Computers and Artificial Intelligence；Vol.3, No.2; 2026
E-ISSN: 3006 -3728 P-ISSN：3006-371X
DOI: https://doi.org/10.70267/cai.26v3n2.6577
Published by: Zeus Press

Current Status and Challenges of IoT Device Identity Authentication Technology

Yixuan Dou*

School of Computer Science and Engineering, Guilin university of technology, Guilin, Guangxi, China

**Corresponding author: Yixuan Dou.*

Abstract

The Internet of Things (IoT) has witnessed exponential growth, integrating billions of devices into our daily lives. A critical challenge in realizing the full potential of IoT lies in ensuring the secure and reliable authentication of these devices. This review paper provides a comprehensive overview of the current status and challenges of IoT device identity authentication technology. We begin by outlining the fundamental requirements for IoT device authentication, considering the resource-constrained nature of many IoT devices and the diverse application scenarios. We explore the historical evolution of authentication methods, from traditional password-based schemes to more sophisticated cryptographic protocols, highlighting their strengths and weaknesses in the context of IoT. The core of this review focuses on analyzing prominent authentication technologies, including symmetric-key based approaches, public-key infrastructure (PKI), and lightweight authentication protocols designed specifically for IoT. Furthermore, we delve into emerging authentication techniques based on physical unclonable functions (PUFs) and blockchain technology. We critically compare the performance, security, and scalability of these different approaches, considering factors such as computational overhead, communication costs, and resilience against various attacks. We address key challenges, including the need for interoperability, the management of device identities throughout their lifecycle, and the mitigation of risks associated with compromised devices. Finally, we offer perspectives on future research directions, emphasizing the importance of developing adaptive authentication mechanisms, enhancing privacy preservation, and addressing the evolving threat landscape in the IoT ecosystem. This review aims to provide researchers, developers, and policymakers with a valuable resource for understanding the current state-of-the-art and the open challenges in IoT device identity authentication.

Keywords

IoT, device authentication, security, identity management, cryptography, PUF, blockchain

1. Introduction

1.1 Background and Motivation

The Internet of Things (IoT) has experienced exponential growth, connecting billions of devices ranging from simple sensors to complex industrial machines. This proliferation of interconnected devices offers unprecedented opportunities for automation, data collection, and improved efficiency across various sectors.

However, the widespread adoption of IoT also introduces significant security vulnerabilities. Device identity authentication is crucial for establishing trust and ensuring the integrity of IoT ecosystems. Without robust authentication mechanisms, malicious actors can easily compromise devices, intercept sensitive data, and launch large-scale attacks. A key challenge lies in the resource-constrained nature of many IoT devices, which limits the feasibility of implementing computationally intensive security protocols. Furthermore, the heterogeneity of IoT devices, with varying processing power, memory capacity, and communication protocols, complicates the development of standardized and universally applicable authentication solutions. The need for lightweight and adaptable authentication methods is therefore paramount to secure the future of IoT.

1.2 Problem Statement and Scope

The proliferation of IoT devices introduces significant security vulnerabilities, primarily stemming from inadequate identity authentication. This review addresses the critical problems of weak or non-existent authentication mechanisms, susceptibility to impersonation attacks, and the potential for unauthorized access to sensitive data. Specifically, we examine vulnerabilities exploited through replay attacks, man-in-the-middle attacks, and compromised device credentials. The scope of this review encompasses a range of authentication technologies, including pre-shared keys, public key infrastructure (PKI), and lightweight authentication protocols tailored for resource-constrained devices. We consider IoT applications across diverse sectors, such as smart homes, industrial control systems, and healthcare, focusing on the challenges of securing devices with limited processing power, memory, and battery life, where the trade-off between security and performance is crucial. We also consider the impact of the number of devices, n, on the overall system security.

1.3 Contribution and Organization

This review makes several key contributions to the field of IoT security. First, it provides a comprehensive overview of existing IoT device identity authentication technologies, categorizing them based on underlying principles. Second, it identifies critical challenges and open research questions related to scalability, security, and resource constraints in IoT environments. Finally, it offers insights into potential future research directions. The remainder of this paper is organized as follows: Section 2 presents background information on IoT architectures and security requirements. Section 3 details the various authentication technologies. Section 4 discusses the challenges. Section 5 concludes the paper and suggests future work.

2. Historical Overview of Device Authentication

2.1 Traditional Authentication Methods

Traditional authentication methods, while foundational to network security, present significant challenges when applied to the Internet of Things (IoT). Password-based authentication, the simplest approach, relies on a shared secret between the device and the server. However, IoT devices often have limited processing power and storage, making them vulnerable to brute-force and dictionary attacks, especially with weak or default passwords. Furthermore, the sheer scale of IoT deployments necessitates robust password management, which is often lacking.

