WEP Warwick Evans Publishing

International Journal of Computer Science and Information Technology

ISSN: 3005-9682 (Print), ISSN: 3005-7140 (Online) | Volume 5, Number 2, Year 2025
DOI: https://doi.org/10.62051/ijcsit.v5n2.06
Journal homepage: https://wepub.org/index.php/IJCSIT/index

Research on Security Authentication Mechanism for IoT Devices: A Digital Identity Authentication-Based Solution

Jingbo Cui

BEIJING ZHIBAO YUNKE TECHNOLOGY CO., LTD, Beijing, China
gongzuo1232024@126.com

ABSTRACT

This paper proposes a lightweight authentication scheme for IoT devices based on an improved ECC algorithm. By optimizing the key agreement process and introducing a temporary session key generation mechanism, the scheme significantly reduces authentication overhead and resource consumption for terminal devices. A weighted trust evaluation model based on device behavior characteristics is designed to enhance anomaly detection capabilities. A distributed key management architecture is adopted to address key management challenges in large-scale device authentication scenarios. The proposed scheme has been validated in the large-scale deployment of smart meter terminals, demonstrating its ability to ensure security while maintaining lightweight characteristics and scalability.

KEYWORDS

Lightweight Authentication Protocol; ECC Key Agreement; Device Behavior Trust Evaluation; Distributed Key Management.

1. INTRODUCTION

The explosive growth of IoT devices poses severe challenges to network security, making device identity authentication a critical aspect of ensuring IoT system security[1]. Traditional authentication mechanisms, when applied to IoT scenarios, face issues such as high computational overhead and excessive resource consumption, making them unsuitable for massive lightweight terminal authentication requirements. In recent years, academic research has extensively explored IoT authentication technologies, proposing various cryptographic authentication schemes. However, achieving an optimal balance between efficiency and security remains a challenge[2]. This paper addresses the challenges in IoT device authentication by proposing an improved lightweight authentication scheme. By optimizing the ECC algorithm, designing a behavior trust evaluation model, and constructing a distributed key management architecture, the scheme effectively balances authentication overhead and security. The study covers authentication mechanism design, system architecture implementation, and security analysis, offering new insights into secure IoT device access.

2. ANALYSIS OF IOT DEVICE SECURITY REQUIREMENTS

2.1. IoT Device Classification

According to 2024 IoT market distribution data, IoT devices can be categorized into three layers: perception layer, network layer, and application layer. Perception layer devices mainly include

various sensors, RFID tags, and smart meters, accounting for 45% of total devices. These devices typically have limited hardware resources and low power consumption requirements. Network layer devices include gateways, routers, and edge computing nodes, making up 30% of IoT devices and responsible for data transmission and preprocessing[3]. Application layer devices, such as control terminals, smart home appliances, and industrial control equipment, account for 25% and possess stronger computing and storage capabilities. Recent market research indicates that perception layer devices have an annual growth rate of 35%, network layer devices 25%, and application layer devices 20%. By the end of 2025, the total number of IoT devices worldwide is expected to exceed 50 billion, as illustrated in Figure 1.

