International Journal for Housing Science and Its Applications
Publish August 10, 2025. Volume 46, Issue 4 Pages 181-191

https://doi.org/10.70517/ijhsa46414

Distributed Ledger Enabling Trusted Traceability and Quality Gating Enhancement for Software Development Security Testing in the Power Industry

Kongsheng Lin[1], Xiangyu Lei[1] and Heng Xia[1,*]
[1] Digital Operation Center, Guangxi Power Grid Co., LTD., Nanning, Guangxi, 530000, China
Corresponding authors: (e-mail: 18767164710@139.com).

Abstract Power industry software, as a core tool for modern power equipment control and management, is facing increasingly severe cybersecurity threats. Distributed ledger technology provides new ideas for power software security detection due to its decentralization, transparency and tamper-proof characteristics. This paper discusses the application of distributed ledger technology in the security detection of software development in the electric power industry, and proposes a trusted traceability and quality access control reinforcement method based on distributed ledger. The research designs the traceability data model and smart contract system to realize the trusted collection, storage and verification of security data; at the same time, it proposes the sensitive data aggregation method based on homomorphic encryption and the tamper-proof technology of RSA asymmetric encryption, and constructs the data communication structure of Overlay structure, which guarantees the complete transmission of electric power software security detection data and traceability tracking. The experimental results show that compared with SHA256 algorithm and DyRH model, the average value of the error localization time of this method is reduced to 9.23ms, which is 8.6ms and 4.1ms less than the control group, respectively; the accuracy rate of the error localization reaches 98.33%, which is improved by 4.77% and 1.79%; and in the test of the anti-attack performance, the average number of tampered data is only 189, which is respectively reduced by 184 and 156. The study proves that distributed ledger technology can effectively enhance data credibility, strengthen traceability, and enhance the strength of system quality access control in software development security detection in the power industry, which provides a new technical path and solution for the information security of the power system.

Index Terms distributed ledger, power industry, software development, security detection, credible traceability, quality access control

I. Introduction

In the rapid development of the Internet, the power industry is facing unprecedented cybersecurity threats. As a national critical infrastructure, the power system has long been not a simple collection of physical equipment, but a complex system that deeply integrates information technology [1]. Among them, power industry software has become a core tool for modern power equipment control and management, from power stations to transmission lines to household meters, behind which there is a large amount of data interaction and intelligent control, which provide a convenient way to maintain the efficient operation of the power system, fault detection and repair, such as the power application software package, DSIM power electronics simulation software, PSCAD, and the online State Grid, etc. [2]-[6]. However, their security and reliability are facing more and more serious challenges head-on. First, hackers, viruses, malware through network infiltration and attack means, steal sensitive information, interfere with power system operation and control, and may even lead to power system paralysis, equipment failure and data loss, resulting in serious harm, and the annual attack rate can be more than 50% year-on-year growth [7], [8]. Secondly, the new energy grid-connected power generation makes the power system information expansion, the network attack area increases, the detection workload of the power monitoring software increases, and part of the software is co-developed by multiple enterprises, in the coordinated operation, the quality of the data transmission decreases [9], [10]. Thirdly, there is a dependency relationship between the series of software in the power industry, and the vulnerability of its open source components leads to an increase in the risk of the software supply chain, in which the chain of vulnerability traceability is not connected [11], [12].

In recent years, distributed ledger technology, as an emerging financial technology, has received widespread attention can be used for transaction settlement, security upgrades, supply chain tracking and many other aspects

[13]-[15]. Distributed ledger technology is a technology that shares and verifies data through multiple nodes, and its core principles include consensus mechanism, encryption algorithm and distributed storage. It has the characteristics of decentralization, transparency and non-tampering. This technology can effectively improve the security and reliability of data while protecting the privacy of users, specifically, since distributed ledger technology does not rely on any centralized institution, it can improve the system's resistance to attack and trustworthiness [16], [17]. The data on the distributed ledger is visible to all participants and cannot be tampered with due to authentication and synchronization through multiple nodes, which improves the transparency and trust in the market [18], [19]. Distributed ledger technology can reduce intermediate links, simplify the transaction process, improve transaction efficiency and reduce costs [20]. Distributed ledger technology has injected new kinetic energy into the trusted traceability and quality optimization of software security testing in the power industry.

In the current rapid development of the Internet, the power industry is facing unprecedented cybersecurity threats. As a national critical infrastructure, the power system has long been not a simple collection of physical equipment, but a complex system that deeply integrates information technology. Among them, power industry software has become the core tool for modern power equipment control and management, from power stations to transmission lines to household meters, behind which there is a large amount of data interaction and intelligent control, which provide convenient maintenance of the efficient operation of the power system, fault detection and repair, such as the power application software package, DSIM power electronics simulation software, PSCAD, online national network, etc.. However, their security and reliability are facing more and more serious challenges. First, hackers, viruses, malware through network infiltration and attack means, steal sensitive information, interfere with power system operation and control, and may even lead to power system paralysis, equipment failure and data loss, resulting in serious harm, the annual attack rate can be increased by more than 50% year-on-year. Secondly, the new energy grid-connected power generation makes the power system information expansion, network attack area increases, the detection workload of the power monitoring software increases, and part of the software co-developed by a number of enterprises, in the coordinated operation, the quality of the data transmission declines. Thirdly, there is a dependency relationship between the series of software in the power industry, and the vulnerability of its open source components leads to an increase in the risk of the software supply chain, in which the vulnerability traceability chain is not connected.