Challenge-response protocols offer an improvement by introducing a dynamic element. The server sends a challenge (e.g., a random number R) to the device, which then performs a calculation based on R and a shared secret key K to generate a response. The server verifies the response using its own copy of K. While more secure than simple passwords, these protocols can still be susceptible to replay attacks if the challenges are not sufficiently unique or time-sensitive. Moreover, the computational overhead of cryptographic operations can be a burden for resource-constrained IoT devices. Other legacy methods, such as MAC address filtering, are easily circumvented through spoofing, rendering them inadequate for securing IoT ecosystems. These limitations highlight the need for more sophisticated and lightweight authentication mechanisms tailored to the specific constraints of IoT environments.

2.2 Evolution of Cryptographic Protocols

The evolution of cryptographic protocols has been central to securing device authentication, with early protocols laying the groundwork for modern IoT security. Diffie-Hellman key exchange, introduced in 1976,

enabled two parties to establish a shared secret key over an insecure channel, a significant advancement for secure communication. However, its susceptibility to man-in-the-middle attacks necessitates additional authentication mechanisms. RSA, a public-key cryptosystem, offered both encryption and digital signatures, providing a means for verifying device identity. The computational intensity of RSA, particularly with larger key sizes required for stronger security ($n > 2048$ bits), poses a challenge for resource-constrained IoT devices. Symmetric-key algorithms like AES (Advanced Encryption Standard) provide efficient encryption and authentication, crucial for data confidentiality and integrity. AES's lower computational overhead makes it more suitable for IoT devices compared to RSA, especially when implemented with smaller key sizes (e.g., AES-128). The trade-off between security strength, computational cost, and energy consumption remains a critical consideration when selecting cryptographic protocols for IoT device authentication. The ongoing development of lightweight cryptography aims to address these limitations, offering tailored solutions for the unique constraints of IoT environments.

Table 1: Comparison of Traditional Authentication Methods in IoT.

Authentication Method	Description	Advantages	Disadvantages	Vulnerabilities in IoT
Password-Based	Relies on a shared secret password between the device and server.	Simple to implement. Minimal computational overhead.	Weak passwords can be easily compromised. Requires robust password management.	Susceptible to brute-force and dictionary attacks due to weak/default passwords. Scale of IoT makes password management difficult.
Challenge-Response	Server sends a challenge (e.g., random number R) to the device, which calculates a response based on R and a shared secret key K.	More secure than simple passwords, introduces a dynamic element.	Requires cryptographic operations. Potential computational overhead.	Susceptible to replay attacks if challenges aren't unique enough or are not time-sensitive. Overhead for resource-constrained devices.
MAC Address Filtering	Allows or denies network access based on the device's Media Access Control (MAC) address.	Simple to implement.	Easily bypassed.	MAC addresses can be easily spoofed, making it ineffective security measure.

2.3 Early IoT Authentication Approaches

Early IoT authentication attempts largely involved adapting established methods like password-based authentication and simple cryptographic techniques. Pre-shared keys (PSKs) were common, offering basic security but lacking scalability and manageability for large deployments. Challenges arose from the resource-constrained nature of many IoT devices, making complex cryptographic algorithms computationally expensive and energy-intensive. Furthermore, the diverse range of devices and communication protocols hindered the development of standardized authentication frameworks. The inherent vulnerabilities of these early approaches often resulted in weak security and susceptibility to attacks such as replay attacks and man-in-the-middle attacks, highlighting the need for more robust and tailored solutions for IoT environments.

3. Symmetric-Key Based Authentication

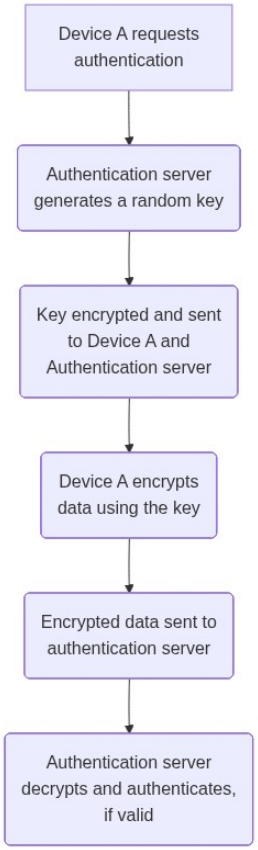
3.1 Overview of Symmetric-Key Cryptography

Symmetric-key cryptography, also known as secret-key cryptography, relies on a single, shared secret key for both encryption and decryption. This key, denoted as k, must be securely distributed between the communicating parties before any secure communication can occur. The encryption process transforms plaintext P into ciphertext C using the encryption algorithm E and the secret key k, represented as $C = E(k, P)$. Conversely, decryption uses the same key k and a decryption algorithm D to recover the original plaintext,$P = D(k, C)$. The security of the system hinges entirely on the secrecy of the key; if the key is compromised, all communication is vulnerable.

In the context of IoT device authentication, symmetric-key cryptography can be employed to verify the identity of a device. A pre-shared key can be stored on both the device and the authentication server. The device can then use this key to encrypt a challenge message from the server, and the server can decrypt the response to verify the device's identity. This approach is efficient in terms of computational resources, making it suitable for resource-constrained IoT devices.

