Discover Applied Sciences

Research

Decentralized storage technology of network information security level secret key of distribution automation terminal

Jin Yi[1] · Weijie Huang[1] · Lianghao Huang[1] · Guozheng Huang[1] · Guangyong Zheng[1] · Yongle Li[1]

Received: 12 December 2024 / Accepted: 9 May 2025
Published online: 29 May 2025
© The Author(s) 2025 OPEN

Abstract
To improve the management efficiency of network information in distribution automation terminals, a study was conducted on the decentralized storage technology of network information security level keys for distribution automation terminals. This technology utilizes a linear geometric hierarchical management scheme, manages keys through a key derivation tree structure, and encompasses the construction of key derivation trees, secure storage of root keys, and key exchange protocols to achieve effective distribution of keys in the network. Experimental results have shown that this technology can flexibly manage the keys of distribution automation terminals based on information security levels, improving the management efficiency of network information.

Article Highlights

1. Security - Oriented Classification: Distribution automation terminals are classified into five network information security levels considering their running state. This classification enables more precise security management strategies tailored to different terminal security needs.
2. Innovative Key Management: A linear geometric hierarchical key management scheme is proposed. It uses the key derivation tree method, constructs a key derivation tree, and sets up a root key secure storage mechanism and key exchange protocol to achieve efficient key management.
3. Experimental Verification: The decentralized storage technology is tested in a city's power system. Experimental results show that it can effectively classify security levels, has short encryption and decryption times, low storage overhead, and can identify and prevent security threats.

Keywords Distribution automation · Terminal network · Information security level · Secret key · Distributed storage technology · Derived tree

✉ Lianghao Huang, huangwengdangsbm@163.com | [1]Jiangmen Power Supply Bureau of Guangdong Power Grid Co., Ltd., Jiangmen 529000, Guangdong, China.

1 Introduction

The distribution automation terminal, a critical component of the power system, performs the essential function of monitoring medium and low voltage distribution networks' operations, thereby playing a crucial role in ensuring the stable and efficient operation of the power system [1]. This technology not only facilitates real-time monitoring and precise control of distribution network information but also possesses the capability for rapid fault management and the implementation of advanced applications.

As the "nerve endings" of the power system, the distribution automation terminal goes deep into the medium and low voltage distribution network, collecting key data such as voltage, current, and power in real time. This data is transmitted to the main station through advanced communication technology, enabling real-time monitoring and remote control of the distribution network's operational status, thereby ensuring a stable power supply. In the event of a fault, these terminals can quickly locate and report the issue, automatically perform isolation and recovery operations, and reduce power outage duration. Furthermore, the distribution automation terminal also supports various advanced applications, including load forecasting, power quality analysis, and distributed energy management. Through data mining and analysis, they provide scientific basis for power system planning, scheduling, and efficient utilization of clean energy. Distribution automation terminal is the core system of power system to realize the operation monitoring of medium and low voltage distribution network, which has the functions of distribution network information monitoring and control, fault handling and advanced application [2]. And considering multiple scenarios of automation equipment failures, the active distribution network reliability assessment provides key data support. Its importance is evident. From the perspective of modernizing the power system, it constitutes a key component in promoting the transformation of the power system towards intelligence and efficiency. By implementing automated monitoring and control of the distribution network, the operational management level of the power system has been significantly improved, effectively reducing operating costs. Distribution automation terminals play a crucial role in improving power supply reliability. A reliable power supply is the fundamental guarantee for the development of modern social economy and the normal operation of people's lives. Distribution automation terminals can timely detect and handle various problems in the distribution network, minimize the occurrence of power outages, and providing solid power security for social and economic development and people's lives. Exploring the network security protection ideas for distribution automation systems is crucial. In the power system, the distribution automation terminal is a part of the power monitoring system [3]. The power industry is an important energy pillar industry, and the power monitoring system is also a key information infrastructure. Therefore, higher security requirements should be placed on the distribution automation terminal network. Due to diverse channels in the distribution automation terminal network, the Internet space is affected by many uncontrollable factors [4], and the distribution automation terminal has many security structural vulnerabilities and threats, such as invasion, forged communication data, data being eavesdropped, deception of master station and terminal, and data tampering [5], posing huge security risks to the operation of the power system. The rapid development of distribution automation terminals has led to issues like widespread distribution and prominent network security threats. The overall security protection goal is to eliminate risks in the main station, distribution terminals [6], and communication links, prevent power supply interruptions from network security threats, and ensure the safe and stable operation of the power system. Network information security level protection is a basic system for improving network information security capabilities and levels, maintaining social stability, and promoting healthy information construction [7]. Its core idea of network information security level protection is to divide the security policies, responsibilities, and security requirements of computer information systems into different levels, providing protection accordingly [8]. It involves reasonable investment, classification guidance, and step-by-step implementation based on the importance and security needs of basic information networks and systems, ensuring safe operation and information security [9], improving comprehensive information security protection capabilities, ensuring and promoting the healthy development of information construction, promoting the development and industrialization of information security and basic information science and technology, and thereby affecting economic development. By formulating unified management norms and technical standards, citizens, legal persons, and other organizations implement classified security protection for their information systems, with graded protection based on system importance and content [10]. Level protection of network information security is crucial for distribution automation terminals and is key to improving their security. How to effectively ensure the security of keys has become an important research area in information security [11]. Storing keys in a distributed manner has become a trend to enhance key security. Although

distributed storage keys enhance security and reduce the risk of single point leakage by dispersing information, they are not absolutely secure. In complex network environments, collaborative attacks or exploiting vulnerabilities may still threaten key security. However, distributed storage can recover by splitting keys into multiple sub key stores, estorable using specific algorithms and protocols like key derivation tree methods. This process follows preset rules in a secure environment, ensuring accurate and secure key recovery and normal system use. Key protection remains an important cryptographic research field, and decentralized storage can effectively solve partial key loss issues [12]. Developing distributed storage management tools has simplified key management. Key management and operation keys each have their own emphasis. The former focuses on the full lifecycle management of keys, carefully designing every step from generation to destruction to ensure security, compliance, and efficiency. This includes setting key parameters based on security requirements, planning secure storage policies, coordinating key updates and secure destruction, while managing key usage permissions to achieve fine-grained control. The latter focuses on using keys to perform specific operations such as encryption, decryption, signature verification, etc., to ensure data security and business functionality implementation. The operation key emphasizes the accurate and timely use in actual business processes, ensuring that cryptographic operations meet business requirements. In short, managing keys is responsible for macro planning and security assurance, while operating keys focuses on key applications in specific businesses.

