Enterprise Internal Threat Authentication Traceability Technology Based on Key Authentication System

Jian Hu[1,2,*], Wei Wu[1], Tao Chuan[1] and Qiuxia Peng[1]

[1]*China Southern Power Grid Yunnan Power Grid Co., Ltd. Information Center, Yunnan, 650217, China*
[2]*School of Computer Science and Engineering, South China University of Technology, Guangzhou, 510006, China*
E-mail: csghujian@126.com
[*]*Corresponding Author*

Received 06 May 2025; Accepted 19 June 2025

Abstract

In the current background of highly digitized enterprise information systems, insider threats have become the main source of risk for enterprise network security. This paper proposes an internal threat authentication and traceability technology based on a cryptographic key-based identity authentication system. By integrating asymmetric keys, behavior signatures, and log analysis, the system binds user identity with actions and enables full-process traceability. After deploying the system in a real enterprise environment, simulation tests show that the authentication system identifies malicious behaviors such as permission abuse, phishing attacks, and script injection with a success rate as low as 1.1% to 3.3%, effectively preventing such operations. At the same time, the success rate of normal user authentication is as high as 99.9%, reflecting its high reliability. Through behavior chain structure recording and abnormal behavior map identification mechanism, the

Journal of Cyber Security and Mobility, Vol. 14_3, 623–652.
doi: 10.13052/jcsm2245-1439.1435

system can trace malicious operation paths within seconds, greatly improving emergency response efficiency. After the system is deployed, the average data leaked by enterprises in information leakage incidents has dropped from 512MB to 37MB, effectively shortening the life cycle of the attack chain. The analysis of security return on investment shows that the integrated key authentication system can maintain a return rate of more than 60% under medium and high intensity investment, and has good economic benefits and popularization prospects.

Keywords: Key authentication system, insider threat traceability, chained behavioral signatures, information security, digital identity binding.

1 Introduction

Under the background of accelerating digital transformation, enterprises increasingly depend on information systems, and network security threats are becoming increasingly complex and hidden [1]. Traditional security protection methods mostly focus on external attacks. However, internal threats – such as malicious employee actions, credential misuse, and unauthorized access – are a major cause of frequent information security incidents. Internal threats are harder to detect due to legitimate access, posing serious risks to data and business continuity.

Among many internal threat incidents, difficulty tracing the source, difficulty proving evidence, and late early warning have become the main pain points in enterprise security governance [2]. The core of this problem lies in the lack of sufficient individual identification and non-repudiation in the current authentication mechanism, which makes it difficult to clarify the responsible subject even if the attack is discovered. Therefore, building an authentication system that can not only effectively authenticate users' identities but also have strong traceability capabilities for improving enterprises' ability to deal with internal threats is of great practical significance.

As the core technology in cryptography, the key authentication system plays a fundamental role in user identification and communication encryption [3]. By introducing public-private key pairs, digital signatures, and timestamp mechanisms, unique identification and verifiable records of operational behaviors can be realized without reducing the system's convenience [4]. Based on this, combined with log audit and behavior analysis mechanisms, key authentication can be extended to the full-process tracking and accurate positioning of threat behaviors, significantly improving

the traceability of security incidents and the clarity of responsibility attribution.

This paper proposes a technical framework for enterprise internal threat authentication and traceability based on a key authentication system. The framework integrates identity authentication, behavior signature, and multi-dimensional log integration analysis to realize the active identification and controllable tracking of internal threat behaviors. By establishing a full-chain trusted authentication mechanism, this article aims to provide enterprises with practical security enhancement solutions, improve their response efficiency and handling capabilities in the face of internal attacks, and build a more robust and traceable enterprise network security architecture that effectively addresses the complexity of internal threats.

The structure of this article is arranged as follows. Section 2 introduces the theoretical basis of key authentication and reviews relevant research. Section 3 introduces the current status of internal threat traceability technology in enterprises and identifies the existing limitations. Section 4 describes the experimental platform and evaluates the performance of the system through real-world simulations and comparative analysis. Section 5 summarizes the research findings of this article and outlines future research directions. To support the proposed framework, we first review the theoretical foundations and relevant research in key authentication systems, which form the basis for our design.

2 Theoretical Basis and Related Research

2.1 Basic Theory of Key Authentication System

Key authentication system is the core component of modern cryptography, which is mainly used to ensure identity authentication, data encryption and integrity verification in information transmission [5, 6]. According to the different ways of using keys, the system is generally divided into symmetric and asymmetric key authentication systems [7]. In the symmetric key system, both communicating parties use the same key for encryption and decryption operations, which has the advantages of high computing efficiency and simple implementation. Still, there are great challenges in key distribution and management. However, an asymmetric key system uses public and private keys for encryption and decryption, which has stronger security and scalability and is the foundation of most current identity authentication mechanisms.

The private key is used for the user's identity authentication and operation signature in the asymmetric key system. In contrast, the public key is used by other entities to verify the user's behavior, thus realizing a non-repudiation and integrity guarantee [8, 9]. Common key authentication mechanisms include digital signature technologies based on RSA, ECC, and other algorithms, which can effectively prevent identity forgery and data tampering and provide strong technical support for building a secure communication environment [10]. In addition, combining a timestamp and dynamic challenge-response mechanisms can further prevent replay attacks and improve the dynamic security of the authentication system.

The importance of key authentication systems in enterprise security systems has become increasingly prominent, especially in accurately tracing user operations [11]. By attaching signature information based on private key generation to each sensitive operation, enterprises can build a complete "identity-behavior-time" trinity trusted behavior chain. When an abnormality occurs in the system, or an internal threat occurs, the operating subject can be quickly located through signature verification, assisting in traceability and responsibility tracing and greatly enhancing enterprises' initiative in handling security incidents.

To efficiently deploy the key authentication system in the enterprise environment, it is necessary to solve practical problems such as complex key management, imperfect private key protection mechanisms, and multi-terminal collaborative authentication [12]. To this end, in recent years, researchers have continuously explored and innovated in key life cycle management, hardware-based key storage, and decentralized identity authentication combined with blockchain technology. Based on these theoretical bases and technological developments, this article will further build a key authentication system model suitable for enterprise internal threat authentication and traceability in subsequent chapters to provide theoretical support and technical paths for actual deployment.

2.2 Current Status of Enterprise Internal Threat Authentication and Traceability Technology of Key Authentication System

With the continuous evolution of network security threats, internal threats of enterprises have gradually become key hidden dangers in the information security system [13]. According to multiple security survey reports, more than one-third of security incidents stem from illegal operations or malicious behaviors by insiders, which often take advantage of their legitimate access

rights to the system and make traditional border protection measures difficult to detect. In response to this challenge, enterprises have gradually realized that they must strengthen management and control at the identity authentication and behavior traceability level to establish a more granular security monitoring and responsibility tracking mechanism.

In the existing practice, some enterprises have tried to introduce a key authentication system to replace the traditional username and password authentication method [14, 15]. Compared with weak passwords or shared accounts, key-based identity authentication can more effectively ensure the uniqueness of users' identities and improve the credibility of operational behaviors. However, this system still faces many challenges in its implementation, such as the untraceability after key leakage, the unperceptibility of the key usage process, and the lack of a unified audit mechanism linked to behavior logs, which leads to its internal threat traceability. Limited effect.