Advanced Encryption Standard (AES) is a widely adopted symmetric-key algorithm known for its strong security and performance. AES operates on blocks of data of 128 bits and supports key sizes of 128, 192, or 256 bits. However, for highly constrained IoT devices, lightweight block ciphers are often preferred. These ciphers, such as PRESENT, SIMON, and SPECK, are designed to minimize resource consumption in terms of memory footprint, energy usage, and computational complexity. They typically achieve this by employing simpler operations and smaller key sizes compared to AES, while still providing an acceptable level of security for many IoT applications. The choice of algorithm depends on the specific security requirements and resource limitations of the IoT device and the overall system.

Figure 1: Symmetric-Key Authentication Flow Diagram



Lightweight Symmetric-Key Protocols for IoT

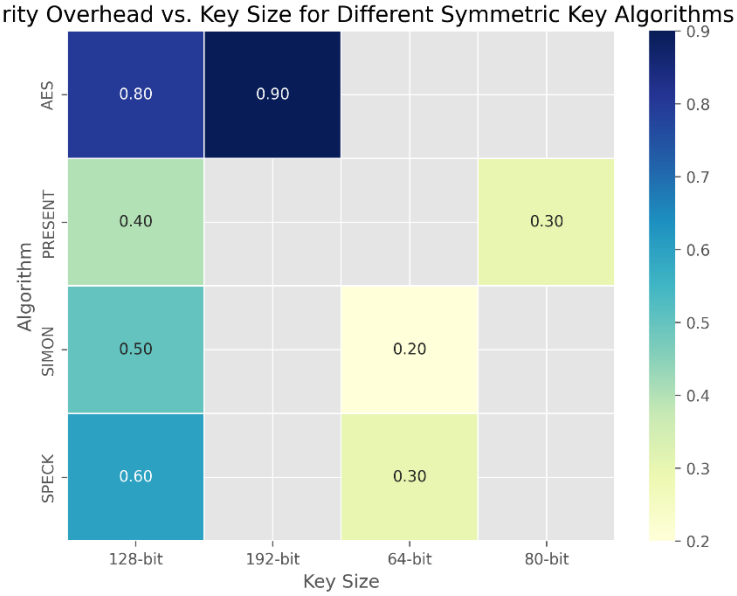
Lightweight symmetric-key protocols are crucial for securing IoT devices due to their computational efficiency and low memory footprint, making them suitable for resource-constrained environments. Several such protocols have been developed, each with its own strengths and weaknesses in terms of security, performance, and implementation complexity.

PRESENT is a block cipher specifically designed for hardware implementations in constrained environments. It utilizes a Substitution-Permutation Network (SPN) structure with a small block size of 64 bits and key sizes of 80 or 128 bits. The S-box in PRESENT is a simple 4-bit to 4-bit substitution, contributing to its hardware efficiency. The permutation layer is bit-wise, further simplifying the hardware design. The lightweight nature of PRESENT makes it a viable option for applications where hardware resources are severely limited, such as RFID tags and sensor nodes. However, its relatively small block size can make it vulnerable to certain attacks if not implemented carefully.

SIMON and SPECK are two block ciphers developed by the National Security Agency (NSA) with a focus on both hardware and software performance. They are designed to be flexible, offering a range of block and key sizes to suit different security requirements and resource constraints. SIMON is optimized for hardware implementations, while SPECK is optimized for software implementations. Both ciphers are based on the Feistel network structure, which simplifies the encryption and decryption processes. SIMON uses bitwise operations like AND, XOR, and bitwise rotation, making it very efficient in hardware. SPECK, on the other hand, uses modular addition, XOR, and bitwise rotation, which are well-suited for software implementations on modern processors. The availability of different block and key size options (n= 32, 48, 64, 96, 128 and k = 64, 72, 96, 128, 144, 192, 256 for SIMON and SPECK respectively) allows designers to tailor the cipher to the specific needs of their application.

Another notable lightweight symmetric-key algorithm is the Advanced Encryption Standard (AES) in its reduced-round variants. While the full AES is relatively resource-intensive, reducing the number of rounds can significantly decrease its computational cost, making it more suitable for IoT devices. For example, AES-128 with a reduced number of rounds (e.g., 6 or 8 rounds instead of the standard 10) can offer a reasonable trade-off between security and performance. The security analysis of reduced-round AES is crucial to ensure that the chosen number of rounds provides sufficient protection against known attacks. The choice of a specific lightweight symmetric-key protocol depends on the specific application requirements, including the level of security needed, the available resources, and the performance constraints.

Figure 2: Security overhead vs. Latency for different symmetric key algorithms



3.2 Key Management Issues

Symmetric-key based authentication, while computationally efficient, faces significant hurdles in key management within the diverse and often resource-constrained IoT landscape. These challenges primarily revolve around key distribution, secure storage, and efficient revocation.

