Journal of Cloud Computing:
Advances, Systems and Applications

RESEARCH

Open Access

Blockchain enabled zero trust based authentication scheme for railway communication networks

Yuan Feng[1,2], Zhangdui Zhong[1,2], Xiaofang Sun[1,3], Lei Wang[4], Yunlong Lu[1,2*] and Yongsheng Zhu[5*]

Abstract

With the introduction of emerging technologies such as cloud computing, the railway communication network has the characteristics of complex structure and blurred boundaries, which leads to a series of security threats including information leakage and malicious access. Specifically, the third-party cloud services are difficult to be supervised, and network traffic is untrustworthy. To ensure system security, we propose a zero-trust security model in this paper. Then, we introduce blockchain and Merkle tree to build a distributed identity storage scheme for guaranteeing reliable, confidential and efficient data updates, and improving authentication efficiency. Furthermore, the proxy was introduced for two-way authentication with cloud servers, so that internal and external threats could be counteracted. Moreover, reputation assessment mechanism has been adopted to reduce the possibility of nodes accessing malicious cloud services. Performance analysis demonstrated that the proposed security model is able to enhance the security, efficiency and stability of the system, and consequently can guarantee the safety and reliability of railway transportation.

Keywords Railway communication network, Blockchain, Zero-trust, Authentication, Network security

Introduction

In the context of China's continuous urbanization and the rising willingness of the nation to travel, railway has gradually become the first choice of green travel for travelers by virtue of its large capacity, high speed, low energy consumption, economy and convenience. In September 2019, the Central Committee of the Communist Party of China and the State Council issued the Outline of the Construction of a Strong Transportation Country [1], specifying the development goals of modern railway in China as safe, convenient, efficient, green and economic. The application of emerging technologies in the railway industry, such as 5G, cloud computing, big data, Internet of Things, artificial intelligence, satellite communication, blockchain, etc., can promote the realization of a new generation of intelligent railway system with comprehensive perception and deep interconnection, and comprehensively improve the level of railway business services. At present, China, mainly uses private networks to carry railway communication services. Although the private network can ensure continuous and reliable network connection coverage, the network scale and bandwidth resources are limited, making it difficult to carry new railway services with high bandwidth, panconnectivity and intelligence. In order to adapt to the

*Correspondence:
Yunlong Lu
yllu@bjtu.edu.cn
Yongsheng Zhu
zhuys@rails.cn
[1] Collaborative Innovation Center of Railway Traffic Safety, Beijing, China
[2] State Key Lab of Rail Traffic Control & Safety, Beijing Jiaotong University, Beijing 100084, China
[3] School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100084, China
[4] Industrial and Commercial Bank of China Shandong Branch, Ji Nan 250001, Shan Dong, China
[5] Institute of Computing Technologies, China Academy of Railway Sciences Corporation Limited, Beijing 100081, China

trend of diversified development of railway business, the convergence of public and private networks is gradually becoming an inevitable trend for railway communication network construction, while using private networks to carry highly reliable demand services such as train operation control information. Based on 5G public networks, we provide exclusive network capacity through resource isolation and other technical means to carry railway low latency and large bandwidth data services, covering the whole scenario of railway and realizing public network exclusively [2]. Under this trend, how to ensure data and node trustworthiness and secure operation of the railway system under the increasingly complex network architecture has become an important research direction.

Authentication is the beginning of establishing trustworthiness, and the security and confidentiality of authentication credentials are the cornerstone of the network for secure and reliable communication. The centralized network architecture stores the authentication credentials in the data center, which often suffers from the single point of failure and makes it difficult to guarantee data trustworthiness [3]. Blockchain is considered an adaptable alternative for building trusted distributed platforms with features such as interoperability, tamper resistance, decentralization, and consistency. Blockchain technology, with its features of decentralization, immutability, collective maintenance, traceability, openness and transparency, can establish trust in an untrustworthy environment at low cost and realize the decentralized preservation of authentic, reliable, and effective data. It can effectively solve the problem of secure storage of authentication credentials and secure access control in cloud servers. The distributed IoT device authentication mechanism proposed in the literature [4] for the IoT scenario uses blockchain to record the digital certificates of devices in the network, which effectively solves the single point of failure problem and improves the trustworthiness of the IoT system. The literature [5] proposes a blockchain-based security authentication mechanism for Radio Frequency Identification(RFID) systems, in whose system, the identification and communication keys of each node are stored in a distributed blockchain network composed of multiple servers for two-way authentication of the communicating parties. With the help of distributed ledger, consensus mechanism and asymmetric encryption, the literature [6] designed a mechanism for common verification of the nodes in the whole network, and only the certificates of the nodes that get more than half of the verification passed can be recorded to achieve the authentication of smart devices. The literature [7] constructed a blockchain-based entity identifying information storage network, which saves the identity information of people, devices, and applications on the blockchain, verifies the entity identifying information in close proximity and improves the efficiency of data access. This paper builds a distributed authentication credential storage model based on blockchain technology, which is used to eliminate the single point of failure problem in data centers. The Merkle Tree structure is used to store the authentication credentials of users, devices and public cloud services with a user name, device ID and cloud service number as the primary keys respectively, which improves the data query efficiency.

However, resource-constrained nodes such as Internet of Things (IoT) and mobile devices cannot directly participate in the mining and consensus process due to the required proof of work (PoW) computation contributions, which poses a significant challenge for blockchain applications for it and other mobile services. The Mobile Edge Computing (MEC) [8] architecture was introduced to leverage the computing power available in the mobile environment. On-premises data centers and servers are deployed by service providers at the "edge" of the mobile network, such as the base stations of the radio access network. MEC is a key technology to meet the stringent low-latency requirements of next generation networks [9]. Mobile devices can access edge servers to enhance their computing capabilities (e.g., IoT sensor data processing). With this feature, edge computing becomes a promising solution for mobile blockchain applications with the following benefits. First, by introducing more miners, the robustness of the blockchain network is naturally improved. Second, mobile users are incentivized from rewards earned during the consensus process. However, edge computing services are deployed by providers to maximize their benefits. Thus, the question of pricing for edge services arises. Correspondingly, considering the pricing adopted by edge computing service providers, miners also need to optimize their demand for edge computing services to solve PoW to maximize their earnings. Resource allocation and pricing are common optimization techniques employed in wireless networks [10].For example, in [11], the authors proposed a new waterfilling solution for resource allocation by understanding the power allocation procedure dynamically and considering the changes of the increasing rates on each subchannel. In [12], the authors considered edge computing-enabled mobile blockchain networks, where IoT devices or mobile users can access and utilize resources or computing services provided by edge computing service providers to support their blockchain applications. A prototype of an edge computing system for mobile blockchain is presented. A pricing scheme is then proposed for edge computing services for mobile blockchains. Some typical numerical results are given to show the important findings of the proposed pricing scheme.

However, most of the existing research on cloud computing assisted access control based on blockchain technology is limited by the traditional security model. This network boundary-based security model only enforces security policies at the boundary of the region, and the default region is trusted, that is, only Identity authentication is performed when a new device enters the network. Once the authentication is passed, the default device is trusted. With the increasing dynamic degree of network devices and operators, the internal trustworthiness of the system is decreasing, and the security rules based on the network location are becoming increasingly difficult to function. To address this situation, a dynamic node trustworthiness assessment mechanism needs to be introduced. The literature [13] applied blockchain technology to contract management by assessing node trustworthiness based on the number of contracts signed and constructing a blockchain with alternating trustworthiness and Proof of Stake (PoS) as the consensus mechanism. The literature [14] constructed a data storage and data sharing mechanism in the Telematics scenario, which uses a coalition chain and smart contract technology to weigh the trustworthiness assessment by combining the credit judgment of itself and geographically close nodes for the nodes to be evaluated. The literature [15] proposed a mechanism for trustworthiness assessment in multiple dimensions such as service quality and participation, and introduces a trustworthiness feedback mechanism to motivate the nodes in the network to improve their trustworthiness by providing effective services. In this paper, we design a two-way authentication protocol between the web proxy and the public cloud service, and send only the Merkle Tree Root composed of authentication credentials in the authentication application and verification messages, which reduces the amount of network transmission data and improves the efficiency of authentication while safeguarding the confidentiality of authentication credential data.

Under the trend of high integration of public-private networks oriented to the railway, the security model of partition isolation is more and more difficult to monitor massive network traffic, and a distributed security model with functions of identity authentication and dynamic credibility evaluation needs to be proposed. However, the existing research often only focuses on the direction of single identity authentication or weighted trust evaluation, which is difficult to adapt to the security requirements of the new generation network. However, existing research tends to focus only on the direction of single-time authentication or weighted trust assessment, which is difficult to adapt to the security needs of next-generation networks. In this paper, the concept of zero trust is introduced into the railway communication network. With the help of the characteristics of zero trust model real-time authentication, least privilege, and variable trust [16], the network location and trust degree are decoupled without relying on the physical security mechanism of the network transport layer, to provide effective protection for railway data interaction and business access integrated with public and private networks. Nowadays, zero-trust security models built on untrustworthy networks have attracted more and more attention from academia and industry. In 2013, PagerDuty [17] started to build a zero-trust network and initially completed its deployment a year later, which is mainly used to solve the security interaction problem among servers in public cloud platform scenarios. In 2014, Google published a series of articles for introducing the Beyond Corp [18] security architecture model it is deploying, which is based on user identity rather than network location for access control and can better adapt to enterprise network requirements such as mobile office for cloud services and access to multiple types of client devices. For the public-private network convergence scenario of the railway system, this paper introduces blockchain technology and zero-trust concept to build a secure and trustworthy zero-trust model for data and nodes, and designs authentication and reputation assessment mechanisms to guarantee safe and reliable operation of the railway communication system. For the public-private network convergence scenario of rail transit system, this paper introduces blockchain technology and zero-trust concept, constructs a zero-trust model for data and node security and trustworthiness, evaluates the trustworthiness of public network cloud services in multiple dimensions, and designs a reputation assessment mechanism to further reduce the possibility of internal nodes of rail transit system accessing malicious cloud services and guarantee safe and reliable operation of the system.

Intelligent reflecting surface (IRS) has been proposed as a potential solution to improve the performance of many aspects for future wireless communication. Ma [19] proposed an algorithm, optimal beam reflection based on federated learning (OBR-FL), for high-speed communication with sparse channel state information (CSI). The trained model can determine the corresponding IRS configuration matrix according to the user's CSI to achieve the optimal communication rate. Sun [20] leveraged Intelligent Reflective Surfaces (IRS) to improve the efficiency of learning model aggregation/distribution. It formulates the total training delay minimization problem under the constraint of available energy of IoT devices to jointly optimize the phase shift of IRS, communication resource scheduling, and the transmission power and local computing frequency of IoT devices. In addition, an efficient multi-dimensional resource management

algorithm is further developed to solve the formulated training delay minimization problem. Kang [21] considered the integration of the IRS enhanced dynamic spectrum access (DSA) technology to a mobile edge computing(MEC) system, and studied the pertinent joint optimization of the phase shift coefficients of the IRS, the transmission powers, the central processing unit (CPU) frequencies, as well as the task offloading time allocations of the secondary users (SUs) to maximize the average computation bits of the SUs. Based on the flexibility of the IRS to adjust its beamforming (BF) vector in each transmission frame, Chen [22] proposed three different dynamic IRS beamforming (DIBF) schemes. Under the DIBF framework, the computational rate maximization problem is formulated for time division multiple access (TDMA) and non-orthogonal multiple access (NOMA) schemes by jointly optimizing IRS BF and resource allocation. An analytical comparison of the computation rates of TDMA and NOMA-based uplink offloading schemes is provided. These recent works also have some help for our research on MEC [23–26].