Currently, many researchers have conducted research on key management. Saikia et al. utilized Delaunay triangulation technology [13] to effectively distribute keys between sensor nodes in wireless sensor networks, fully utilizing distributed keys with the minimum number of keys per sensor node, providing high probability secure communication links and network flexibility. Gupta et al. applied the quantum lightweight identity based two party authenticated key exchange protocol to the Internet of Things [14], generating secret session keys to share confidential information on the public Internet. This method set up a lattice-based two-party authenticated key protocol, using identity-based encryption to eliminate certificate management overhead, improving network security. Vasudevan et al. applied an integrated method of energy-saving switching and key distribution protocols to dense mobile networks [15]. This method, based on a blockchain assisted key distribution protocol customized by a MAC integrity scheme, combined with an uplink reference signal switching mechanism, achieves energy-saving secure network coding, providing security support for mobile networks. "Poor management" in key management of distribution automation terminal networks refers to existing methods that fail to fully meet the requirements of security, adaptability, and efficiency. Specifically, the lack of security and stability in key generation, storage, distribution, updating, and usage affects the operation of the power system. The criteria for judgment include security (ensuring data security), adaptability (matching network characteristics), and efficiency (not affecting system operation). Failure to meet these standards is considered as "poor management". In response to these shortcomings, this article first studies the distributed storage technology of keys. This technology greatly enhances the security of keys and reduces the risk of single point of failure by dispersing key information to multiple nodes in the network. An innovative five level network information security classification system based on terminal operating status has been proposed. This mechanism can implement more precise and effective security management strategies based on the security needs of different terminals, providing finer grained protection for the distribution automation terminal network. A novel linear geometric layered key management scheme has been designed, which fully utilizes the network information security layered protection mechanism to achieve efficient and orderly management of keys. This scheme not only simplifies the key management process, but also significantly improves the security and availability of keys. In the key management scheme, the key derivation tree method is innovatively adopted. This method not only maintains the logical relationship and hierarchical structure between keys, but also generates a series of derived keys as needed to meet the diverse requirements of different security levels for keys in terminal networks. This innovation greatly enhances the flexibility and adaptability of key management. We have established a comprehensive root key secure storage mechanism to ensure that the root key is not illegally obtained or tampered with. At the same time, an efficient key exchange protocol was designed to ensure the secure exchange and transmission of keys in the terminal network, further improving the security and reliability of the entire key management system. Through the successful implementation of the key management scheme and mechanism mentioned above, this article not only theoretically verifies its effectiveness and feasibility, but also provides practical guidance for achieving distributed storage of keys in distribution automation terminal networks. This distributed storage method not only improves the security of keys, but also reduces the complexity of key management, laying a solid foundation for efficient management of network information in distribution automation terminals.

2 Network information security level secret key decentralized storage technology

This paper addresses the critical issue of key management in network information security for distribution automation terminals by introducing innovative solutions to enhance key security and management efficiency. These solutions include leveraging distributed storage, establishing security levels, implementing a layered key management approach, using a key derivation tree, developing secure root key storage, and creating a robust key exchange protocol. The paper successfully constructs an efficient and secure key management system.

2.1 Distribution automation terminal gateway settings

Select the HR YWSJ-3000 portable operation and maintenance safety audit device as the communication gateway for distribution automation terminals. This device, designed to mobile operation and maintenance control standards, prevents unauthorized access, supports retrospective maintenance tracking, and provides network security audits. It ensures safe operation and maintenance of distribution automation terminals [16]. The application scheme is shown in Fig. 1.

Figure 1 shows the configuration scheme of the distribution network automation terminal gateway, which involves selecting the HR YWSJ-3000 portable operation and maintenance security audit device as the communication gateway for the distribution automation terminal, and presenting the connection method and data exchange path of the device in the network. In terms of connection method, the device supports USB mapping and is connected in series between the mobile storage medium and the distribution network automation terminal through a USB cable to achieve secure reading and writing of the mobile storage medium; It also supports connecting power distribution automation terminals with video cables and USB cables, connected in series between the display, mouse, and keyboard, to obtain and display terminal desktop information for operational control. In terms of data exchange, the device can effectively prevent hacker intrusion and malicious access, while supporting operation and maintenance behavior tracing, providing a basis for network security auditing, and ensuring the safe operation and maintenance of distribution automation terminal equipment.

The operation and maintenance supervision structure diagram of portable operation and maintenance safety audit device in distribution automation terminal is shown in Fig. 2.

In the operation and maintenance supervision structure of the distribution network automation terminal shown in Fig. 2, there are multiple vulnerable links, including the operation and maintenance terminal with weak security protection, the operated object that stores critical data (distribution automation terminal), the network connection parts that are vulnerable to eavesdropping and tampering (such as network ports, serial ports, USB and HDMI lines), and the data transmission links that may be attacked by man in the middle. These vulnerabilities can all lead to system intrusion, data leakage or tampering, thereby affecting the normal operation of the power system.

Analyzing the operation and maintenance supervision structure diagram of distribution automation terminal, the supervision by portable operation and maintenance safety audit device includes:

Before the operation and maintenance, connect the device in series between the operation and maintenance terminal and the object to be operated and maintained through the network port, serial port, USB and HDMI.
Authenticate the identity of operation and maintenance personnel in the device through passwords, fingerprints, etc.
Complete the operation and maintenance terminal equipment authentication through USB Key.

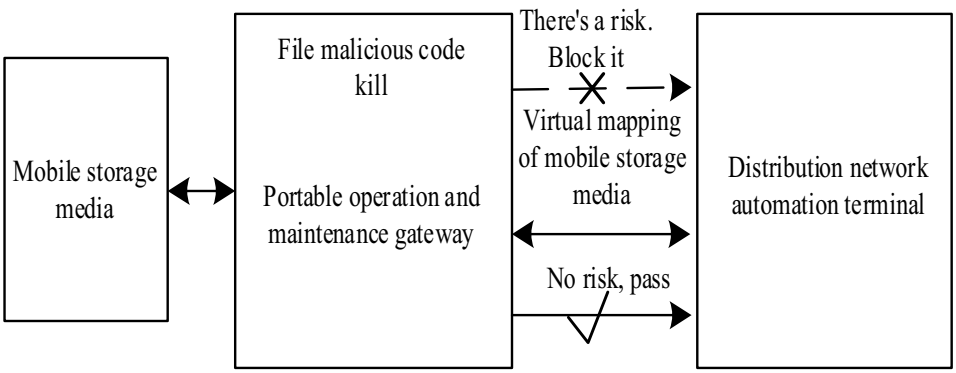


Fig. 1 Distribution network automation terminal gateway setting scheme

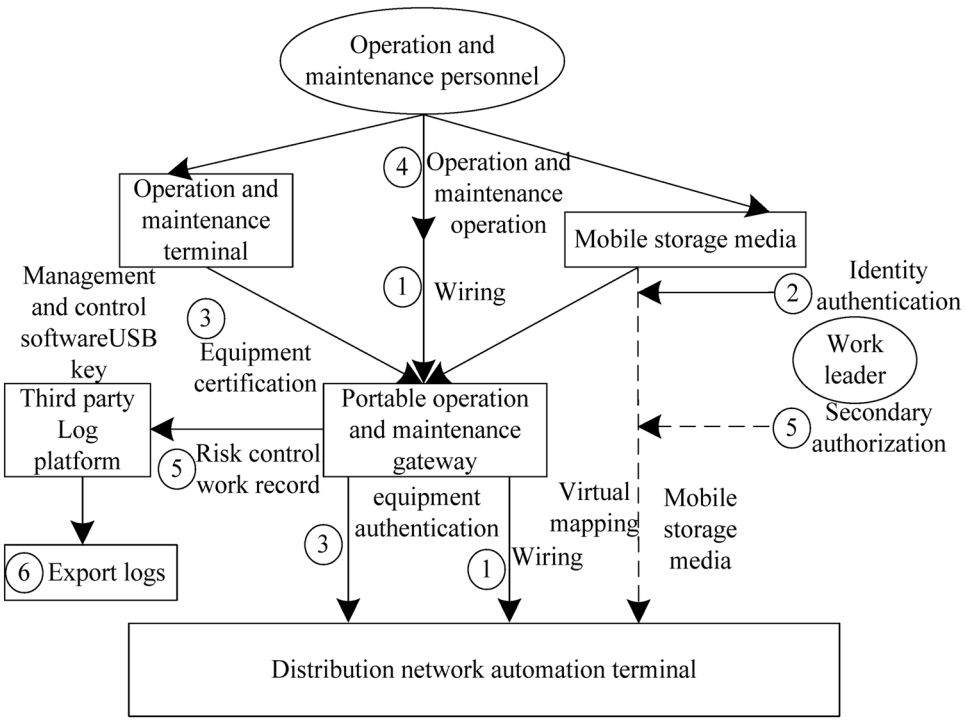


Fig. 2 Operation and maintenance supervision structure of distribution network automation terminals

During the operation and maintenance, the device controls illegal outreach, high-risk operation instructions, attack behaviors and malicious codes.
Record the operation screen, information transmission, communication message, risk control and interface use, etc., and the person in charge of the work will make a second authorization according to the situation.
After the operation and maintenance work, the operation and maintenance and audit records in the device can be uploaded to the third-party audit log management platform.