Key distribution, the process of securely sharing the secret key between the IoT device and the authentication server, is particularly problematic. Pre-shared keys (PSKs), while simple to implement, lack scalability and are vulnerable to compromise. If one device's key is compromised, the security of the entire network using that key is at risk. More sophisticated methods like the Kerberos protocol, while offering improved security, introduce complexity and require a trusted third party, which may not be feasible in all IoT deployments. The need for secure channels during key exchange, often involving complex protocols like Diffie-Hellman, adds overhead and can be computationally expensive for constrained devices.

Secure key storage on IoT devices is another major concern. Many IoT devices have limited processing power and memory, making it difficult to implement robust security measures. Storing keys in plain text is unacceptable, but implementing strong encryption algorithms can strain resources. Furthermore, tamper-proof

hardware security modules (HSMs), while providing the best protection, significantly increase device cost, making them impractical for many low-cost IoT applications. Techniques like obfuscation and white-box cryptography offer some protection, but are not foolproof and can be broken with sufficient effort.

Key revocation, the process of invalidating a compromised or outdated key, is crucial for maintaining security. In symmetric-key systems, this can be challenging, especially when dealing with a large number of devices. Revoking a key typically requires updating the key on both the device and the authentication server. This can be difficult to achieve reliably, particularly in scenarios where devices are offline or have intermittent connectivity. Furthermore, efficient revocation mechanisms are needed to prevent compromised devices from continuing to access the network. The propagation of revocation information across the network needs to be timely and secure to minimize the window of vulnerability. The trade-off between security and efficiency is a constant consideration in designing key management schemes for IoT devices.

4. Public-Key Infrastructure (PKI) for IoT

4.1 PKI Fundamentals and Certificates

Public-Key Infrastructure (PKI) provides a robust framework for secure communication and authentication, crucial for the burgeoning Internet of Things (IoT). At its core, PKI relies on asymmetric cryptography, utilizing key pairs consisting of a public key and a private key. The public key, as the name suggests, is openly distributed, while the private key is kept secret and securely stored. This asymmetry allows for both encryption and digital signatures.

The cornerstone of PKI is the digital certificate. A digital certificate is an electronic document that binds a public key to an identity, such as a device, user, or organization. These certificates are issued by trusted third parties known as Certificate Authorities (CAs). The CA verifies the identity of the certificate applicant before issuing the certificate, ensuring the legitimacy of the public key. The certificate itself is digitally signed by the CA using its private key, providing assurance of its authenticity and integrity. When a device presents its certificate, other devices can verify the CA's signature using the CA's public key, confirming the certificate's validity and establishing trust.

Several cryptographic algorithms are employed within PKI to generate key pairs and perform encryption/decryption and signing/verification operations. RSA (Rivest-Shamir-Adleman) is a widely used algorithm based on the mathematical properties of prime numbers. The security of RSA relies on the difficulty of factoring large numbers into their prime factors. The key size, typically measured in bits (e.g., 2048 bits or 4096 bits), determines the strength of the encryption. Elliptic Curve Cryptography (ECC) offers comparable security to RSA but with smaller key sizes. ECC is based on the algebraic structure of elliptic curves over finite fields. The shorter key lengths of ECC make it particularly attractive for resource-constrained IoT devices, where computational power and memory are limited. For example, an ECC key of 256 bits can provide a similar level of security to a 3072-bit RSA key. The choice of algorithm, key size, and certificate management practices are critical considerations in designing a secure PKI for IoT deployments.

4.2 Lightweight PKI Implementations for IoT

Addressing the resource constraints of IoT devices, lightweight PKI implementations offer a viable path for secure identity authentication. Traditional PKI, with its reliance on computationally intensive algorithms and large certificate sizes, is often impractical for devices with limited processing power, memory, and bandwidth. Therefore, specialized PKI solutions have emerged, focusing on minimizing overhead while maintaining an acceptable level of security.

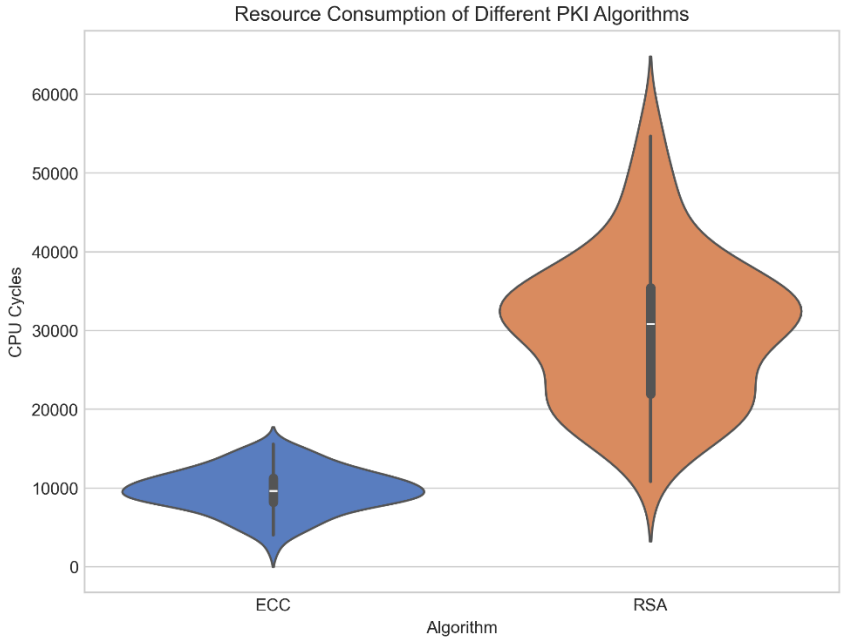
One prominent approach involves the adoption of Elliptic Curve Cryptography (ECC). ECC offers comparable security strength to RSA with significantly smaller key sizes. For example, a 256-bit ECC key provides roughly the same security level as a 3072-bit RSA key. This reduction in key size translates to smaller certificates, faster cryptographic operations, and lower energy consumption, making ECC particularly well-suited for resource-constrained IoT devices. Common ECC curves used in IoT include NIST curves like P-256 and Edwards curves like Curve25519. The efficiency of ECC stems from the mathematical properties of elliptic curves, which allow for efficient key exchange and digital signature algorithms.

