Hindawi
Security and Communication Networks
Volume 2022, Article ID 9896689, 17 pages
https://doi.org/10.1155/2022/9896689

Research Article

Zero-Trust-Based Protection Scheme for Users in Internet of Vehicles

Letian Fang,[1] **Chunshang Wu**,[2] **Yukun Kang**,[2] **Wei Ou**,[2] **Donghao Zhou**,[3] **and Jun Ye**[2]

[1]*School of Food Science and Engineering, Hainan University, Haikou, China*
[2]*School of Cyberspace Security, Hainan University, Haikou, China*
[3]*School of Computer, National University of Defense Technology, Changsha, Hunan, China*

Correspondence should be addressed to Wei Ou; ouwei@hainanu.edu.cn

Received 1 October 2021; Revised 28 November 2021; Accepted 21 April 2022; Published 12 May 2022

Academic Editor: Weizhi Meng

At present, the Internet of Vehicles technology is developing rapidly, but in the process of networking it may be attacked by hackers. In view of the tampering attack on the user's device and identity, we establish a multifactor authentication scheme to achieve dual identity authentication through device fingerprint authentication and PKI authentication. In response to the attack by hackers in the application of data transmission, we use the SM series of state secret algorithms for data encryption and take advantage of the immutable and decentralized characteristics of blockchain to ensure the security and integrity of data collection and transmission. Through the zero-trust security network architecture, the security level of the system in the process of data transmission is effectively improved, the identity-centered dynamic access control is carried out, the user's behavior is monitored in real time, and the malicious nodes are screened and eliminated, which improves the stability and security of the Internet of Vehicles data transmission system. By adopting the identity authentication pass rate, fingerprint authentication pass rate, API authentication pass rate, and SPA packet transmission acceptance rate as the factor set, the evaluation level of the vehicles is calculated. The experimental results show that compared with the traditional boundary-centered security protection, our scheme can protect a wider range of application security, even if there are security problems, the loss is less. Through the training simulation of the convolutional neural network, the classification accuracy of the trust level is improved.

1. Introduction

In recent years, with the rapid development of mobile Internet and industrial intelligence, the automotive industry is constantly changing to intelligence and networking. Internet of Vehicles has become an important research field. The Internet of Vehicles refers to the realization of an all-around network connection within vehicles, between vehicles and people, between vehicles and vehicles, between vehicles and roads, and between vehicles and service platforms with the help of a new generation of mobile communication technology [1]. The Internet of Vehicles improves the intelligence level and automatic driving ability of vehicles and brings great convenience to people's transportation. At the same time, it will help the government to establish an intelligent transportation system and build a new business form of automobile and transportation. Figure 1 shows the Internet of Vehicles communication scenario.

The Internet of Vehicles system contains massive private data of relevant users and vehicles. The cloud service platform of Internet of Vehicles includes key data such as vehicle management and transportation, service of information content, and personal information. Therefore, data security is an important issue of Internet of Vehicles. In the traditional Internet of Vehicles, the information of users and vehicles exposed in public is easily stolen, interfered, or even modified, as the Internet of Vehicles is a part of wireless communication. At present, the academic community believes that the threat to data security of Internet of Vehicles mainly comes from the following two aspects:

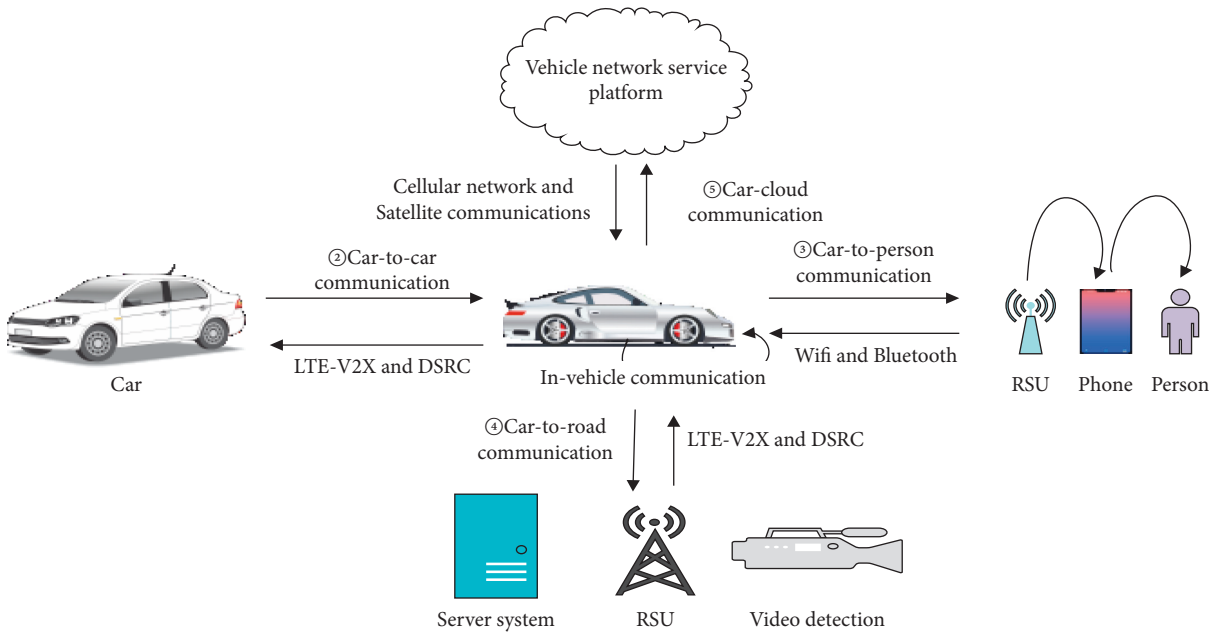

Figure 1: Communication scenarios of vehicle networking.

(i) The attacker attacks the vehicle-linked network transmission. In the process of wireless communication, the attacker obtains the private data from users on the vehicle node in the communication channel by launching an eavesdropping attack. After the eavesdropping attack, the attacker can also coordinate a tampering attack, falsify the collected private data, and then send the wrong information to the users.

(ii) The attacker attacks the application side of the Internet of Vehicles. When the road traffic infrastructure RSU, traffic cameras, and other devices that receive communication information are captured by an attacker, a node capture attack will come. In addition, if the smart device related to the Internet of Vehicles application is lost, attackers may use the authentication information in them to have access to resources and services illegally. There are also attacks initiated by system insiders. For example, an administrator who has access to user passwords illegally embezzles and uses users' information, which is stored in the system server to launch attacks on the network. Such ghost-type attacks will also threaten the security of the Internet of Vehicles network. The safety problems are diversely faced by the Internet of Vehicles, and the defense solution we need to do should be comprehensive. It is the direction that we need to solve urgently to establish a three-dimensional and reliable security defense system for the Internet of Vehicles.

The protection measures of data security introduced in the existing research mainly focus on data encryption technology, data access control technology, corresponding integrity protection, data existence and availability proof, and virtualization security technology. The above technologies can ensure the security of user private data, to a certain extent. In the Internet of Vehicles environment, with the high-speed movement of vehicles, the network topology and the external environment of vehicles are constantly changing, and unknown network attacks will continue to emerge. However, the existing research is still based on traditional border security. By dividing the security area, the network is divided into an external network and an internal network. The traditional border security takes the defense in depth model as the center and carries out security protection by building a "wall." By default, the interior of the border is not secure, which cannot prevent malicious attacks launched by attackers from the interior, and there are great security risks. In the Internet of Vehicles, data are assets and have a high value. To deal with the shortcomings of traditional security protection, a new security concept focusing on data should be adopted. The zero-trust business security takes identity as the center and establishes a dynamic portable boundary. For the cloud PAN-interconnected vehicle networking system of people, vehicles, and roads, the zero-trust security system is more suitable. Compared with the traditional scheme, we take the lead in using the zero-trust security architecture in the Internet of Vehicles. While ensuring the security of data flow transmission of the Internet of Vehicles, the efficiency of system security identification is improved, and a new mode is used to manage the Internet of Vehicles. Therefore, we propose a zero-trust-based data protection scheme for users in the Internet of Vehicles.

The zero-trust security architecture adheres to the principle of "never trust and always verify." Its access control is based on the core of identity. The subject of data transmission will be continuously authenticated. Then, the zero trust will rely on the trust evaluation model to conduct an intelligent behavior analysis of the entire access process of the visitor, which can timely respond to the security threats of the Internet of Vehicles system data and update the

vehicle nodes' trust value in real time. Finally, through the trusted access gateway, the control of the dynamic access authority of the asset equipment is realized. The zero trust will automatically resist eavesdropping attacks on the acquisition of private data in the communication channel and prevent malicious operations such as tampering attacks. Once a node is evaluated as a malicious node, it will no longer be able to access the database. At present, communication technology is adopted to realize the interconnection between vehicles, roads, and data processing platforms and perform cloud processing on data. In the blockchain network [2], the decentralized features of the blockchain can effectively prevent the excessive centralization of data in the cloud and reduce the risk of database attacks. After the data are stored in the block, the traceable feature of the blockchain data can trace historical records such as user's identity authentication and vehicle's device fingerprint. The timestamp in the block can resist replay attacks. After using the commercial cryptographies SM2, SM3, and SM4 to encrypt the data of the Internet of Vehicles, it is transmitted to the blockchain network [3, 4]. The identification of vehicles is realized by device fingerprint technology. The device fingerprint technology includes device fingerprint extraction and device fingerprint authentication. The equipment fingerprint extraction is to actively collect the characteristic information related to vehicles and generate a unique identifier for each vehicle according to the fingerprint generation algorithm. The device fingerprint authentication is an important part of the whole identity authentication process. When a vehicle accesses the cloud data, the cloud platform first calculates the device fingerprint of the vehicle and compares it with the existing fingerprint in the database to realize the identity authentication of the vehicle. Through the authentication center CA in the PKI system, the identity authentication and authorization of Internet of Vehicles users are carried out. The users can transmit on the alliance chain. This research will effectively protect the private information of Internet of Vehicles users [5].