In recent years, distributed ledger technology, as an emerging financial technology, has received widespread attention can be used for transaction settlement, security upgrades, supply chain tracking and many other aspects. Distributed ledger technology is a technology that shares and verifies data through multiple nodes, and its core principles include consensus mechanism, encryption algorithm and distributed storage. It is characterized by decentralization, transparency, and non-tampering. This technology can effectively improve the security and reliability of data while protecting the privacy of users. Specifically, since distributed ledger technology does not rely on any centralized institution, it can improve the system's resistance to attack and credibility. Due to verification and synchronization through multiple nodes, data on the distributed ledger is visible to all participants and cannot be tampered with, improving market transparency and trust. Distributed ledger technology can reduce intermediate links, simplify the transaction process, improve transaction efficiency and reduce costs. Distributed ledger technology injects new momentum into the trusted traceability and quality optimization of software security testing in the power industry.

Based on the characteristics of distributed ledger technology, this study proposes a distributed ledger-enabled trusted traceability and quality access control enhancement method for the traceability difficulties and data security problems faced by software development security testing in the electric power industry. The study first establishes a traceability data model based on PROV data model, and designs a smart contract system to realize trusted storage and verification of traceability data; Second, a sensitive data aggregation method based on homomorphic encryption is proposed to reduce the communication overhead and secure the data; finally, an Overlay structure data communication mechanism based on RSA asymmetric encryption is constructed to realize the tamper-proof protection of sensitive data. Through MATLAB simulation experiments, the proposed method is evaluated and verified from three dimensions of credibility enhancement, data traceability and security, which proves the effectiveness and advancement of the method in the security detection of software development in the power industry.

II. Application of distributed ledgers in security detection

In the inspection and testing industry, blockchain technology, as a distributed, tamper-proof ledger system, has great potential to enhance the credibility and transparency of data. The introduction of blockchain technology can realize the monitoring and traceability of the whole process of inspection and testing, the whole process of monitoring can be realized through the real-time recording and sharing of the blockchain, and traceability refers to the ability to trace back to the origin of the inspection and testing data and the entire processing process. The introduction of distributed ledger can realize the monitoring and traceability of the whole process in the power industry software development safety inspection, thus improving the overall operational efficiency and credibility of the industry and strengthening its quality access control.

II. A.Distributed Ledger

Distributed ledger is a key feature of blockchain that enables all network participants to share the same ledger without relying on a centralized institution. In the application of security testing industry, distributed ledger has the following features:

Decentralization: the distributed ledger of the blockchain does not depend on a single entity or institution, but is maintained and verified by multiple nodes in the network. This decentralized feature improves the robustness and attack resistance of the whole system.

Consensus Mechanism: Distributed ledgers use consensus mechanisms to ensure that nodes in the network agree on changes to the ledger. Common consensus algorithms include proof-of-work and proof-of-equity.

Synchronized update: Each node in the distributed ledger has a complete copy of the ledger and keeps it synchronized through the protocol. This ensures data consistency, so that even if one node fails or behaves maliciously, the other nodes can still maintain data integrity.

Together, these two foundational principles form the infrastructure of the blockchain, providing a more secure, transparent, and trustworthy solution for data management for software development security testing in the power industry.

II. B.Data Security and Tamperability

One of the application scenarios of distributed ledger in software development security testing in the power industry is to enhance data security and non-tamperability and strengthen quality access control.

Data security: blockchain stores data through decentralization, eliminating the risk of a single point of failure in traditional centralized systems. Each participating node has a complete copy of the data, guaranteeing redundancy and availability. At the same time, the use of encryption algorithms ensures the confidentiality of the data, and only users with the appropriate permissions can access sensitive information.

Non-tamperability: The non-tamperability of the blockchain is realized through the hash link between blocks and the consensus mechanism. Once the data is recorded in the block, any attempt to tamper with the data will destroy the hash link, which is quickly detected by the system. This ensures the integrity of the inspection and testing data and makes the data more trustworthy.

II. C.Practical needs for traceability and retroactivity

Traceability traceability is a key practical need in the power industry software development safety testing, distributed ledger provides an ideal solution for this.

Ensure the credibility of the data source: Distributed ledger can trace back the source of inspection and testing data, including sample collection, testing equipment and other information. Through traceability, the credibility of the data can be ensured, preventing forgery and tampering of the data source.

Improve the efficiency of problem troubleshooting: when problems or anomalies occur, it is crucial to quickly troubleshoot the root cause of the problem. Distributed ledger traceability can help quickly locate the problem and find the link where the anomaly occurs, thus improving the efficiency of troubleshooting.

Meet regulatory compliance needs: Blockchain technology provides traceability and transparency to help meet regulatory compliance requirements for security testing.