Beyond ECC, lightweight PKI implementations often incorporate optimizations in certificate management. Techniques like certificate compression and efficient certificate validation algorithms are employed to reduce the burden on IoT devices. Certificate compression aims to reduce the size of certificates by removing redundant information or using more efficient encoding schemes. Efficient certificate validation algorithms minimize the computational cost of verifying the validity of a certificate chain. This can involve techniques like caching intermediate certificates or using pre-computed hashes.

Furthermore, the concept of implicit certificates has gained traction in the IoT domain. Implicit certificates eliminate the need for explicit certificate revocation lists (CRLs) by embedding the certificate's validity period directly into the certificate itself. This reduces the overhead associated with CRL management, which can be significant in large-scale IoT deployments. However, implicit certificates require careful consideration of key management and compromise scenarios.

Another optimization strategy involves offloading computationally intensive tasks to more powerful edge servers or cloud platforms. IoT devices can delegate certificate validation or signature generation to these external entities, reducing the processing burden on the devices themselves. This approach requires secure communication channels between the IoT devices and the external servers to prevent man-in-the-middle attacks. The trade-off here lies in the increased reliance on network connectivity and the potential for latency. The selection of a suitable lightweight PKI implementation depends heavily on the specific requirements of the IoT application, including the security level, resource constraints, and network characteristics.

Figure 3: Resource consumption of different PKI algorithms



4.3 Scalability and Trust Management Issues

Scaling Public Key Infrastructure (PKI) to accommodate the massive deployment of IoT devices presents significant hurdles. Traditional PKI architectures, designed for relatively smaller and more manageable user bases, often struggle to handle the sheer volume of certificates required for millions or even billions of IoT devices. The computational overhead associated with certificate generation, distribution, storage, and validation becomes a major bottleneck. Furthermore, the diverse nature of IoT devices, ranging from low-power sensors to resource-intensive gateways, necessitates tailored PKI solutions that can cater to varying processing capabilities and network bandwidth constraints. Efficient certificate management techniques, such as hierarchical certificate authorities (CAs) and delegated trust models, are crucial for distributing the workload and reducing the burden on a central CA. Novel approaches like lightweight certificate formats and optimized cryptographic algorithms are also essential for minimizing resource consumption on constrained devices.

Trust management and certificate revocation are equally critical concerns in IoT PKI. Establishing and maintaining trust in a vast network of interconnected devices requires robust mechanisms for verifying the

authenticity and integrity of certificates. The compromise of a single device can potentially jeopardize the security of the entire network, making timely and effective certificate revocation paramount. However, traditional certificate revocation lists (CRLs) can be impractical for IoT due to their size and the limited bandwidth available to many devices. Alternative revocation methods, such as Online Certificate Status Protocol (OCSP) stapling and bloom filter-based revocation schemes, offer more efficient solutions for disseminating revocation information. Moreover, the dynamic nature of IoT environments, where devices may frequently join or leave the network, necessitates automated and scalable revocation processes that can adapt to changing conditions. The development of decentralized trust models and blockchain-based certificate management systems are also being explored as potential solutions for enhancing trust and resilience in IoT PKI.

Table 2: Characteristics and comparison of different trust management schemes.