The main contributions of this paper are summarized as follows:

(1) Based on the zero-trust security model, we build a converged network security architecture for public-private networks in railway scenarios. Then, we introduce network agents to bind users and devices in real time, further improving the security of the network.
(2) We propose to build a distributed identity access authentication and credential storage model based on decentralized blockchain technology to eliminate the single point of failure problem in the data center. We further use the Merkle Tree structure to store users, devices and public network cloud services. The identity authentication credentials are based on the user's name, device ID and cloud service number as the main keys, which improves the efficiency of data query.
(3) We design a two-way authentication protocol between blockchain-based network proxy and public network cloud server. Only the Merkle Tree Root composed of authentication credentials and verification messages is stored, which guarantees the confidentiality of authentication and credential data, reduces the amount of network transmission data as well as improves the authentication efficiency.

The remainder of this paper is organized as follows. Section 2 explains the architectural changes of railway communication systems under the trend of public-private network convergence, the security issues faced by public-private convergence networks, and briefly introduces the basics of the zero-trust model. In Section 3, we propose a security model for railway public-private convergence networks, including system architecture, data storage structure, two-way authentication and reputation assessment. Section 4 evaluates the performance of the proposed security model and proves that the model can improve the security, efficiency and stability of public-private convergence networks. Finally, conclusions are drawn in Section 5.

Public-private converged network architecture

The railway business mainly includes five categories: low bandwidth bearing for production class business, high bandwidth bearing for production class business, broadband communication class for non-production class business, pan-connectivity class for non-production class business, and intelligent overhaul bearing for vehicle base [2]. Figure 1 shows the railway dedicated network architecture and two public-private converged network architectures. Among them, the railway dedicated network is built exclusively for base stations, frequencies, core networks, etc., and is highly isolated from the public network, providing highly secure and reliable customized network services within the industry. On the one hand, the public-private converged network based on local area slicing uses edge computing technology to organically combine local processing and service offloading, while meeting multiple service requirements of high confidential data without leaving the field and ultra-low latency data processing. On the other hand, the public-private converged network based on wide-area slicing provides logical isolation of services through network slicing and Quality of Service (QoS) control to achieve a flexible configuration of services on demand.

Unlike the dedicated railway industry private network, the public-private converged network under the two networking methods uses a public network to carry business data and carry out data processing on the edge cloud server or cloud server provided by the third party. If the internal data of railway industry is uploaded to the malicious cloud server, it will not only cause the leakage of confidential data about the industry, but also affect the normal operation of the railway system severely, which will endanger the safety of people's life and property and destroy social harmony and stability. Therefore, before accessing cloud services, the public network cloud nodes must be authenticated. As more and more elements are involved in the network and the network changes faster and faster, the once-and-for-all single authentication gradually becomes unreliable. The cloud server must be authenticated before each application accesses the cloud

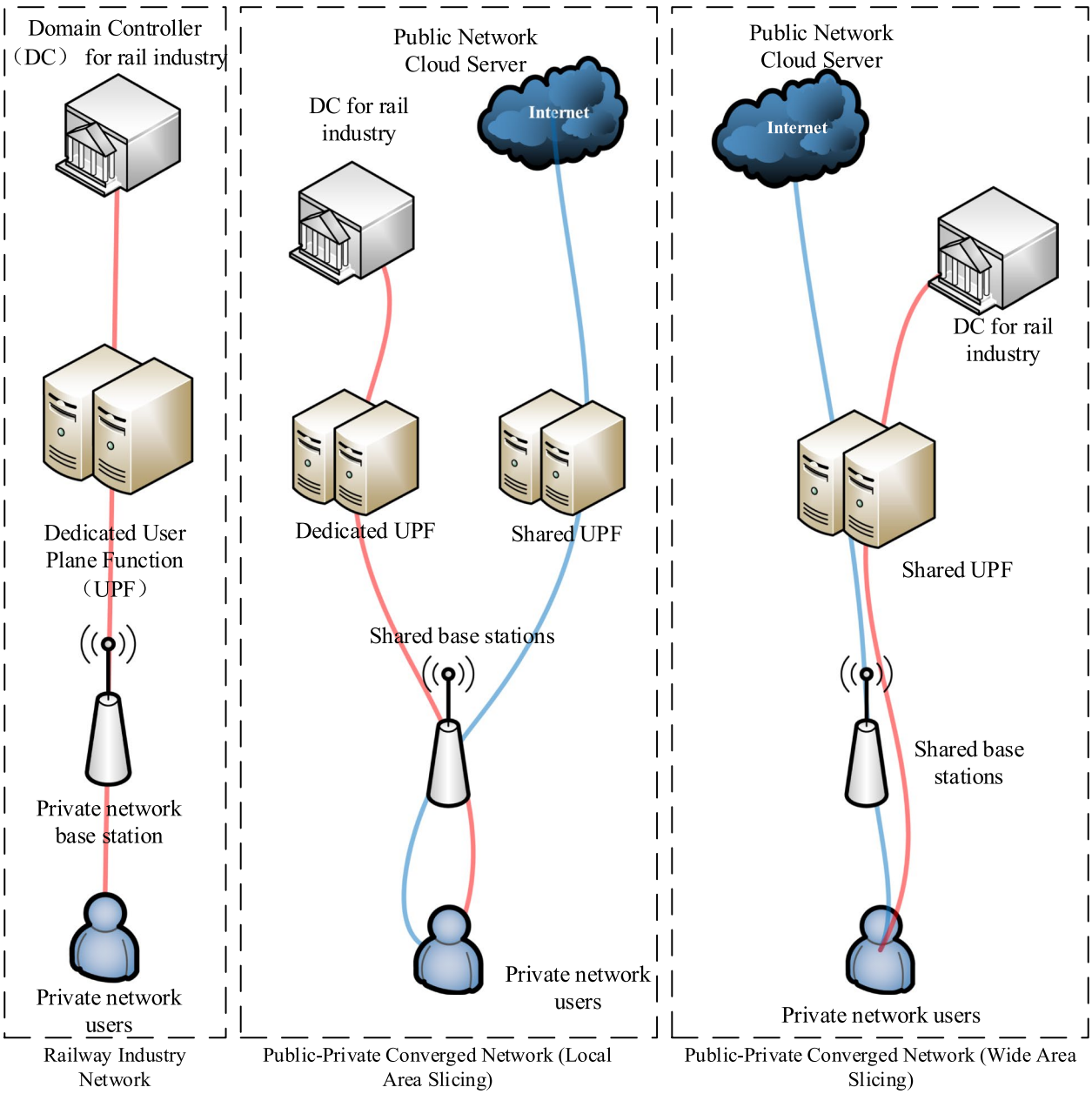

Fig. 1 Railway public-private converged network architecture

service. At the same time, as data is transmitted using the public network, there may be data eavesdropping and theft in the process, so as little data as possible with confidentiality performance should be transmitted while ensuring effective authentication.

Zero trust model

The zero-trust model does not rely on security boundaries, decouples network locations and trust levels, is suitable for public-private converged networks with fuzzy boundaries, and can combat threats from both inside and outside the system. In this paper, we study the security authentication mechanism based on the zero-trust model. This section introduces the features and basic concepts of the zero-trust model.

The traditional security model is a network boundary-based security model, which generally formulates security policies based on network area division and enforces policies only at the network boundary, lacking global protection and enforcement of security

policies. The use of traditional security models for protection in rail transit public-private converged networks lacks inspection mechanisms for internal system traffic, making it difficult to resist lateral attacks introduced by internal malicious nodes; the division of network areas to judge the level of node trust makes the deployment of hosts lack physical and logical flexibility, making it difficult to adapt to a highly dynamic network of equipment and personnel; centralized data storage may also bring single point of failure problem, causing the collapse of the whole system. To address the above issues, the network location and trust level should be decoupled, and a zero-trust security model that enforces security policies everywhere should be constructed.

The zero-trust model has the following five characteristics.

1) The network is always in a dangerous environment.
2) Threats exist both outside and inside the network.
3) The location of the network is not related to the trustworthiness of the network.
4) All devices, users and traffic in the network should be authenticated and authorized.
5) The network should calculate a dynamic security policy based on as much data as possible.

Zero-trust network breaks the inherent thinking of protection based on security boundaries and has attracted wide attention. In order to adapt to the characteristics of environmental monitoring such as multiple networks coexisting and discrete management, the literature [27] built an ecological environmental monitoring network based on the zero-trust idea, which avoided the occurrence of large-scale information security incidents and ensured the healthy operation of environmental monitoring network. In the literature [28], with the features of "identity-centric", "minimal access control", "security policy does not distinguish between internal and external networks", combined with the Software-Define-Perimeter (SDP), the SDP architecture based on zero-trust security model is built to resume the virtual network security boundary on the cloud and secure the enterprise's data assets.

According to the basic features of zero-trust network, the zero-trust network architecture shown in Fig. 2 is constructed in the railway public-private network convergence scenario. The system that provides support for the zero-trust architecture is called the control plane, which is responsible for authentication and authorization of users, devices and cloud services, the dynamic configuration of the data plane, monitoring of network traffic and dynamic assessment of the trustworthiness of

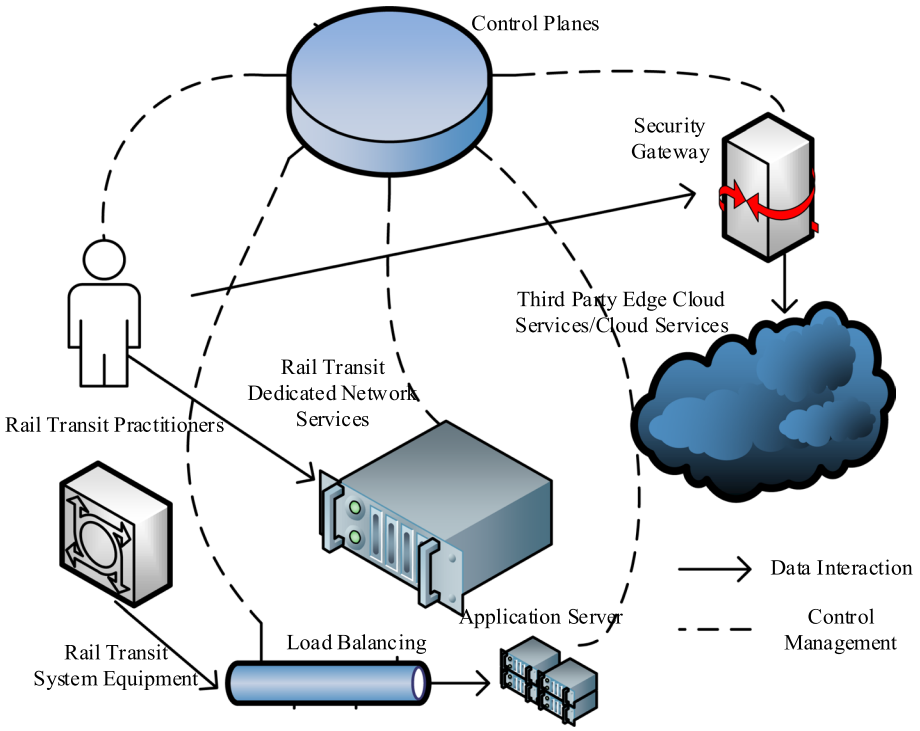

Fig. 2 Zero trust network architecture

each component in the network. The rest of the network is called the data plane and is configured by the control plane. Each access request in a zero-trust network requires strong authentication, using distributed storage to guarantee the legitimacy and confidentiality of authentication credentials, and credential rotation, i.e., changing or updating keys or passwords, when necessary [16].