By applying distributed ledger in software development security testing in the electric power industry, it can meet the actual needs, improve data security, ensure data credibility, and effectively achieve the goal of traceability and retroactivity. This is of great significance for building a more secure and efficient inspection and testing system.

II. D.Distributed Ledger Traceability System

The distributed ledger traceability system in the security testing of software development in the power industry is shown in Figure 1, including the foreground system and the background system. In the backend design, it mainly includes user management, system management, data analysis, index analysis and other functions. In the front-end development, it includes report display, data tracking, interface design, interaction design and so on. Develop the user interface, provide the interface to verify the inspection and testing data, and integrate the distributed ledger verification function. Record the history of validation operations and store it on the distributed ledger to ensure the traceability of the validation history.

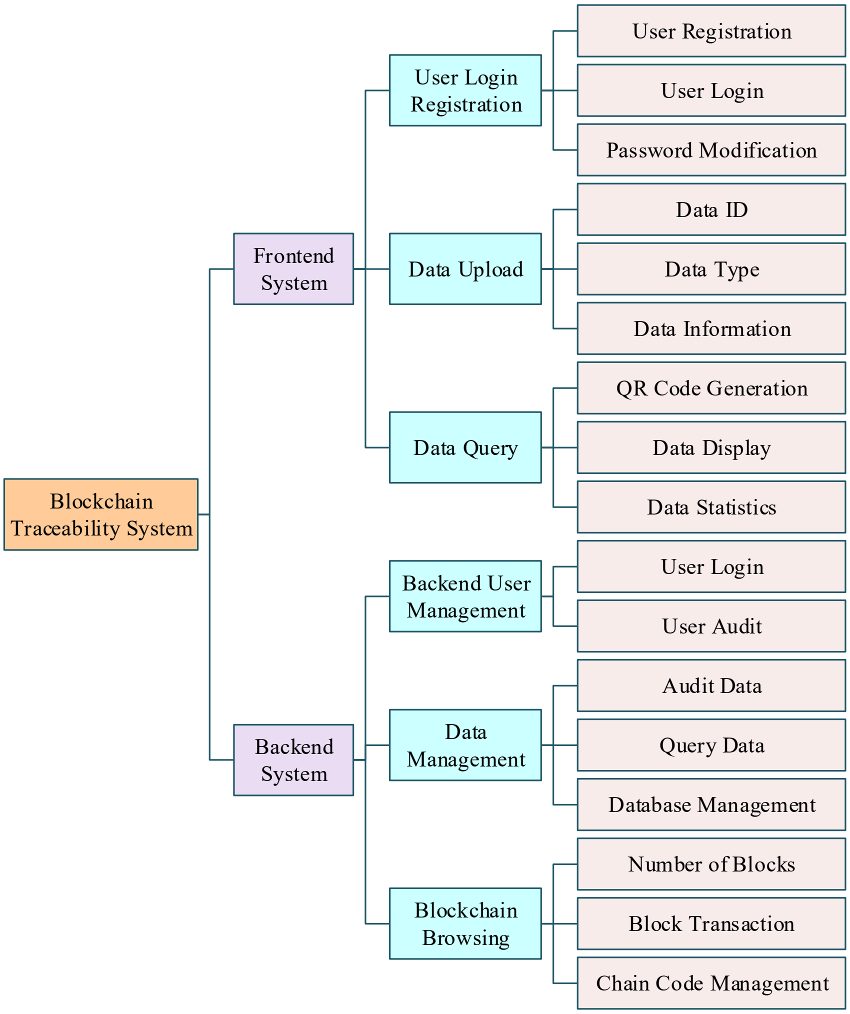

Figure 1： The traceability system of distributed books

III. Enhanced methodology for credible traceability and quality gating

III. A. Distributed Ledger Based Data Traceability Approach

Aiming at the problems of centralized storage and easy tampering of data that exist in traditional traceability systems, this paper proposes a distributed ledger-based data traceability scheme for software development security testing in the electric power industry based on the distributed, hard-to-tamper and traceable characteristics of blockchain. The main challenge of the traceability system is the trusted collection, trusted storage and trusted verification of traceability data. This paper assumes that the relevant data have been acquired, does not consider how they are specifically collected, and focuses on the storage and validation of traceability data. This paper establishes a traceability data model based on the PROV data model and designs a set of contracts for traceability data management, and stores the traceability data on the blockchain through smart contracts. For the authenticity verification of the identities of the parties involved in data traceability, it relies on cryptographic techniques to solve the problem, involving hash algorithms and digital signatures.

III. A. 1) Authenticity verification of participants' identity

Trusted identity authenticity verification is the first barrier to secure data traceability. Data traceability involves a large number of participating subjects, including data sources, data transmitters, data reviewers, and data users, who jointly participate in and maintain the blockchain. Each party first registers as a user in the blockchain, and each user generates a public/private key pair after registration. The public key is used to identify the user within the system, and the private key is used for digital signatures to ensure the authenticity of the user's identity and to allow recipients of the data to use it to confirm the source of the data and prevent it from being forged. The implementation is based on the secp256k1 Elliptic Curve Mathematics for Digital Signature Algorithm (ECDSA). The public key is computed from the private key, but the private key cannot be derived from the public key. The question of whether the data has been tampered with is solved using the keccak256 hash algorithm. Assuming that user A needs to pass data M to user B, A first calculates the hash value of the data using the keccak256 hash algorithm, signs the data using the private key, and then sends the data together with the signature. After receiving the message, B uses the public key of A to decrypt the signature, obtains the provided hash value of the data, and compares it with the result obtained by re-performing the hash operation on the data. If the two values are the same, it means that the message is indeed sent by A and the data content has not been tampered with.