Currently, the enterprise security system mostly exists in isolated modules, and there is a lack of coordination mechanisms between the identity authentication system and the security audit system, making it difficult to effectively combine the authentication information with the follow-up behavior analysis [16]. In actual scenarios, even if digital signatures or multi-factor authentication methods are used, it is still difficult to achieve complete threat behavior restoration and accurate traceability if authentication records cannot be organically integrated with security logs, such as specific operation behaviors, access resources, and operation time. Therefore, how to open up the authentication and traceability chain and build a unified key-driven security incident audit system has become one of the core issues of research.

Some emerging technology directions, such as blockchain-based key authentication, multi-dimensional log fusion analysis platforms, and artificial intelligence-based abnormal behavior detection systems, are gradually being introduced into enterprise security construction [17, 18]. These technologies try to improve traceability capabilities while ensuring authentication security. However, they are still in the experimental or pilot stage and lack systematic, easy-to-deploy, and scalable general solutions [19]. Therefore, exploring an authentication traceability technology that deeply integrates the key authentication system with the enterprise intranet environment has important practical significance and provides a new technical path for improving the overall network security protection capability. Building upon the theoretical insights, we next examine the current state of internal threat traceability technologies in enterprises, highlighting the limitations and practical challenges that motivate our proposed model.

3 Establishment of Enterprise Internal Threat Authentication Traceability Model Based on Key Authentication System

3.1 Design of Threat Traceability Model Based on Key Authentication

In the security management of enterprise information systems, the identification and traceability of internal threats have always been a difficult problem in information security. Traditional means such as log analysis and access control have many limitations when faced with complex behaviors such as camouflage and permission abuse [20, 21]. To address these challenges, this paper proposes the Internal Threat Authentication and Tracing Model Based on Key System (ITAT-KS), a novel approach to traceability based on key authentication. Through strong binding of user identity, chain encryption of operation behavior, and key authentication of access trajectory, this model realizes accurate identification, responsibility tracing, and security audit of malicious behavior. The formula for generating user identity binding value is shown in (1).

$$\mathrm{H_{uid}} = \mathrm{H(UID \| K_{priv} \| T)} \tag{1}$$

Among them, H_{uid} represents the user identity binding hash value, *H* represents the security hash function, *UID* represents the user unique identifier, K_{priv} represents the user private key, and *T* represents the timestamp. The behavioral chain encryption formula is shown in (2).

$$\mathrm{E_i} = \mathrm{E_{K_i}(A_i \parallel E_{i-1})} \tag{2}$$

Where E_i represents the encryption result of the i operation, E_{Ks} represents the symmetric encryption function, A_i represents the i operation behavior, and E_{i-1} represents the encryption result of the previous operation. This model mainly includes two core modules: the key authentication module and the behavior traceability module. Among them, the key authentication module is used to build a strong identity-binding mechanism for users and their operations within the enterprise and realize trusted authentication and non-repudiation of user behaviors. The behavior traceability module realizes efficient restoration and visual tracking of suspicious operation paths by comparing the encrypted records of key operation chains with behavior tags [22]. The model is designed based on the "minimum trust unit + chain authentication structure" to ensure that every operation behavior is traceable and every data access is well documented. The minimum trust unit identification

formula and the identity binding mapping formula are shown in (3) and (4).

$$\mathrm{K_m} = \mathrm{H(UID \| R \| DF)} \tag{3}$$

$$\mathrm{B_{id}} = \mathrm{Map(K_m, S_i)} \tag{4}$$

Among them, K_m represents the master key, H represents the security hash function, *UID* represents the user job number, R represents the role identifier, *DF* represents the device fingerprint, B_{id} represents the identity binding object, and S_i represents the i system or service module.

In this paper, the internal security incidents of enterprises often have the characteristics of "strong concealment", "good disguise of operational legality," and "difficult traceability of responsibility". The traditional account authority system has made it difficult to meet the behavior traceability requirements in the current complex system of enterprises [23]. On the one hand, the key-based method can build a stronger authentication mechanism than the traditional identity; on the other hand, it can encrypt and bind the operation behavior layer by layer "like a blockchain" through the encryption chain method, thereby achieving high traceability.

The biggest advantage of this model lies in its key coupling chain traceability structure. In each user operation or sensitive behavior, the system will take the current user identity key as the starting point to generate behavior nodes. Then, it will generate operation signatures for the nodes and pass them to subsequent behaviors [24]. Form a dynamic encryption behavior chain so that even if an attacker tampers with the data or tries to disguise it, bypassing the chain structure for "forgery behavior" or "breakpoint erasure" is impossible. The chain traceability behavior tracking mechanism based on the key coupling is shown in Figure 1.

The figure shows that this mechanism efficiently traces internal threats through multi-level key management and behavior log chain recording. Firstly, the system completes the key generation through RSA and ECC algorithms, and the user terminal combines KMS to form a public-private key pair, which is used in the multi-level authentication framework. User terminal operation logs are signed by private keys to ensure non-repudiation and monitor behaviors involving sensitive data access, file operations, network requests, and permission changes in real time. The log hash is organized into a Merkel tree and forms a chain structure, which is highly tamper-proof. The signature log is encrypted by AES-GCM and then stored in fragments, and the public key and private key are combined for access control. Anomaly detection identifies threat behaviors through rule matching, triggers reverse

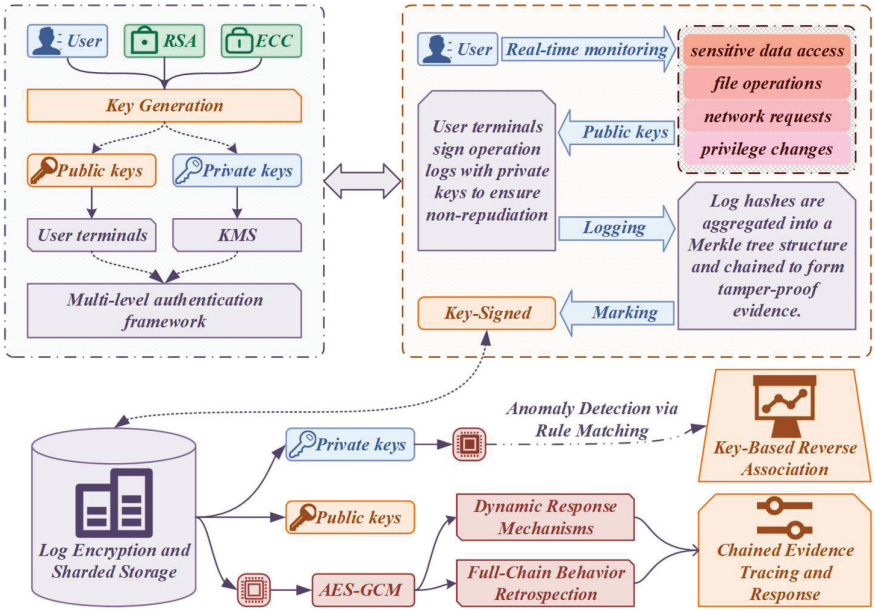

Figure 1 Chain traceability behavior tracking mechanism based on key coupling.

key association and full-chain traceability response, and ultimately forms a dynamic response mechanism and a complete evidence chain, significantly improving the enterprise's ability to visualize, trace, and hold accountable complex internal threats.