In order to guarantee the security of authentication, the confidentiality of the information used for authentication and authorization must be guaranteed first in the zero-trust model. For the security model proposed in this paper, the reliability and confidentiality of the authentication credentials used for authentication need to be safeguarded first. The centralized database storage model inherently has a single point of failure problem, and an attacker only needs to invade the data center to tamper or delete data, then the reliability of the data in the network will be greatly damaged, which eventually leads to the collapse of the whole network. Therefore, this paper introduces blockchain technology to realize distributed authentication credential storage and constitute a tamper-evident credential chain. With the characteristics of distributed storage and tamper-evident, blockchain can effectively eliminate the problem of the single point of failure of centralized database and improve data reliability. As one of the key technologies of blockchain, Merkle tree, with the help of hash binary tree structure, can realize fast difference location and fast comparison of large amounts of data. Merkle tree is a hash binary tree, which is a hash of all the transaction information in the current block. The structure of Merkle tree is shown in Fig. 3. The advantage of this storage structure is that if you need to verify whether the multiple transaction information stored in two Merkle trees is consistent, you only need to compare the root values of the two Merkle trees to see if they are consistent, which can quickly verify a large amount of data. if the verification fails, you can also quickly locate the location of data inconsistency according to the Merkle tree.

Using blockchain technology and Merkle tree to store identity authentication credentials can guarantee the confidentiality and validity of identity information and achieve fast difference location and information updates. At the same time, storing with the Merkle tree structure realizes efficient identity authentication based on zero-knowledge proof.

After authentication, the zero-trust network follows the principle of least privilege, i.e., only granting entities the privileges they need to complete their tasks, thus minimizing the possibility of users or applications abusing their privileges. When users or applications need to request higher access privileges, they need to apply to the control plane. Due to the highly dynamic nature of people, devices and cloud services, zero-trust networks

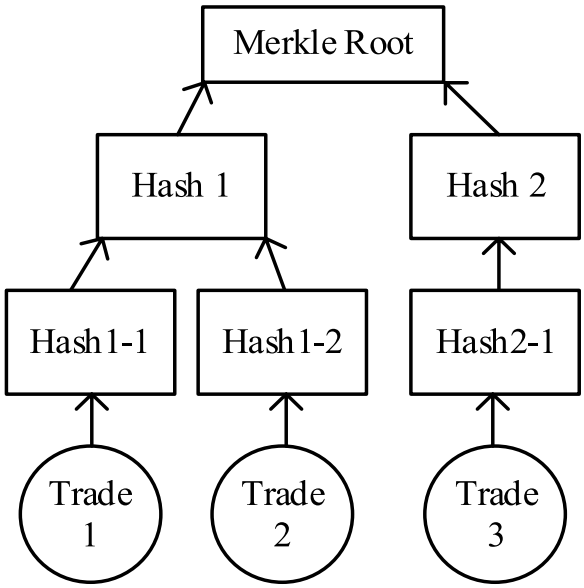

Fig. 3 Schematic diagram of Merkle tree structure

introduce the concept of variable trust, where network participants initiate session requests in an untrustworthy manner and continuously accumulate trust in the process of information interaction. The trust engine in the control plane determines the trustworthiness of each network participant based on its multidimensional behavior. Based on the trustworthiness of each participant, the network can develop fine-grained authorization rules to realize dynamic security policies.

In practice, to ensure the safe and reliable operation of the rail system, all network traffic must be encrypted before transmission and authenticated before processing. And all traffic in the network must be monitored and thus enforced security policies implemented; and devices are regularly scanned, patched or rotated for device security issues.

Blockchain-based trustworthy authentication scheme

This section proposes a cloud computing assisted security model for the rail transit public-private fusion network based on blockchain and zero trust, including system architecture, identity information registration and storage, two-way authentication protocol and reputation evaluation mechanism. In the system architecture proposed in this paper, the blockchain stores user identities and additional information for all users, enabling distributed storage of node identities for efficient authentication based on zero-knowledge proofs. With secure authentication, the confidentiality of the information used for authentication and authorization in the zero-trust model

can be guaranteed, so the blockchain and authentication together guarantee the reliability and security of the zero-trust model.

System architecture

Under the trend of public-private network convergence in the railway industry, in order to guarantee the safe and reliable operation of the railway communication system, this paper constructs a blockchain-based zero-trust network security model for railway, and the system architecture is shown in Fig. 4. The system is composed of two logical domains, the control plane and the data plane. The control plane mainly includes three components: data storage system, policy engine and trust engine, which are responsible for information registration, authentication, access authorization control and reputation assessment of users (working accounts of railway staff), devices (handheld terminals, vehicle terminals, etc.) and public network services, and are strongly configurable to implement fine-grained control according to the security level requirements of railway services. Data plane components include agents generated by user and device binding, public network cloud services and policy enforcement components, etc. The main work is to forward authentication applications, access applications and interaction information between public and private networks, etc., which can process data packets at high speed.

Each component in the system architecture implements the following functions respectively.

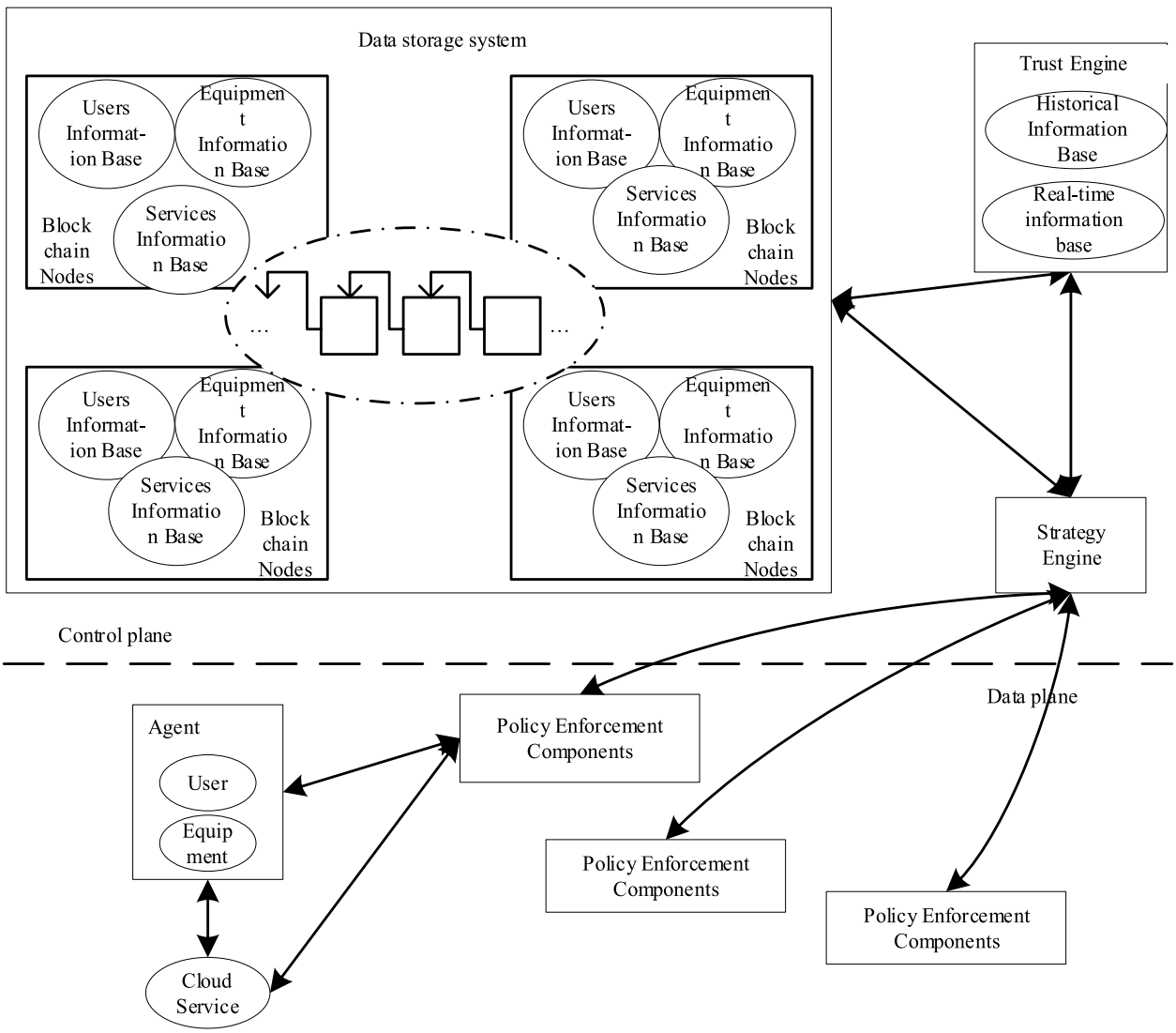

Fig. 4 Blockchain-based zero trust system architecture for railway

1) Agent: The proxy is the main body of the application for accessing the public network cloud service, and is generated by real-time binding of users and devices when issuing authentication applications. It can confirm the legal identities of practitioners and operators at the same time, further decouple the network location and credibility, and improve the safety of railway systems.
2) Cloud services: Provided by untrustworthy third parties in the public network, including edge cloud services and cloud services, which can provide customized services according to railway business needs, such as automatic ticketing business, video monitoring business, and intelligent feeder business, thus promoting the realization of a new generation of intelligent railway.
3) Policy enforcement component: Interacting with a policy engine to realize two-way authentication between agent and cloud service, enforcing security commands issued by policy engine, monitoring the behavior of public network cloud service in multiple dimensions, as well as providing data for the trust engine to generate reputation value of cloud service. Policy enforcement components need to be widely deployed in the network and as close as possible to users and devices, and can be filled by devices such as load balancers in practical applications in railway.
4) Policy engine: Receiving and processes authentication requests, interacting with the data storage system to determine the legitimacy of the node identity, and interacting with the trust engine to determine the trustworthiness of the cloud service, as well as deciding whether the agent can safely access the service according to the developed security rules. In the railway scenario, servers can be set at each field section and station.
5) Trust engine: It is responsible for the reputation assessment of public network cloud services and calculates the reputation value of public network cloud services in a certain period quantitatively based on the cloud service behavior data provided by the policy execution component and updates it periodically. The historical information base stores the reputation values generated in the previous reputation assessment phase, and the real-time information base stores the latest reputation values generated in this phase. Servers can be set at each field section and station in the railway scenario.
6) Data storage system: The data structure of the Merkle tree is used to store the authentication credentials of users, devices and cloud services in a distributed manner, and blockchain technology is used to form a blockchain of credentials among multiple nodes to achieve distributed storage to guarantee the authenticity and confidentiality of authentication credentials. In the railway scenario, blockchain nodes can be set at each railroad bureau for mutual backup.