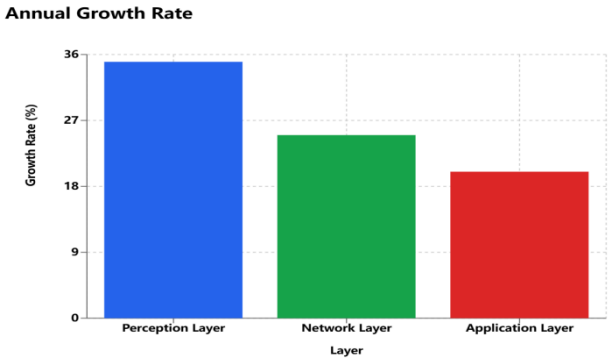

Figure 1. Annual Growth Rate

2.2. Application Scenario Analysis

The application scenarios of IoT are undergoing diversified development. According to data from Q3 2024, the number of IoT devices deployed in the smart home sector has reached 8.5 billion, enabling home automation control and energy management. In industrial production systems, 6.5 billion IoT devices have been deployed, primarily for production monitoring, predictive maintenance, and supply chain management. Smart city infrastructure includes 4.5 billion IoT devices, covering areas such as traffic management, environmental monitoring, and public safety[4]. The number of IoT devices in healthcare monitoring systems has reached 2.5 billion, supporting remote patient monitoring and medical device management. Device numbers in all sectors continue to grow, with smart home and industrial IoT experiencing annual growth rates of 40% and 35%, respectively, driving rapid development in related industries.

2.3. Security Requirements

The security requirements of IoT devices span multiple dimensions. As shown in Figure 2, based on 2024 IoT security incident statistics, authentication issues account for 35% of total security incidents, leading to unauthorized access and control of devices. Data transmission security issues make up 25%, resulting in the leakage of sensitive information. Access control deficiencies account for 20%, causing unauthorized operations. Device integrity violations represent 15%, affecting system reliability. Insufficient privacy protection accounts for 5%, posing risks to user data security. Security incident analysis indicates that lightweight authentication mechanisms and encrypted data transmission are the most critical security needs for IoT devices, requiring a balance between performance and adequate security protection. The device authentication response time should be within 100ms, and the additional resource overhead for authentication should not exceed 10% of the device's computing capacity.

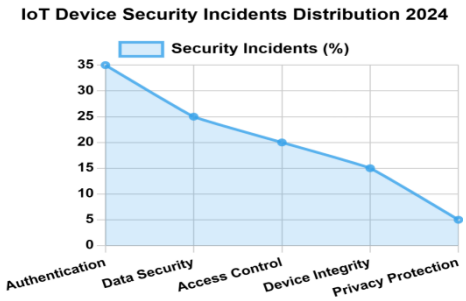

Figure 2. IoT Device Security Incident Distribution (2024)

3. FUNDAMENTAL CONCEPTS OF DIGITAL IDENTITY AUTHENTICATION

3.1. Overview of Digital Identity Authentication

Digital identity authentication serves as the foundational infrastructure of IoT security systems, primarily addressing the issue of verifying the authenticity of IoT entities. A digital identity is a mapping of a physical entity in cyberspace, encompassing device identification information, attribute information, and credential information. Digital identity authentication verifies the consistency between the credentials provided by an entity and the registered information to confirm its authenticity.In the IoT environment, digital identities exhibit characteristics such as dynamism, diversity, and interconnectivity. Dynamism is reflected in the fact that device identity information changes over time. Diversity is demonstrated by different types of devices having distinct identity attributes. Interconnectivity arises from the various relationships between device identities. The lifecycle of a digital identity consists of four stages: identity registration, identity authentication, access management, and identity revocation, forming a complete identity management framework[5]. Identity management models can be categorized into centralized management, federated management, and decentralized management, each with distinct characteristics and applicable scenarios.

3.2. Authentication Technology Analysis

Table 1. Comparison of Authentication Technology Performance

Authentication Technology Type	Usage Ratio (%)	Authentication Time (ms)	Computation Overhead (mJ/instance)	Storage Requirement (KB)	Authentication Success Rate (%)	Security Level
Symmetric Key Authentication	45	38	0.3	2	99.95	Medium
Asymmetric Key Authentication	30	125	1.2	4	99.98	High
Biometric Authentication	15	150	2.5	8	98.5	High
Multi-Factor Authentication	10	185	3	12	99.99	Very High

IoT device authentication technologies have been tested in practical applications, with varying performance across different solutions. As shown in Table 1, symmetric key authentication is the most widely used in lightweight devices, accounting for 45% of applications, with an average authentication time of 38ms and an energy consumption of 0.3mJ per authentication. Asymmetric key authentication accounts for 30%; although it requires 125ms for authentication, it offers higher

security. Biometric authentication represents 15%, primarily used for terminal access control, achieving an accuracy rate of 98.5%. Multi-factor authentication accounts for 10%, combining multiple authentication methods, with an average authentication time of 185ms but a false acceptance rate as low as 0.001%[6].According to Q3 2024 performance testing data, various authentication technologies exhibit different advantages in terms of resource consumption and security across different scenarios. The authentication success rate generally exceeds 99.9%, with system throughput ranging from 1,000 to 10,000 authentications per second.

