nodes, establishing distributed trust through blockchain technology. The scheme focuses on the use of computationally inexpensive cryptographic primitives for improved efficiency. Additionally, message synchronization is verified during the authentication process. Overall, the BSRA protocol offers a secure and efficient solution for remote authentication in fog-enabled IoT systems.

In Table 2, a summary of the advantages and disadvantages of the surveyed schemes is provided.

Table 2. Summary of surveyed schemes.

Ref	Advantage	Disadvantage
[45]	Lightweight scheme ensures secure message transmission, mutual authentication, and key agreement in blockchain-based WBANs.	Lack of formal security analysis, and potential scalability issues in large-scale WBAN deployments.
[46]	The proposed AKA protocols provide end-to-end security in IoT environments, addressing current security problems and meeting requirements.	The schemes have trade-offs, with Scheme 1 offering fast authentication but vulnerability to public key attacks, and Scheme 2 providing secure public key verification but slower performance.
[47]	Privacy-aware authentication protocol integrates PUFs and blockchain, providing security, resistance to attacks, and scalability for multi-server CE-IoT systems.	Protocol efficiency is moderate, with relatively long session key establishment and MC synchronization times for single requests.
[48]	The proposed protocol ensures data integrity, fine-grained access control, and security against various attacks in a cloud-assisted TMIS environment.	The specific efficiency of the protocol is not provided, and the comparison with related protocols lacks detailed information.
[49]	Two-factor authentication protocol using hash functions, secure session key establishment, and robust defense against invasive attacks on IoT devices.	The specific efficiency and practical performance of the protocol are not provided, and further analysis is needed for different attack scenarios.
[50]	The proposed LMDS authentication technique for medical IoT systems reduces computational time, enhances security, and supports scalability.	The specific details of the security mechanisms and the potential limitations of the LMDS technique are not provided.
[51]	High security, Lightweight authentication system, Privacy preservation, Reduced computation costs, Decentralized system.	Complexity in implementation, Dependency on blockchain infrastructure, May require additional hardware resources, Reliance on MSR cryptographic algorithm.
[52]	Blockchain-based authentication framework reduces computational load, offers lightweight consensus, and enhances decentralization and efficiency for IoT devices.	The limitations of integrating the authentication values into smart contracts and the scalability of the proposed framework for a larger number of devices
[53]	Lightweight authentication scheme, Use of consortium blockchain for entity trust, LiIDCoin digital token for proving entity authenticity, Lifecycle management through manipulation of LiIDCoins, Satisfies security requirements	Limited to consortium blockchain, Dependency on the HLF platform, Limited analysis on real-world IoT applications, Limited application to cross-domain authentication scenarios, Privacy enhancement and fine-grained trust management not fully addressed
[54]	ECC-based authentication protocol, Suitable for single/multigateway scenarios, Achieves forward and backward secrecy, Efficient security attributes at reasonable computation cost	Limited to IIoT environment, ECC dependency for authentication, Limited real-world implementation analysis, Informal security analysis limitations
[55]	Efficient three-factor authentication protocol using a fuzzy extractor on the blockchain platform, providing security and privacy protection in heterogeneous IoT environments.	Additional complexity and overhead in terms of communication, computation, and storage requirements.
[56]	Signature-based 3-factor authentication using ECC and hash chains, Resistance to cryptographic attacks and formal security verification, Bandwidth and energy savings, reduced computing and communication costs	Dependency on publish-subscribe pattern and message queue telemetry transport, Potential limitations in scalability and adaptability to evolving IoT environments.
[57]	PUFTAP-IoT protocol addresses security vulnerabilities in IoT environments, provides secure mutual authentication.	High communication and storage overheads of PUFTAP-IoT in large-scale IoT deployments and different environments
[58]	Anonymous authenticated access control system for IoT group communication, Effective handling of access control with non-transferable, one-of-a-kind assets like user biometrics, Strong login and authentication step to quickly identify rogue users.	Limited discussion on scalability and adaptability to different IoT environments, Performance analysis and comparison research may not cover all aspects of system overhead improvement.
[59]	The proposed secure user authentication scheme for cloud-assisted IoT systems offers improved security, efficiency, and resource utilization.	The lack of scalability and resilience of the scheme to advanced attacks in diverse IoT environments
[60]	Authentication, security, data integrity, compatibility, zero-day attack mitigation, resilience.	Implementation complexity, potential resource overhead.
[61]	Addresses certificate management, key escrow, batch verification, pseudonym update, and device revocation, Practical security, efficiency, and affordability with low computational and communication costs.	Need to focused on the PBFT consensus algorithm without addressing other potential limitations, Limited discussion on the scalability and adaptability to non-agricultural IoT scenarios,
[62]	Quick authentication for new group managers, Secure against potential attacks, better security and functionality with lower computation cost and communication overhead.	Need to focused on optimizing group key generation and updating algorithm without addressing other potential limitations, Potential need for further optimization to reduce communication overhead in the proposed scheme.
[63]	Decentralized blockchain-based solution for device authentication in IoT-based EI networks, Resilient against attacks with distributed registration authorities, Easy integration with existing infrastructure and scalability.	The exploration of more sophisticated cryptographic primitives and integration with other blockchain-based solutions is needed. Further investigation is required for machine learning-based attack detection and scalability improvement through sharding.
[64]	Provably secure anonymous authentication for edge computing-enabled IoT, protecting against partial key-escrow	High communication cost, inability to counter ES impersonation attack, Limitation in scalability and adaptability to different IoT environments.