Trust Management Scheme	*Key Characteristics*	*Advantages*	*Disadvantages*	Suitability for IoT
Hierarchical Certificate Authorities (CAs)	*Organizes CAs in a tree-like structure, with a root CA at the top and subordinate CAs below. Each CA certifies the CAs below it.*	*Scalability due to distributed workload, simplified certificate management, efficient certificate issuance and revocation within sub-domains.*	*Single point of failure at the root CA, complexity in configuring and managing the hierarchy.*	Well-suited for large-scale IoT deployments where device groups can be managed by different subordinate CAs.
Delegated Trust Models	*Transfers trust authority from a central entity to other entities, allowing them to issue certificates or make trust decisions on behalf of the central entity.*	*Reduced burden on the central authority, increased flexibility and agility in trust management, improved scalability.*	*Requires careful design to prevent abuse of delegated authority, potential for trust delegation loops, needs robust access control.*	Suitable for IoT environments with diverse device types and varying trust requirements, allowing localized trust management.
Certificate Revocation Lists (CRLs)	*Lists revoked certificates, which clients check before trusting a certificate.*	*Simple and widely supported, direct indication of revoked certificates.*	*Large size, high bandwidth consumption, latency in updating CRLs, not ideal for resource-constrained devices.*	Less suitable for bandwidth-constrained IoT devices but can be used if combined with techniques like delta CRLs.
Online Certificate Status Protocol (OCSP) Stapling	*The server presents the OCSP response along with the certificate during the TLS handshake.*	*Reduces the load on OCSP responders, improves client privacy, real-time revocation status verification.*	*Requires server-side configuration and support, increased server-side processing, potential for server-side performance bottlenecks.*	Good choice for IoT servers with sufficient resources to perform stapling but not appropriate for constrained clients.
Bloom Filter-Based Revocation Schemes	*Uses Bloom filters to represent revoked certificates, allowing for probabilistic membership testing.*	*Compact representation of revoked certificates, low bandwidth consumption, faster revocation checks compared to CRLs.*	*Probability of false positives (reporting a valid certificate as revoked), requires careful parameter tuning.*	Well-suited for bandwidth-constrained IoT devices that need to efficiently check for certificate revocation.
Blockchain-Based Certificate Management	*Uses a decentralized blockchain to store and manage certificates and revocation information.*	*Increased transparency and auditability, enhanced security against tampering, improved resilience against single points of failure.*	*Higher computational overhead, challenges in achieving consensus, scalability limitations, regulatory concerns.*	Emerging solution with potential for enhancing trust and resilience in IoT PKI, particularly in decentralized environments.

5. Emerging Authentication Technologies

5.1 Physical Unclonable Functions (PUFs)

Physical Unclonable Functions (PUFs) offer a promising hardware-based approach to device identity authentication. They leverage inherent, random variations in the physical microstructure of integrated circuits that arise during manufacturing. These variations, which are uncontrollable and unique to each device, serve as a fingerprint. When challenged with a specific input, a PUF generates a unique and unpredictable output, known as the response. This challenge-response pair (CRP) forms the basis for authentication.

Several types of PUFs exist, including arbiter PUFs, ring oscillator PUFs, and SRAM PUFs. Arbiter PUFs rely on manufacturing variations in the delays of nominally identical paths. Ring oscillator PUFs exploit frequency differences between nominally identical ring oscillators. SRAM PUFs utilize the unpredictable power-up state of SRAM cells.

Advantages of PUFs include their inherent resistance to cloning, as replicating the exact physical characteristics is extremely difficult. They also eliminate the need for storing secret keys in memory, reducing vulnerability to software attacks. However, PUFs can be sensitive to environmental conditions like temperature and voltage, which can affect the reliability of the responses. Additionally, some PUF designs may exhibit limited CRP space or susceptibility to modeling attacks, requiring careful design and implementation. The reliability of a PUF is often quantified by its bit error rate (BER), which represents the probability of an incorrect output for a given challenge. A lower BER indicates higher reliability.

5.2 Blockchain-Based Authentication

Blockchain technology offers a promising avenue for decentralized and secure IoT device identity management and authentication. Its inherent characteristics, such as immutability, transparency, and distributed consensus, address several vulnerabilities present in traditional centralized authentication systems. By leveraging a blockchain, each IoT device can be assigned a unique identity stored as a transaction on the chain. This creates a tamper-proof record of device registration and ownership.

Authentication processes can then be built upon this foundation. For instance, a device requesting access to a network or service can present its identity, which is verified against the blockchain. Smart contracts can automate this verification process, enforcing pre-defined access control policies based on device attributes or roles. The decentralized nature of the blockchain eliminates the single point of failure associated with centralized servers, enhancing resilience against attacks. Furthermore, the cryptographic security of blockchain ensures that device identities and authentication credentials are protected from unauthorized access and manipulation. The use of hash functions like SHA-256 ensures data integrity, where any alteration to the device data will result in a different hash value, immediately revealing tampering. This approach enhances trust and security in IoT ecosystems, particularly in scenarios involving numerous devices and sensitive data.

5.3 Other Promising Technologies

Beyond the aforementioned techniques, several other promising authentication methods are emerging for IoT devices. Device fingerprinting, for instance, leverages inherent hardware and software characteristics to create a unique identifier for each device. This fingerprint, composed of attributes like clock skew, radio frequency variations, and software configurations, can be used to verify device identity without relying on traditional credentials. The robustness of device fingerprinting lies in the difficulty for an attacker to replicate these subtle, device-specific traits.