In combination with the convolutional neural network, the vehicle and user identities are collected to extract behavioral features, and then the feature values are fuzzily calculated according to different weights to obtain the trust value. Finally, the user's trust is inputted into the model to achieve the prediction of trust level and improve the accuracy of trust level evaluation.

The rest of this study is organized as follows: in Section 2, we mainly introduce the research status of data security of the Internet of Vehicles at home and abroad. In Section 3, we mainly introduce the overall architecture and process of data protection scheme for Internet of Vehicles based on zero trust. In Section 4, we mainly introduce the simulation experiment of this scheme. In Section 5, we do a safety analysis. In Section 6, we mainly summarize the article.

2. Background

Zhang et al. [6] proposed a reliable and efficient system based on edge computing and blockchain, which is designed to ensure the reliability of edge devices during interactions and improve transmission efficiency. Mostafa et al. [7] proposed a layered adjustable autonomy (LAA) as a dynamically adjustable autonomy model for a multiagent system. Poongodi et al. [8] have proposed the improved versions of blockchain technology to strengthen various real-time complex applications at a flourishing rate. The results of the simulation kernel show that the proposed architecture justifies all the essential characteristics and effectuates the optimal use of 5G network sharing by each network entity. Kumar et al. [9] proposed an optimized location-aided routing protocol that is the modified version of location-aided routing protocol. Xiong et al. [10] proposed an efficient and large-scale batch verification scheme with group testing technology based on ECDSA, which analyzes the application of the presented protocols in Bitcoin and Hyperledger Fabric. Wang et al. [11] proposed PERT, a privacy-enhanced retrieval technology for cloud-assisted IoT, which preserves data privacy by hiding the information of data transmission between the cloud and the edge servers. Mostafa et al. [12] conducted tests on the AFC agent, and the results show that the agent successfully controls the UAV in three performed test cases and a total of nine implemented missions. Zhang et al. [13] proposed a covert communication model combined with smart contracts to covertly transfer information in the blockchain environment, using encryption algorithms and two-round protocols to ensure data privacy. Wang et al. [14] proposed a new certificateless scheme, which utilizes the most advanced blockchain technology and smart contracts to build a reliable and efficient CLS scheme. Lian et al. [15] proposed a new joint learning system, COFEL, which can reduce communication time through layer-based parameter selection and enhance privacy protection by using a local differential privacy mechanism for selected parameters. Zhang et al. [16] proposed a secure and efficient data storage and sharing scheme based on blockchain-based mobile-edge computing. IoT devices only need to submit the data and random key share allocated to edge nodes, and edge nodes use the recovered signature private key to realize data signature and homomorphic encryption. Song et al. [17] proposed a security arrangement method based on matrix eigenvalue calculation. Compared with existing security arrangement methods, this method has stronger robustness and efficiency, making the scheme more suitable for repeated polymerization. Balamurugan et al. [18] proposed a subspace tracking algorithm with low computational complexity for tracking DOA to provide a seamless connection. Compared with traditional DOA estimation methods, the proposed DOA tracking method takes less time to track the current position of UAV target, and the tracking process is not affected by a signal-to-noise ratio.

Wang [19] put forward a nondual pair authentication scheme for Internet of Vehicles messages based on elliptic curve cryptography. This scheme adopts random pseudonyms to achieve conditional privacy protection. Xie et al. [20] came up with an improved secure certificateless aggregation authentication scheme based on elliptic cryptographic curves. Li et al. [21] proposed a password-based serverless cross-domain vehicle-to-vehicle authentication

and key agreement protocol. Xin et al. [22] proposed an event-driven lightweight algorithm to quickly identify the false position of vehicles and detect the erroneous behavior claiming the false position. Shi and Wang [23] put forward a resist conspiracy Sybil attack detection method based on spatiotemporal analysis based resist conspiracy Sybil (STARCS) attack. Si [24] proposed a lightweight authentication scheme suitable for vehicle-mounted self-organizing networks. The trusted authority (TA) obtains the identification information of the onboard unit (OBU) through calculation, which can significantly improve the randomness of the signature of the message and avoid the counterfeit attack, hence improving the security of the solution. Zhang [25] proposed a 5G vehicular network authentication scheme based on a reputation system. A one-way hash function is adopted to generate the credit references to restrict the vehicles whose reputation score is below the threshold from participating in the authentication process. Zhang [26] constructed the vehicular cloud computing structure formed by the collaboration among vehicles and designed a security authentication mechanism that can achieve a privacy protection based on an identity-based signcryption scheme and a short-group signature scheme. Chen et al. [27] proposed an E-forensics framework of Internet of Vehicles based on the blockchain technology. It implements a remote repository of E-forensics by using the features of decentralized storage for blockchain technology. Ma [28] proposed a trust management model based on the blockchain to realize the reliability and synchronization of existing reputation data. In trust calculation, the RSU relies on a weighted voting mechanism to evaluate the credibility of the message. Xu [29] studied the vehicle attribute recognition technology in surveillance video and bayonet image, mainly studied the fine-grained vehicle type recognition and body color recognition using the convolution neural network technology framework, and developed the vehicle attribute recognition prototype system on this basis.