Ref	Advantage	Disadvantage
	attacks, leveraging blockchain, and demonstrating good security and performance.	
[65]	Blockchain-based authentication scheme for fog-enabled IoT, ensuring security even if a fog node is compromised, utilizing efficient cryptographic primitives.	Reliance on blockchain technology, additional computational and storage overhead lead to potentially affecting the overall performance and scalability of the system.

6. EVALUATION AND ANALYSIS

This section presents an analysis of various security requirements and vulnerabilities inherent in the surveyed schemes, along with an exploration of different methodologies employed. Furthermore, it provides an in-depth assessment of the efficacy and performance metrics of the evaluated methodologies.

In Table 3, we analyze the security aspects of the reviewed articles concerning anonymous authentication protocols within IoT platforms. Table 3 outlines the parameters utilized for evaluating the articles, including Anonymous and Unlinkable Sessions, Forward/Backward Security, Mutual Authentication, Untraceability, Data Verifiability, Key Agreement, and Scalability. Each article is scrutinized to determine its support for these security requirements. For instance, the extent to which it enables anonymous and unlinkable sessions, forward/backward security, mutual authentication, untraceability, data verifiability, key agreement, and scalability. Moreover, the evaluation examines the shortcomings of each article in meeting these security prerequisites. For example, some articles may excel in providing mutual authentication but fall short in ensuring untraceability. Through this comprehensive review, it becomes evident that no single article achieves complete coverage of all security and privacy requirements. Each article contributes differently to the overall security posture of IoT-based systems, with varying levels of support for the identified parameters. Consequently, the evaluation provides insights into the strengths and weaknesses of existing anonymous authentication protocols in IoT platforms, guiding future research directions for enhancing the security and privacy of such systems.

Table 3. Different security requirements in the surveyed schemes

Ref	F1	F2	F3	F4	F5	F6	F7
[45]	✓	✓	✓	-	-	-	-
[46]	-	-	✓	-	✓	-	-
[47]	✓	✓	✓	✓	-	-	✓
[48]	✓	✓	✓	✓	✓	-	✓
[49]	-	-	✓	-	-	-	✓
[50]	-	-	✓	-	✓	-	-
[51]	✓	-	✓	-	-	✓	✓
[52]	-	-	✓	-	-	-	✓
[53]	-	-	✓	-	-	-	✓
[54]	✓	✓	✓	✓	-	✓	-
[55]	✓	✓	✓	✓	✓	✓	-
[56]	✓	✓	✓	✓	-	-	-
[57]	✓	✓	✓	✓	-	-	-
[58]	✓	✓	✓	-	-	-	-
[59]	✓	✓	✓	✓	-	-	-
[60]	-	-	✓	-	✓	-	-
[61]	✓	✓	✓	-	-	✓	✓
[62]	✓	✓	✓	-	-	✓	
[63]	-	✓	✓	-	-		✓
[64]	✓	✓	✓	-	-	✓	-
[65]	✓	✓	✓	✓	-	✓	-

F1=Anonymous and Unlinkable Sessions, F2=Forward/Backward Security, F3=Mutual Authentication, F4=Untraceability, F5= Data verifiability, F6=Key Agreement, F7=Scalability.