This model mainly introduces a dynamic behavior key chain, binds identity authentication with operational behavior, designs an extensible chain signature structure, supports cross-system behavior authentication and traceability, and proposes a suspicious behavior discrimination mechanism based on a behavior feature map to improve the accuracy of internal threat identification [25]. To verify the model, we deployed the system in the internal document management and data operating system of a real enterprise and successfully identified and traced three simulated permission abuse incidents, proving the model's usability and practical value.

3.2 Design and Implementation of Key Authentication Module

As the primary component of the model, the key authentication module assumes the core responsibilities of basic authentication and behavioral node signature [26]. Based on the internal identity management system of the

enterprise, this module binds the identity information of each user to a master authentication key through the key generation algorithm. It updates it regularly to ensure the security and timeliness of the key [27]. On this basis, before all users perform sensitive operations, the system will force key signature verification to prevent anonymous operations or identity forgery. The formula of the master authentication key derivation function is shown in (5).

$$\sigma_{\mathrm{i}} = \mathrm{Sign}(\mathrm{K_m}, \mathrm{A_i}, \mathrm{T_i}) \tag{5}$$

Where σ_i represents the *i* operation signature, A_i represents the operation content, and T_i represents the timestamp. The behavior chain update formula is shown in (6).

$$\mathrm{C_i} = \mathrm{C_{i-1}} + \mathrm{N_i} \tag{6}$$

Among them, C_i represents chain update, C_{i-1} represents master authentication key, and N_i number of keys. The concrete implementation of this module can be divided into four sub-components: key generator, identity binder, behavior verifier, and key updater. The key generator is triggered when the user is employed or the authority changes and generates a unique master key according to the user's job number, role, device fingerprint, etc.; The identity binder is responsible for mapping and binding the key with the operation of each business system of the user so that each operation must pass the key signature authentication; The behavior verifier verifies whether the operation key matches the registration key in real-time, effectively resisting camouflage attacks; The key updater refreshes the key periodically or eventfully to ensure that the key system under long-term use still has security strength [28]. The key-driven user behavior authentication and update module architecture are shown in Figure 2.

As can be seen from the figure, this architecture integrates a key driver, device fingerprint, dynamic change of permission, and binding strategy to form a multi-level authentication and protection mechanism. At the upper layer of the architecture, user rights changes are triggered by LWM (Local Management Module) and 5GM (5G Management Module). Then keys are generated, and identity binding is completed through GID (Global Identity Identification) and UID binding tools. The middle layer shows the key authentication processes of the enterprise financial management system, including object strength analysis, signature authentication, business system interaction, and device fingerprint verification. The Validator module determines the verification results after processing large data. The bottom layer introduces an intelligent terminal binding strategy to effectively prevent and

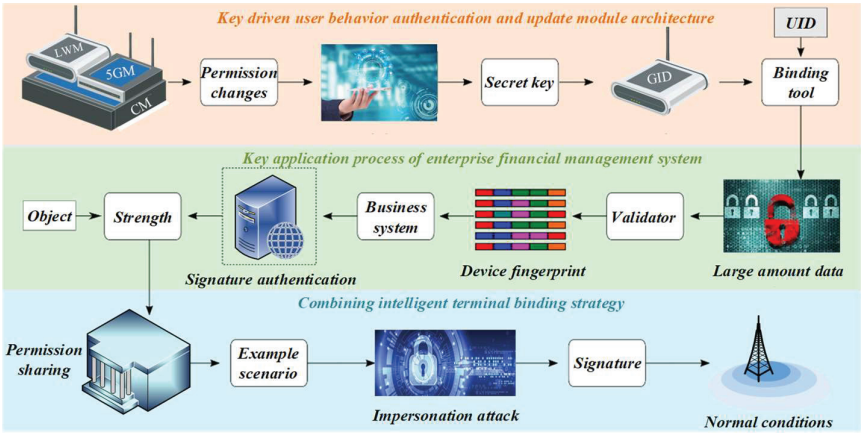

Figure 2 Key-driven user behavior authentication and update module architecture.

control permission sharing and identity counterfeiting under normal conditions with the "example scenario-simulated attack-signature" process. This system improves authentication accuracy and traceability capabilities through a multi-point fusion mechanism. It is especially suitable for enterprise-level application scenarios that are sensitive to permissions and have a high incidence of attacks.

The core advantage of the key authentication module is that it breaks the traditional paradigm of "account password login to complete authentication". It emphasizes the "continuous authentication" of operation behavior; every key operation requires key signature verification. This method improves the unforgeability of identity and enables subsequent traceability to have a complete and continuous trusted path [29]. Especially when dealing with "permission sharing", "remote operation," or "third-party access" scenarios, this module can clearly define the attribution of responsibilities and reduce internal risks.

This paper takes the enterprise financial management system as an example of the actual deployment. By setting multi-level key strengths for employees with different authority levels and combining the intelligent terminal binding strategy, a "person-terminal-behavior" triple binding system is formed. For example, when an employee tries exporting a large data report remotely, the system will pop up a key signature request and compare it with the local signature history. If it is abnormal, it will immediately give an alarm and block the operation. This mechanism greatly improves security and is especially suitable for financial and data-intensive enterprises. The authority

level key strength function formula is shown in (7).

$$\mathrm{S_{key}} = \mathrm{f(L_{perm})} = \alpha \cdot \log_2(\mathrm{L_{perm}} + 1) \tag{7}$$

Among them, S_{key} represents the key strength assigned to the user, L_{perm} represents the user privilege level, α represents the security factor, and f represents the key strength calculation function. The formula of operation behavior anomaly scoring function is shown in (8).

$$\mathrm{A_{score}} = \sum_{\mathrm{i=1}}^{\mathrm{m}} \mathrm{w_i} \cdot |\mathrm{B} - \mathrm{B_i}| \tag{8}$$

Among them, A_{score} represents the deviation score between the current operation and the historical behavior, *m* represents the number of behavior dimensions, B_i represents the i index of the current behavior, *B* represents the behavior value in the historical average or normal range, and w_i represents the weight coefficient of this behavior dimension. The key authentication module is not only the security cornerstone of the entire model, but also the prerequisite for the implementation of the internal traceability mechanism. Through the deep integration of key binding and behavior verification, the "identity encryption confirmation" of every key behavior of internal users is realized, providing solid support for the traceability of the behavior chain.

3.3 Construction and Analysis of Behavior Traceability Module

The behavior traceability module is the second core component of this model. Its main goal is to record, correlate, reconstruct, and visualize the user behavior information generated after key authentication, finally realizing real-time traceability and risk warning of suspicious behaviors. This module is built on the chained key structure mentioned above. A complete user behavior chain is formed by forming each operation node into a behavior hash block and chaining it with context logic in chronological order.