Biometric authentication, commonly used in smartphones, is also being explored for IoT devices, particularly those with human interaction capabilities. This could involve voice recognition for smart speakers, facial recognition for security cameras, or even gait analysis for wearable devices. The challenge lies in adapting these techniques to resource-constrained IoT environments and ensuring the privacy of sensitive biometric data. Factors such as computational cost (C) and energy consumption (E) must be carefully considered, minimizing the ratio C/E to ensure feasibility. Furthermore, research into behavioral biometrics, which analyzes patterns in device usage, offers a non-intrusive approach to continuous authentication, enhancing security throughout the device's lifecycle.

Table 3: Comparison of Authentication Latency for Blockchain vs Traditional Methods.

Feature	Traditional Centralized Authentication	Blockchain-Based Authentication
Network Dependency	Limited dependency - authentication server handles most processing. Lower latency if network is reliable.	High dependency - authentication requires network consensus. Latency can be affected by network congestion and confirmation times.
Computational Complexity	Lower - Generally involves simple password or key comparisons on the authentication server.	$O(n)$ Computational - Involves cryptographic operations (hashing, signature verification) and smart contract execution, which are more computationally intensive. (n = number of devices)
Data Lookup	Fast - Data stored in a central, readily accessible database.	Can take longer-$O(\log n)$ - Requires querying the distributed ledger; can be slower depending on block size and consensus mechanism. (n = number of blocks in ledger)
Trust Model	Relies on trust in a single authority (central server). Susceptible to single-point-of-failure attacks.	Distributed trust; consensus mechanism ensures data integrity. More resilient to attacks.
Typical Latency (Approximate)	Milliseconds (e.g., 1-10 ms)	Seconds (e.g.,1-10 s) depending on the blockchain and network conditions
Scalability	Scalability can be limited by the central server's capacity. Additional servers can add complexity.	Limited by the consensus mechanism and block creation time. Sharding and other techniques improve it.
Latency Factors (Latency depends on)	Server processing and Network latency	Block Size, Confirmation Times, Consensus Mechanism,Smart Contract

6. Comparison and Challenges

6.1 Comparative Analysis

A comprehensive comparison of IoT device authentication technologies reveals distinct trade-offs across several key attributes. Pre-shared keys (PSKs), while simple to implement, suffer from poor scalability and security vulnerabilities, especially when a key is compromised. Public key infrastructure (PKI) offers stronger security through digital certificates and cryptographic algorithms like RSA and ECC, but introduces higher computational overhead and complexity in certificate management. Lightweight authentication protocols, such as those based on Physically Unclonable Functions (PUFs), present a promising alternative by leveraging unique device hardware characteristics for authentication, reducing reliance on complex cryptographic operations. However, PUF-based schemes can be susceptible to modeling attacks and environmental variations, impacting reliability. Blockchain-based authentication provides a decentralized and tamper-proof approach, improving security and trust. However, the performance overhead associated with blockchain transactions can be a limiting factor, particularly for resource-constrained devices. The cost implications also vary significantly, with PSKs being the least expensive and PKI and blockchain solutions incurring higher costs due to infrastructure and computational requirements. Scalability is another critical factor, where PSKs struggle with large deployments, while PKI and blockchain offer better scalability with proper design. The selection of an appropriate authentication technology depends heavily on the specific application requirements, considering the balance between security, performance, scalability, and cost.

Table 4: Comparison of Various IoT Authentication Technologies.

Feature	PSK	PKI	PUF	Blockchain
Security	Low	High	Medium	High
Performance	High	Medium	High	Low
Scalability	Low	High	Medium	High
Cost	Low	High	Medium	High
Complexity	Low	High	Medium	High
Key Management	Simple	Complex	Simple	Decentralized
Vulnerabilities	Key Compromise	Certificate Revocation, DoS	Modeling Attacks, Environmental Sensitivity	Transaction Overhead, Scalability Issues

6.2 Open Challenges and Research Gaps

IoT device identity authentication, despite advancements, faces several open challenges and research gaps. Interoperability remains a significant hurdle. The diverse ecosystem of IoT devices, utilizing varying communication protocols and security standards, makes seamless authentication across different platforms difficult. Standardized authentication protocols and frameworks are needed to ensure devices from different manufacturers can securely interact.

Lifecycle management of device identities presents another challenge. IoT devices often have long lifespans, during which their security requirements may evolve. Secure mechanisms for updating authentication credentials, revoking compromised identities, and decommissioning devices are crucial. Research is needed to develop efficient and scalable identity management solutions that can adapt to the dynamic nature of IoT deployments.

Furthermore, IoT devices are increasingly vulnerable to sophisticated attacks. Traditional authentication methods may not be sufficient to withstand advanced threats such as side-channel attacks, fault injection attacks, and machine learning-based attacks. Lightweight and robust authentication schemes are required that can provide strong security guarantees while minimizing resource consumption. Exploring the application of emerging technologies like blockchain and federated learning for enhanced security and privacy in IoT authentication is also a promising research direction. The resilience of authentication mechanisms against physical attacks, especially in resource-constrained devices, warrants further investigation. Addressing these challenges is crucial for building a secure and trustworthy IoT ecosystem.