Table 4 provides a comprehensive overview of different attacks present in the surveyed schemes within the realm of surveyed authentication protocols for IoT platform. These attacks pose significant threats to the security and integrity of sensitive data and operations. The parameters evaluated in this table include Replay Attack, Impersonation/Capture Attack, Jamming/Desynchronization Attacks, Key Leakage, Machine Learning Attacks, Man-in-the-Middle Attack, Physical Attack, Denial of Service (DoS), Insider Attack, Password Exposure, and Decentralization. Replay Attack refers to the malicious act of intercepting and retransmitting data to gain unauthorized access or achieve other nefarious goals. Impersonation/Capture Attack involves an attacker posing as a legitimate entity to gain access to sensitive information or perform unauthorized actions. Jamming/Desynchronization Attacks disrupt communication channels or synchronization processes, leading to system dysfunction or data manipulation. Key Leakage occurs when cryptographic keys are compromised, enabling unauthorized access to encrypted data. Machine Learning Attacks exploit vulnerabilities in machine learning algorithms or models to manipulate data or compromise system integrity. Man-in-the-Middle Attack intercepts communication between two parties to eavesdrop on or alter the exchanged data. Physical Attack involves the direct manipulation or tampering of hardware components to gain unauthorized access or disrupt system operations. DoS Attack floods the system with excessive traffic or requests, rendering it unable to fulfill legitimate requests. Insider Attack involves malicious actions by individuals with authorized access to the system, exploiting their privileges to compromise security. Password Exposure occurs when passwords or authentication credentials are exposed to unauthorized parties, leading to potential breaches. Decentralization refers to the distribution of system components or functions across multiple nodes, enhancing resilience against single points of failure or attacks. Each surveyed article addresses a combination of these attacks through various mechanisms and strategies tailored to the specific requirements and challenges of IoT-based systems. By comprehensively evaluating how each scheme tackles these threats, stakeholders can make informed decisions regarding the implementation of surveyed authentication protocols to safeguard data and operations. Table 4 serves as a valuable reference point for assessing the effectiveness and robustness of different approaches in mitigating security risks in IoT environments.

Table 4. Different attacks in the surveyed schemes

Ref	F1	F2	F3	F4	F5	F6	F7	F8	F9	F10	F11
[45]	✓	✓	✓								
[46]	✓	✓		✓						✓	
[47]	✓	✓	✓	✓	✓						
[48]	✓	✓		✓		✓	✓		✓		✓
[49]	✓	✓		✓	✓	✓	✓	✓			
[50]											
[51]	✓	✓		✓		✓					
[52]		✓				✓		✓			✓
[53]	✓			✓		✓		✓			
[54]	✓	✓	✓				✓		✓		
[55]	✓	✓			✓	✓	✓	✓	✓		
[56]	✓	✓				✓	✓		✓		
[57]	✓	✓		✓		✓	✓		✓	✓	
[58]	✓	✓		✓		✓					✓
[59]		✓	✓				✓		✓	✓	
[60]		✓						✓		✓	✓
[61]	✓	✓				✓		✓			✓
[62]	✓	✓			✓	✓	✓		✓		
[63]	✓	✓			✓	✓		✓			✓
[64]	✓	✓				✓				✓	
[65]	✓	✓	✓		✓	✓	✓		✓	✓	

F1=Replay Attack, F2=Impersonation / Capture Attack, F3=Jamming/Desynchronization Attacks, F4=Key Leakage, F5=Machin Learning attacks, F6=Man-in-the middle attack, F7=Physical attack, F8=Denial of Service (DoS), F9=Insider attack, F10=Password Exposure, F11=Decentralization.