Identity information storage scheme design

The traditional storage structure stores all the information about network participants in the database in order, and the authenticated party must send the complete authentication credentials for comparison and confirmation by the system when conducting authentication. When registering a large amount of identity information data, the traditional storage structure not only increases the amount of data transmitted in the network and reduces the authentication efficiency, but also increases the risk of identity information leakage, reduces authentication reliability, and ultimately threatens network security. In this paper, we propose a Merkle tree-based storage structure that only sends and compares the Merkle tree root value of all identifying information during authentication, which reduces the risk of privacy leakage while reducing the amount of network data transmission and improving authentication efficiency.

Users, devices, and cloud services must register their identity information as credentials for two-way authentication before joining the network for interaction, and store it in the credential blockchain. The authentication credentials are stored in a Merkle tree structure and encapsulated into blocks that are uploaded to each blockchain node for distributed storage. The storage structure of authentication credential data is shown in Fig. 5. The user's authentication credentials include authentication method, login credentials, affiliated person and creation time, etc. The authentication method can be password, biometric identification, etc., and the login credentials will be changed accordingly with the authentication method. The authentication credentials of the device include the manufacturer of the device, the factory date, the geographical location where the device was registered, and the IP address of the device. The authentication credentials for cloud services include the service developer, version number, release date, and update time. The more detailed the description of the user, device, and cloud service, the more secure the authentication will be. When storing the authentication credentials of users, devices, and cloud services, user name, device ID, and the cloud service number should be used as primary keys, respectively, to facilitate data query and update.

To accommodate the highly dynamic nature of network participants, each identity credential tree should be given a certain validity period by the control plane, and only the identity credentials within the validity period

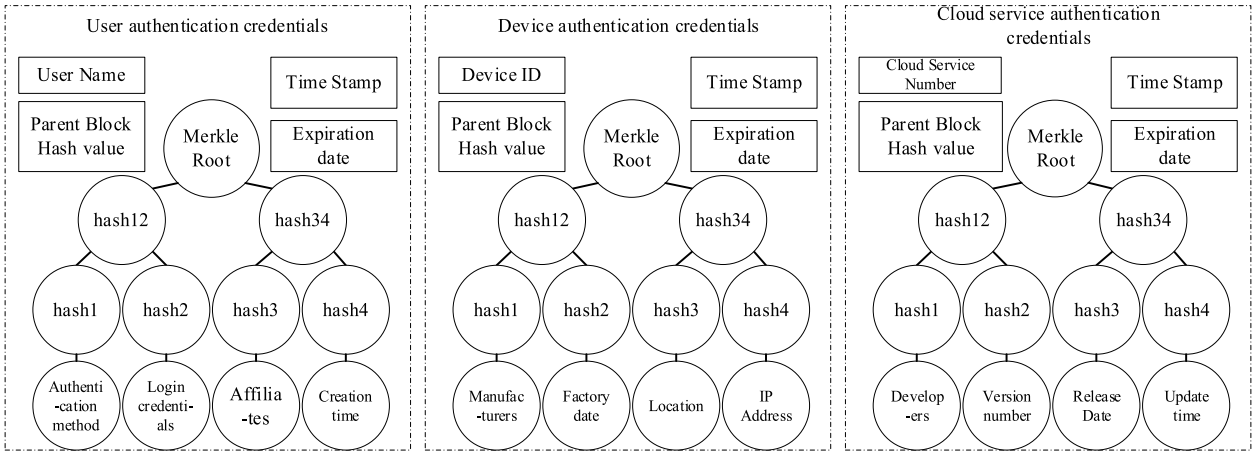

Fig. 5 Authentication credential tree

have legitimacy. When the identity information of users, devices and cloud services changes or the credentials expire, an identity credential update request is initiated to the control plane with the identity credential tree generated from the latest identity information. Upon receiving the request, the control plane can quickly locate the updated location of the identity credential tree with the help of the Merkle tree, generate a new identity credential tree, and set a new expiration date for the new identity credentials. An expired and persistently un-updated authentication credential tree will be logged by the control plane as stale. The invalidated authentication credential tree will no longer be available for authentication.

Thanks to the Merkle tree data structure, in the process of bi-directional authentication between the user and device agents and the public cloud service, only the root value of the respective authentication credentials needs to be sent instead of all the information to verify the identity of both parties, realizing zero-knowledge proof-based authentication, reducing the amount of data to be sent, improving authentication efficiency, and at the same time safeguarding the confidentiality of the authentication credential data transmitted in the public network confidentiality. The purpose of building a blockchain-based data storage system is to eliminate the problem of the single point of failure in centralized data centers and to guarantee the authenticity, reliability and confidentiality of authentication credential data. According to this feature, a polling mechanism or other low-overhead consensus mechanism can be chosen to allocate bookkeeping rights to improve system efficiency.

Identity authentication protocol design

To ensure that both communicating parties in the public-private converged network have legitimate identities, this section proposes a two-way authentication protocol. In the common one-way authentication, only the client verifies the identity of the cloud server, which is difficult to resist the lateral attacks launched by internal malicious nodes and may cause the collapse of trust within the system, while the access to public cloud services is not secured. The introduction of two-way authentication can counter both internal and external threats to the system, further securing the public-private converged network of railway.

After completing the registration of identity information, users in the railway industry can send authentication requests to the public network. Only when the two-way authentication is successful can the cloud service provide relevance to the user. In order to simplify the node processing process in the network and improve the authentication efficiency, the authentication process proposed in this paper uses symmetric encryption algorithm for data encryption and the relatively simple MD5 (Message-Digest Algorithm 5) as the hash algorithm for generating the authentication credential tree, which has low forward computation overhead and low processing latency while minimizing the security cost.

Two-way authentication is divided into two phases, preparation and authentication, and the specific process is shown in Fig. 6.

(1) Authentication preparation phase:

The user and the device it uses are bound to generate a proxy, and the authentication credential tree of the proxy is generated based on the device and user information and stored in secure hardware such as the Hardware Trusted Platform Module (TPM).

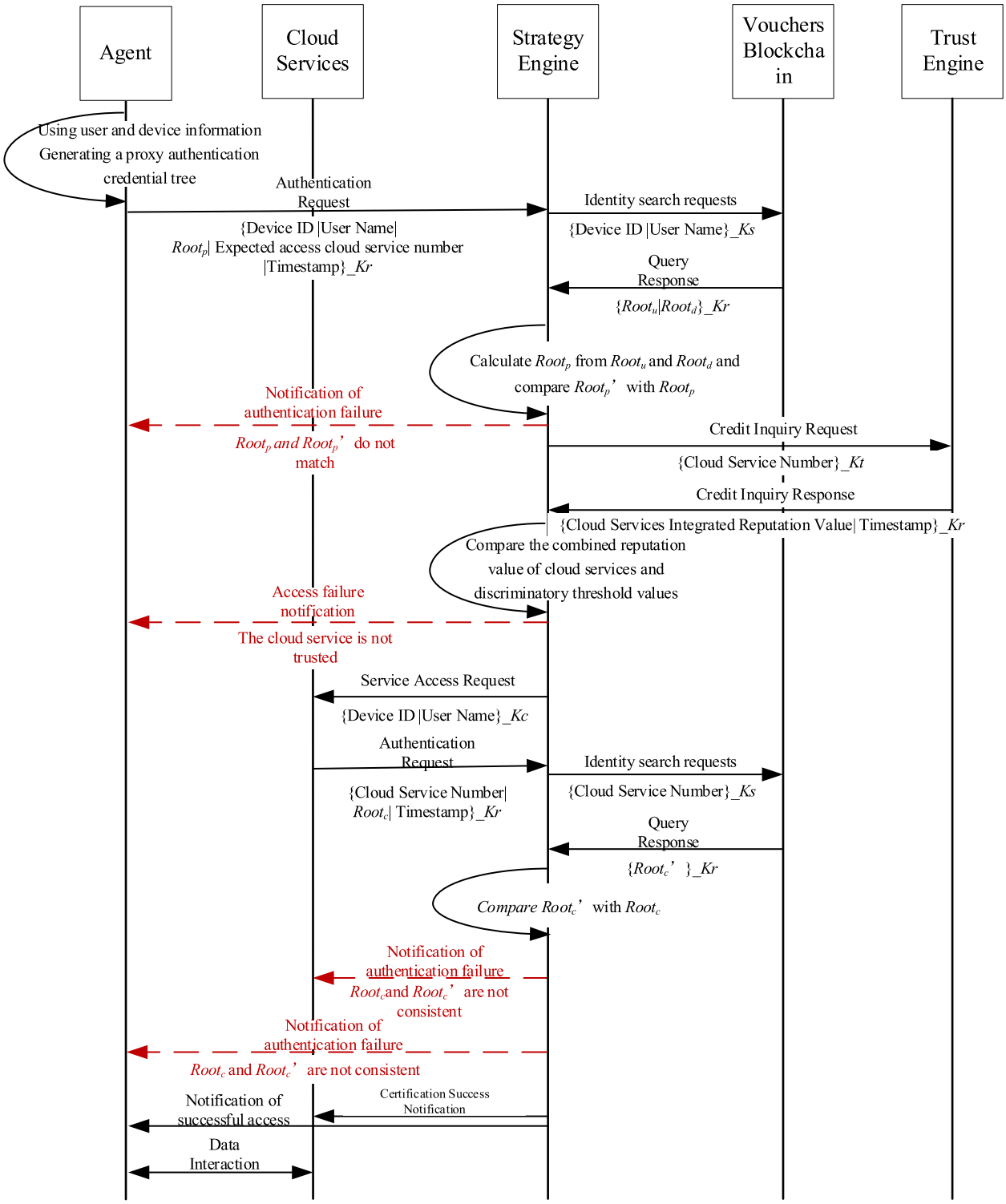

Fig. 6 Authentication process

(2) Two-way authentication phase.