III. A. 2) Trusted storage of traceability data

A traceability data model is built based on the PROV data model (PROV-DM) to describe traceability records in order to track changes in the data and identify the entities that caused the changes, and the traceability data is stored on a distributed ledger through smart contracts.

Let's first briefly consider the case where a data source uploads data to the blockchain, according to the definition of PROV-DM, the data object M that wants to be traced back to the data, i.e., the entity, needs to compute the hash value of the data $H(M)$. The user A is the owner or creator of the data M, defined as an agent, after which a digital signature operation needs to be performed on the data. Since A does not further process the data, the activity refers to the time when the data source acquires the data. Therefore, the traceability record (PR) contains at least: the hash value $H(M)$ of the data to be traced, the timestamp timestamp, the owner signature sig, i.e., $PR=\left(H(M), timestamp, sig\right)$. In addition to this, define the class, format and attributes of the traceability object, the type of activity and the type of agent, etc.

Other participants of data traceability (e.g., user B) can also edit the data, but must record the operations done on the data in the chain for future verification, then the traceability record needs to contain: the hash value of the previous version of the data $H(M)$, the timestamp and the hash value of the signature, the hash value of the current version of the data (after modification of the data) $H(M')$, the operation performed activity, operator signature sig_k, i.e. $PR=\left(H(M'), H\left(H(M), sig, timestamp\right), activity, sig_k\right)$.

III. A. 3) Smart Contracts

The traceability data model based on the PROV data model can describe the traceability information, however, it has not addressed how to record the necessary metadata and data for later verification in a reliable and permanent way. In this paper, based on the Ethernet platform, the traceability records are stored in the distributed ledger through smart contracts, which can be regarded as autonomous agents in the distributed ledger, and are automatically executed when the preset conditions are met, which reduces manual intervention, thus realizing trustworthy storage and trustworthy verification of traceability records.

The construction and execution of a smart contract can be divided into the following three steps: (1) multiple users participate in the formulation of a smart contract through an agreement; (2) the smart contract is propagated through the P2P network and stored in the distributed ledger; (3) when the contract is triggered, it can automatically execute the contract content according to the set conditions.

The main components of a smart contract include state and logic. In this paper, we design a set of smart contracts based on the traceability data model, which defines the structure of traceability data, the logic of reading and writing traceability data by the participants, which are: Object.sol, Agent.sol, Event.sol and the corresponding ProvObject.sol, ProvAgent.sol and ProvEvent.sol. The top level is the contract name, the middle level is the contract name, the middle level is the contract name, the middle level is the contract name, the middle level is the contract name, the middle level is the contract name, the middle level is the contract name, the middle level is the contract name, the middle level is the contract name, and the middle level is the contract name. The top level is the contract name, the middle level is the attributes (if present) and the bottom level is the methods.

Contracts are propagated through the network via P2P and each node receives a copy. The verification node in the distributed ledger will verify the contract, the verification is mainly whether the private key signature of the contract participant matches the account or not, and only the contract that passes the verification will finally be written into the distributed ledger. After the contract is deployed to the distributed ledger, the application binary interface (ABI) of the contract will be returned, including variables, events and methods that can be called. Interaction with the contract enables storage and querying of traceability data. Smart contracts provide a safe and reliable mechanism for the transmission and storage of security testing data for software development in the power industry, ensuring that the data is difficult to tamper with and reliable.

III. B. Anti-tampering methods for sensitive data

In this paper, we propose a distributed ledger-based anti-tampering method for sensitive data to ensure the security of the whole data traceability system in order to strengthen the quality gating of the system.

III. B. 1) Data Extraction and Authentication

In order to improve the security of sensitive data in the transmission of software development security detection data in the electric power industry, it is necessary to extract the features and attributes of the data before designing the anti-tampering algorithm for sensitive data, so as to establish the sensitive data sets and their effective association rules based on the obtained information to ensure that there is an inward correlation between the sensitive data. Assuming that there are sensitive datasets P and Q in the mobile network, the data sets corresponding to P and Q are expressed as intra-item information, and $R(P \cup Q)$ is the number of items in the intra-item set that have data in both P and Q. If U is the total number of items, the probability of co-occurrence of P and Q, i.e., the confidence level $R(P \Rightarrow Q)$, is calculated as follows:

$$R(P \Rightarrow Q) = \frac{R(P \cup Q)}{U} \tag{1}$$

Construct the association rule of P and Q according to the result obtained from equation (1), $R(P)$ is the number of items in the set of corresponding items in P that contain data in P, then the association rule $C(P \Rightarrow Q)$ between P, Q is shown as follows:

$$C(P \Rightarrow Q) = \frac{R(P \cup Q)}{R(P)} \tag{2}$$

After completing the extraction of sensitive data sets, it is necessary to authenticate this part of sensitive data. First of all need to authenticate the front-end user identity information, user identity data usually in the form of distributed existence, the need for user identity information centralized processing, will be processed after the user identity information $S(c)$ expressed in the following form:

$$S(c) = S_i \cdot 3^i + S_{i-1} \cdot 3^{i-1} + \cdots + S_1 \cdot 3^1 + S_0 \cdot 3^0 \tag{3}$$

In Eq. (3), $S_i \sim S_0$ is the user identity information flow and the total number of information flows is $(i+1)$ $bits$.