2.2 Distribution automation terminal network information security level protection mechanism

Considering the running state of distribution automation terminal, the network information security level of distribution automation terminal is divided into the following contents: (1) User independent protection level; Users decide how to protect resources. (2) System audit protection level; This level supports stronger independent protection ability. It has access audit capability, creating and maintaining audit tracking records of protected objects, recording date, time, user and event type of security-related events. All security-related operations can be recorded, so that when security problems occur in the system, the person responsible for the accident can be analyzed and traced according to the audit records. (3) Safety mark protection level; It has all the functions of the second-level system audit protection level, and implements mandatory access control for visitors and their access objects. The rights of visitors are restricted by assigning different security tags [17] to the visitors and the objects to be accessed. (4) Structured protection level; Extends the first three levels' capabilities to all visitors and objects, supporting formal security policies. Its structure is also structured, providing considerable anti-permeability ability. This level implements systematic security protection. (5) Access verification protection level; It has all the functions of the fourth level, and also has the ability to arbitrate whether visitors can access certain objects. Therefore, the security protection mechanism at this level is impervious to attacks and tampering, possessing robust anti-penetration capabilities. The network information security level's protective strength gradually escalates from the first to the fifth level, with each subsequent level (fifth, fourth, third, second, and first) building upon and complementing the previous, ensuring a cohesive and comprehensive security framework. Five-level information systems can be interconnected, and interconnected information systems should be classified and determined, and hierarchical protection should be implemented. Above the third level, it needs to be protected.

This article proposes that protection should be prioritized above the third level, rather than being limited to the fifth level, mainly related to the security protection capabilities, system importance, and actual security needs of each level. From the perspective of the progressive nature of security protection capabilities, from the first level to the fifth level, the

protection ability of network information security levels gradually increases. The third level already has relatively complete basic security protection capabilities, but there are still shortcomings for important information systems. Higher levels can further enhance security. In actual distribution automation terminal networks, after considering the importance of the system and conducting risk assessments, it is found that the data and business carried by systems higher than the third level are more critical to the stable operation of the power system. Once these systems are attacked, they may cause serious consequences, with a wide range of impacts and a high degree of harm, while the impact of attacks on third level and below systems is relatively limited. In addition, security protection requires corresponding costs to be invested, with the fifth level as the key protection boundary, which means that almost all systems must be protected according to the highest standards. This can lead to high costs in practice, and some systems may not require such a high level of protection. Taking the third level as the boundary can not only focus on ensuring the security of critical systems, but also achieve a good balance between cost and security, enabling the rational utilization of resources.

The rule-based access control method is used to control the user behavior in the network communication of distribution automation terminal. This article chooses rule-based access control methods instead of role-based access control, mainly considering the characteristics of distribution automation terminal networks. The network has numerous nodes and diverse user and data types. Rule based access control can develop flexible rules based on various factors such as terminal status, data security level, and user permission level to meet complex security requirements. Its rules are clear, easy to understand and operate, for example, by setting the relationship between users and keywords to clarify the usage permissions of users at different security levels, thereby simplifying the implementation of security policies. At the same time, this method can also develop specific rules for various security threats, effectively ensuring network security.

There are other access control methods besides rule-based access control. Role based access control (RBAC) is suitable for scenarios with clear roles and fixed permissions, but lacks flexibility in handling dynamic permission requirements. Although discretionary access control (DAC) is flexible, its permission management is too decentralized and poses security risks, making it less suitable for distribution automation terminal networks. Mandatory Access Control (MAC) has high security, but its management is complex and may affect system efficiency. In the distribution automation terminal, users belong to the subject and keywords belong to the object. The difference between subject levels is reflected in the right to use objects. Users with low security levels face more restrictions in network communication and can only use keywords consistent with their level. If keywords inconsistent with the level are used beyond authority during communication [18], the system will deal with the corresponding violations. High-level users usually have higher authority, and the level setting of users and keywords is managed by the system security officer.

When safeguarding the network information security level of distribution automation terminals, the object keywords are categorized into five confidentiality levels: prohibit, top secret, confidential, secret, and public, with the intensity of confidentiality arranged as follows: prohibit > top secret > confidential > secret > public. Correspondingly, user entities are classified into four levels: top secret, confidential, secret, and public. In the network information security level protection of distribution automation terminals, the access rights of different levels of subjects to objects are set as shown in Table 1.

After the user logs in to the distribution automation terminal and authenticates, their security level is determined. Keywords inaccessible to this level are identified based on Table 1. When a user uses the distribution automation terminal for network communication, if a keyword that does not match the user's security level appears in the information, the distribution automation terminal will detect it and handle it accordingly.

2.3 Distribution automation terminal network information security level key management

With the development of IoT technology, distribution automation terminals face increasing network security threats like data breaches, illegal access, and malicious control. These threats may affect the stable operation of the power system.

Formal security models, based on cryptographic security definitions and assumptions, describe and prove key management scheme security. A formal security model for distribution automation terminal key management includes:

Table 1 Access control permission table

Subject/object	Publicity	Secret	Confidential	Top secret	Prohibit
Publicity	Permit	Prevent	Prevent	Prevent	Prevent
Secret	Permit	Permit	Prevent	Prevent	Prevent
Confidential	Permit	Permit	Permit	Prevent	Prevent
Top secret	Permit	Permit	Permit	Permit	Prevent

Security objectives: Clarify objectives the scheme needs to achieve, such as confidentiality (preventing key leakage), integrity (preventing key tampering), availability (ensuring that keys can be accessed and used correctly when needed), etc.

Threat model: Define possible types of attackers, attack capabilities, and attack methods, such as internal attackers, external attackers, passive attacks, active attacks, etc.

Security assumptions: List basic assumptions the solution relies on, such as cryptographic algorithm security, communication channel security, and computing resource limitations.

Security proof: Based on security objectives and threat models, using cryptographic theory and tools to prove the security of key management schemes.

According to the network information security level protection mechanism of distribution automation terminals, the portable operation and maintenance security audit device adopts a linear geometric layered key management scheme to manage the keys of distribution automation terminals. This scheme is an innovative contribution of this article and not an existing key distribution scheme. It has a unique design that takes into account the operational status and security requirements of distribution automation terminals. For example, when dealing with cloud outsourcing data security sharing, the collaboration between data owners and various parties differs significantly from traditional solutions. Meanwhile, this scheme has unique construction rules, such as setting keys through specific vector inner product relationships for different access groups, which have not been seen in existing research. In addition, this key distribution scheme is part of the entire innovation management system, closely coordinated with network information security level classification, key derivation tree method, root key secure storage mechanism, and key exchange protocol to jointly enhance the security and efficiency of key management.

The framework diagram of network information security level key management is shown in Fig. 3.

According to Fig. 3, the scheme includes trusted third parties, data owners, distribution automation end users and cloud service providers. When using hierarchical key management for secure sharing of cloud outsourcing data [19], the data owner acts as the authorization center, encrypting shared data and transmitting the ciphertext to the cloud service provider's server. In addition, the data owner defines the hierarchical structure of the sharing group, and at the same time completes the sharing request of outsourcing data by the distribution automation end users. All distribution automation terminal users can make access requests to cloud service providers, and only those who have obtained private information and symmetric encryption keys can decrypt the ciphertext corresponding to their sharing rights [20].