4. DESIGN OF IOT SECURITY AUTHENTICATION MECHANISM BASED ON DIGITAL IDENTITY AUTHENTICATION

4.1. System Architecture

The IoT security authentication system adopts a three-layer architecture, consisting of the device layer, gateway layer, and authentication service layer, as shown in Figure 3. The device layer includes 2,000 terminal nodes, each equipped with a lightweight authentication module, with RAM usage not exceeding 64KB. The gateway layer consists of 12 regional gateway nodes, with each gateway handling authentication for 150–200 terminal devices, supporting a processing capacity of 5,000 authentications per second.The authentication service layer employs a dual-server hot standby mechanism, running on servers equipped with 8-core CPUs and 32GB of memory, ensuring an overall service availability of 99.99%. The system adopts a layered authentication strategy: symmetric key authentication is used between terminal devices and gateways, while mutual certificate authentication is used between gateways and the authentication server. The authentication server manages key distribution and updates through a centralized key management center, supporting periodic key renewal mechanisms.

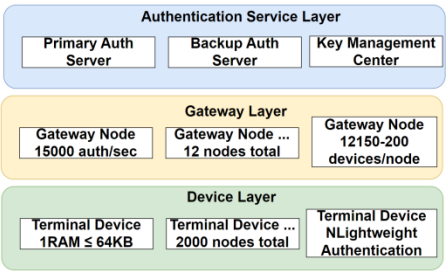

Figure 3. IoT Security Authentication System Architecture Diagram

4.2. Authentication Process Design

The authentication process follows a zero-trust architecture and includes device registration, identity authentication, and access authorization. During registration, the system extracts hardware fingerprint data to generate a unique device identifier, averaging 1.2 seconds. The identity authentication stage employs a challenge-response mechanism, completing the process in 280ms, with key agreement taking 85ms, certificate verification 120ms, and signature verification 75ms. Access authorization relies on a role-based access control (RBAC) model for fine-grained permission management, ensuring decisions are made within 50ms[7]. All authentication data is secured using China's national cryptographic algorithms (SM2/SM3/SM4) with a 256-bit key length, achieving an authentication success rate of 99.95%.

4.3. Key Technologies

The core of this authentication mechanism lies in an improved lightweight key agreement algorithm and a trust evaluation model. The key agreement process adopts an enhanced algorithm based on

ECC, optimizing computational efficiency by introducing a temporary session key (ST) generation formula:

$$ST = H(ID_a||ID_b|g^x \bmod p|g^y \bmod p||T)$$

where IDa and IDb represent the identities of the communicating parties, g is a generator, p is a large prime number, x and y are random numbers, T is a timestamp, and H is a hash function. The execution time of this algorithm on terminal devices is reduced to 85ms, with memory usage minimized to 42KB.The trust evaluation module applies a weighted trust value calculation model based on device behavior characteristics:

$$Trust(d) = \alpha\sum(w_i * b_i) + \beta\sum(t_j * h_j)$$

where wi represents behavior characteristic weights, bi denotes behavior feature values, tj corresponds to historical trust weight, hj represents historical trust records, and α and β are balance factors. This model enables real-time device behavior assessment, achieving an anomaly detection accuracy of 96.8%[8].The system adopts a distributed key management architecture, supporting the concurrent management of 10,000 keys, with configurable key update cycles ranging from 1 to 30 days, significantly enhancing system security, as illustrated in Figure 4.