In Table 5, the evaluation of surveyed authentication protocols in IoT platforms is presented with a focus on Computational Costs and Communication Costs. These parameters are crucial considerations in assessing the practical feasibility and efficiency of implementing such protocols in real-world scenarios. Computational Costs refer to the amount of computational resources, such as processing power, required to execute the authentication protocols. Higher computational costs can impose significant overhead on IoT devices, which often have limited resources in terms of processing capabilities and energy consumption. Therefore, protocols with lower computational costs are generally preferred as they enable more efficient utilization of IoT resources and prolong device lifespan. Communication Costs, on the other hand, pertain to the amount of data exchanged between IoT devices and other components of the system during the authentication process. This includes both the volume of data transmitted and the frequency of communication, as excessive communication can lead to congestion, latency, and increased energy consumption in IoT networks. Protocols with lower communication costs optimize network bandwidth usage and reduce the burden on communication channels, enhancing overall system performance and scalability. In Table 5, each surveyed article is evaluated based on how it addresses and mitigates Computational Costs and Communication Costs within the context of authentication in IoT platforms. By comparing these parameters across different protocols, stakeholders can gauge the trade-offs between security, computational efficiency, and communication overhead. This comparative analysis helps in identifying the most suitable protocol for specific deployment scenarios, considering factors such as device capabilities, network constraints, and security requirements. Furthermore, Table 5 serves as a valuable resource for researchers, developers, and decision-makers involved in the design and implementation of IoT-based systems, providing insights into the practical implications of various authentication protocols in terms of computational and communication costs. By understanding these costs, stakeholders can make informed decisions regarding protocol selection, deployment strategies, and resource allocation, ultimately ensuring the security and efficiency of IoT platforms in diverse application domains.

Table 5. Computational and Communication Costs

Ref	Computational cost	Communication cost
[45]	$10T_h + 8T_{XOR} + T_{sym}$	2880 bit
[46]	$6T_{EA}+8T_{EM}+4T_h$	
[47]	$8T_{GM} + 25T_h + 2T_{puf} + T_{MreDe} + T_{MreEn} + T_{Ga}$	3808 bit
[48]	$2T_{bp} + 13T_{mul} + 2T_{rng} + 9T_h$	3456 bit
[49]	$2T_{put} + 6T_{HMAC}$	1608 bit
[51]	$2T_{md} + 2T_{me} + T_{ae} + T_{ad}$	1888 bit
[53]		1467 bit
[54]	$35T_h + T_{fe} + 20T_{ecm} + 4T_{eca}$	4416 bit
[55]	$18T_h + 14T_x + 2T_{fe} + 2T_{ecm}$	1024 bit
[56]	$10T_{ecm} + 7T_h + 4T_{eca}$	2560 bit
[57]	$34T_h + 3T_{rg} + T_{puf} + 2T_{fe}$	1837 bit
[58]	$8T_h + 4T_{exp} + 2T_{bp}$	
[59]	$6T_{EM} + 31T_h + T_{fe}$	2720 bit
[60]	$6T_{EA} + 2T_{Em} + 5T_h$	2824 bit
[61]	$(9n + 3)T_{ecm} + (7n - 2)T_{eca} + 9nT_h$	4256 bit
[62]	$8T_h + 4T_c$	1056 bit
[63]	$6T_{EM}$	1408 bit
[64]	$4T_{EM} + T_{EA} + 5T_h + T_e$	3616 bit
[65]	$27T_h + T_{puf} + 2T_{sym}$	3680 bit

T_{XOR}= XOR operation, T_{sym} = Symmetric encryption, T_{EA}: elliptic curve addition operation, T_{EM}: elliptic curve multiple operation, T_h: one-way hash function, T_{GM}=Scalar multiplication on G, T_{PUF}=PUF generation, T_{MreDe}=MRE decryption, T_{MreEn}=MRE encryption, T_{Ga}=Addition on G, T_{bp}=bilinear pairing operation, T_{mul}=scalar multiplication operation, T_{rng}=random number generation, T_{HMAC}=computing a hashed message authentication code, T_{me}=MSR encryption,T_{md}= MSR decryption, T_{ae}=AES encryption, T_{ad}=AES decryption, T_{fe}=Fuzzy extractor function, T_{ecm}= ECC point multiplication, T_{eca}= ECC point addition, T_{rg}=random nonce generation, T_{exp}=Modular Exponential Operation, T_c=Chebyshev mapping, T_e=Modular exponentiation.