Pseudorandom function F is defined as: $K \times D \rightarrow RG$. Among them, K is F's collection of keys, D and RG express the domain and interval of F. For $k \in K$, $F_k(x) = F(k, x)$ represent an example of F, suppose $Rand = \{g | g : D \rightarrow RG\}$ is for obedience D till RG set of all functions, h_F is a polynomial time adversary. With regard to $Rand$ or F functions in $g : D \rightarrow RG$, adversary h_F is able to access to the prophecy machine.

Setting access groups of distribution automation terminals $V_i, V_j \in V$, the indirect key calculation formula from V_i to V_j is:

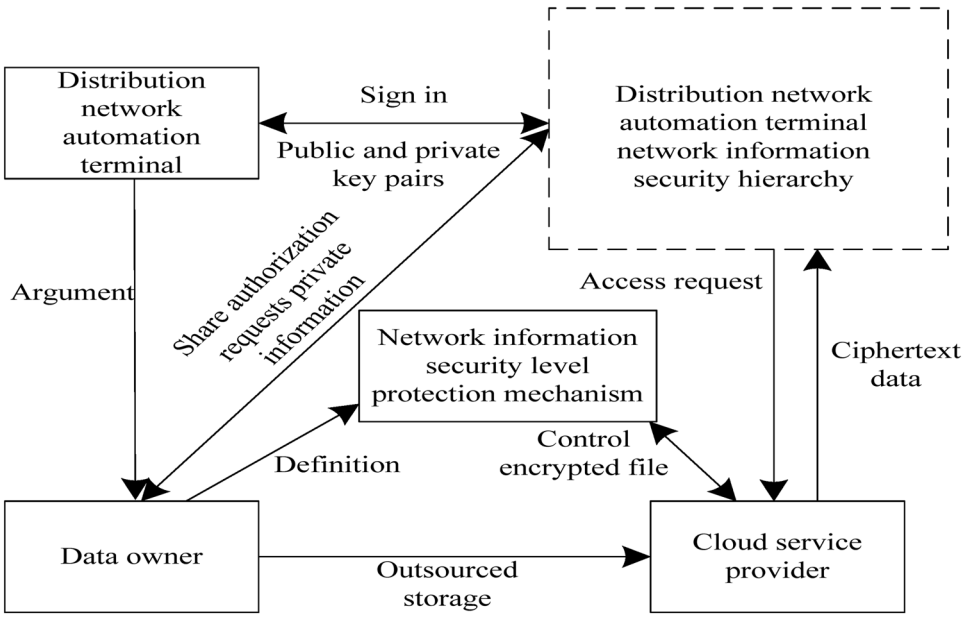


Fig. 3 Information security level secret key management scheme

$$k_{i,j} = \begin{cases} (k_{j,j} - w_{i,1}k_{i,i})w_{i,2}^{-1}, V_j \le V_i \\ 0, \text{other} \end{cases} \quad (1)$$

In the formula (1), $k_{i,i}$ and $k_{j,j}$ respectively for distribution automation terminal access groups of V_i and V_j's corresponding symmetric encryption key; $w_{i,1}$ and $w_{i,2}$ respectively through pseudo-random function F act on access groups V_i's private information.

The construction rules of information security level secret key management scheme for distribution automation terminals are as follows:

(1) For any access group V_i, private vector X_i and open vectors A_i's inner product between is equal to its corresponding symmetric encryption key, that is $X_i \times A_i^T = k_{i,i}$;
(2) If $V_i, V_j \in V$ and $V_i \in Anc(V_j, G)$, the distribution automation terminal accesses the group V_i's private vector of X_i and its public vector A_i's inner product of equals the indirect secret key $k_{i,j}$, namely $X_i \times A_i^T = k_{i,j}$;
(3) If $V_i, V_j \in V$ and $V_i \notin Anc(V_j, G)$, the distribution automation terminal accesses the group V_i's private vector of X_i and its public vector A_i's inner product of is equal to 0, that is $X_i \times A_i^T = 0$.

For $V_i, V_j \in V$ and $V_i < V_j$, needs to insert a new node V_t, namely $V_i < V_t < V_j$, randomly select two new nonzero vectors Y_t and Z_t and a $k_{t,t}$ respectively as groups V_t's corresponding private information and symmetric encryption key. If the access group V_t and there are distribution automation end users in the network, then use the secure channel to $((Y_t, Z_t), k_{t,t})$ and transmission to distribution automation end users, and then the access rights to all are lower than V_t's access group of is re-selected with a symmetric encryption key. Then complete the re-encryption of the data related to the distribution automation terminal and send it to the cloud service provider.

If the hierarchy contains $n + 1$ groups from which the data owner wants to delete a group, and sets the deleted distribution automation terminal access group as V_t, you must have access to all below V_t's access group of is updated to obtain its new symmetric encryption key [21]. Then complete the re-encryption of the data related to the distribution automation terminal and transmit it to the cloud service provider. In the key management framework for the network information security of distribution automation terminals, numerous keys are involved, necessitating the assignment of distinct keys to various security levels. Consequently, the decentralized storage of these keys is of paramount importance.

2.4 Distribution automation terminal network secret key decentralized storage technology based on secret key derivation tree

In the secret key management scheme for distribution automation terminal network's information security, the secret key tree method is used to store the secret key in a decentralized way. Figure 4 shows the structure diagram of this secret key distributed storage technology based on the secret key derivation tree.

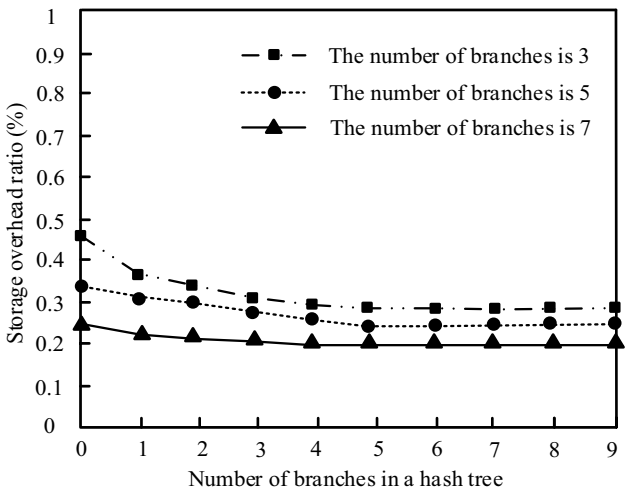


Fig. 4 Secret key decentralized storage technology

Analyzing the distributed storage technology of network key of distribution automation terminal in Fig. 4, the encryption and decryption process of distribution automation terminal information is completed by the client running on the private cloud. This process is divided into two parts: encryption and uploading of distribution automation terminal information and downloading and decrypting of distribution automation terminal information.

2.4.1 Distribution automation terminal network secret key generation and decentralized storage

In the context of decentralized storage of the network information security level secret key for distribution automation terminals, the process of generating the network secret key for such terminals is as follows:

(1) The length of the secret key generated by RSA encryption algorithm is 1024 bits [22].

(2) Generating two large prime numbers p and q, calculate $n = p \times q$.

(3) Calculate n Euler function of $\phi(n) = (p-1) \times (q-1)$.

(4) From $(1, \phi(n))$ randomly select one from the $\phi(n)$ number of coprime e as an encryption key.

(5) Calculate the satisfaction $ed = 1 \bmod \phi(n)$'s decryption key of the equation will encrypt the key e, n open, the secret key d will be decrypted according to the network information security level for decentralized storage.

The key splitting process of distribution automation terminal network is as follows:

(1) The sub-key management server independently and randomly constructs one $t-1$ polynomial of degree $f(x) = K + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1}$.

(2) Selection of sub-key management server t a different number x_t and will x_t bring in the above polynomials and calculate them to get the corresponding ones t individual y_t.