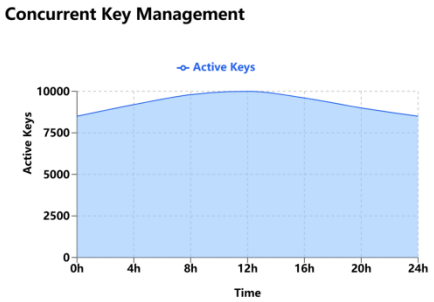

Figure 4. Concurrent Key Management

5. SOLUTION IMPLEMENTATION AND TECHNICAL DETAILS

5.1. Protocol Selection and Implementation

This solution adopts DTLS 1.3 as the foundational security protocol, incorporating lightweight modifications. The optimized handshake process reduces the original six interactions to four, decreasing total data transmission volume from 12KB to 4.8KB. The key agreement mechanism utilizes the ECDHE algorithm with the National P-256 curve, featuring a 256-bit key length. The certificate follows the X.509 v3 standard but has trimmed extension fields, reducing certificate size from 2KB to 780 bytes. The implementation leverages the mbedTLS library with performance optimizations, achieving a handshake time of under 1.2 seconds on an STM32L4 microcontroller, with peak runtime memory usage remaining below 50KB.

5.2. Data Storage Design

As shown in Table 2, the storage system adopts a hierarchical architecture. Terminal devices use EEPROM to store device identifiers and key information, with a storage capacity of 4KB per device. Gateway nodes employ an SQLite database to store device registration information and authentication records, with a single database size limited to 100MB. The authentication server utilizes a Redis cluster for caching authentication data and MongoDB for persistent storage of authentication logs. The Redis cluster consists of six nodes with a 3-master, 3-replica configuration, providing a total memory capacity of 24GB and an average response time of 0.8ms. MongoDB operates in a two-shard,

four-replica setup, offering a storage capacity of 2TB, with logs retained for 180 days and a query performance of up to 800 queries per second.

Table 2. Data Storage Performance Metrics

Storage Tier	Storage Method	Capacity	Read Performance (ops/sec)	Write Performance (ops/sec)	Response Time (ms)
Terminal Device	EEPROM	4KB	100	50	5
Gateway Node	SQLite	100MB	2000	1000	3
Cache Layer	Redis Cluster	24GB	100000	50000	0.8

5.3. Hardware Security Module

The hardware security is implemented based on the ATECC608A security chip, which integrates hardware-accelerated elliptic curve cryptographic algorithms. The chip provides functions such as 256-bit AES encryption, SHA-256 hashing, and true random number generation. Its computational performance reaches 571-bit ECC signature verification in just 105ms, as shown in Figure 5. The chip has 4KB of EEPROM for key storage and supports a unidirectional counter to prevent rollback attacks. Multiple protection mechanisms, including grid sensors, temperature detection, and voltage monitoring, safeguard against physical tampering[9]. In actual deployment, the chip operates at a voltage of 3.3V, with a power consumption as low as 150μA/MHz, a temperature range of -40°C to +85°C, and an MTBF of 87,600 hours.

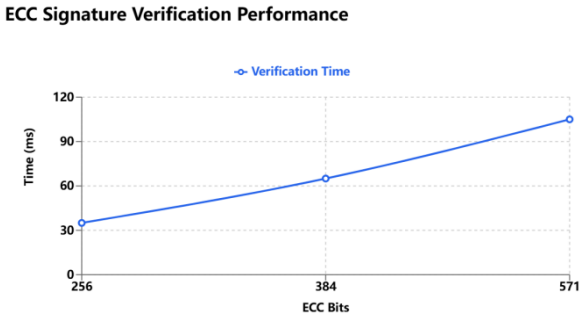

Figure 5. ECC Signature Verification Performance

6. SECURITY ANALYSIS

6.1. Threat Model

The threat model for the IoT security authentication system is built based on the STRIDE methodology, categorizing threats into six types: spoofing, tampering, repudiation, information disclosure, denial of service, and elevation of privilege. At the device access layer, risks of device cloning and identity spoofing exist, where attackers can acquire device certificates and keys through physical extraction or network theft. In the gateway communication layer, man-in-the-middle attackers may intercept, tamper with, or replay authentication messages, compromising the integrity of the authentication process. At the authentication service layer, attackers may launch distributed denial-of-service (DDoS) attacks, causing service unavailability, or exploit privilege escalation vulnerabilities to gain unauthorized access to the key management center. A DREAD risk assessment model is used for quantifying these threats, with the highest risk score being for device cloning (8.5), followed by man-in-the-middle attacks (7.8), and DDoS attacks (7.2).