7. CONCLUSION

In this paper, recently developed authentication techniques for IoT were surveyed. The analysis included a comprehensive comparison of these methods to highlight their respective strengths, weaknesses, and vulnerabilities against specific attacks. By understanding the distinct characteristics of each technique, we can better align them with the security requirements of IoT systems. Evaluation of computational and communication costs underscores the need for balancing security requirements with practical considerations such as resource constraints and network efficiency. Protocols that strike a judicious balance between security and performance emerge as promising candidates for real-world deployment, offering scalable and efficient solutions for securing IoT platforms. Moreover, the analysis of attacks and countermeasures underscores the dynamic nature of security threats facing IoT systems, necessitating continuous innovation and adaptation in security protocols and practices. Looking forward, as IoT systems continue to proliferate and face escalating threats, there will be a pressing need to enhance existing authentication techniques. This will involve refining protocols, integrating new technologies like blockchain or biometrics, and implementing stronger encryption methods. Furthermore, ongoing modifications and advancements in authentication strategies will be essential to keep pace with evolving cyber threats and ensure the resilience and trustworthiness of IoT deployments in the future. Finally, future works should emphasize the development of standardized frameworks and testing environments to evaluate the effectiveness and interoperability of authentication protocols across diverse IoT ecosystems. This will facilitate the adoption of secure and scalable solutions capable of meeting the evolving demands of real-world deployments. Furthermore, interdisciplinary approaches that combine artificial intelligence and behavioral biometrics hold significant promise for enhancing real-time threat detection and user authentication. AI-driven models can analyze patterns and anomalies in user behavior, contributing to more dynamic and context-aware security measures. Additionally, exploring multi-factor authentication systems that blend traditional methods with novel biometric and environmental sensors can add layers of robustness to IoT security.

REFERENCES

[1] Abdul-Qawy, A. S., Pramod, P. J., Magesh, E., & Srinivasulu, T. (2015), **“The internet of things (iot): An overview”**, International Journal of Engineering Research and Applications, 5(12), 71-82.

[2] Kiamansouri, E., Barati, H., & Barati, A. (2022), **“A two-level clustering based on fuzzy logic and content-based routing method in the internet of things**, Peer-to-Peer Networking and Applications, 15(4), 2142-2159.

[3] López, T. S., Ranasinghe, D. C., Patkai, B., & McFarlane, D. (2011), **“Taxonomy, technology and applications of smart objects”**, Information Systems Frontiers, 13, 281-300.

[4] Sharma, N., Shamkuwar, M., & Singh, I. (2019), **“The history, present and future with IoT”**, Internet of things and big data analytics for smart generation, 27-51.

[5] Akbari, M. R., Barati, H., & Barati, A. (2022), **“An overlapping routing approach for sending data from things to the cloud inspired by fog technology in the large-scale IoT ecosystem”**, Wireless Networks, 28(2), 521-538.

[6] Akbari, M. R., Barati, H., & Barati, A. (2022), **“An efficient gray system theory-based routing protocol for energy consumption management in the Internet of Things using fog and cloud computing”**, Computing, 104(6), 1307-1335.

[7] Shojarazavi, T., Barati, H., & Barati, A. (2022), **“A wrapper method based on a modified two-step league championship algorithm for detecting botnets in IoT environments”**, Computing, 104(8), 1753-1774.

[8] Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013), **“Internet of Things (IoT): A vision, architectural elements, and future directions”**, Future generation computer systems, 29(7), 1645-1660.

[9] Onumanyi, A. J., Abu-Mahfouz, A. M., & Hancke, G. P. (2020), “**Low power wide area network, cognitive radio and the Internet of Things: Potentials for integration**”, Sensors, 20(23), 6837.

[10] Lee, I., & Lee, K. (2015), “**The Internet of Things (IoT): Applications, investments, and challenges for enterprises**”, Business horizons, 58(4), 431-440.

[11] Chataut, R., Phoummalayvane, A., & Akl, R. (2023), “**Unleashing the power of IoT: A comprehensive review of IoT applications and future prospects in healthcare, agriculture, smart homes, smart cities, and industry 4.0**”, Sensors, 23(16), 7194.