3. Scheme

3.1. Architecture. We mainly describe the capacities of overall architecture in the zero-trust philosophy, including the following capabilities: zero-trust drive authentication mechanism, identity security infrastructure, and trusted access gateway. The authentication mechanism of zero trust is the core capability of the entire program architecture. The identity security infrastructure implements trusted access by establishing trusted basic permissions between trusted access subjects and trusted access objects. The trusted access gateway supports single sign-on (SSO) to avoid frequent authentication and improve ease of use. First, based on the user's access behavior to the device and the access environment of the device and then relying on the continuous trust evaluation model and the access control model, the intelligent behavior analysis of the entire access process of the visitor is carried out. Then, the risk coefficient of the visitor is intelligently adjusted, and then a continuous trust assessment of the credibility of users and asset equipment is achieved. The following step is to dynamically adjust access control strategies based on the evaluation results. Finally, the dynamic access authority control of the mobile subject is realized through the trusted access gateway, as shown in Figure 2.

There are varieties of mobile subjects in the Internet of Vehicles, including equipment hardware parameters, network environment, intelligent systems, sensors, signals, user information, etc. We can regard these access subjects as the attribute set of the application. Based on the device information of multidimensional mobile subjects, such as device hardware parameters, network environment, intelligent systems, sensors, and signals, a unique device identifier called device fingerprint is generated through a model algorithm. The device fingerprint is stable and does not change even when the device system is upgraded or parameters are changed. In addition, device fingerprints cannot be tampered and can identify the risks of terminal environment. Generation rules of the device fingerprint are placed in the cloud platform. During the registration process of the device management, the device fingerprint is automatically generated according to the device parameters and then it will be stored in the device fingerprint library, as shown in Figure 3. In the process of device login authentication, based on the collected multidimensional device information, the model algorithm of the cloud platform analyzes the collected data and calculates the device fingerprint, matching it with the device fingerprint library to achieve enhanced authentication.

Through continuous active scanning, passive detection, and secure access to the control area, continuous trust evaluation and access control are carried out on the vehicle IoT terminal to solve the counterfeiting and malicious access. High-confidence equipment adopts a trusted chip + - trusted OS56 to directly identify the identity. Embedded devices adopt device tags, such as mobile device identification code, application developer identifier, unique device identification code, RFID6 electronic tags, and cryptographic modules attached to the outside of the device, all of which can help establish device identity. For low-intelligence IoT devices, digital fingerprints can also be used to construct device identification to solve the problem involved in device access identity management. Having an established fingerprint database improves the accuracy of zero-trust architecture devices. Since each user has only one unique identity fingerprint, when it is employed, any changes to the identity fingerprint will be dynamically detected by the trust engine, which leads to the engine's restricting permissions of the related user.

Under the zero-trust framework, during the communication between the car and the cloud, commercial cryptography ensures the security of the system. The two-way identity authentication between the car and the cloud realizes the anti-interception, anticounterfeiting, and antireuse of the authentication information, ensuring the authenticity of the users and the vehicle management cloud platform. In terms of security transmission requirements, the system must ensure the confidentiality and integrity of the communication process. The vehicle can realize the communication function with the cloud server through the vehicle