(3) The sub-key management server sends the corresponding y_t distribute to the sub-key storage server, and make corresponding records on the management server.

The key derivation tree is constructed, and the sub-key and the sharing scheme of network users with different information levels in the distribution automation terminal network are established. Determine the storage number of sub-keys of different network nodes of the distribution automation terminal, and store the calculation results in the database of the key management server. Select the corresponding confidential information to be encrypted, and use the generated secret key to encrypt the information. Accord to that sub-key sharing scheme establish by the key management server, the sub-key management server will correspondingly y_t distribute to the sub-key storage server and make corresponding records on the management server.

The key recovery process of distribution automation terminal is as follows:

(1) Let t of n sharers show their sub-keys, and get t point of $(x_1, y_1), (x_2, y_2), \cdots, (x_t, y_t)$.

(2) Lagrange interpolation formula (for key recovery):

$$f(x) = \sum_{j=1}^{t} y_j \prod_{1 \le i \le j, i \ne j} \frac{x - x_t}{x_j - x_i} \tag{2}$$

In the process of key recovery in the distribution automation terminal network, the point $(x_i, y_j)\,(i = 1, 2, \cdots, t)$ corresponding to the sub keys of t sharers is known. By using this formula to recover the key generation polynomial $f(x)$, the original key is obtained. This is based on the Lagrange interpolation principle and is used in key management to recover the complete key from partial sub key information.

Key recovery result formula:

$$f(x) = K + a_1 x + a_2 x^2 + \cdots + a_{t-1} x^{t-1} \tag{3}$$

(3) $K = f(0)$.

After recovering the key generation polynomial $f(x)$ using formula (2), substitute $x = 0$ into the polynomial to obtain the original key k [23]. This step completes the calculation of the final key that needs to be recovered from the polynomial, and is a key step in the key recovery process.

Select the information to be decrypted, decrypt the confidential information with the recovered secret key, and destroy the secret key after successful decryption.

2.4.2 Construction of secret key derived tree of distribution automation terminal network

The secret key distributed storage technology uses a hash tree with secret key as the derivation structure. In the hash tree with key, a key tree manages numerous information encryption keys derived from the root key, with lower-level keys controlling smaller information ranges. The value of the leaf node is the secret key to a single information block. The size of information controlled by the secret key at the same level should be the same. To minimize the storage overhead, each layer has the same number of branches. In this way, it is not necessary to store the whole tree structure, but only the number of layers and the number of branches of leaf nodes of each node can be stored to calculate the whole tree structure.

When establishing the key derivation tree, the root node of the key state hash tree is set as the root key K_r, the status of all nodes $S_{x,y}$ all are 0, which means it has never been revoked. The key value of each child node is calculated by using the key and state value of the parent node. That is to say, the number 1 with the key in the hash tree is the layer for calculating x. The key calculation formula for the derived tree node corresponding to y is:

$$K(x,y) = H\left(K_{parent}, x \| y \|^{*} S_{x,y}\right) \tag{4}$$

Among them, K_{parent} is $K(x,y)$'s secret key corresponding to the parent node, which is a known secret key,$H()$ is the encryption algorithm used by the secret key. Use $x\|y$ in order to ensure that all block keys are different from each other, add before"*"the $S_{x,y}$ in order to avoid the problem that two keys are the same which may be caused by direct serial connection.

When a distribution automation terminal user performs a key revocation operation on some nodes in a hash tree with a key and a state, the state value of the key of the corresponding node is revoked at first $S_{x,y} = S_{x,y} + 1$, indicating that this node has been revoked once, and the key is recalculated according to the formula in the process of key calculation, which is used as the information encryption key and distributed to the new users of distribution network automation terminal. New users of distribution automation terminal use this secret key to encrypt their own information. The secret key of the original distribution automation terminal user cannot decrypt this information, which ensures the security of the new user information of the distribution automation terminal.

When the distribution automation terminal communicates with the network, there is data overflow in the storage data type of the state value S. When the number of secret key updates exceeds $S_{x,y}$'s field of, add one more"*"in the calculation formula $S_{x,y}$, the formula for adjusting the key calculation of key derived tree nodes during data overflow is:

$$K(x,y) = H\left(K_{parent}, x \| y \|^{**} S_{x,y}\right) \tag{5}$$

Make the corresponding $S_{x,y} = 0$. When it exceeds the number domain again, repeat this process to ensure that the information security level key management scheme of the distribution automation terminal can always run.

The key management scheme for information security level of distribution automation terminal network proposed in this article includes multiple formulas that play a core role in key management and distributed storage technology. Among them, formula (1) is innovatively used to calculate indirect keys, demonstrating a new approach to key management mechanisms in this paper. Formulas (4) and (5) respectively address the node key calculation and data overflow situation in the key derivation tree, and are the core computing methods of key distributed storage technology, reflecting the important contribution of this paper. In addition, formulas (2) and (3) are based on the classical Lagrange interpolation principle and have been effectively applied in the key recovery process of distribution automation terminal networks in this article. Although these principles are not original to this article, they have been appropriately applied and explained in specific contexts.

2.4.3 Secure storage mechanism of root key and key exchange protocol

The safe ensures the security of the root key in the key derivation tree and the efficiency of use. The root secret key is safely stored in the public cloud, while the private cloud only bears the calculation overhead derived from the secret key, without bearing storage overhead. This process involves the distribution of root keys among different computing nodes in public and private clouds. To meet the requirements of key distribution, a key exchange protocol is designed for the information security level key management scheme of distribution automation terminal

network. Secret key exchange is divided into two processes: information encryption and uploading and information download and decryption. Use K_r represents the root key, BS represents a hash tree configuration represen that state of the key, K_{f,x_i,y_i} represents the secret key corresponding to the information group, $< P_0, P_1 \cdots >$ represents the access rights list of distribution automation end users, KU_A and KR_A respectively represent the public key and the private key of the distribution automation terminal user, $E_{KU_{KDS}}$, E_{KU_A} and $D_{KR_{KDS}}$, D_{KR_A} respectively indicate the use of corresponding public key encryption and private key decryption, KU_{KDS}, KR_{KDS} represents the public key and private key of the key distribution server.

In the distribution automation terminal network, when a new information group f establishing, the key exchange needs the following steps:

(1) The terminal users of distribution network automation will build a clear text safe. $< K_r, BS, P_0, P_1 \cdots >$ as an encrypted configuration of information group, it is sent to the client of distribution network automation terminal.
(2) The distribution automation terminal client, which firstly sends the plaintext safe to the key distribution server and requests the information encryption key, and then use KU_A and KU_{KDS} encrypt the root keys separately, and the safe will be encrypted after encryption completed and send $< E_{KU_{KDS}}(K_r), E_{KU_A}(K_r), BS, P_0, P_1 \cdots >$ to the public cloud for storage.
(3) The key distribution server returns K_{f,x_i,y_i} encrypt information for distribution network automation terminal client. It should be noted that in step (2), if the performance of the key distribution server reaches the bottleneck, the plaintext safe will be sent to the newly-built key distribution center to increase the key distribution capacity.

When the distribution network automation terminal client computing node C_i of a private cloud receives a part of the downloaded and decryption information group f of the distribution network automation terminal users, the following steps are taken.

(4) The secret key distribution server obtains the encrypted safe from the public cloud $< E_{KU_{KDS}}(K_r), BS, P_0, P_1 \cdots >$.
(5) The secret key distribution server passes through $< P_0, P_1 \cdots >$ judge C_i whether you have access rights. If the distribution automation terminal client C_i access is allowed, and the key distribution server uses its own private key to decrypt the root key in the safe. $< D_{KR_{KDS}E_{KU_{KDS}}(K_r)}, BS, P_0, P_1 \cdots >$. The secret key K_{f,x_i,y_i} passed by the key distribution server K_r and hash tree configuration calculation with secret key. If necessary, send the plaintext safe to the newly-built key distribution center for key distribution.
(6) The secret key distribution server returns K_{f,x_i,y_i} to the distribution network automation terminal client for information decryption.