7. Future Perspectives and Conclusion

7.1 Future Research Directions

Future research in IoT device identity authentication should prioritize several key areas to address the evolving threat landscape and inherent limitations of current methods. Adaptive authentication mechanisms, capable of dynamically adjusting security levels based on contextual factors such as device location, network conditions, and user behavior, present a promising avenue. This involves developing algorithms that can efficiently analyze real-time data streams and trigger appropriate authentication protocols, minimizing disruptions for legitimate users while effectively thwarting malicious actors.

Furthermore, privacy-preserving authentication techniques are crucial, particularly in sensitive IoT applications like healthcare and smart homes. Research should focus on employing cryptographic methods like zero-knowledge proofs and homomorphic encryption to enable device authentication without revealing sensitive user data or device characteristics. The challenge lies in balancing strong security with minimal computational overhead, ensuring feasibility for resource-constrained IoT devices.

Finally, the integration of Artificial Intelligence (AI) and Machine Learning (ML) offers significant potential for enhancing IoT security. AI-based solutions can be developed to detect anomalous device behavior, identify sophisticated attack patterns, and automate threat response. For instance, ML models can be trained on vast datasets of network traffic and device logs to distinguish between legitimate and malicious activities, even in the presence of evolving attack strategies. However, research must also address the potential vulnerabilities of AI-based security systems themselves, such as adversarial attacks and data poisoning, to ensure their robustness and reliability. The exploration of federated learning, where models are trained locally on devices without sharing raw data, can also improve privacy and scalability.

7.2 Conclusion

In summary, this review has highlighted the critical role of robust identity authentication in securing the rapidly expanding Internet of Things ecosystem. We have examined the prevalent authentication mechanisms, ranging from pre-shared keys and cryptographic approaches to emerging biometric and blockchain-based solutions, noting their respective strengths and weaknesses in the context of IoT's unique constraints. Our analysis reveals that while significant progress has been made, a universal, scalable, and energy-efficient authentication solution remains elusive. The trade-off between security, computational overhead, and resource limitations continues to be a central challenge.

Looking ahead, the future of IoT device identity authentication will likely be shaped by several key trends. We anticipate increased adoption of lightweight cryptographic algorithms and hardware-based security modules to enhance security without compromising performance. Furthermore, the integration of artificial intelligence and machine learning techniques for anomaly detection and adaptive authentication promises to provide a more dynamic and resilient security posture. Finally, standardization efforts and collaborative initiatives are crucial for fostering interoperability and establishing trust across diverse IoT deployments. Addressing these challenges and capitalizing on these emerging trends will be essential for realizing the full potential of a secure and trustworthy IoT landscape. The ongoing research and development in this field are vital for building a future where billions of interconnected devices can operate safely and reliably.

References

[1] H. Kim and E. A. Lee, "Authentication and Authorization for the Internet of Things," IT Professional, vol. 19, no. 5, pp. 27-33, 2017.

[2] Z. A. Alizai, N. F. Tareen, and I. Jadoon, "Improved IoT device authentication scheme using device capability and digital signatures," in 2018 International Conference on Applied and Engineering Mathematics (ICAEM), 2018, pp. 1-5.

[3] B. Kim, S. Yoon, Y. Kang, and D. Choi, "Puf based iot device authentication scheme," in 2019 International Conference on Information and Communication Technology Convergence (ICTC), 2019, pp. 1460-1462.

[4] T. Nandy, M. Y. I. B. Idris, R. M. Noor, L. M. Kiah, L. S. Lun, N. B. A. Juma'at, et al., "Review on security of internet of things authentication mechanism," IEEE Access, vol. 7, pp. 151054-151089, 2019.

[5] J. R. Wallrabenstein, "Practical and secure IoT device authentication using physical unclonable functions," in 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), 2016, pp. 99-106.

[6] M. Liyanage, A. Braeken, P. Kumar, and M. Ylianttila, Eds., IoT security: Advances in authentication. John Wiley & Sons, 2020.

[7] Y. Sharaf-Dabbagh and W. Saad, "On the authentication of devices in the Internet of Things," in 2016 IEEE 17th International Symposium on A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2016, pp. 1-3.

[8] Ali, S. Sabir, and Z. Ullah, "Internet of things security, device authentication and access control: a review," arXiv preprint arXiv:1901.07309, 2019.

[9] Y. Atwady and M. Hammoudeh, "A survey on authentication techniques for the internet of things," in Proceedings of the international conference on future networks and distributed systems, 2017.

[10] M. El-Hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "A survey of internet of things (IoT) authentication schemes," Sensors, vol. 19, no. 5, 1141, 2019.

[11] S. Miri Kelaniki and N. Komninos, "A Study on IoT Device Authentication Using Artificial Intelligence," Sensors, vol. 25, no. 18, 5809, 2025.

[12] Lucia, B. Isong, N. Gasela, and A. M. Abu-Mahfouz, "Device authentication schemes in IoT: a review," in 2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC), 2019, pp. 1-6.

Funding

This research received no external funding.

Conflicts of Interest

The authors declare no conflict of interest.

Acknowledgment

This paper is an output of the science project.