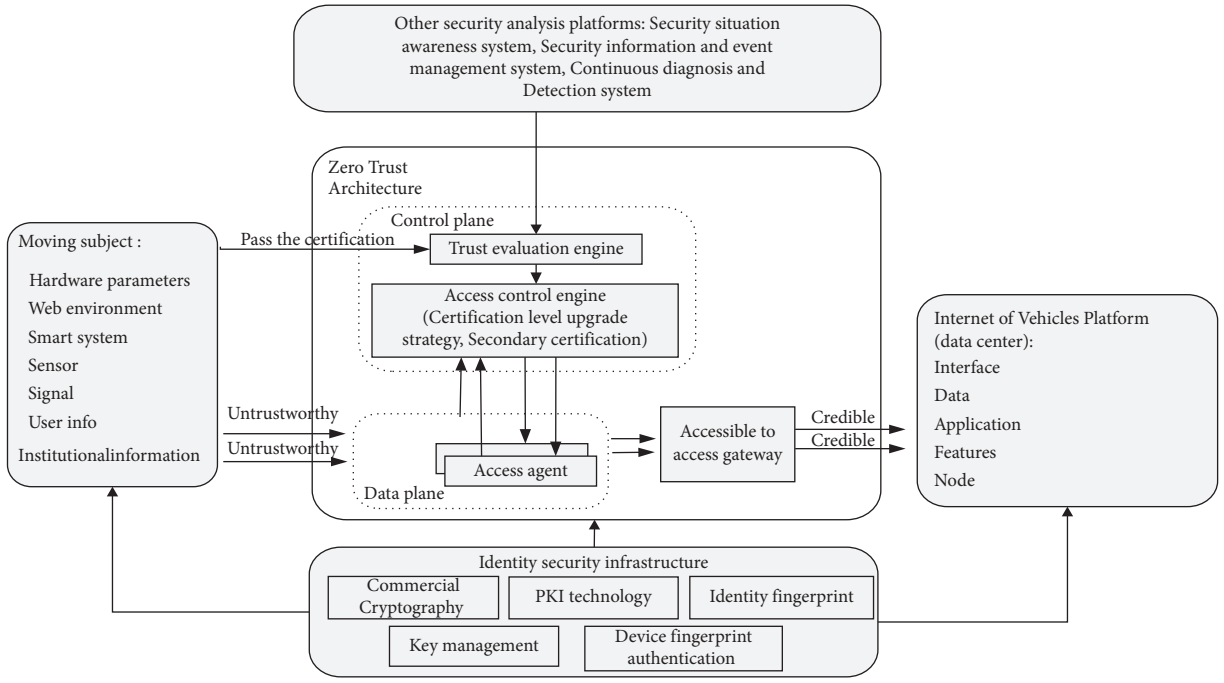

Figure 2: Structure of zero-trust-based data protection system for the Internet of Vehicles.

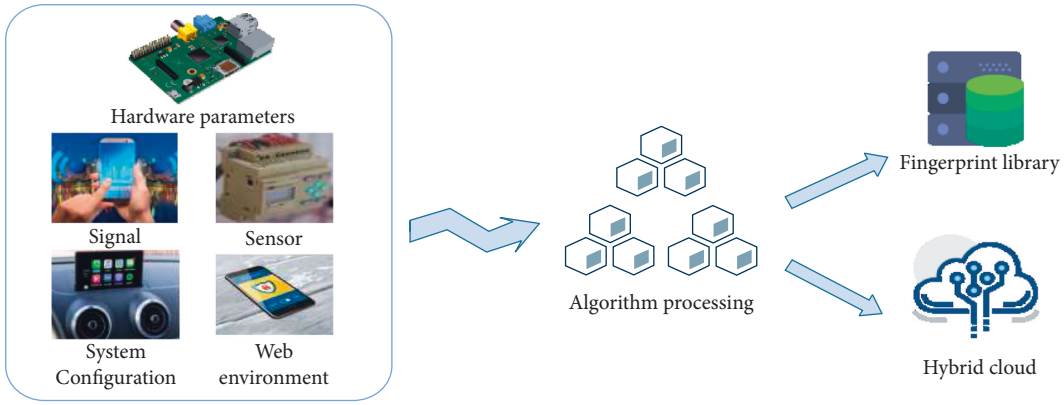

Figure 3: Verification process of device fingerprint library.

terminals and the Bluetooth communication modules. The vehicle realizes various security functions by configuring the cryptographic module. Through the encryption and verification of SM2, SM3, and SM4 commercial cryptography, the information security of user registration will be improved, and the transmission of vehicle data will be difficult to be tampered with and disclosed.

In the cloud server, the server cryptography machine performs authentication operations using the public key stored in it. In the Internet of Vehicles system, an SM2 key protocol algorithm is adopted to negotiate a session key, and secure transmission of sensitive data between the cloud server and the vehicle is completed. In the Internet of Vehicles system, the cloud server employs the server cipher machine that adopts SM4 and HMAC-SM3 algorithms to protect the confidentiality and integrity of user data and authentication data. At the same time, the vehicle calls cryptography modules that apply SM4 and HMAC-SM3 algorithms to protect the confidentiality and integrity of key data such as identification data, vehicle collection, and control data.

In the Internet of Vehicles system, the PKI is widely applied and plays different roles among different objects. In the Internet of Vehicles system, the application and related data security of the Internet of Vehicles include a four-layer key system: CA public keys, the cloud server key pair, the car Bluetooth communication module key pair, and the Bluetooth communication key, all of which are all key components of the PKI in the identity security infrastructure. PKI can guarantee the authenticity, integrity, confidentiality, and nonrepudiation of the identities of both parties. The source of trust of the asymmetric key system is the CA certificate,

which is used to verify the cloud server certificate and the car Bluetooth communication module certificate. In the zero-trust framework, the signature key of the cloud server key pair is used to authenticate the identity of the cloud server and the encryption key is used to realize the secure transmission of data between the server and the car. The public key is issued by the CA to form a cloud server certificate. The private key is stored in the cipher machine of the cloud server. The public key is issued by the CA to form the car Bluetooth communication module certificate, while the private key is stored in the car Bluetooth cryptographic module.