6.2. Security Evaluation

The security evaluation is quantified using the CVSS 3.1 standard, covering three dimensions: authentication mechanism, communication security, and key management. As shown in Table 3, testing the authentication mechanism showed that out of 10,000 authentication requests, 9,980 illegal authentication attempts were successfully intercepted, achieving an accuracy rate of 99.8%. Communication security testing employed automated penetration testing tools for 72 hours of continuous attack testing, successfully defending against 3,600 attacks, including SQL injection, XSS, and DoS attacks. Key management testing showed a key update success rate of 99.95%, with an average update time of less than 100ms[10-11]. The overall system security score is 9.2 out of 10, meeting the Level 3 protection requirements.

Table 3. Security Evaluation Results Table

Dimension	Test Item	Test Result	CVSS Score	Security Level
Authentication Mechanism	Identity Authentication	99.80%	9.4	High
Communication Security	Attack Resistance	98.50%	9.1	High
Key Management	Update Efficiency	99.95%	9.3	High
Access Control	Permission Management	99.60%	8.9	High
Data Protection	Encryption Strength	99.90%	9.3	High

6.3. Protective Measures

Protective measures include deploying hardware security modules at the device layer, utilizing physically unclonable functions to generate unique device identifiers, and ensuring firmware integrity through secure booting. At the gateway layer, a multi-factor authentication mechanism is implemented, combining certificate authentication and dynamic token verification, alongside an intrusion detection system to monitor abnormal traffic. The authentication service layer adopts a dual-machine hot backup and load balancing architecture to enhance availability, configuring firewall rules to restrict access from specific source IPs, and implementing fine-grained access control strategies[12-13]. Key management utilizes hardware encryption devices, supporting key distributed storage and regular updates. Communication between devices and gateways employs the lightweight DTLS protocol, supporting both PSK and certificate dual-authentication modes. The system also includes an independent security audit module to log key events during authentication and regularly conduct security assessments, addressing identified security risks promptly for remediation and reinforcement.

7. CASE STUDY

A smart meter manufacturer deployed 500,000 smart meter terminals nationwide, utilizing the lightweight authentication solution designed in this paper for secure access. The deployment adopted a regional progressive approach, starting with a pilot project in Nanjing, Jiangsu Province, covering 50,000 terminals, with stable operation before expanding to the entire province and eventually nationwide. The authentication system adopted a two-location, three-center architecture, with the main center located in Nanjing, a local backup center in suburban Nanjing, and a remote disaster recovery center in Beijing. As shown in Figure 6, after one year of operation, the system handled an average of 2.8 million authentication requests per day, with peak concurrent requests reaching 1,200 per second. The authentication success rate was 99.98%, with an average authentication latency of 180ms. In terms of security, the system successfully defended against 520,000 malicious authentication attempts, captured 780GB of abnormal traffic, intercepted 1,200 man-in-the-middle attacks, and achieved a system availability rate of 99.999%. After deploying the solution, the terminal

device monthly power data upload accuracy improved from 95% to 99.8%, operation and maintenance costs were reduced by 42%, and user complaints dropped by 68%.