The behavior traceability module mainly includes four functional components: behavior chain recorder, node label analyzer, traceability engine, and visual audit platform [30]. The behavior chain recorder encapsulates every certified critical operation into a structured log and encrypts it. The node label analyzer classifies and labels behaviors to provide a feature comparison basis for subsequent suspicious behavior identification. The traceability engine carries out path tracking based on the time window and behavior chain, tracing and reconstructing specific risk events. The visual audit platform

graphics the chain data for administrators to trace the source with one click. The formula of the structured record function of the behavior chain is shown in (9).

$$\mathrm{I} = \mathrm{H}(\mathrm{C_n}) = \mathrm{H}(\mathrm{H}(\ldots(\mathrm{H}(\mathrm{N_1})\ldots))) \tag{9}$$

Among them, *I* represents the structured behavior log, *H* represents the encryption function, and C_n represents the user identity. The behavioral abnormality scoring function formula is shown in (10).

$$\mathrm{S_{anomaly}} = \sum_{\mathrm{i=1}}^{\mathrm{n}} \mathrm{Dev}(\mathrm{A_i}, \mu) \tag{10}$$

Among them, $S_{anomaly}$ represents the abnormal score, A_i represents the label generated by the i operation, μ represents the mean of the normal behavior distribution, and n represents the number of samples. This module introduces cryptographic hash blocks. Even if the attacker has administrator privileges, he cannot modify the information of any behavior node alone because its behavior chain will become invalid when it is interrupted. At the same time, the analysis of node labels and behavior maps allows the system to automatically identify "abnormal paths", "high-frequency and high-risk operations," or "permission cross-boundary behaviors", greatly improving the sensitivity of discovering internal threats.

The biggest advantage of the behavior traceability module is that its behavior chain is highly readable, the analysis is highly automated, and the traceability map is intuitive and easy to use. Traditional log analysis makes restoring the complete operation path difficult, especially in large-scale multi-department collaborative systems. Still, this module can build the operation trajectory of a certain risk event in a few seconds, providing a quick response basis for the security team. The behavioral chain readability scoring function formula is shown in (11).

$$\mathrm{R_{chain}} = \frac{1}{\mathrm{n}} \sum_{\mathrm{i=1}}^{\mathrm{n}} (\lambda_1 \cdot \mathrm{C_{tag}(i)} + \lambda_2 \cdot \mathrm{V_{op}(i)}) \tag{11}$$

Among them, R_{chain} represents the readability score of the entire behavior chain, n represents the number of log nodes in the operation chain, $C_{tag}(i)$ represents the label clarity of the i operation, $V_{op}(i)$ represents whether the i operation has visual mapping features, λ_1 and λ_2 represent weight parameters. The behavior traceability module realizes efficient analysis and tracking of internal threats of enterprises through encrypted chain records,

behavior tag identification and visual presentation. Complementing the key authentication module, it jointly builds a complete closed-loop "authentication + tracking" internal threat governance system. In response to these challenges, the next section introduces a novel threat traceability model based on key authentication, aiming to bridge the gap between theory and enterprise practice.

4 Experimental Results and Analysis

Focusing on the actual needs of internal threat authentication and traceability, this study designs and constructs an experimental platform based on a key authentication system. The experiment's data mainly comes from user behavior logs, security audit records, and access control data in a simulated enterprise intranet environment, covering terminal login information, resource access path, operation command execution records, and time stamps. These data can reflect the characteristics of normal user behavior and contain simulated abnormal behavior data generated through script injection, private key abuse, ultra vires, etc., aiming to comprehensively evaluate the effect of a key authentication mechanism in identification and traceability. In terms of software and hardware configuration of the experimental platform, the system is based on open open-source operating system, adopts a high-performance multi-core server as the core computing node, and is equipped with 64 gigabytes of memory and high-speed solid-state storage devices to ensure the real-time performance of key calculation and log processing. The software part integrates a digital certificate management module, key distribution and update mechanism, log audit system and behavior analysis engine. The key functions are implemented by Python and Java languages, and the database adopts relational structure storage and full-text index optimization strategy. The overall experimental environment is highly controllable and scalable. It can effectively simulate the identity authentication and behavior traceability processes in multiple scenarios within the enterprise, providing a solid foundation for verifying the practicality and security of the research model. The key distribution efficiency pairs are shown in Table 1.

As seen from the above table, the distribution efficiency based on the key authentication system is better than the traditional manual distribution and automatic scripting methods. Its average distribution time is only 180 ms, much lower than 720 ms for manual methods and 430 ms for automated scripts, indicating that it is more suitable for large-scale deployment. In terms of error rate, the key authentication system is only 0.3%, which is

Table 1 Comparison of key distribution efficiency

Distribution Method	Average Distribution Time (ms)	Error Rate (%)	Maximum Delay (ms)	Distribution Success Rate (%)
Manual Distribution	720	4.5	1200	93.2
Automatic script	430	2.1	800	96.7
Key authentication system	180	0.3	350	99.6

significantly lower than manual (4.5%) and automatic script (2.1%), which is extremely advantageous in the complex network structure of enterprises. In addition, its maximum delay is 350 ms, almost one-third of the manual method's, indicating that it can maintain high performance even under high concurrency. The distribution success rate reaches 99.6%, which further reflects the leading position of the key authentication system in security and stability. In the network security environment, fast and accurate key distribution is very important to block the internal threat propagation chain, so this system has a wide application prospect.

To further quantify the system's adaptability across multiple platforms, we conducted deployment and testing on three typical enterprise environments: Windows Server, Ubuntu Linux, and Android enterprise terminals. The evaluation results show that the system maintains a high authentication success rate – 99.5% on Windows, 99.7% on Linux, and 99.3% on Android – demonstrating reliable cross-platform performance. The average authentication delay remains within an acceptable range, recorded at 190 ms on Windows, 175 ms on Linux, and 210 ms on Android. Additionally, the error rate stays below 0.6% across all platforms. These findings confirm that the system can operate efficiently and stably in heterogeneous environments, making it suitable for large-scale enterprise applications involving diverse terminal devices and operating systems.

To compare the performance differences in delay and error rate between manual distribution, automated script distribution, and distribution mechanisms based on key authentication systems, to evaluate the practical feasibility of authentication systems in the high concurrency environment within the enterprise, this paper compares the delay and error rate of different key distribution mechanisms, and the results are shown in Figure 3.

As can be seen from the figure, SKD compares symmetric key distribution, and PKD compares public key key distribution. In the figure on the left, as the network congestion rate increases from 20% to 100%, the overall delay of SKD remains between 100 and 150 ms, while the PKD

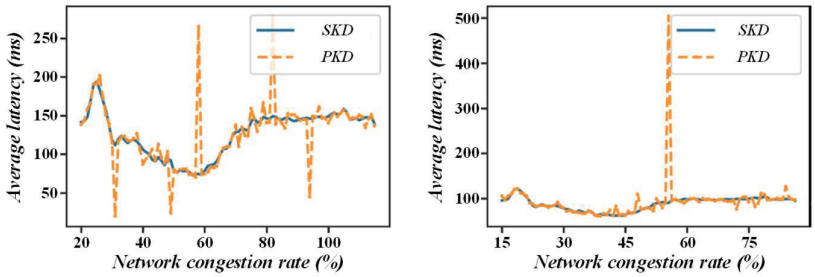

Figure 3 Comparison of delay and error rate of different key distribution mechanisms.