[12] Rehman, A., Saba, T., Kashif, M., Fati, S. M., Bahaj, S. A., & Chaudhry, H. (2022), “**A revisit of internet of things technologies for monitoring and control strategies in smart agriculture**”, Agronomy, 12(1), 127.

[13] Javed, A. R., Shahzad, F., ur Rehman, S., Zikria, Y. B., Razzak, I., Jalil, Z., & Xu, G. (2022), “**Future smart cities: Requirements, emerging technologies, applications, challenges, and future aspects**”, Cities, 129, 103794.

[14] Sun, P. J. (2019), “**Privacy protection and data security in cloud computing: a survey, challenges, and solutions**”, Ieee Access, 7, 147420-147452.

[15] Munirathinam, S. (2020), “**Industry 4.0: Industrial internet of things (IIOT)**” In Advances in computers (Vol. 117, No. 1, pp. 129-164). Elsevier.

[16] Karale, A. (2021), “**The challenges of IoT addressing security, ethics, privacy, and laws**”, Internet of Things, 15, 100420.

[17] Obaid, O. I., & Salman, S. A. B. (2022), **“Security and Privacy in IoT-based Healthcare Systems: A Review”**, Mesopotamian Journal of Computer Science, 2022, 29-39.

[18] Chen, J. Q., & Benusa, A. (2017), **“HIPAA security compliance challenges: The case for small healthcare providers”**, International Journal of Healthcare Management, 10(2), 135-146.

[19] Sun, Y., Lo, F. P. W., & Lo, B. (2019), **“Security and privacy for the internet of medical things enabled healthcare systems: A survey”**, IEEE Access, 7, 183339-183355.

[20] Hasan, M. K., Ghazal, T. M., Saeed, R. A., Pandey, B., Gohel, H., Eshmawi, A. A., ... & Alkhassawneh, H. M. (2022), **“A review on security threats, vulnerabilities, and counter measures of 5G enabled Internet- of- Medical- Things”**, IET communications, 16(5), 421-432.

[21] Hamidi, H. (2019), **“An approach to develop the smart health using Internet of Things and authentication based on biometric technology”**, Future generation computer systems, 91, 434-449.

[22] Newaz, A. I., Sikder, A. K., Rahman, M. A., & Uluagac, A. S. (2021), **“A survey on security and privacy issues in modern healthcare systems: Attacks and defenses”**, ACM Transactions on Computing for Healthcare, 2(3), 1-44.

[23] Nauman, A., Qadri, Y. A., Amjad, M., Zikria, Y. B., Afzal, M. K., & Kim, S. W. (2020), **“Multimedia Internet of Things: A comprehensive survey**”, Ieee Access, 8, 8202-8250.

[24] El-Hajj, M., Fadlallah, A., Chamoun, M., & Serhrouchni, A. (2019), **“A survey of internet of things (IoT) authentication schemes”**, Sensors, 19(5), 1141.

[25] Rajakumari, S., Azhagumeena, S., Devi, A. B., & Ananthi, M. (2017, February), **"Upgraded living think-IoT and big data"**, In 2017 2nd International Conference on Computing and Communications Technologies (ICCCT) (pp. 181-184). IEEE.

[26] Gupta, B. B., & Quamara, M. (2020), **"An overview of Internet of Things (IoT): Architectural aspects, challenges, and protocols"**, Concurrency and Computation: Practice and Experience, 32(21), e4946.

[27] Ray, P. P. (2018), "A survey on Internet of Things architectures", Journal of King Saud University-Computer and Information Sciences, 30(3), 291-319.

[28] Yaqoob, T., Abbas, H., & Atiquzzaman, M. (2019), **"Security vulnerabilities, attacks, countermeasures, and regulations of networked medical devices—A review"**, IEEE Communications Surveys & Tutorials, 21(4), 3723-3768.

[29] Riggs, H., Tufail, S., Parvez, I., Tariq, M., Khan, M. A., Amir, A., ... & Sarwat, A. I. (2023), **"Impact, vulnerabilities, and mitigation strategies for cyber-secure critical infrastructure"**, Sensors, 23(8), 4060.