In the Internet of Vehicles system, the zero-trust framework can ensure the safety of the whole system. It contains two parts: the control plane and the data plane. In the control plane, the trust evaluation engine and access control engine are connected to form effective contact and communication with each module. On the one hand, the trust evaluation engine receives node devices, people, applications, systems, and directly connected devices. On the other hand, it maintains contact with the data center, including Internet of Vehicles cloud systems. At the same time, the trust evaluation engine can share data with other security analysis platforms and also transmit information with the access control engine. The access agent is the key node of zero-trust architecture for authentication, can efficiently and effectively verify the information received by the zero-trust system each time, and ensure the security of the entire Internet of Vehicles system.

The data center of the Internet of Vehicles platform will be built on the blockchain network and will be deployed in the cloud server. The center will include a user interface, data visualization processing, application services, and basic user functions. The whole system takes the vehicle equipment in the connected car environment and users' system as blockchain network nodes, to build a decentralized chain alliance. It decides to charge to an account through consultation and achieve consistency by the consensus mechanism. Therefore, members of the nodes will achieve data exchange in the case of not fully trusting. Members can enter or exit the league chain only through the authorization of these organizations. Important data such as the node's public key information, the node's historical communication behavior data, and smart contract-based access control strategy are stored in the blockchain, and all blockchain nodes jointly maintain the communication security among the nodes of the Internet of Vehicles. However, the nodes of the Internet of Vehicles usually have limited computing and storage resources. Therefore, the vehicle node is regarded as a lightweight node of the blockchain, which only stores the block header of the blockchain but does not participate in "mining." To improve the speed of the blockchain network, the communication behavior data of the vehicle nodes are collected by its adjacent RSVs, while the collection process is performed by predefined smart contracts. Round-side units are authorized as full nodes of the blockchain to generate and validate new blocks, while vehicle-borne units, as lightweight nodes of the blockchain, do not participate in the "mining" process of the blockchain, thus causing no additional overhead to the vehicle nodes.

In the process of evaluating vehicle trust levels, we introduce a trust level classification model based on the convolution neural network algorithm. The preset convolution neural network is used to train the data of vehicle nodes and complete the trust level classification of vehicle nodes. A CNN model has four typical characteristics: local connection, weight sharing, pooling operation, and multilayer structure. The CNN can automatically learn features from data through multilayer nonlinear transformation, to replace manually designed features, and its deep structure makes it have strong expression and learning ability. The CNN has a special structure of weight sharing, and its layout is closer to the actual biological neural network, which reduces the complexity of the network. In particular, the image of a multidimensional input vector can be directly input into the network, which avoids the complexity of data reconstruction in the process of feature extraction and classification. As an input-output mapping, the CNN can learn a large number of mapping relationships between input and output. Without the precise mathematical expression between input and output, the convolutional neural network can have the ability of mapping between input and output pairs by using the known pattern to train the convolutional neural network. Combined with the CNN model, the efficiency of the algorithm in the cluster environment has been greatly improved. It can efficiently process the experimental data and complete the effective classification of the trust value of vehicle nodes.

3.2. Work Flow. During the process of trust evaluation in the equipment of the vehicle network, we should not only authenticate the static attributes of the device, such as its attribute, ID, and network environment, but also evaluate the dynamic attributes of the device, such as its real-time request, dynamic operation, and evaluation success rate. In particular, it is very important to calculate and update the trust value of the dynamic attributes of each node. In the zero-trust network architecture, the initial trust value of the device is 0, so we need to collect and authenticate the static attributes of the device. First of all, we will collect the identity fingerprints of users of the Internet of Vehicles and store the fingerprints in the cloud server to verify and authenticate the identity of users of the Internet of Vehicles by using the identity fingerprint database. At the same time, the digital certificate issued by a Certification Authority (CA) of public key infrastructure (PKI) technology is used for verification, together with identity fingerprint database authentication as a way to achieve the dual authentication. Therefore, the credibility and security of the device can be improved. Figure 4 shows the overall process.

3.2.1. Identity Registration. When the device on the vehicle needs to communicate with the edge device, it must first apply for registration with a trusted vehicle management center. The specific registration process is as follows:

First, the vehicle management center chooses N random numbers $C_1, C_2, \ldots, C_N$, to form the challenge set $C = \{C_1, C_2, \ldots, C_N\}$, and then sends C to the onboard equipment.