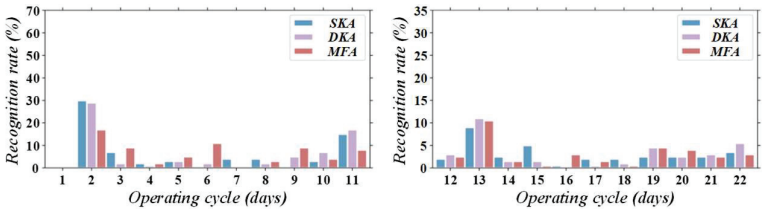

Figure 4 The effect of authentication mechanism on improving the recognition rate of phishing attacks.

fluctuates significantly, especially at the congestion rate of about 60%, the peak delay is close to 270 ms. The figure on the right further shows that within the finer congestion rate range of 15% to 80%, SKD delay performance is stable, most of which remains below 100 ms. PKD fluctuates violently at about 55% and the delay soars to nearly 500 ms. It can be seen that SKD has stronger delay stability and anti-congestion ability. At the same time, PKD can easily cause delay peaks when predicting failure or network drastic changes, suggesting that the choice of key distribution mechanism is crucial to system performance.

This paper analyzes the effect of the authentication mechanism on the improvement of the recognition rate of phishing attacks to evaluate the key-based authentication system's recognition ability in dealing with phishing attacks and explore the improvement of its recognition rate compared with the traditional account password mechanism. The results are shown in Figure 4.

According to the data in the figure, SKA stands for static key authentication, DKA stands for dynamic key authentication, and MFA stands for multi-factor authentication. At the beginning of the operation, the recognition rate of SKA was the highest, close to 30%, DKA was about 25%, and MFA was slightly less than 20%. However, from the second day, the recognition

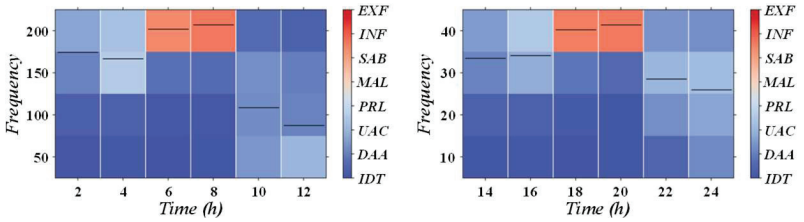

Figure 5 Distribution and frequency of internal threat types.

rate decreased rapidly, and the recognition rate of each mechanism was generally lower than 10% from the third to the 11th day. In the subsequent cycle from day 12 to day 22, the recognition rate fluctuated slightly, mostly between 5% and 10%, among which MFA performed slightly better on days 14 and 15, with a recognition rate of about 15%. The overall trend shows that the authentication mechanism is more sensitive to phishing attack identification in the early stage. Still, as the system running time increases, the identification efficiency decreases, suggesting that combining dynamic update mechanisms or behavior modeling is necessary to improve long-term protection capabilities.

This paper analyzes the distribution and occurrence frequency of internal threat types in enterprises to classify and count different types of internal threat behaviors, analyze their occurrence frequency, and provide a basis for policy optimization and resource allocation. The results are shown in Figure 5.

It can be seen from the figure that in the statistics from 0:00 to 12:00, the frequency of information leakage (INF) incidents is the highest between 6 and 8 hours, exceeding 200 times, which is much higher than other types such as privilege abuse (PRL) and unauthorized access (UAC), these two types of threats are mostly concentrated below 50 times. In the distribution from 14:00 to 24:00, INF events peaked again from 18:00 to 20:00, with a frequency of more than 40 times, while other threats such as data leakage (EXF) and destructive behavior (SAB) also appeared relatively concentrated in the same period. The overall analysis shows that information leakage incidents are most active during rush hour, suggesting that it is necessary to focus on strengthening data monitoring and authority management in critical periods.

By simulating different attack behaviors, the table shows the identification and interception capabilities of key-based authentication systems in various threat environments. The authentication success rate of normal users is as high as 99.9%, which shows the high reliability of the system in

Table 2 Authentication success rate and attack simulation

Type of Attack	Total Authentication Requests	Number of Successful Authentications	Number of Interception Failures	Success Rate (%)
Normal user	5000	4995	5	99.9
Phishing accounts	1000	12	988	1.2
Secret stealing script implantation	800	9	791	1.1
Abuse of authority	700	23	677	3.3

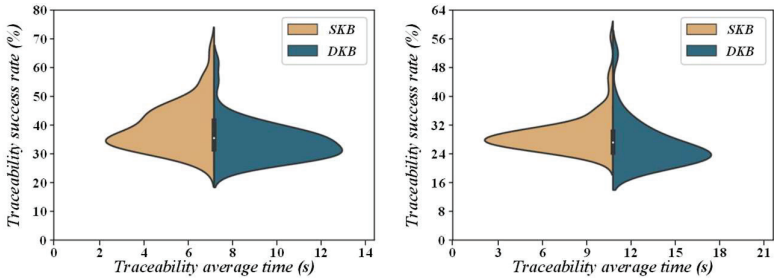

Figure 6 Change of traceability time and success rate.

quickly identifying legitimate users. On the contrary, for simulated phishing accounts, secret stealing scripts, and permission abuse, the authentication success rates are only 1.2%, 1.1%, and 3.3%, respectively, indicating that the system has strong threat identification capabilities and can effectively intercept malicious access. This low-tolerance strategy is crucial to network security because most insider threats often disguise themselves as legitimate operations. Without accurate authentication mechanisms, information leakage or out-of-control authority will lead to. By linking with the behavior recognition module, the authentication system improves the semantic depth of authentication, effectively enhances traceability ability, and has positive significance for building a trusted computing environment.

This paper analyzes the changes in traceability time and success rate under different security systems to compare them and evaluate the degree to which the key authentication system improves the efficiency of threat traceability. The results of the analysis are shown in Figure 6.

The left chart shows that in the interval with an average traceability time of about 7 seconds, the traceability success rate of SKB is concentrated between 30% and 50%, while the success rate distribution of DKB in the same time frame is more scattered. Still, some peaks are close to 70%. In

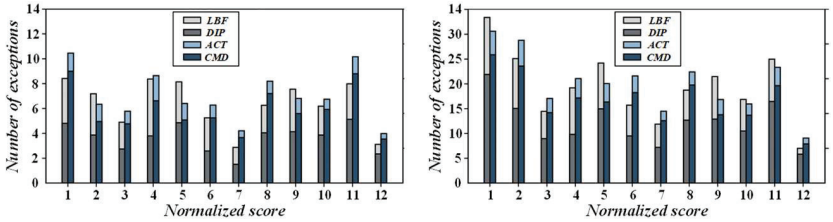

Figure 7 Correlation diagram between user behavior characteristics and authentication anomalies.

the figure on the right, when the traceability time is extended to more than 10 seconds, the success rate of SKB has a significant downward trend, with most distributions below 40%, while the performance of DKB remains in a relatively stable range of 30%–50%. DKB ensures the success rate, has stronger adaptability to traceability time, and is suitable for authentication traceability needs in complex and persistent threat scenarios.

This paper analyzes the correlation between user behavior patterns and authentication anomalies to explore the relationship and build a behavior-aware authentication mechanism to provide data support. The results are shown in Figure 7.