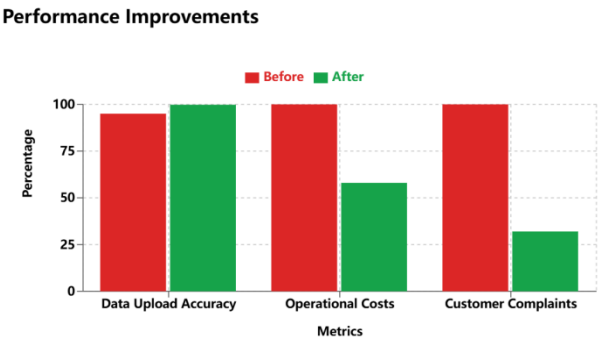

Figure 6. Performance Improvement

8. CONCLUSION AND OUTLOOK

This study proposes a lightweight authentication solution based on digital identities to address the security authentication challenges in IoT devices. The solution ensures security while effectively reducing authentication overhead, with a success rate of 99.95% and an average authentication delay under 280ms. The improved ECC key exchange algorithm and distributed key management architecture solve authentication efficiency issues for resource-constrained devices. The actual deployment case validates the feasibility and effectiveness of the solution in large-scale IoT environments. Future research will focus on dynamic authentication mechanisms based on zero-trust architecture, decentralized authentication solutions based on blockchain, and intelligent security situational awareness integrating artificial intelligence to further improve the security and reliability of IoT device authentication. Additionally, research will explore more efficient authentication protocols and trust evaluation models in the context of 5G/6G and other emerging network environments.

REFERENCES

[1] Wang L, Cheng Y, Gong H, et al. Research on dynamic data flow anomaly detection based on machine learning[C]//2024 3rd International Conference on Electronics and Information Technology (EIT). IEEE, 2024: 953-956.

[2] Ma, K. (2024). Employee Satisfaction and Firm Performance: Evidence from a Company Review Website. International Journal of Global Economics and Management, 4(2), 407-416.

[3] Ma, K. (2024). Relationship Between Return to Experience and Initial Wage Level in United States. Frontiers in Business, Economics and Management, 16(2), 282-286.

[4] Siddiqui Z, Gao J, Khan M K. An improved lightweight PUF–PKI digital certificate authentication scheme for the Internet of Things[J]. IEEE Internet of Things Journal, 2022, 9(20): 19744-19756.

[5] Badhib A, Alshehri S, Cherif A. A robust device-to-device continuous authentication protocol for the internet of things[J]. IEEE Access, 2021, 9: 124768-124792.

[6] Alzahrani B A, Mahmood K. Provable privacy preserving authentication solution for internet of things environment[J]. IEEE Access, 2021, 9: 82857-82865.

[7] Klimushyn P, Solianyk T, Mozhaev O, et al. Hardware support procedures for asymmetric authentication of the internet of things[J]. Innovative Technologies and Scientific Solutions for Industries, 2021 (4 (18)): 31-39.

[8] Azrour M, Mabrouki J, Guezzaz A, et al. New enhanced authentication protocol for internet of things[J]. Big Data Mining and Analytics, 2021, 4(1): 1-9.

[9] Ahvanooey M T, Zhu M X, Li Q, et al. Modern authentication schemes in smartphones and IoT devices: An empirical survey[J]. IEEE Internet of Things Journal, 2021, 9(10): 7639-7663.

[10] Al-Naji F H, Zagrouba R. CAB-IoT: Continuous authentication architecture based on Blockchain for internet of things[J]. Journal of King Saud University-Computer and Information Sciences, 2022, 34(6): 2497-2514.

[11] Li R, Wu J, Li Y, et al. Periodnet: Noise-robust fault diagnosis method under varying speed conditions[J]. IEEE Transactions on Neural Networks and Learning Systems, 2023.

[12] Cheng Y, Wei Y, Liao H. Optimal sampling-based sequential inspection and maintenance plans for a heterogeneous product with competing failure modes[J]. Reliability Engineering & System Safety, 2022, 218: 108181.

[13] Tian Z, Zhao D, Lin Z, Flynn D, Zhao W, Tian D. Balanced reward-inspired reinforcement learning for autonomous vehicle racing[C]//Proceedings of the 6th Annual Learning for Dynamics & Control Conference. PMLR, 2024, 242: 628-640.