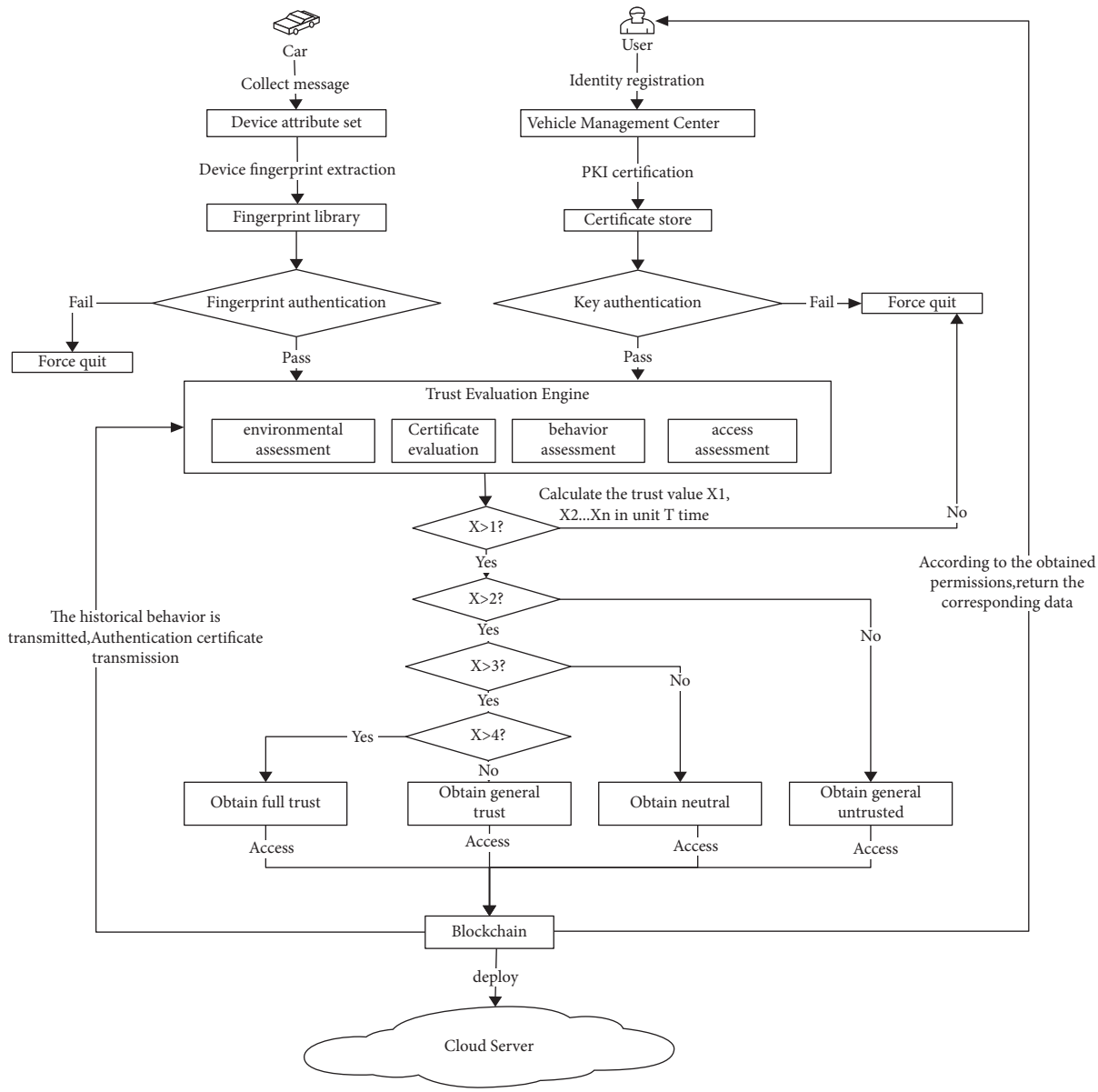

Figure 4: The work flow.

Second, after receiving C, the onboard device calculates the PUF function $R_i = \mathrm{PUF}_{\mathrm{Vi}}(C_i)$, obtains $R = \{R_1, R_2, \ldots, R_n\}$, and sends R to the vehicle management center through the secure channel.

Third, the train federation management center generates a pseudonym $\mathrm{AID_i}$ for the received R and obtains $\mathrm{AID} = \{\mathrm{AID}_1, \mathrm{AID}_2, \ldots, \mathrm{AID}_N\}$. The $\{\mathrm{ID_{Vi}}, \mathrm{AID}, R\}$ is stored in a secure storage area, and then the {AID, R} is sent to the blockchain network. Then, the unused list is written by the PoS consensus algorithm, and the AID is finally sent to the vehicle device.

After the onboard device receives the AID, it will be stored in the safe storage area with the corresponding C.

The advantage of this management mode is that it can guarantee effective communication between vehicles and edge nodes, improve the information processing ability of the whole system, and improve the efficiency of information communication. Identity registration plays a key role in system information processing. Identity identification is the basis of subsequent identity authentication to ensure an efficient and orderly information system.