The figure above shows that LBF stands for login frequency behavior, DIP stands for device and IP usage pattern, ACT stands for access time consistency, and CMD stands for command operation habit. The overall number of anomalies is low in the figure on the left. When the normalized score is 1, CMD features cause the most anomalies, reaching about 12 times, while LBF has the least, only 6 times. As scores rose to 6 and 7, the number of abnormalities for each behavioral characteristic fluctuated between 7 and 10 overall. The right panel shows a significant increase in the number of abnormalities under the high-risk score, especially at scores of 5 and 6, with more than 25 abnormalities related to DIP and ACT and nearly 20 abnormalities related to CMD. Overall, CMD features have a higher frequency of abnormalities in the low-risk stage. In contrast, DIP and ACT abnormalities are more significant in the high-risk stage, suggesting that these behavioral features strongly correlate with authentication abnormalities and have potential threat traceability value.

This paper analyzes the stress resistance test of the authentication success rate under different attack means to evaluate the robustness of the key authentication system and compare the system's stress resistance ability. The results are shown in Figure 8.

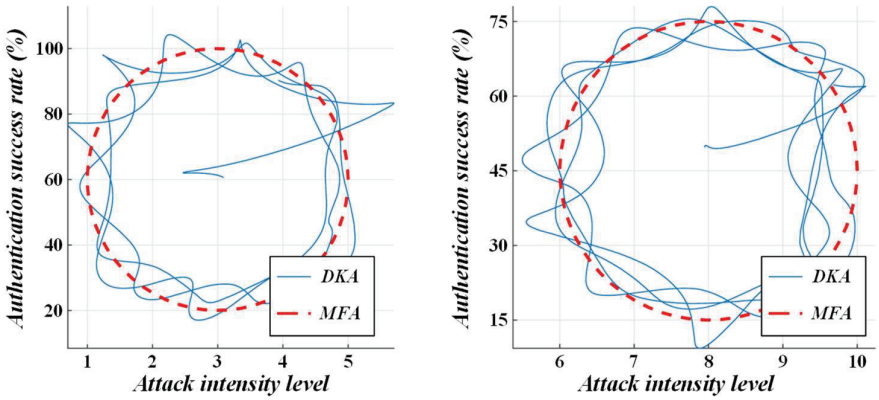

Figure 8 Stress test chart of authentication success rate under different attack methods.

Table 3 Comparison of certification traceability response time and efficiency

Scene Classification	Average Identification Time (s)	Mean Traceability Time (s)	Traceability Success Rate (%)	Pre-intervention Data Breach Volume (MB)
No traceability mechanism	98.2	Untraceable	21.4	512
Log analysis system	44.6	61.2	74.5	231
Key authentication system	15.3	12.7	96.9	37

As you can see from the chart, DKA stands for Dynamic Key Authentication, and MFA stands for Multi-Factor Authentication. The left half of the figure shows that between attack strength levels 1 to 5, the authentication success rate of DKA fluctuates greatly, from the lowest of about 20% to the highest of close to 95%. In contrast, the success rate of MFA is more stable, always remaining at about 75% or so. In the right half, when the attack intensity level is 6 to 10, the certification success rate of DKA decreases as a whole, with the lowest dropping to about 15%, but it still maintains a performance of more than 70% at individual level points; In contrast, MFA still maintains a relatively stable trend, fluctuating between 60% and 70%. The compressive performance of MFA is more stable at high attack intensity, while DKA has a higher peak at low intensity. Still, the anti-interference ability is not as stable as that of MFA.

Authentication traceability response efficiency is the core indicator to measure the emergency response capability of network security systems. The comparative analysis of the three mechanisms shows that in the traditional "no traceability mechanism" scenario, the average identification time is as

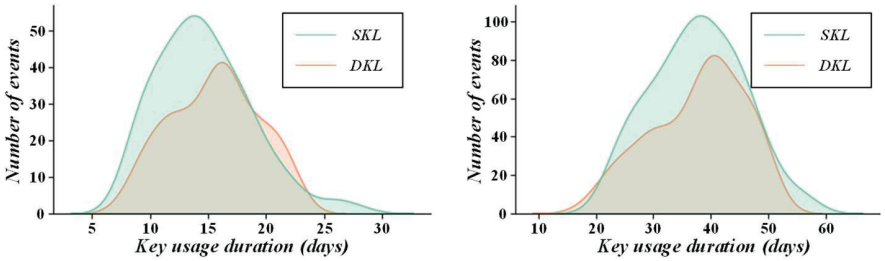

Figure 9 Correlation diagram between key life cycle and security events.

high as 98.2 seconds, and the traceability success rate is extremely low, only 21.4%. Most threatening behaviors cannot be effectively stopped, resulting in an average of more than 500MB of data leakage each time. After the introduction of the log analysis system, although the traceability capability has been improved (74.5% success rate), there is still a significant delay in identification and response, resulting in a data leakage of 231MB. The key-based authentication system completes threat identification in an average of 15.3 seconds and can locate the responsible subject in 12.7 seconds. The traceability success rate is close to 97%, significantly better than the first two. The amount of leakage before intervention was only 37MB, indicating that the system can quickly intervene before the information leakage. This system greatly shortens the life cycle of the attack chain through the strong correlation between behavior identification and key authentication. It provides a realistic path for building an active defensive network security architecture.

To explore the time distribution relationship between key life cycles and internal threat events and provide suggestions for key rotation strategies, this paper analyzes the correlation between key life cycles and security events. See Figure 9 for specific results.

As you can see from the figure, SKL stands for static key life cycle, and DKL stands for dynamic key life cycle. The figure on the left shows that in the short life cycle scenario, the number of events triggered by SKL peaks around the 15th day of use, with the number of events being about 55, while the peak of DKL is slightly lower, about 45, occurring between the 14th and 16th days. The diagram on the right shows the performance over a longer life cycle. The peak value of SKL safety incidents appeared on about the 40th day, corresponding to 100 incidents. At the same time, the peak value of DKL was also concentrated in the same period, but the peak value was about 80 times, and the overall number was always lower than that of SKL. DKL has more

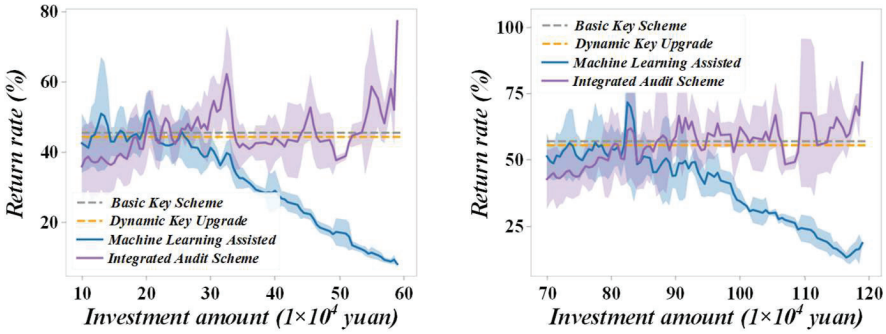

Figure 10 Simulation analysis diagram of security return on investment based on key authentication system.

advantages in controlling security risks over a long period, while the static key mechanism significantly increases the number of security incidents and higher risks over time.