The main advantage of the key exchange protocol is that the key distribution server can remain stateless in essence, and can obtain high parallelism and security.

The CK model, as a security model for key exchange protocols, mainly focuses on the definition of protocol security and adversary capabilities. In the CK model, the capabilities of the adversary (attacker) are usually more powerful than in the BR model, which may include: complete control of network traffic: the adversary is able to listen, intercept, modify, or inject any message into the network. Obtaining participant information: Adversaries may obtain some or all of the participant's internal state, including long-term keys, session keys, session state, etc. [24]. Session key inquiry: An adversary can request the session key of a completed session. Session state disclosure: The adversary may request the disclosure of the internal state of a session, such as temporary information.

The CK model requires the protocol to generate secure session keys even with adversaries present. Use strong encryption algorithm (AES) to encrypt session keys and transmitted data. Design security experiments to simulate adversary attack behavior and verify protocol performance under these attacks. Key isolation ensures session key generation doesn't rely on information controllable or obtainable by adversaries. Through the key negotiation process between participants, a session key known only to both parties is jointly generated.

The CK model also focuses on protocol forward security, meaning if a participant's long-term key is leaked, previously established session keys should remain secure. Long-term key leakage will not damage past session keys, the highest standard of forward security.

In the CK model, Diffie Hellman key exchange protocol ensures secure negotiation of session keys. Digital signatures and public key encryption authenticate participants' identities to prevent man in the middle attacks. Timestamps and

random numbers prevent replay attacks. Implement a comprehensive error handling mechanism and logging function to detect and fix issues during protocol execution.

For continuous distribution automation terminal information in the key tree, send the highest node key within authority and key tree structure to the client. The client can derive the key itself, saving communication overhead with only one communication. This fast method improves key management level through efficient key decentralized storage.

3 Experimental test

The electric power system of a city is selected as the test object of the secret key distributed storage technology, and the portable operation and maintenance gateway of HR YWSJ-3000 of Zhuhai Hongrui is used as the operation and maintenance gateway of the distribution automation terminal of the electric power system. The startup time of the distribution automation terminal operation and maintenance gateway is less than 1 min, and when the network port is connected, the number of concurrent support operation and maintenance terminals is higher than 7.

Classify network information security levels based on the user situation of distribution automation terminals. Collect relevant information from different users, classify users into different subject security levels based on the proposed network information security level protection mechanism, and determine corresponding object security levels and access control permissions. The classification results are recorded in Table 2 to verify the effectiveness of this technology in classifying user security levels.

From the classification results of information security for distribution automation end users in Table 2, different end users are accurately classified into corresponding security levels. For example, for user ID 51816421, the subject security level is public, the object security level is secret, and the access control permission is allowed. This provides a basic basis for the subsequent distributed storage of keys.

Using the distributed storage technology studied in this article to store distributed keys for distribution automation terminals, encryption and decryption operations were performed on information of different sizes (24KB-16384KB). The encryption time, key processing time, decryption time, and total time were calculated for each information size, and the results were recorded in Table 3. By analyzing these time data, evaluate whether the encryption, decryption efficiency, and key processing performance of this technology meet the needs of distribution automation terminals when processing information of different scales.

Analysis of information encryption and decryption time of distribution automation terminal in Table 3 shows that encryption, decryption, and key processing time are all less than 500 ms with different information sizes, and total key processing time is less than 100 ms. The experimental results show that processing information encryption and decryption using this technology takes less time, meeting the required processing time for distribution automation terminals. The time to process the secret key is the fragmentation time after encryption plus the assembly time before decryption, which is related to the length of the secret key. Due to equipment and experimental environment, encryption and decryption time does not increase linearly, but generally increases with information size.

Table 2 Results of information security classification of end-user in distribution network automation

End user ID	Main security level	Object security level	Access control authority
51,816,421	Publicity	Secret	Permit
11,354,512	Secret	Confidential	Permit
20,541,811	Confidential	Publicity	Prevent
13,842,004	Publicity	Confidential	Permit
25,942,341	Secret	Top secret	Permit
16,484,564	Prohibit	Confidential	Prevent
95,438,461	Confidential	Publicity	Prevent
71,806,189	Publicity	Confidential	Permit
38,451,601	Publicity	Top secret	Permit
28,456,104	Secret	Secret	Permit

Table 3 Information encryption and decryption time of distribution network automation terminal

Information size/KB	Encryption time/ms	Key processing time/ms	Decryption time/ms	Total time/ms
24	35	28	18	81
64	52	34	28	114
128	72	58	42	172
256	94	81	56	231
512	125	94	72	291
1024	146	115	91	352
2048	175	135	105	415
4096	225	175	135	535
8192	284	226	167	677
16,384	452	285	256	993

Taking the hash tree with branch numbers of 3, 5, and 7 as an example, calculate the percentage of storage cost of the distribution automation terminal key state hash tree to the original scheme's storage cost. By changing the depth and number of branches of the hash tree, simulating different storage structures, and analyzing their impact on storage overhead, the statistical results are shown in Fig. 5, in order to explore the optimization effect of this technology in storage.

Experimental results in Fig. 5 show that as the depth of the hash tree using secret keys and states increases, storage cost decreases. For the same depth, more branches result in lower storage overhead. With 7 branches, a minimum storage overhead of 0.2 can be achieved. It should be noted that in the distribution automation terminal, the root secret key of the hash tree with secret key and state is protected by the safe and stored in the public cloud. When needed, the public cloud sends it to the private cloud to derive the secret key and decrypt the file. The private cloud only bears the storage and calculation overhead of the tree structure, not the root secret key storage.

Calculate the changes in the number of key trees when storing keys using this technique under different key revocation rates. Set different numbers of terminals (10, 20, and 30) and observe the stability of the number of key trees under various key revocation rates. The statistical results are shown in Fig. 6 to verify the effectiveness of key derivation tree technology in saving key tree management and storage overhead.

As shown in Fig. 6, when the key revocation rate differs, the number of key trees remains unchanged regardless of the number of terminals. At 10, 20, and 30 terminals, the number of key trees remains constant at 6, 12, and 16, respectively. This is because the technique used in this article is to store the key in a decentralized manner in the distribution automation terminal, with the number of key derived trees remaining unchanged. The secret key of distribution automation terminal is revoked frequently, and the derived tree technology adopted here effectively saves secret key tree management and storage overhead, providing an effective basis for reliable operation of distribution automation terminal.