[30] Mohanty, J., Mishra, S., Patra, S., Pati, B., & Panigrahi, C. R. (2021), **"IoT security, challenges, and solutions: a review"**, Progress in Advanced Computing and Intelligent Engineering: Proceedings of ICACIE 2019, Volume 2, 493-504.

[31] Khattak, H. A., Shah, M. A., Khan, S., Ali, I., & Imran, M. (2019), **"Perception layer security in Internet of Things"**, Future Generation Computer Systems, 100, 144-164.

[32] Jing, Q., Vasilakos, A. V., Wan, J., Lu, J., & Qiu, D. (2014), **"Security of the Internet of Things: perspectives and challenges"**, Wireless networks, 20, 2481-2501.

[33] Nastase, L. (2017, May), **"Security in the internet of things: A survey on application layer protocols"**, In 2017 21st international conference on control systems and computer science (CSCS) (pp. 659-666). IEEE.

[34] Tewari, A., & Gupta, B. B. (2020), **"Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework"**, Future generation computer systems, 108, 909-920.

[35] Ngu, A. H., Gutierrez, M., Metsis, V., Nepal, S., & Sheng, Q. Z. (2016), **"IoT middleware: A survey on issues and enabling technologies**", IEEE Internet of Things Journal, 4(1), 1-20.

[36] Chaqfeh, M. A., & Mohamed, N. (2012, May), **"Challenges in middleware solutions for the internet of things"**, In 2012 international conference on collaboration technologies and systems (CTS) (pp. 21-26). IEEE.

[37] Nebbione, G., & Calzarossa, M. C. (2020), **"Security of IoT application layer protocols: Challenges and findings"**, Future Internet, 12(3), 55.

[38] Karagiannis, V., Chatzimisios, P., Vazquez-Gallego, F., & Alonso-Zarate, J. (2015), **"A survey on application layer protocols for the internet of things"**, Transaction on IoT and Cloud computing, 3(1), 11-17.

[39] Deep, S., Zheng, X., Jolfaei, A., Yu, D., Ostovari, P., & Kashif Bashir, A. (2022), **"A survey of security and privacy issues in the Internet of Things from the layered context"**, Transactions on Emerging Telecommunications Technologies, 33(6), e3935.

[40] Cresitello-Dittmar, B. (2016), **"Application of the blockchain for authentication and verification of identity"**, Independent Paper.

[41] Chenchev, I., Aleksieva-Petrova, A., & Petrov, M. (2021), **"Authentication Mechanisms and Classification: A Literature Survey"**, In Intelligent Computing: Proceedings of the 2021 Computing Conference, Volume 3 (pp. 1051-1070). Springer International Publishing.

[42] Patwary, A. A. N., Naha, R. K., Garg, S., Battula, S. K., Patwary, M. A. K., Aghasian, E., ... & Gong, M. (2021), **"Towards secure fog computing: A survey on trust management, privacy, authentication, threats and access control"**, Electronics, 10(10), 1171.

[43] Nandy, T., Idris, M. Y. I. B., Noor, R. M., Kiah, L. M., Lun, L. S., Juma'at, N. B. A., ... & Bhattacharyya, S. (2019), **"Review on security of internet of things authentication mechanism"**, IEEE Access, 7, 151054-151089.

[44] Ferrag, M. A., Maglaras, L. A., Janicke, H., Jiang, J., & Shu, L. (2017), **"Authentication protocols for internet of things: a comprehensive survey"**, Security and Communication Networks, 2017.

[45] Xu, J., Meng, X., Liang, W., Peng, L., Xu, Z., & Li, K. C. (2020), **"A hybrid mutual authentication scheme based on blockchain technology for WBANs"**, In Blockchain and Trustworthy Systems: First International Conference, BlockSys 2019, Guangzhou, China, December 7–8, 2019, Proceedings 1 (pp. 350-362). Springer Singapore.

[46] Lee, D. H., & Lee, I. Y. (2020), **"A lightweight authentication and key agreement schemes for IoT environments"**, Sensors, 20(18), 5350.

[47] Zhang, Y., Li, B., Liu, B., Hu, Y., & Zheng, H. (2021), **"A privacy-aware PUFs-based multiserver authentication protocol in cloud-edge IoT systems using blockchain"**, IEEE Internet of Things Journal, 8(18), 13958-13974.