This paper analyzes the security ROI based on a key authentication system to analyze the ROI of enterprises after deploying it and verify its commercial feasibility from the perspective of cost and risk avoidance. The results are shown in Figure 10.

As can be seen from the figure in the left figure, when the security investment amount is between 1×10^4 yuan and 6×10^4 yuan, the return rate of the basic key scheme and dynamic key upgrade is maintained in the range of 55% to 65%, with small fluctuations; The return rate of the integrated audit certification system is relatively more stable, about 60%; However, after investing more than 3×10^4 yuan in machine learning-assisted certification, the rate of return began to drop rapidly, from about 55% to less than 30%. The figure on the right further shows that in the higher investment range, the rate of return of the Machine Learning Assisted system continues to drop, with the lowest being close to 20%. At the same time, the Integrated Audit Scheme maintains a stable level of about 60%–65% throughout the entire high investment range, showing Better pressure resistance and economic benefits. This analysis shows that although highly intelligent solutions have technical advantages, a stable and controllable authentication mechanism is more suitable for continuous deployment in terms of return on investment. We now provide a detailed explanation of the key authentication module, which serves as the core of the identity binding and signature mechanism in our proposed system.

5 Conclusion

The proposed key authentication system demonstrates strong effectiveness in addressing internal enterprise threats, achieving a 99.9% authentication success rate and high traceability accuracy. It performs reliably under high-concurrency conditions with low latency and error rates, and significantly reduces data leakage and attack lifecycle duration. The system also offers high economic returns and practical deployment value through advanced identity chaining and behavior mapping. Looking ahead, integration with blockchain and AI is planned to enhance automation and adaptability, positioning the system as a scalable, secure, and cost-effective enterprise security solution. Through the deployment and simulated attack test in a real enterprise environment, the effectiveness, efficiency, and economy of the system have been fully verified, and the following conclusions are drawn:

(1) In the simulation test, the authentication success rate of the key authentication system for normal users is as high as 99.9%, far exceeding the traditional username and password method. The authentication success rates under the three attack types of phishing accounts, secret theft scripts, and permission abuse are only 1.2%, 1.1%, and 3.3%, respectively, indicating that the system can accurately intercept malicious behaviors with high accuracy. At the same time, the average response time of each attack identified by the system is 15.3 seconds, the average traceability time is 12.7 seconds, and the traceability success rate is as high as 96.9%, which is significantly better than the 74.5% of the log analysis system and the 21.4% without traceability mechanism. This proves that the key-based chain authentication mechanism can greatly improve the ability to identify and hold accountable abnormal behaviors while ensuring that normal business processes are not disturbed.

(2) In the performance test, the average delay of key distribution is 180 milliseconds, the error rate is only 0.3%, the maximum delay does not exceed 350 milliseconds, and the distribution success rate is as high as 99.6%. Compared with manual distribution (average 720ms, error rate 4.5%) and automatic script distribution (430ms, error rate 2.1%), the system shows strong stability and anti-network congestion ability, especially in high concurrency scenarios with proper delay control, the authentication process is almost unaware, ensuring the balance between user experience and system load. This provides a feasibility guarantee for large and medium-sized enterprises to deploy a unified authentication mechanism among multiple systems.

(3) After the system is deployed, enterprises' average data leakage volume in information leakage incidents drops from 512MB to 37MB, and the life cycle of the attack chain is significantly shortened. Regarding security investment, the return on investment of the authentication system under medium and high-intensity investment is stable at more than 60%, which is higher than the performance of machine learning-assisted authentication, which fluctuates to less than 30% in high-cost scenarios. The data show that the key authentication system is not only mature in technology and flexible in deployment but also has outstanding economic benefits and can achieve the optimal balance between cost and risk.

Although the proposed key authentication and traceability system has been proven effective, there are still some limitations that need to be addressed. Firstly, the current implementation relies on a controlled enterprise intranet environment; Its performance in more open or heterogeneous network environments needs further validation. Secondly, although the system exhibits high authentication and traceability accuracy, the overhead caused by encryption operations may affect the performance of large-scale deployments. Thirdly, the behavior analysis module relies on predefined rules and thresholds, which may limit its ability to detect previously unknown or adaptive threats. These limitations highlight the necessity for continuous improvement and integration of more adaptive, intelligent, and scalable mechanisms.

In future research, several directions will be explored to further enhance the system's capabilities. First, we aim to integrate blockchain-based distributed ledger technologies to strengthen tamper-resistance and decentralization of identity verification records. Second, incorporating AI-powered behavior modeling and anomaly detection can further improve the system's adaptability and automation. Third, expanding the authentication traceability model to support heterogeneous environments such as cloud-native platforms and IoT networks is also a critical direction. Finally, privacy-preserving mechanisms such as zero-knowledge proofs and homomorphic encryption will be studied to ensure that traceability does not compromise data confidentiality. These directions are expected to contribute to the evolution of intelligent, adaptive, and secure enterprise network systems.

The enterprise internal threat authentication and traceability technology based on key authentication proposed in this paper shows high practicability and advancement in the theoretical model, system implementation, and experimental verification. By constructing a three-dimensional identity chain

of "user-terminal-behavior" and introducing chain signatures and abnormal behavior map analysis mechanisms, the efficiency and accuracy of enterprises' response to complex internal threats have been effectively improved. In the future, combined with emerging technologies such as blockchain and artificial intelligence, this system is expected to further improve the level of intelligence under multiple scenarios and platforms and become one of the core supporting technologies for enterprises to build a trusted network security system.

Funding

This work was sponsored in part by the Yunnan Province Major Science and Technology Special Program (202302AD080002-3) and the Southern Power Grid Corporation Science and Technology Project (YNKJXM20230272).

References

[1] Wang, K., Hu, C., and Shan, C. "Process-oriented security assessment of network services," Computer Networks, vol. 264, pp. 111225, 2025.

[2] Zhong, Y., and Li, X. "Network information security protection method based on additive Gaussian noise and mutual information neural network in cloud computing background," Egyptian Informatics Journal, vol. 30, pp. 100673, 2025.

[3] Abdussami, M., Dwivedi, S. K., Al-Shehari, T., Saravanan, P., Kadrie, M., Alfakih, T., Alsalman, H., and Amin, R. "DEAC-IoT: Design of lightweight authenticated key agreement protocol for Intra and Inter-IoT device communication using ECC with FPGA implementation," Computers and Electrical Engineering, vol. 120, pp. 109696, 2024.

[4] Ali, H., and Ahmed, I. "LAAKA: Lightweight Anonymous Authentication and Key Agreement Scheme for Secure Fog-Driven IoT Systems," Computers & Security, vol. 140, pp. 103770, 2024.

[5] Babu, P. R., Kumar, S. A. P., Reddy, A. G., and Das, A. K. "Quantum secure authentication and key agreement protocols for IoT-enabled applications: A comprehensive survey and open challenges," Computer Science Review, vol. 54, pp. 100676, 2024.

[6] Braeken, A. "Flexible hybrid post-quantum bidirectional multi-factor authentication and key agreement framework using ECC and KEM," Future Generation Computer Systems, vol. 166, pp. 107634, 2025.