Use this technology to store keys in the distribution automation terminal network and calculate the time cost of generating key distribution for different numbers of users. Gradually increase the number of users and record the

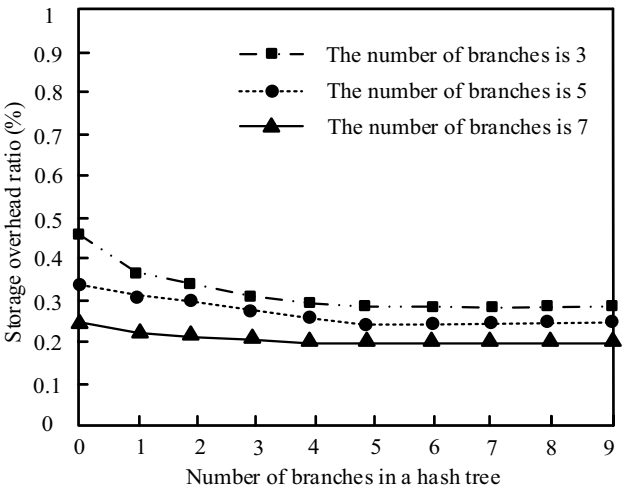


Fig. 5 Storage overhead ratio

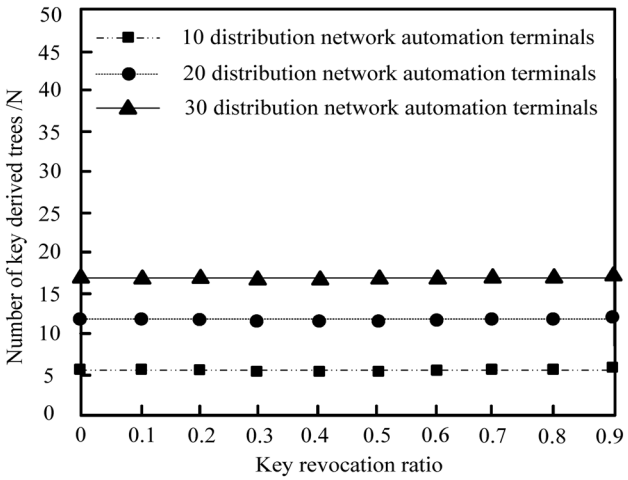


Fig. 6 Comparison of the number of secret key trees

corresponding time cost. When the number of users reaches 450, record the maximum time cost. The statistical results are shown in Fig. 7, and then evaluate the time efficiency of this technology in achieving key distributed storage under different user sizes.

As seen from the experimental results in Fig. 7, when this technology stores the secret key in the distribution automation terminal network, the time overhead remains low with different users. When the number of users reaches 450, the maximum time cost is 463 ms. Using this technology to dynamically manage the secret key of the distribution automation terminal network enables quick distributed storage of the secret key and improves operation efficiency. When encrypting and decrypting large files, the impact on total encryption and decryption time is significantly reduced, which is practical.

By using this technology to store keys in the distribution automation terminal network, monitoring the information of the distribution automation terminal during network communication, identifying illegal external connections, attack behaviors, and high-risk instructions, as well as the blocking effect on high-risk instruction communication, the statistical results are recorded in Table 4 to test the security protection ability of this technology for distribution automation terminal information communication.

Experimental results in Table 4 show that using this technology to store the secret key in the distribution automation terminal network can effectively identify illegal outreach, attack behavior and high-risk instructions. After identifying high-risk instructions, information communication can be blocked in time to ensure the distribution automation terminal maintains a reliable running state.

At present, there are various solutions in the field of key management for distribution automation terminal networks. For example, Saikia et al. used Delaunay triangulation technology to distribute keys to sensor nodes in wireless sensor networks, and improved the security of the network by optimizing the key distribution between nodes. Gupta et al. applied a quantum lightweight identity based two party authentication key exchange protocol to the Internet

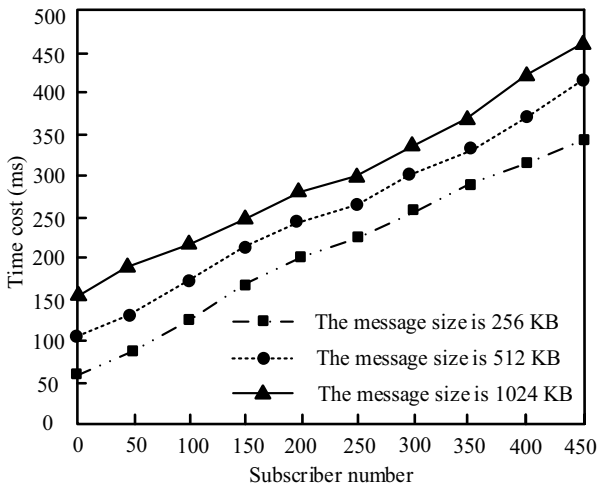


Fig. 7 Key distribution generation time overhead

Table 4 Information communication security of distribution network automation terminal

Session sequence number	Identify content	Controls
1	High risk order	Prevent
2	Illegal outreach	Prevent
3	Aggressive behavior	Prevent
4	Illegal outreach	Prevent
5	Aggressive behavior	Prevent
6	Illegal outreach	Prevent
7	Aggressive behavior	Prevent
8	Illegal outreach	Prevent
9	High risk order	Prevent
10	Illegal outreach	Prevent

of Things, leveraging the characteristics of quantum technology to enhance the security of key exchange. Vasudevan et al. proposed an integrated method for energy-efficient switching and key distribution protocols, aiming to meet the dual requirements of energy efficiency and security in dense mobile networks. The comparative content and advantage analysis are shown in Table 5.

From this, it can be seen that the distributed storage technology for distribution automation terminal network information security proposed in this article demonstrates significant advantages in terms of security level granularity, key management flexibility, key management efficiency, security assurance, and targeted application scenarios. Compared with other solutions, this technology is more in line with the actual needs of distribution automation terminal networks, and has stronger targeting and practicality. At the same time, this technology also considers factors such as scalability, resource consumption, and implementation and maintenance difficulty, providing a new solution for the safe operation of the power system. Through continuous research and innovation, we believe that this technology will further promote the development of the power system and bring greater improvements to the safety and reliability of the power grid.

To present the key findings of this study more clearly, the findings are summarized in table form as follows, as shown in Table 6:

4 Conclusion

This article studies the distributed storage technology for network information security of distribution automation terminals. This technology divides distribution automation terminals into different security levels and uses a linear geometric layered key management scheme to achieve distributed storage of keys, thereby improving the level of network information management. Firstly, the design of this technology considers the operational status of distribution automation terminals and the network information security level protection mechanism, setting information security levels for distribution automation terminals, setting five security levels for terminals. This approach eliminates single point risks and improves system security and reliability. Secondly, this technology uses the key derivation tree method to construct a key derivation tree, combined with the root key secure storage mechanism and key exchange protocol, to manage and distribute terminal keys. This method reduces the risk of key leakage and prevents malicious attackers from obtaining sensitive information. Experimental results show significant advantages. As information scale increases, encryption, decryption, and key processing time gradually increases, but remains within 993ms, meeting practical application requirements.

However, limitations exist. Although the key derivation tree method can effectively construct key derivation trees, it may face computational complexity challenges in large-scale networks, requiring further optimization of the algorithm to improve efficiency. Future research will explore more efficient and secure key management mechanisms to address evolving network security threats.

In conclusion, the distributed storage technology for network information security of distribution automation terminals provides a new solution for the safe operation of power systems. Through continuous research and innovation, we believe that this technology will further promote the development of the power system and bring greater improvements to the safety and reliability of the power grid.