1) The agent sends an authentication request to the policy engine, which includes the device ID, user name, root value $Root_p$ of the agent authentication credential tree, the cloud service number that the agent expects to access, and a timestamp. The message is encrypted using the policy engine's key *Kr*.
2) The policy engine applies to the credential blockchain to take out the authentication credential root values $Root_u$ and $Root_d$ of the corresponding device and user based on the device ID and user name, and the message is encrypted by the data storage system key *Ks*. Then the policy engine performs a hash operation on the two received root values to get the authentication credential root value $Root_p$'of the agent and compares it with $Root_p$ to verify the legitimacy of the agent identity.
3) If $Root_p$' is different from $Root_p$, the policy engine returns the authentication failure notification to the agent and ends this authentication process; if they are the same, the policy engine sends a reputation query request to the trust engine, which contains the cloud service number that the agent expects to access and is encrypted with the trust engine's key *Kt*.
4) The trust engine returns the comprehensive reputation value of the cloud service to the policy engine, and the policy engine compares the comprehensive reputation value with the preset threshold value: if the value is lower than the threshold, the cloud service is considered untrustworthy, and the policy engine reports to the agent to return the access failure notification; otherwise, the policy engine sends a service access application to the cloud service, and the message contains the device ID and user name of the agent that is expected to access the cloud service, and is encrypted with the cloud service key *Kc*.
5) The cloud service sends an authentication request message to the policy engine, containing the cloud service number, the root of the authentication credential tree for the cloud service, $Root_c$, and a timestamp, and encrypts it with the policy engine key *Kr*.
6) The policy engine authenticates the cloud service similar to the proxy and compares the $Root_c$, sent by the cloud service with the $Root_c$,' taken from the credential blockchain: if they are different, the policy engine sends an authentication failure notification to the cloud service and an access failure notification to the proxy; otherwise, the policy engine sends an authentication success notification to the cloud service and an access success notification to the proxy. Otherwise, the policy engine sends an authentication success notification to the cloud service and an access success notification to the agent.

After two-way authentication is completed, the agent can confirm the identity of the public network cloud service registered in the control plane of the private network and initiate service access application to the public network. The public network cloud service can also verify the legitimacy of the internal personnel and equipment of the system, thus realizing safe and reliable information interaction between the public network and the private network of the railway industry.

Credibility assessment mechanism

In order to quantify the trustworthiness of the public network cloud service under the railway public-private network convergence scenario, the reputation evaluation mechanism of the public network cloud service is constructed as shown in Fig. 7. Considering the computation capability, storage capability, service capability and network performance of the cloud service, its performance in terms of computation speed, computation correct rate, storage speed, storage capacity, response time, the request acceptance rate and packet loss rate is recorded respectively. The policy enforcement component in the network will use the same test data to perform periodic tests on each public cloud service, record the performance of the public cloud service and send the test results to the trust engine. The trust engine combines the real-time reputation value during the current cycle and the historical reputation value obtained from the previous test cycle to obtain the combined reputation value of the cloud service. The period of reputation value evaluation can be set for a few hours to a few days, depending on the actual frequency of changes and security requirements of the public network cloud services in the rail communication system.

1) The result of computational speed test is

$$R_{\text{speed}} = \begin{cases} 1, & t_{\text{com}} < T_{\text{com}} \\ 1 - \frac{t_{\text{com}} - T_{\text{com}}}{T_{\text{com}}}, & \mathrm{T}_{\text{com}} \le t_{\text{com}} \le 2T_{\text{com}} \\ 0, & 2T_{\text{com}} < t_{\text{com}} \end{cases} \quad (1)$$

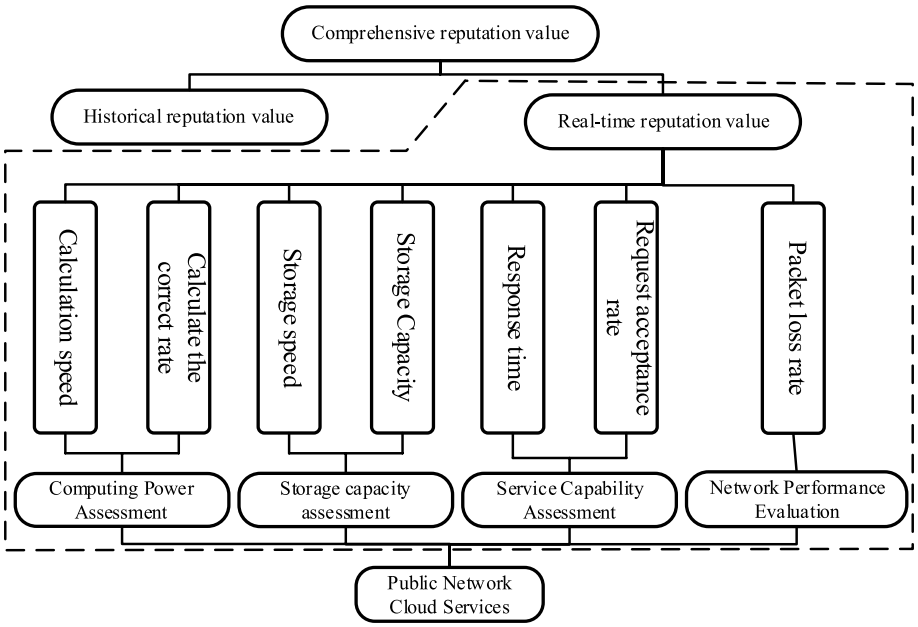

Fig. 7 Public network cloud service reputation assessment mechanism

where R_{speed} is the result of the computational speed test, t_{com} is the time taken for this computational speed test, and T_{com} is expressed as the acceptable time set by the system for the computation.

2) The result of calculation correctness test is

$$R_{\text{accu}} = \frac{C_{\text{corr}}}{C_{\text{total}}} \tag{2}$$

where R_{accu} is the result of the computation correctness test, C_{corr} represents the number of times the public cloud service performs computation tasks with correct results in this test cycle, and C_{total} is the total number of times the public cloud service performs computation tasks in this test cycle.

3) The result of storage speed test is

$$R_{\text{rnw}} = \begin{cases} 1, & t_{\text{rnw}} < T_{\text{rnw}} \\ 1 - \frac{t_{\text{rnw}} - T_{\text{rnw}}}{T_{\text{rnw}}}, & T_{\text{rnw}} \le t_{\text{rnw}} \le 2T_{\text{rnw}} \\ 0, & 2T_{\text{rnw}} < t_{\text{rnw}} \end{cases} \tag{3}$$

where R_{rnw} is the result of the storage speed test, t_{rnw} is the elapsed time of this storage speed test, and T_{rnw} is the system set storage acceptable latency.

4) The result of storage capacity test is

$$R_{\text{store}} = \frac{D_{\text{idle}}}{D_{\text{total}}} \tag{4}$$

where R_{store} is the result of the storage capacity test, D_{idle} is the storage capacity available for the public cloud service in this test cycle, and D_{total} is the total storage capacity of the public cloud service.

5) The result of response time test is

$$R_{\text{res}} = \begin{cases} 1, & t_{\text{res}} < T_{\text{res}} \\ 1 - \frac{t_{\text{res}} - T_{\text{res}}}{T_{\text{res}}}, & T_{\text{res}} \le t_{\text{res}} \le 2T_{\text{res}} \\ 0, & 2T_{\text{res}} < t_{\text{res}} \end{cases} \tag{5}$$

where R_{res} is the result of the response time test, t_{res} is the elapsed time of this response time test, and T_{res} is the acceptable response time set by the system.

6) The result of request acceptance rate test is

$$R_{\text{acpt}} = \frac{N_{\text{acpt}}}{N_{\text{total}}} \tag{6}$$

where R_{acpt} is the result of the request acceptance rate test, N_{acpt} is the number of service requests accepted by the public cloud service in this test cycle, and N_{total} is the total number of service requests received by the public cloud service.

7) The result of packet loss rate test is

$$R_{plr} = 1 - \frac{P_{loss}}{P_{total}} = \frac{P_{arr}}{P_{total}} \tag{7}$$

where R_{plr} is the result of the packet loss rate test, P_{loss} is the number of data packets that the public network cloud service failed to receive in the test period, P_{arr} is the number of data packets successfully received by the public network cloud service in the test period, and P_{arr} is the test period. The total number of data packets sent to the public network cloud service in the cycle.

The real-time reputation value of the public cloud service is obtained by integrating the test results of each of the above dimensions using a weighted summation. According to the QoS requirements in practical applications, different weights can be assigned to each dimension. Considering that the behavior of public network cloud services generally has continuity, the historical reputation value is incorporated into the reputation evaluation mechanism, and the reputation value evaluation results obtained in the previous test cycle are weighted and summed with the current real-time reputation value evaluation results to obtain the comprehensive reputation value of public network cloud services. R in Eq. (8) is the comprehensive reputation value, R_{his} and R_{new} are the historical reputation value and real-time reputation value respectively, w_{his} and w_{new} are the weights of historical reputation value and real-time reputation value respectively, and there is:

$$R = w_{his}R_{his} + w_{new}R_{new} \tag{8}$$

For a new service in the network, the system should assign an initial reputation value to it. Based on the definition of reputation value described above, it can be seen that the reputation value can take a range of [0,1], with a reputation value of 0 indicating that the node is completely untrustworthy and a reputation value of 1 indicating that the node is completely trustworthy. Since the system does not have any information related to the trustworthiness of the new entry service, the initial reputation value can generally be set to 0.5.

The combined historical reputation value and real-time reputation value of the public network cloud service for periodic reputation assessment can quickly reflect the trustworthiness of the highly dynamic cloud service in the public network, help the control plane of the railway system to judge its reliability, and then decide whether to trust and access the service. The dynamic reputation value calculation mechanism can effectively defend against attacks from malicious cloud services and guarantee the safe operation of the railway system.

Performance analysis

Security analysis

The blockchain-based zero-trust architecture for railway public-private networks has the following security features.

Data privacy protection

Use the Merkle tree structure to store the authentication credentials of users, devices, and cloud services, and only transmit the user name, device ID, and cloud service number in the network without involving more detailed identity information, ensuring that the identity information does not exist in the credential block chain. Only the data storage system of the control plane and the authenticator know the details of the authentication credentials, thus protecting data privacy and ensuring the confidentiality of the authentication credentials. In this paper, we use HLPSL [29] (High-Level Protocol Specification Language) in AVISPA [30]. (Automated Validation of Internet Security Protocols and Applications) software AVISPA is a software for automatic validation of Internet security protocols and applications, which provides a modular role-based language HLPSL and integrates various advanced automatic analysis techniques in the backend shown in Fig. 8.

The results of using AVISPA to analyze traditional authentication protocols that do not use the Merkle tree structure to store authentication credentials are shown in Fig. 9. The red box shows the result of this formal analysis of the security protocol, and the result shows UNSAFE, which shows that the traditional model is difficult to guarantee the data security of the authentication credentials.

Figure 10 shows the results of using AVISPA to analyze the authentication protocol proposed in this paper. As shown in the red box, the result is shown as SAFE, which shows that the storage of authentication credentials based on Merkle tree structure can effectively improve the security of data compared with the traditional model.