Test all the parameters in the user identity information, introduce the minimum paradigm method to differentially analyze the test results, and reset the calculation of the information flow sparsity degree. Assuming that the mapping conditions are met between the user identity information and the information flow after the reset, match the identity information with the parameter differentiation test results, if the matching results show that the user identity information has a small sparsity degree, the corresponding parameter security is better, and vice versa the security degree is worse. Introduce the global search matching algorithm to authenticate the sensitive data, if the opposite end shows no difference, it is determined that the information passes the authentication, i.e., the information meets the requirements of the security testing of software development in the electric power industry.

III. B. 2) Data aggregation

Sensitive data aggregation is mainly to aggregate and process the sensitive data received by the intermediate aggregation transmitted by the child nodes to achieve the purpose of reducing the communication overhead. Homomorphic encryption algorithm is introduced to directly aggregate the sensitive data received by the intermediate nodes, and the main steps of homomorphic encryption algorithm to cluster the data are shown below:

1) Data preparation

Obtain the sensitive data to be aggregated and encrypt it. Immediately after the sub-node receives the query request from the originating node, it detects the monitoring area, stores the sensitive data X_i in the memory, and encrypts X_i to guarantee the security of the sensitive data. Let ID_i be the node threshold and Enc_i be the encryption function, the ciphertext G_i is obtained as follows:

$$G_i = Enc(X_i) = X_i + ID_i \tag{4}$$

The homomorphic hash message verification code of the sensed data is computed, and the originating node determines the integrity of the data by combining the computation results, let λ be a large prime number, and $H(\cdot)$ be the homomorphic hash function, then the corresponding homomorphic hash verification code is computed as follows:

$$H(X_i) = \lambda^{X_i} \tag{5}$$

The obtained ciphertext information and the homomorphic hash authentication code $(G_i, H(X_i))$ are jointly uploaded into the upper layer aggregation node.

2) Data Aggregation

In the data aggregation phase, the ciphertext is first aggregated by end-to-end encryption, and the sensitive data received by the upper layer aggregation node can be directly aggregated without decryption. Then aggregate node ID, set the total number of nodes as M, $i \in M$, to get the aggregation function G_A as follows:

$$G_A = \sum_{i=1}^{M} G_i = \sum_{i=1}^{M} X_i + \sum_{i=1}^{M} ID_i \tag{6}$$

The hashed message CAPTCHA is then aggregated and processed by the upper level aggregation node with the aggregation function H_A as shown below:

$$H_A = \prod_{i=1}^{M} H(X_i) = (\lambda^{X_1})(\lambda^{X_2})\cdots(\lambda^{X_M}) \tag{7}$$

Finally, the sensitive data aggregation result (G_A, H_A) is uploaded to the upper aggregation node, and the data aggregation operation is repeated until the final result of the aggregated data is obtained at the beginning.

3) Data Validation

In data validation, it is necessary for the originating node to decrypt the received aggregated data, using $D(\cdot)$ to represent the Dec decryption function, to obtain the decryption function K_Y as shown below:

$$K_Y = D(G_A) = G_A - \sum_{i=1}^{M} ID_i = \sum_{i=1}^{M} X_i \tag{8}$$

Recalculate the decrypted sensitive data and check its homomorphic message authentication code at the same time, if there is a $H(K_Y) = \lambda^{K_Y}$, then the sensitive data is secure, otherwise the sensitive data has been tampered with and discarded.

III. B. 3) Encryption and anti-tampering methods

After clustering and processing the sensitive data, the distributed ledger is introduced to encrypt the sensitive data in order to prevent the sensitive data from being tampered and other security threats during transmission. Each block in the blockchain is connected to keep the blockchain general by establishing an Overlay structure for mobile network data communication. Let B be the set of all blocks, B_1 be the set of surviving blocks, B_s be the set of idle blocks, $b(x, y)$ be the main block of the data transmission chain of the mobile network, and x, y correspond to the horizontal and vertical coordinates, then the expression for the width of the block chain W under the Overlay structure is:

$$W = \left\{ b(x,y) \middle| \ x \in B_1 \cap B_s, y \in B \right\} \tag{9}$$

During sensitive data transmission, the block sends messages intermittently to the main block, let B_c be the constructed mobile network data communication structure and α be the neighboring block, then the inter-block connection expression is shown below:

$$B_c = \alpha B \cap W \tag{10}$$

Let α take the value of k, then its neighboring blocks are $k-1$ and $k+1$, substituting $k-1$, k and $k+1$ into Eq. (10), we can find the information of two consecutively existed blocks, and complete the connection between multiple data transmission blocks.