[7] Cai, J., Zhang, Z., Li, M., and Li, N. "A group authenticated key agreement protocol for secure communication between distributed power terminal devices," Computers and Electrical Engineering, vol. 118, pp. 109214, 2024.

[8] Chen, Y., Xin, Z., Zhang, B., and Jia, J. "A security authentication and key agreement scheme for railway space-ground integrated network based on ideal lattice," Journal of Network and Computer Applications, vol. 240, pp. 104194, 2025.

[9] Cheng, Q., Ma, Y., Wei, F., and Li, X. "An efficient anonymous certificateless authentication and key agreement scheme for smart grids," Computers and Electrical Engineering, vol. 124, pp. 110369, 2025.

[10] Liu, S., Chen, L., Chen, L., Wang, Y., and Zhu, Y. "CLE-based Authenticated Key Agreement with PUF-Secured Key for Vehicle-to-Infrastructure," Vehicular Communications, pp. 100942, 2025.

[11] Wang, X., Xie, Y., Shui, D., and Ge, S. "An improved biometric authentication and key agreement scheme based on fuzzy extractor for Wireless Body Area Networks," Journal of Information Security and Applications, vol. 91, pp. 104047, 2025.

[12] Ghani, A., Jan, S. U., Chaudhry, S. A., Ahmad, R., Das, A. K., and Kim, D. H. "Enhancing security and trust using efficient privacy-preserving authentication in vehicular edge computing networks," Vehicular Communications, vol. 54, pp. 100921, 2025.

[13] Goswami, C., Basak, A., Ghosh, R., Adhikari, A., and Sarkar, P. "Lightweight authenticated key agreement scheme for IoMT network using generalized Chinese Remainder Theorem," Computer Networks, vol. 263, pp. 111212, 2025.

[14] Jin, C., Zhou, P., Chen, Z., Qin, W., Chen, G., Zhang, H., and Weng, J. "EPAKA: An efficient and privacy-preserving authenticated key agreement scheme based on physical security for VANET," Vehicular Communications, vol. 50, pp. 100847, 2024.

[15] Kuang, Y., Wu, Q., Chen, R., and Liu, X. "Blockchain based lightweight authentication scheme for internet of things using lattice encryption algorithm," Computer Standards & Interfaces, vol. 93, pp. 103981, 2025.

[16] Kumar, P., Pal, A. K., and Islam, S. H. "2F-MASK-VSS: Two-factor mutual authentication and session key agreement scheme for video surveillance system," Journal of Systems Architecture, vol. 153, pp. 103196, 2024.

[17] Jin, D., Hu, Y., Chen, B., He, G., Chen, J., and Shen, Z. "TIAN: A time series Imaging Association Network for human abnormal behavior detection," Information Fusion, vol. 118, pp. 102906, 2025.
[18] Lee, T.-F., Ye, X., and Huang, W.-J. "Lightweight privacy-preserving authenticated key agreements using physically unclonable functions for internet of drones," Journal of Information Security and Applications, vol. 87, pp. 103915, 2024.
[19] Magara, T., and Zhou, Y. "EMAKAS: An efficient three-factor mutual authentication and key-agreement scheme for IoT environment," Cyber Security and Applications, vol. 3, pp. 100066, 2025.
[20] Pan, G., Tan, H., Zheng, W., Vijayakumar, P., Wu, Q. M. J., and Sivaraman, A. "Three-factor authentication and key agreement protocol with collusion resistance in VANETs," Journal of Information Security and Applications, vol. 90, pp. 104029, 2025.
[21] Prajapat, S., Rana, A., Kumar, P., Das, A. K., and Susilo, W. "Privacy-preserving authentication protocol for user personal device security in Brain–Computer Interface," Computer Standards & Interfaces, vol. 94, pp. 104009, 2025.
[22] Surapaneni, P., Bojjagani, S., and Khan, M. K. "VESecure: Verifiable authentication and efficient key exchange for secure intelligent transport systems deployment," Vehicular Communications, vol. 49, pp. 100822, 2024.
[23] Thapliyal, S., Wazid, M., Singh, D. P., Das, A. K., and Islam, S. H. "Robust authenticated key agreement protocol for internet of vehicles-envisioned intelligent transportation system," Journal of Systems Architecture, vol. 142, pp. 102937, 2023.
[24] Tong, Q., Yin, L., Liu, Y., and Xu, J. "Append-only Authenticated Data Sets based on RSA accumulators for transparent log system," Computer Standards & Interfaces, vol. 93, pp. 103978, 2025.
[25] Ullah, S., Nasir, H. M., Kadir, K., Khan, A., Memon, A., Azhar, S., Khan, I., and Ashraf, M. "End-To-End Encryption Enabled Lightweight Mutual Authentication Scheme for Resource Constrained IoT Network," Computers, Materials and Continua, vol. 82, no. 2, pp. 3223–3249, 2025.
[26] Wang, M., and Wang, Z. "A distributed identity management and cross-domain authentication scheme for the Internet of Things," Future Generation Computer Systems, vol. 169, pp. 107818, 2025.
[27] Wang, X., Xie, Y., Shui, D., and Ge, S. "An improved biometric authentication and key agreement scheme based on fuzzy extractor for

Wireless Body Area Networks," Journal of Information Security and Applications, vol. 91, pp. 104047, 2025.
[28] Xia, Y., Zhang, J., Man, K. L., and Dong, Y. "Handover Authenticated Key Exchange for Multi-access Edge Computing," Journal of Network and Computer Applications, vol. 234, pp. 104071, 2025.
[29] Yalçın, G. C., Kara, K., Edinsel, S., Kaygısız, E. G., Simic, V., and Pamucar, D. "Authentication system selection for performance appraisal in human resource management using an intuitionistic fuzzy CIMAS-ARLON model," Applied Soft Computing, vol. 171, pp. 112786, 2025.
[30] Yu, X., Wang, Y., and Huang, X. "Quantum-resistant ring signature-based authentication scheme against secret key exposure for VANETs," Computer Networks, vol. 262, pp. 111213, 2025.

Biographies

Jian Hu received the bachelor's degree in information security from Yununan University in 2014, the master's degree in software engineering from Yununan University in 2016, he is currently a Ph.D. candidate in Electronic Information at South China University of Technology. He is currently working as a Senior Engineer at the Yunnan Power Grid Co., Ltd. Information Center of China Southern Power Grid Co., Ltd. His research areas and directions include cyberspace security, data security, data mining.

Wei Wu, female, Han ethnicity, Kunming City, Yunnan Province, China. She is the Deputy General Manager of the Information Center of China Southern Power Grid Yunnan Power Grid Co., Ltd., a master's student, senior engineer, specializing in power system automation and network security.

Tao Chuan, male, Han ethnicity, Kunming City, Yunnan Province, is the General Manager of the Information Center of China Southern Power Grid Yunnan Power Grid Co., Ltd. He holds a bachelor's degree and is an engineer specializing in power system automation and network security.

Qiuxia Peng, female, Han ethnicity, from Zhaotong City, Yunnan Province, China. She is a master's student and senior engineer at the Information Center of China Southern Power Grid Yunnan Power Grid Co., Ltd. She specializes in power system automation and network security.