Data tamper-proof

Blockchain technology is used to form a blockchain of credentials and store the authentication credential

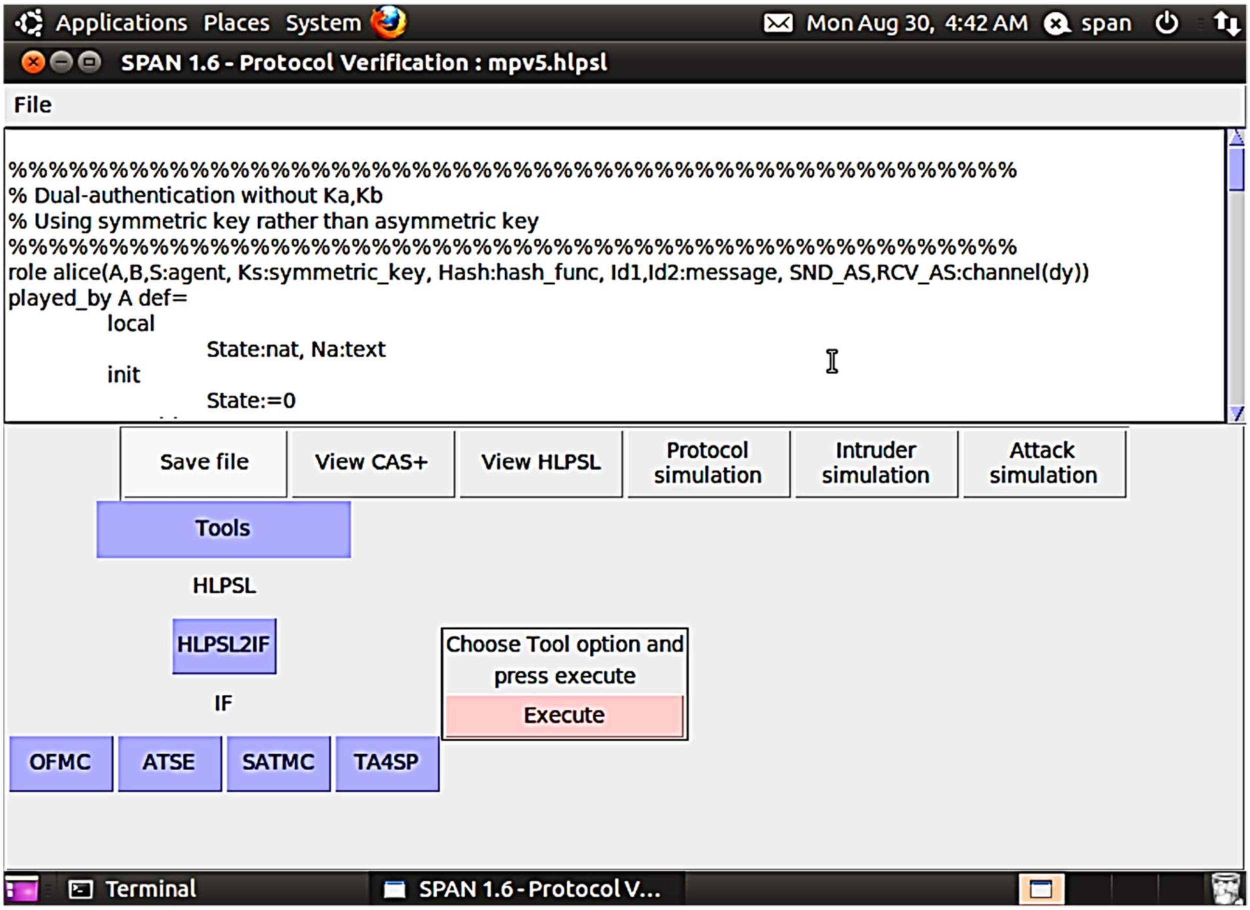

Fig. 8 AVISPA basic operation interface

blocks in a distributed manner at multiple nodes to achieve decentralized storage of authentication credentials and avoid the single point of failure. At the same time, the tamper-proof and traceable features of blockchain also guarantee the authenticity and reliability of authentication credentials.

Anti-identity forgery attack

The identity forgery attack is a kind of attack that steals or forges identity authentication credentials to achieve illegal access [31]. In the security model proposed in this paper, a malicious attacker who wants to illegally access the public cloud service needs to forge all the authentication credentials of both the user and the device in order to get the same Merkle root as the real agent and pass the authentication; however, the authentication credentials are securely stored in the credential blockchain and are difficult to be stolen, thus the system is able to resist the threat of identity forgery attacks.

Anti-replay attacks

Replay attack refers to the attacker sending a packet that has been sent by a real agent to achieve the purpose of spoofing the control plane and thus corrupting the correctness of the identity authentication [32]. In the security model proposed in this paper, the authentication application contains a timestamp and is encrypted using a key that is difficult to tamper with. The control plane can determine the freshness of the message based on the timestamp in the application and thus decide whether to process the application next.

Two-way authentication

The introduction of two-way authentication mechanism in the security model proposed in this paper can avoid the nodes inside the railway industry from accessing the public cloud service with unknown identities, and also ensure that the public cloud service only provides services to legitimate internal railway users and devices. This mechanism also provides a guarantee for safe and reliable operation inside the railway communication system and

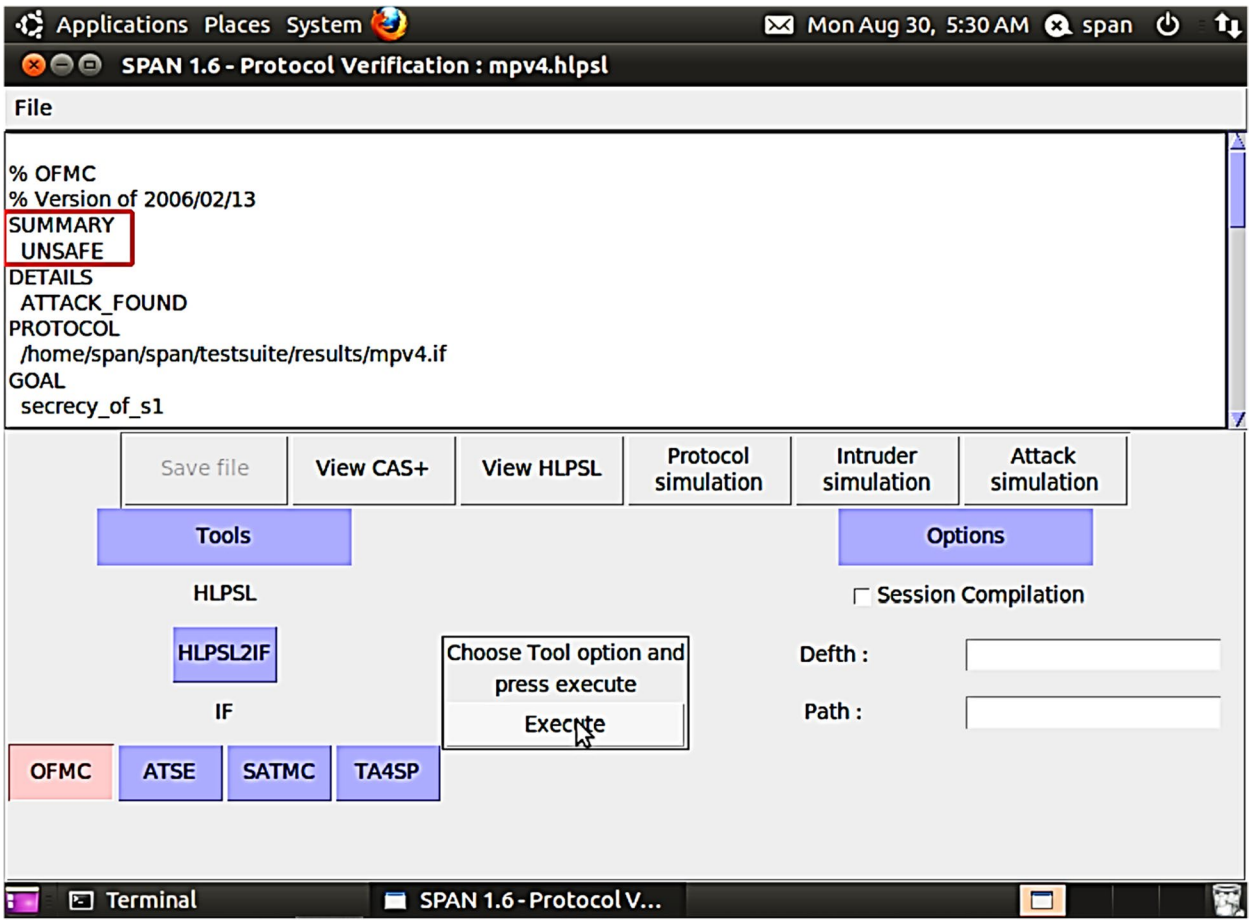

Fig. 9 Traditional authentication protocol analysis results

public network security, further promoting the trend of public-private network convergence.

Identity-based security policy

This paper introduces the concept of zero trust in the construction of the security model, organically combines two-way authentication and reputation assessment mechanism, decouples network location and network security, converts network location-based security policy into identity-based security policy, and thus better adapts to the network architecture with increasingly blurred security boundaries in the process of public-private network convergence development.

Efficiency analysis

Information update efficiency

As mentioned earlier, when active or passive identity information updates occur for users, devices, and cloud services, a Merkle tree generated from the latest identity information is sent to the control plane in the identity credential update request. The control plane compares the two authentication credential trees to quickly locate the location of the different nodes and update the identity information accordingly. In Fig. 5, for example, only four dimensions of identity information are registered, and the traditional data structure needs to compare all four segments of information, while the Merkle tree structure only needs to compare three segments. In practical applications, the more detailed the description of the identity information of the authenticated party, i.e., the more dimensions of the identity information, the higher the security of the system, and the more obvious the advantages of the Merkle tree-based data storage system in terms of information update efficiency. A comparison of the information update complexity of this scheme and the traditional scheme is shown in Fig. 11.