Data communication structure and distributed ledger are used as the basis to add keys for sensitive data block chain connection to guarantee the safe transmission of sensitive data. RSA asymmetric encryption algorithm is introduced to encrypt the sensitive data transmission to reduce the risk of key cracking and avoid the threat of tampering of sensitive data.

Let g_0 and g_1 be the dark text and plain text of sensitive data to be transmitted respectively, Δg is the amount of data change per unit time of the transmission key block, p and q are the upper limit and the lower limit of the sensitive data transmission through the block respectively, and v denotes the amount of data transformations, then the encryption function of the sensitive data transmission block, F, is as follows:

$$F = \frac{W}{2\Delta g} \sum_{q}^{p} \frac{|g_0 - g_1|}{v_q} \tag{11}$$

According to equation (11), sensitive data can be encrypted and processed to guarantee data security and realize tamper-proof sensitive data.

IV. Comparative validation of experiments and simulations

In this paper, MATLAB software will be used to simulate the complex power industry software development security detection system environment, and the simulation results of the proposed trustworthy traceability and quality access control reinforcement method and the existing SHA256 algorithm and classical searchable encryption algorithm DyRH will be compared. Multiple simulations will be performed on random large sample data, and the results of its simulation analysis are statistically significant.

IV. A. Credibility enhancement analysis

In this paper, the blockchain model using SHA256 algorithm, DyRH model and distributed ledger-based trusted traceability and quality access control reinforcement method are simulated and operated respectively for the complex mining system environment. Firstly, the loss rate of the three models is simulated after transmitting the same sample information through 20 terminals, and the comparison results of the loss rate of different models are shown in Fig. 2, and then the simulation simulates the number of terminals or systems through which the same sample information can be transmitted without distortion in the three models, and the comparison results of the data transmission without distortion are shown in Fig. 3. The simulation results of using the Distributed Ledger-based Trusted Traceability and Quality Gating Enhancement method are much better than those of using SHA256 algorithm and DyRH model.The loss rates of SHA256 algorithm, DyRH5 model and this paper's method are 6.97%~9.24%, 4.75%~5.25%, and 3.75%~4.10%, respectively, for the different number of transports, and the number of terminals or systems that can pass through the same sample of information under the undistorted transmission is 3.75%~4.10%. The mean values of the number of terminals or systems passed under distorted transportation are 34, 46 and 51, respectively. It can be seen that the loss rate of this paper's method is greatly reduced when transmitted in the complex environment of software development security testing in the electric power industry, and at the same time, it can pass through a greater number of systems or terminals without distortion in the process of fidelity transmission, which greatly improves the data security and credibility of the data in the security testing of software development in the electric power industry.

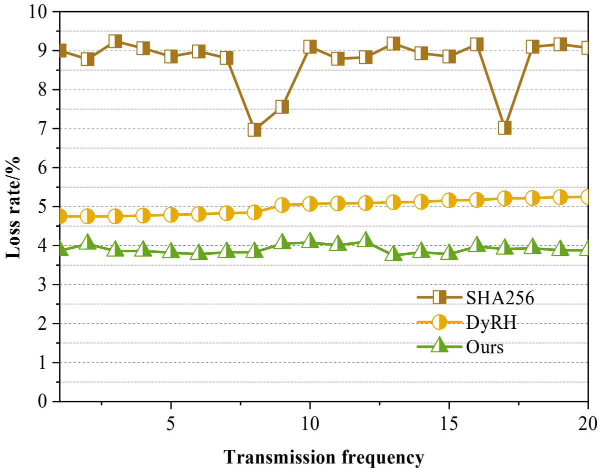

Figure 2: Comparison of loss rate for different models

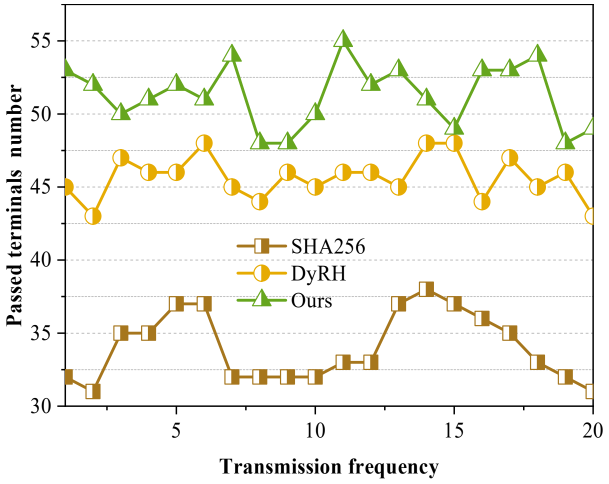

Figure 3： Comparison of undistorted data transmission

IV. B. Traceability analysis of data

Meanwhile, this paper also compares the simulation results of the proposed method and the traceability simulation results with the existing SHA256 algorithm and DyRH model in the MATLAB software simulation environment. Firstly, the time of locating the simulation error for traceability of the three models is simulated, and the results of the error locating time of different models are shown in Fig. 4. Then the simulation simulated the accuracy of the same simulation error sample information traceability in the three models, and the results of the error localization accuracy of different models are shown in Figure 5. Under different numbers of simulated error data, the average value of error localization time of this paper's method is 9.23ms, which is lower than the 17.83ms of SHA256 algorithm and the 13.33ms of DyRH model.The average values of error localization accuracy of the three methods are 93.56%, 96.54%, and 98.33%, respectively, and the accuracy of this paper's method for simulated error data is 4.77% and 98.33% higher than the comparative methods by 4.77% and 1.79%.