[48] Son, S., Lee, J., Kim, M., Yu, S., Das, A. K., & Park, Y. (2020), **"Design of secure authentication protocol for cloud-assisted telecare medical information system using blockchain"**, IEEE Access, 8, 192177-192191.

[49] Mostafa, A., Lee, S. J., & Peker, Y. K. (2020), "Physical unclonable function and hashing are all you need to mutually authenticate iot devices", Sensors, 20(16), 4361.

[50] Alzubi, J. A. (2021), **"Blockchain-based Lamport Merkle digital signature: authentication tool in IoT healthcare"**, Computer Communications, 170, 200-208.

[51] Yang, X., Yang, X., Yi, X., Khalil, I., Zhou, X., He, D., ... & Nepal, S. (2021), **"Blockchain-based secure and lightweight authentication for Internet of Things"**, IEEE Internet of Things Journal, 9(5), 3321-3332.

[52] Al Ahmed, M. T., Hashim, F., Hashim, S. J., & Abdullah, A. (2022), **"Hierarchical blockchain structure for node authentication in IoT networks"**, Egyptian Informatics Journal, 23(2), 345-361.

[53] Zhang, Y., Luo, Y., Chen, X., Tong, F., Xu, Y., Tao, J., & Cheng, G. (2022), **"A lightweight authentication scheme based on consortium blockchain for cross-domain IoT"**, Security and Communication Networks, 2022, 1-15.

[54] Zhao, X., Li, D., & Li, H. (2022), **"Practical three-factor authentication protocol based on elliptic curve cryptography for industrial internet of things"**, Sensors, 22(19), 7510.

[55] Mirsaraei, A. G., Barati, A., & Barati, H. (2022), **"A secure three-factor authentication scheme for IoT environments"**, Journal of Parallel and Distributed Computing, 169, 87-105.

[56] Saqib, M., Jasra, B., & Moon, A. H. (2022), **"A lightweight three factor authentication framework for IoT based critical applications"**, Journal of King Saud University-Computer and Information Sciences, 34(9), 6925-6937.

[57] Lee, J., Oh, J., Kwon, D., Kim, M., Yu, S., Jho, N. S., & Park, Y. (2022), **"PUFTAP-IoT: PUF-based three-factor authentication protocol in IoT environment focused on sensing devices"**, Sensors, 22(18), 7075.

[58] Singh, A., Chandra, H., Rana, S., & Chhikara, D. (2023), **"Blockchain based authentication and access control protocol for IoT"**, Multimedia Tools and Applications, 1-23.

[59] Wang, C., Wang, D., Duan, Y., & Tao, X. (2023), **"Secure and lightweight user authentication scheme for cloud-assisted internet of things**", IEEE Transactions on Information Forensics and Security.

[60] Lau, C. H., Yeung, K. H., Yan, F., & Chan, S. (2023), **"Blockchain- based authentication and secure communication in IoT networks"**, Security and Privacy, 6(6), e319.

[61] Luo, F., Huang, R., & Xie, Y. (2024), **"Hybrid blockchain-based many-to-many cross-domain authentication scheme for smart agriculture IoT networks"**, Journal of King Saud University-Computer and Information Sciences, 101946.

[62] Long, Y., Peng, C., Tan, W., & Chen, Y. (2024), **"Blockchain-Based Anonymous Authentication and Key Management for Internet of Things With Chebyshev Chaotic Maps"**, IEEE Transactions on Industrial Informatics.

[63] Benrebbouh, C., Mansouri, H., Cherbal, S., & Pathan, A. S. K. (2024), **"Enhanced secure and efficient mutual authentication protocol in IoT-based energy internet using blockchain"**, Peer-to-Peer Networking and Applications, 17(1), 68-88.

[64] Zhang, S., & Cao, D. (2024), **"A blockchain-based provably secure anonymous authentication for edge computing-enabled IoT"**, The Journal of Supercomputing, 80(5), 6778-6808.

[65] Guo, Y., Zhang, Z., Guo, Y., & Xiong, P. (2023), **"BSRA: Blockchain-based secure remote authentication scheme for the fog-enabled Internet of Things"**, IEEE Internet of Things Journal.