In Fig. 11, we can see that the horizontal coordinate is the identity information dimension n, the vertical coordinate is the complexity, and the straight line is the Merkle tree-based scheme proposed in this paper, and the straight line with circles is the traditional scheme. The traditional scheme is linearly increasing, while the

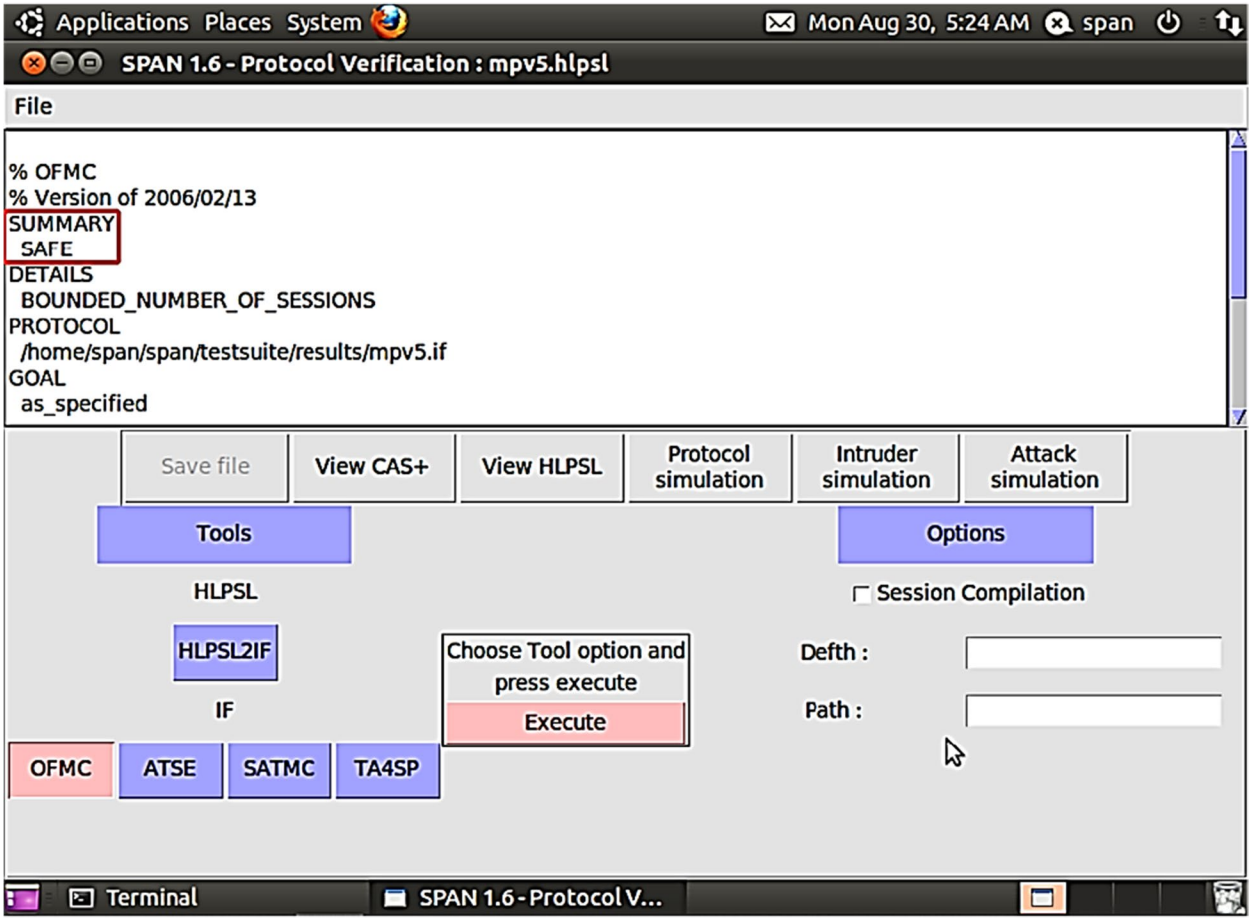

Fig. 10 Results of the Merkle tree-based authentication protocol

complexity of the proposed scheme is gradually slowing down. It can be seen that the larger the dimension of identity information, the greater the advantage of the proposed scheme.

Authentication efficiency

Taking the structure shown in Fig. 5 as an example, the parameters and length of each identity information in the security model constructed in this paper are shown in Table 1.

For the traditional authentication scheme, all the data related to the authenticated party needs to be sent to the system for information matching. In the security model proposed in this paper, only the cloud service number, user name, device ID and the root of the two authentication credential trees need to be sent, and a total of 464 bits of information needs to be sent, which is about half of the transmission overhead of the traditional authentication scheme. A comparison of the length of information to be transmitted for each service and proxy authentication in the traditional scheme and the proposed scheme is shown in Fig. 12.

In Fig. 12, the horizontal coordinates are the service identity information and the proxy identity information, respectively, and the vertical coordinates are the length of the information transmitted during the authentication process in bits per node. In Fig. 12, we can see that the length of information transmitted in the traditional authentication scheme is 260 bits per node for sending service identity information, while the proposed scheme is 180 bits per node, which is less than the traditional authentication scheme. For the proxy identity information, the length of information transmitted in the proposed scheme is much smaller than that in the traditional authentication scheme, which is about half of the transmission overhead of the traditional authentication scheme. Therefore, the scheme proposed in this paper is more efficient than traditional certification solutions.

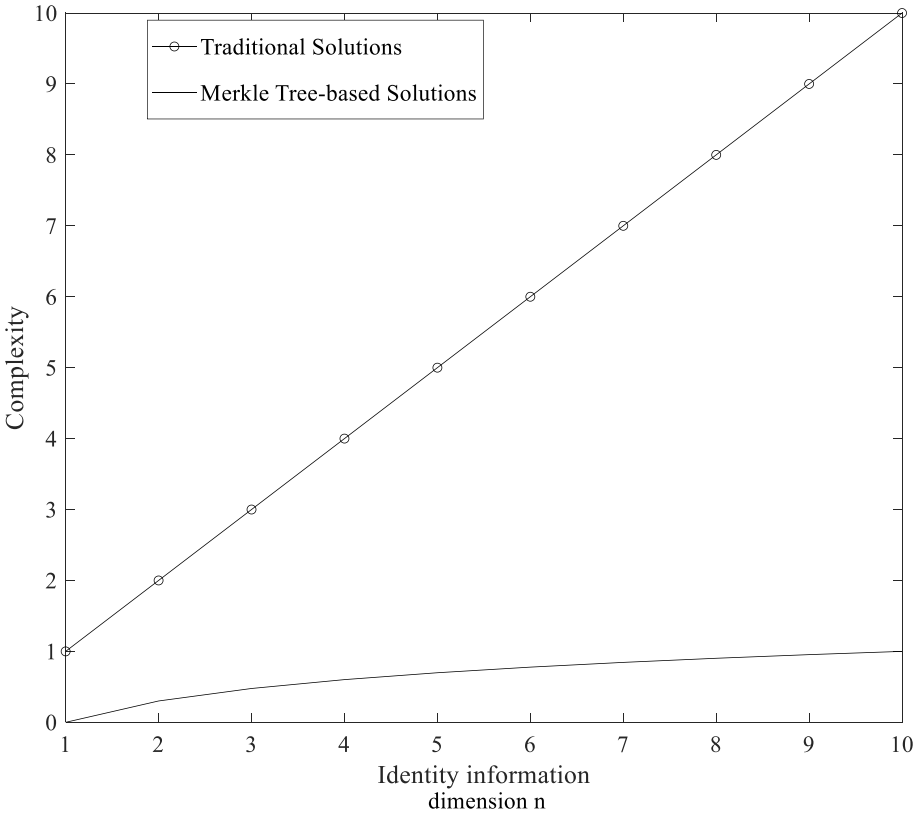

Fig. 11 Comparison of complexity of identity information update

Table 1 Identity information parameters

Member	Identity Information	Description	Minimum length (bit)
Cloud Services	Cloud Service Number	Tens of millions of public network cloud services	64
	Developers	MCC + MNC	48
	Version number	3-digit version number	24
	Release Date	"Year-Month-Day" format	64
	Update time	""Year-Month-Day" format	64
User	User Name	6-20 English characters	48
	Authentication method	Password, fingerprint, etc.	2
	Login credentials	6-30 digits password information is the shortest	48
	Affiliates	8-digit industry employee number	64
	Creation time	"Year-Month-Day" format	64
Device	Device ID	EPC Code	96
	Manufacturers	15-digit enterprise business registration number	120
	Factory date	"Year-Month-Day" format	64
	Location	"Degree - Minute - Second" format	48
	IP Address	IPv6 Addresses	128

Stability analysis

Considering the existence of sudden temporary problems such as network failures or server crashes in public cloud services, the reputation value evaluation mechanism proposed in this paper considers both real-time reputation value and historical reputation value, and

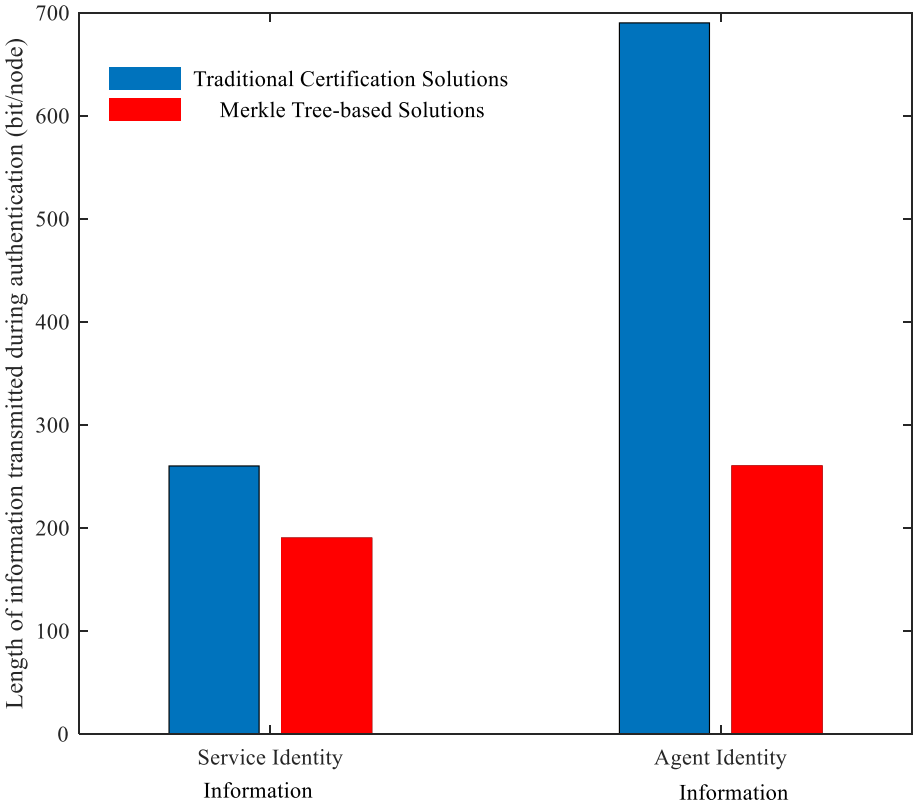

Fig. 12 Certification efficiency comparison

the comprehensive reputation value of cloud services is obtained by weighting the sum of the two. The impact of different historical reputation value settings on the comprehensive reputation value of cloud services is shown in Fig. 13.

Considering the case of abnormal sudden performance of normal services, the tested public network cloud services performed abnormally in the 7th and 12th test cycles, respectively, while they performed normally in other test cycles. From the simulation results in Fig. 13, it can be seen that when the historical reputation value is not considered, the system stability is poor. The larger the historical reputation value is in the comprehensive reputation value, the better the system stability is, and the stronger the ability to fight against the sudden abnormal performance of normal services, but the less sensitive the reaction to the malicious performance of the service is. In other words, the system's operational stability and response sensitivity are mutually constrained. In the practical application of the railway industry, the specific percentage of historical reputation value should be combined with the actual demand and be tested repeatedly before putting into formal use.