The simulation simulation results using the Distributed Ledger-based Trusted Traceability and Quality Gating Enhancement method are much better than those using the SHA256 algorithm and the DyRH model. Therefore, the time required for traceability in the complex environment of software development security detection in the electric power industry using the method of this paper will be further reduced, and the error samples are localized to the accuracy rate is further improved, which greatly enhances the traceability of data in security detection.

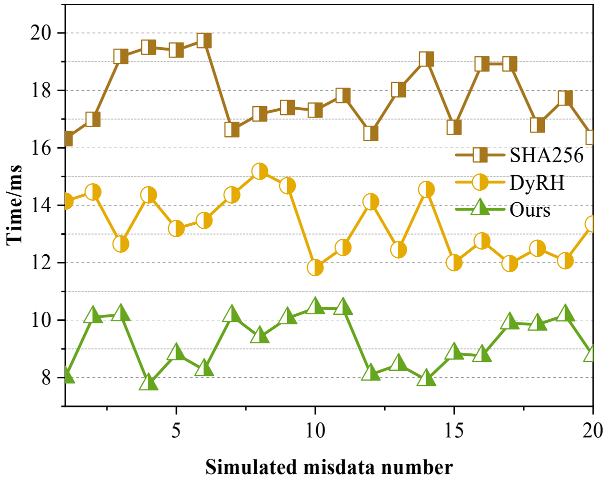

Figure 4: Error location time of different models

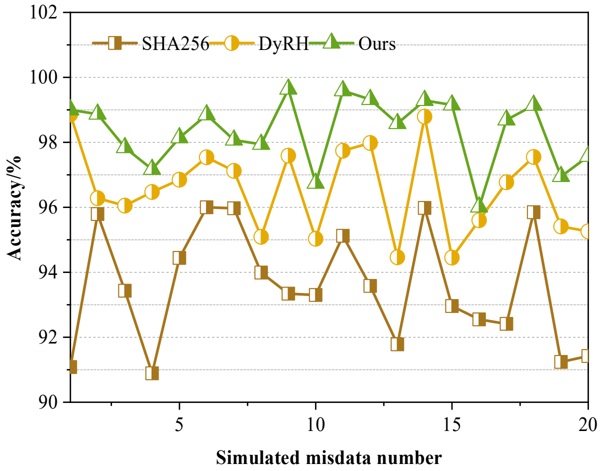

Figure 5: Error location accuracy of different models

IV. C. Security analysis

The number of tampered data of the three methods with different number of messages is analyzed, and Fig. 6 shows the anti-attack performance of different models. The efficiency and security of this paper's method is higher than that of the comparison algorithms, and its number of tampered data is 66~295, with an average value of 189, which is 184 and 156 less than the SHA256 algorithm and the DyRH model, which indicates that this paper's method has a higher quality of access control, and it can provide a better protection of the network information security of the electric power industry.

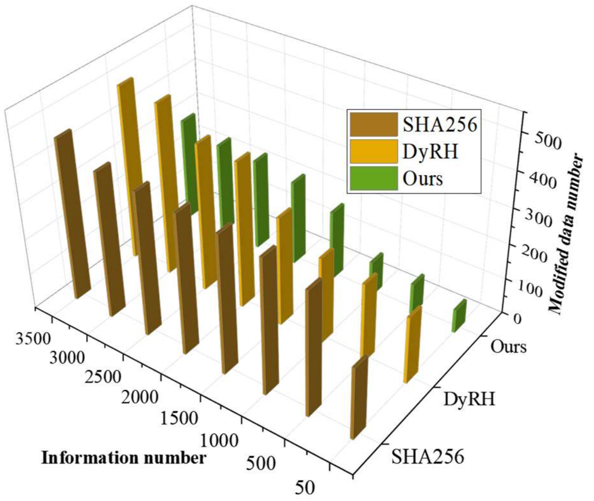

Figure 6: Anti-aggression energy of different models

V. Conclusion

In this paper, a trusted traceability and quality access control enhancement method based on distributed ledger for software development security testing in power industry is proposed. The method effectively solves the data traceability and security problems in software development security detection in the power industry by constructing a PROV data model, designing a smart contract system, realizing homomorphic encrypted data aggregation and RSA asymmetric encryption anti-tampering mechanism. The experimental results show that this method exceeds the traditional method in terms of undistorted transmission capability, and the data loss rate is controlled at 3.75%~4.10%, which is much lower than the 6.97% 295 of SHA256 algorithm, and the average value is 189, which is significantly lower than the comparison method. The study proves that distributed ledger technology can provide efficient and credible traceability and strong quality access control guarantee for software development security detection in the power industry, and has obvious advantages in improving credibility, enhancing traceability accuracy and strengthening security protection, which provides a new technical path for information security guarantee of the power system.