Table 5 Comparison of key management solutions for distribution automation terminal networks

Comparing dimensions	This article's proposal	Other schemes (taking Saikia, Gupta, Vasudevan and others' schemes as examples)
Granularity of security level classification	According to the terminal operating status, it is divided into five levels, refined management, and differentiated security strategies are formulated to achieve precise protection	Lack of detailed division of distribution automation terminals and adoption of universal safety strategies makes it difficult to meet specific needs
Key management flexibility	Dynamically generate derived keys, with strong adaptability and flexible adjustment of key generation and distribution strategies	Poor flexibility, difficult to meet diverse key requirements, and response speed may be limited
Key management efficiency	Linear geometry layered key management scheme simplifies processes and improves efficiency	Insufficient utilization of the hierarchical mechanism results in low management efficiency and may lead to efficiency bottlenecks
Security guarantee	Equipped with root key secure storage and key exchange protocol, providing full process security protection	The security guarantee may not be perfect, and there are potential risks in the process of key storage and exchange
Targeted application scenarios	Specially designed for distribution automation terminal network, tailored to actual needs	Mainly targeting other types of networks, with insufficient specificity for distribution automation terminal networks
Scalability and compatibility	Design considering future expansion needs, compatible with multiple distribution automation terminals	Scalability may be limited, requiring additional adaptation for different terminals
Resource consumption	Optimize the key management process to reduce computation and resource consumption	Possible high resource consumption due to complex algorithms or protocols
Difficulty in implementation and maintenance	The plan is concise and clear, easy to implement and maintain	Possible increased difficulty in implementation and maintenance due to technological complexity

Table 6 Key findings of research on distributed storage of distribution terminal keys

Research contents	Discovery results
Classification of Network Information Security Levels	Based on the information of distribution automation end-users, it is possible to effectively classify the security level of network information and provide a basis for key distributed storage. Different users correspond to different subject security levels, object security levels, and access control permissions (refer to Table 2)
Information encryption, decryption, and key processing time	Under different information sizes, the encryption, decryption, and key processing time of distribution automation terminal information are all less than 500 ms, and the total key processing time is less than 1000 ms, meeting the requirements for encryption and decryption processing time of distribution automation terminal information. And the overall encryption and decryption time increases with the increase of information size (refer to Table 3)
Storage overhead of key state hash tree	As the depth of the hash tree using keys and states increases, storage costs decrease; At the same depth, the more branches there are, the lower the storage overhead. When the number of branches is 7, a minimum storage overhead of 0.2 can be achieved. Private clouds do not need to bear the cost of root key storage, only the storage and computing costs of the tree structure (refer to Fig. 5)
Change in the number of key trees	Under different key revocation rates, the number of key trees remains unchanged regardless of the number of terminals. When there are 10, 20, and 30 terminals, the number of key trees remains stable at 6, 12, and 16, respectively. The derived tree technology saves key tree management and storage costs (refer to Fig. 6)
Key distribution generation time overhead	Using this technology to store keys with different numbers of users results in lower time overhead. When the number of users reaches 450, the maximum time cost is 463 ms, which can quickly achieve distributed key storage and improve key operation efficiency (refer to Fig. 7)
Information and communication security management	Using this technology to store keys can effectively identify illegal external connections, attack behaviors, and high-risk instructions, and promptly block high-risk instruction communication to ensure reliable operation of distribution automation terminals (refer to Table 4)

Author contributions All authors contributed to the study conception and design. Material preparation, data collection and analysis were performed by Weijie Huang, Lianghao Huang, Guozheng Huang, Guangyong Zheng and Yongle Li. The first draft of the manuscript was written by Jin Yi and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.

Funding No funding was received for conducting this study.

Data availability Data is provided within the manuscript or supplementary information files.

Declarations

Ethics approval and consent to participate The research met all applicable standards for the ethics of experimentation.

Consent for publication Not applicable.

Competing interests The authors declare no competing interests.

Open Access This article is licensed under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License, which permits any non-commercial use, sharing, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if you modified the licensed material. You do not have permission under this licence to share adapted material derived from this article or parts of it. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. If material is not included in the article's Creative Commons licence and your intended use is not permitted by statutory regulation or exceeds

the permitted use, you will need to obtain permission directly from the copyright holder. To view a copy of this licence, visit http://creativecommons.org/licenses/by-nc-nd/4.0/.

References

1. Gao Z, Liu Y, Qi F, Chen H. Scale-free topology security mechanism of wireless sensor network against cascade failure. Int J Commun Syst. 2021;34(10):e4810.1-e4810.13.
2. Ai C, Liu HJ. Active distribution network reliability evaluation considering automation equipment failure in multiple scenarios. Modern Electr Power. 2024;41(3):412–20.
3. Li Y, Zhang D, Yeoh PL, He Z, Chen G, Ji Z, et al. Secret key generation for intelligent reflecting surface assisted wireless communication networks. IEEE Trans Veh Technol. 2021;70(1):1030–4.
4. Sun SJ, Minjae J, Yeon HJ, Jaehwan L. A verifier-based password-authenticated key exchange using tamper-proof hardware. Comput J. 2021;64(8):1293–302.
5. Kumar MS, Ramanathan R, Jayakumar M, Yadav DK. Physical layer secret key generation using discrete wavelet packet transform. Ad Hoc Netw. 2021;118:102523.1-102523.15.
6. Deb R, Roy S. A software defined network information security risk assessment based on pythagorean fuzzy sets. Expert Syst Appl. 2021;183:115383.1-115383.17.
7. Zhang YM. A mathematical model of conformal encryption for network data based on block cipher. Comput Simul. 2022;39(03):466–9.
8. Chen J, Miao Y. Research on security evaluation system of network information system based on rough set theory. Int J Internet Protoc Technol. 2021;14(3):155–61.
9. Zhang Q, Zhu L, Li Y, Ma Z, Yuan J, Zheng J, et al. A group key agreement protocol for intelligent internet of things system. Int J Intell Syst. 2022;37(1):699–722.
10. Qiu YC, Zhao LP. Impact resistance prediction of fuselage coatings based on improved neural network. Ordnance Mater Sci Eng. 2022;45(05):148–53.
11. Ree MD, Mantas G, Rodriguez J, Otung IE, Verikoukis C. Distant: distributed trusted authority-based key management for beyond 5g wireless mobile small cells. Comput Commun. 2021;176:218–33.
12. Tseng YM, Chen JL, Huang SS. A lightweight leakage-resilient identity-based mutual authentication and key exchange protocol for resource-limited devices. Comput Netw. 2021;196:108246.1-108246.13.
13. Saikia M. Delaunay triangulation based key distribution for three-dimensional wireless sensor networks. J Interconnect Netw. 2021;21(1):2150009.1-2150009.13.
14. Gupta DS, Ray S, Singh T, Kumari M. Post-quantum lightweight identity-based two-party authenticated key exchange protocol for internet of vehicles with probable security. Comput Commun. 2022;181:69–79.
15. Vasudevan VA, Tayyab M, Koudouridis GP, Gelabert X, Politis I. An integrated approach for energy efficient handover and key distribution protocol for secure nc-enabled small cells. Comput Netw. 2022;206:108806.1-108806.13.
16. Dong X, Hu Y, Wang B, Liu M, Gao W. Lattice-based revocable attribute-based encryption with decryption key exposure resistance. IET Inf Secur. 2021;15(6):428–41.
17. Valle DC, Quezada LF, Dong SH. Bell-ghz measurement-device-independent quantum key distribution. Ann Phys. 2021;533(9):2100116.1-2100116.8.
18. Zhao H, Li H, Xu Y, Huang P, Wang T, Zeng G. Simple continuous-variable quantum key distribution scheme using a sagnac-based Gaussian modulator. Opt Lett. 2022;47(12):2939–42.
19. Qu W, Zhang Y, Lu Y, Wang G. Low-cost lightweight-client twin-field quantum key distribution network with wavelength division multiplexing. Opt Eng. 2022;61(1):016201.1-016201.9.
20. Xiong P, Su Q. Key distribution strategy of wireless sensor network based on multi-hash chain. J Web Eng. 2021;20(3):713–42.
21. Lu Y, Wu F, Huang Q, Tang S, Kong L, Chen G. Shared secret key generation by exploiting inaudible acoustic channels. ACM Trans Sens Netw (TOSN). 2021;18(1):13.1-13.26.
22. Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM. 1978;21(2):120–6.
23. Yuanyuan LI, Xiaoqing YOU, Jianquan LU, et al. A joint image compression and encryption scheme based on a novel coupled map lattice system and DNA operations. Front Inf Technol Electron Eng. 2023;24(6):813–27.
24. Wilson J, Asplund M, Johansson N. Extending the authentication hierarchy with one-way agreement. In: 2023 IEEE 36th computer security foundations symposium (CSF). IEEE; 2023. pp. 214–228.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.