Conclusion

In this paper, we proposed a cloud computing assisted zero-trust security model based on blockchain technology to address the security issues such as complex network architecture, ambiguous security boundaries, and low trustworthiness of data and nodes in railway public-private network convergence scenario. The identity authentication credentials of users, devices and cloud services are stored in a distributed manner using blockchain to eliminate the single point of failure and guarantee reliability and confidentiality in terms of the data storage system. In order to quickly locate the modified and compared information, an identity information storage mechanism based on Merkle tree structure was proposed, which effectively improves the efficiency of identity information update and authentication. In addition, a two-way identity authentication method was designed to bind users and devices in real time and generate proxy to fight against internal and external threats to the system at the same time. Then, we introduced a public network cloud service reputation evaluation mechanism to quantify service performance in multiple dimensions and promote the safe and reliable operation

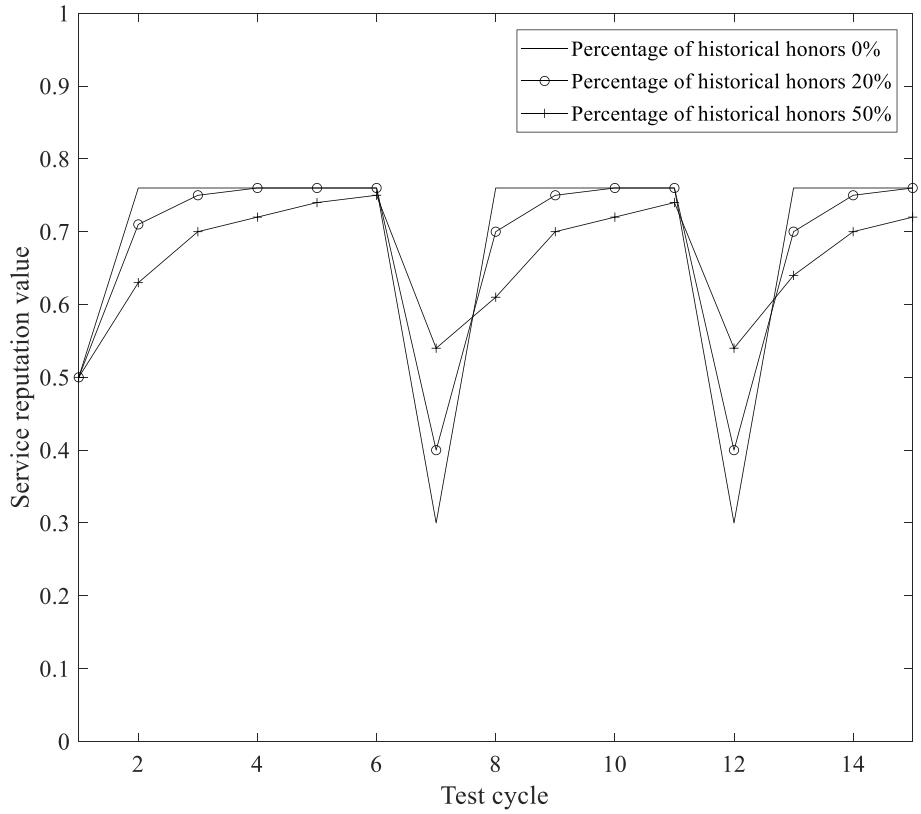

Fig. 13 Impact of historical reputation value on service reputation value

of the railway system. Finally, this paper analyzed the security model in terms of security, efficiency and stability, and proves that the model can guarantee the security of each service and application efficiently and reliably under the converged architecture of railway public-private network.

Authors' contributions

Y. Feng and Y. Lu wrote the main manuscript text. L. Wang and X. Sun prepared the original figures and evaluation results. Z. Zhong, Y. Lu, and Y. Zhu provided ideas and writing instructions for the proposed solution. All authors reviewed the manuscript. The author(s) read and approved the final manuscript.

Funding

This work was supported by the Project of China State Railway Group under Grant N2021W005.

Availability of data and materials

Not applicable.

Declarations

Ethics approval and consent to participate

Not applicable.

Competing interests

I declare that the authors have no competing interests as defined by Springer, or other interests that might be perceived to influence the results and/or discussion reported in this paper.

Received: 8 December 2022 Accepted: 25 February 2023
Published online: 24 April 2023

References

1. The Central Committee of the Communist Party of China, the State Council of the People's Republic of China Outline for Building a Strong Transportation Country [EB/OL]. http://www.gov.cn/zhengce/2019-09/19/content_5431432.htm, 2019-09-19/2021-06-23
2. White Paper on 5G Public Private Network of Railway Industry. Editor in Chief: Nanjing Metro Group Co., Ltd, China United Network Communications Co., Ltd. Jiangsu Branch and Huawei Technology Co., Ltd. Release date: April 2021
3. Bodkhe U, Tanwar S, Parekh K et al (2020) Blockchain for industry 4.0: a comprehensive review. IEEE Access 8:79764–79800
4. Tan C, Chen M-j, Ackah AE (2020) Research on distributed identity authentication mechanism of IoT device based on blockchain. Chin J Internet Things 4(02):70–77
5. Cao S-y, Yao Y-y, Chang X-l (2020) Lightweight secure authentication scheme using blockchain for RFID system in smart factory. Cyberspace Secur 11(09):70–77+93

6. Le L, Yong S (2020) Intelligent device authentication scheme based on blockchain technology. Comput Digit Eng 48(07):1722–1726
7. Peng-guo T, Fei L (2021) A method of user authentication based on blockchain. Commun Tech 54(5):1214–1219
8. Abbas N et al (2018) Mobile edge computing: a survey. IEEE Internet Things J 5(1):450–465
9. Dai Y, Guan YL, Leung KK, Zhang Y (2021) "Reconfigurable Intelligent Surface for Low-Latency Edge Computing in 6G." IEEE Wirel Commun 28(6):72–79. https://doi.org/10.1109/MWC.001.2100229.
10. Zhang H et al (2017) A hierarchical game framework for resource management in fog computing. IEEE Commun Mag 55(8):52–57
11. Xing C, Jing Y, Wang S, Ma S, Poor HV (2020) "New Viewpoint and Algorithms for Water-Filling Solutions in Wireless Communications." IEEE Trans Signal Process 68:1618–1634. https://doi.org/10.1109/TSP.2020.2973488
12. Xiong Z, Zhang Y, Niyato D, Wang P, Han Z (2018) When Mobile Blockchain meets edge computing. IEEE Commun Mag 56(8):33–39. https://doi.org/10.1109/MCOM.2018.1701095
13. Watanabe H, Fujimura S, Nakadaira A et al (2016) Blockchain contract: securing a blockchain applied to smart contracts. In: Proceedings of the 2016 IEEE international conference on consumer electronics (ICCE). IEEE Press, Ha Long, pp 467–468
14. Kang J, Yu R, Huang X et al (2019) Blockchain for secure and efficient data sharing in vehicular edge computing and networks. IEEE Internet Things J 6(3):4660–4670
15. Shala B, Trick U, Lehmann A et al (2020) Blockchain and trust for secure, end-user-based and decentralized IoT service provision. IEEE Access 8:119961–119979
16. Gilman E, Barth D (2017) Zero trust networks. O'Reilly Media, Inc, Boston
17. Chakrabarti A. Lessons learned from five years of multi-cloud at PagerDuty[EB/OL]. https://www.usenix.org/conference/srecon18americas/presentation/chakrabarti. 2018-03-28/2021-06-23
18. Ward R, Beyer B (2014) Beyondcorp: A new approach to enterprise security. USENIX Annul Technical Conference 39(6):6–11
19. Ma D, Li L, Ren H, Wang D, Li X, Han Z (2020) Distributed Rate Optimization for Intelligent Reflecting Surface with Federated Learning. In: 2020 IEEE International Conference on Communications Workshops (ICC Workshops), Dublin, pp 1–6. https://doi.org/10.1109/ICCWorkshops49005.2020.9145388
20. Mao S et al (2023) Intelligent reflecting surface-assisted low-latency federated learning over wireless networks. IEEE Internet Things J 10(2):1223–1235. https://doi.org/10.1109/JIOT.2022.3204637
21. Tian K, Chai H, Liu Y, Liu B (2022) Computation rate maximization for IRS-enhanced dynamic spectrum access assisted MEC system. Phys Commun 52:101697
22. Chen G, Wu Q (2022) Computation Rate Maximization for IRS-Aided Wireless Powered MEC Systems. In: 2022 IEEE wireless communications and networking conference (WCNC). Institute of Electrical and Electronics Engineers (IEEE), Austin, pp 417–422. https://doi.org/10.1109/WCNC51071.2022.9771984
23. Du J et al (2022) Resource pricing and allocation in MEC enabled Blockchain systems: an A3C deep reinforcement learning approach. IEEE Trans Netw Sci Eng 9(1):33–44. https://doi.org/10.1109/TNSE.2021.3068340
24. Feng J, Zhang W, Pei Q, Wu J, Lin X (2022) Heterogeneous computation and resource allocation for wireless powered federated edge learning systems. IEEE Trans Commun 70(5):3220–3233. https://doi.org/10.1109/TCOMM.2022.3163439
25. Feng J, Liu L, Pei Q, Li K (2022) Min-max cost optimization for efficient hierarchical federated learning in wireless edge networks. IEEE Trans Parallel Distrib Syst 33(11):2687–2700. https://doi.org/10.1109/TPDS.2021.3131654
26. Liu L, Zhao M, Yu M, Jan MA, Lan D, Taherkordi A Mobility-Aware Multi-Hop Task Offloading for Autonomous Driving in Vehicular Edge Computing and Networks. In: IEEE Transactions on Intelligent Transportation Systems. https://doi.org/10.1109/TITS.2022.3142566
27. Wei-gang L, Qiang L (2021) Analysis of environment monitoring network security based on zero trust network model. Sichuan Environ 40(03):60–63
28. Xin-yue Y, Gang S, Ya-wei Z (2021) Research on software-defined -perimeter network stealth technology based on zero trust. Commun Techn 54(5):1229–1234
29. Chevalier Y, Compagna L, Cuellar J et al (2004) A high level protocol specification language for industrial security-sensitive protocols. In: Proceeding of the 2004 workshop on specification and automated processing of security requirements (SAPS). Austrian Computer Society, Linz, p 13
30. Genet T. A short span+ avispa tutorial [EB/OL]. http://people.irisa.fr/Thomas.Genet/span/SPAN_AVISPA_tutorial.pdf. 2015-10-15/2021-06-23
31. Ku WC, Chang ST (2005) Impersonation attack on a dynamic ID-based remote user authentication scheme using smart cards. IEICE Trans Commun 88(5):2165–2167
32. Mo Y, Sinopoli B (2009) Secure control against replay attacks. In: Proceeding of the 2009 47th annual Allerton conference on communication, control, and computing (Allerton). IEEE Press, Illinois, pp 911–918

Publisher's Note