References

[1] Jimada-Ojuolape, B., & Teh, J. (2020). Impact of the integration of information and communication technology on power system reliability: A review. IEEE Access, 8, 24600-24615.

[2] Khabdullin, A., Khabdullina, Z., Khabdullina, G., & Tsyruk, S. (2017). Development of a software package for optimizing the power supply system in order to minimize power and load losses. Energy Procedia, 128, 248-254.

[3] Neis, P., Wehrmeister, M. A., & Mendes, M. F. (2019). Model driven software engineering of power systems applications: literature review and trends. IEEE Access, 7, 177761-177773.

[4] Bakulina, A., Kondrateva, O., & Loktionov, O. (2020, April). Software Package Development to Improve Occupational Safety at Electric Power Industry Enterprises. In 2020 V International Conference on Information Technologies in Engineering Education (Inforino) (pp. 1-4). IEEE.

[5] Ait Ouaret, S. C., Imaouchen, Y., Aouzellag, D., & Ghedamsi, K. (2024). A new modeling approach and comprehensive monitoring of electrical faults through spectral analysis in DSIM. Periodica Polytechnica Electrical Engineering and Computer Science, 68(4), 344-355.

[6] Masmali, M., Elimy, M. I., Fterich, M., Touti, E., & Abbas, G. (2024). Comparative Studies on Load Frequency Control with Different Governors connected to Mini Hydro Power Plant via PSCAD Software. Engineering, Technology & Applied Science Research, 14(1), 12975-12983.

[7] Tatipatri, N., & Arun, S. L. (2024). A comprehensive review on cyber-attacks in power systems: Impact analysis, detection, and cyber security. IEEE Access, 12, 18147-18167.

[8] Xu, S., Xia, Y., & Shen, H. L. (2022). Cyber protection for malware attack resistance in cyber-physical power systems. IEEE Systems Journal, 16(4), 5337-5345.

[9] Maghami, M. R., Mutambara, A. G. O., & Gomes, C. (2025). Assessing cyber attack vulnerabilities of distributed generation in grid-connected systems. Environment, Development and Sustainability, 1-27.

[10] Shorthill, T., Bao, H., Zhang, H., & Ban, H. (2021). A novel approach for software reliability analysis of digital instrumentation and control systems in nuclear power plants. Annals of Nuclear Energy, 158, 108260.

[11] Jin, B., Zhou, Z., Long, F., Xu, H., Chen, S., Xia, F., ... & Zhao, Q. (2022, October). Software Supply Chain Security of Power Industry Based on BAS Technology. In 2022 International Conference on Artificial Intelligence of Things and Crowdsensing (AIoTCs) (pp. 556-561). IEEE.

[12] Chen, Y., Jin, Y., Du, L., Li, J., Guo, W., Liu, H., ... & Dong, Y. (2025, April). Research on data traceability method for the whole process of power equipment. In International Conference on Energy Technology and Electrical Power (ETEP 2024) (Vol. 13566, pp. 108-114). SPIE.

[13] Khan, A. A., Laghari, A. A., Rashid, M., Li, H., Javed, A. R., & Gadekallu, T. R. (2023). Artificial intelligence and blockchain technology for secure smart grid and power distribution Automation: A State-of-the-Art Review. Sustainable Energy Technologies and Assessments, 57, 103282.

[14] Straubert, C., & Sucky, E. (2021). How useful is a distributed ledger for tracking and tracing in supply chains? A systems thinking approach. Logistics, 5(4), 75.

[15] Ji, H., Jian, J., Yu, H., Ji, J., Wei, M., Zhang, X., ... & Wang, C. (2021). Peer-to-peer electricity trading of interconnected flexible distribution networks based on distributed ledger. IEEE Transactions on Industrial Informatics, 18(9), 5949-5960.

[16] Papadopoulos, P., Pitropakis, N., & Buchanan, W. J. (2022). Decentralized privacy: a distributed ledger approach. In Handbook of Smart Materials, Technologies, and Devices: Applications of Industry 4.0 (pp. 1805-1830). Cham: Springer International Publishing.

[17] Khan, A. A., Laghari, A. A., Liu, D. S., Shaikh, A. A., Ma, D. D., Wang, C. Y., & Wagan, A. A. (2021). EPS-Ledger: Blockchain Hyperledger Sawtooth-enabled distributed power systems chain of operation and control node privacy and security. Electronics, 10(19), 2395.

[18] Downes, L., & Reed, C. (2020). Distributed ledger technology for governance of sustainability transparency in the global energy value chain. Global Energy Law and Sustainability, 1(1), 55-100.

[19] Muzumdar, A., Modi, C., & Vyjayanthi, C. (2021). A trustworthy and incentivized smart grid energy trading framework using distributed ledger and smart contracts. Journal of network and computer applications, 183, 103074.

[20] Roeck, D., Sternberg, H., & Hofmann, E. (2020). Distributed ledger technology in supply chains: a transaction cost perspective. International Journal of Production Research, 58(7), 2124-2141.