3.2.2. Device Fingerprint Extraction. For common Internet of Vehicles devices, fingerprint information is particularly important for identity confirmation. The device fingerprint ensures the accuracy and efficiency of the whole data transmission process, avoids the tedious verification process of messages in the information transmission, and ensures the stable operation of the whole system. When the data of the device are transmitted remotely, the unique fingerprint information of the device is used as favorable evidence of its authentication. Device fingerprint extraction provides the basis for subsequent device fingerprint identification, which is the first step of system identity operation.

We adopt an active device fingerprint technology to obtain the fingerprint of vehicle equipment. The vehicle equipment hardware, network environment, sensors, signals, system control, and other parameters are obtained by calling the SDK interface, then the equipment fingerprint is generated by using the hash algorithm, and the equipment fingerprint database is built based on certain principles. Without relying on the sensitive authority of the device, two types of identifiers for generating device fingerprints can be collected through the browser platform of device access management. For different IoT devices, the fingerprint parameters can be obtained through the development documents provided by the device manufacturer.

The process of collecting and generating the parameter information of the device fingerprint by calling the SDK interface fully meets the following two requirements, so that the whole process of collecting the device message is transparent and visible and does not interfere with the normal use of the devices:

(i) *Fast Response*. By default, the SDK has a timeout of 3 seconds for establishing a connection. It has a fast response speed and will not fail to obtain fingerprint information because the device access time is too short.

(ii) *Less Resource Consumption*. Calling the SDK interface to extract device information will not occupy too much bandwidth, memory, CPU, and other resources and will not have any impact on the normal operation of the device.

3.2.3. Identity Authentication

(1) PKI Certification. Confirm the identity through PKI's CA certificate management center. In the Internet of Vehicles, users use their identity information to generate digital signatures, which together form CA. In addition to user information, a digital signature includes the name of the certificate authority, certificate validity period, certificate serial number, the hash algorithm used for the signature, and encryption algorithm used for the public key. We can view the certificate validity period to determine the validity of the CA. The vehicle sends its own information to the relevant user, and the user uses the CA's public key to verify the signature of the certificate. As the CA is the only issuer of the certificate, the user can verify the authenticity of the certificate in this way, and the user can use the public key to verify the signature of the vehicle or carry out encrypted communication with the vehicle. At the same time, to prevent the authenticity of the public key used by the user when verifying the CA certificate of the vehicle, we can find another certificate authority to issue a certificate to the public key of the certificate authority. In this way, a nested loop of public key certificate is formed, and the end of the loop is the Root Certificate Authority. The public key certificate nesting cycle can ensure the authenticity of the public key in the communication between the vehicle and the user in the Internet of Vehicles and ensure the overall security of information. It can be concluded that PKI plays a very important role in the whole process. The circular nesting of certificates ensures the security of public keys used in data encryption and improves the efficiency of system authentication. Compared with the traditional vehicle network system, this system has certain advantages in encryption authentication.

(2) Authentication of Device Fingerprint. Equipment fingerprint authentication is a very important identity authentication technology in the Internet of Vehicles system. In the authentication process, the client sends an access request to collect terminal features, and the ECS loads the feature collection code for collection. The server will locate the specific device recorded in the system according to the MAC address, verifying the active fingerprint of the device and judging whether it is a new device. If it is a new device, the new fingerprint will be stored in the device fingerprint database. If the authentication is passed, it means that the current equipment has passed the authentication and can continue to communicate with the system. Otherwise, the system will actively disconnect.

3.2.4. Trust Evaluation.

We built three vehicles in the system and carried out experiments independently. The experiment carried out by the two vehicles is applied as a control experiment and the accuracy of the trust evaluation is verified through multiple experiments. We will describe the process of trust evaluation between the vehicle and the car cloud system by the following steps:

(1) Pass Rate of Client Authentication. First, apply PKI's CA certificate for client authentication as the initial authentication method. Issue the certificate to the authenticated client through the CA certificate management center of PKI. The client authentication process is shown in Figure 5. The client authentication module judges whether the machine logs in locally, whether the access address is abnormal, whether the account password is changed, whether the protocol is changed, etc., to determine whether the client authentication of the vehicle management center is successful. Assign different initial trust values to vehicles that have passed different authentication factors.

(2) Pass Rate of Fingerprint Authentication. As shown in Figure 6 we obtain the fingerprint features of the vehicle equipment including hardware parameters, network environment, intelligent systems, sensors, signals, and other information by calling the SDK interface and then use the algorithm to generate the device fingerprint and build the device fingerprint library based on certain rules. The newly generated device fingerprint is identified in the fingerprint database. We mainly extracted some basic parameters of terminal equipment. If the fingerprint is associated successfully, the device passes the fingerprint identification process. According to the difference in fingerprints of each vehicle, different trust values will be obtained. The trust value obtained by the fingerprint authentication of the three vehicles will be used as in the follow-up trust evaluation.

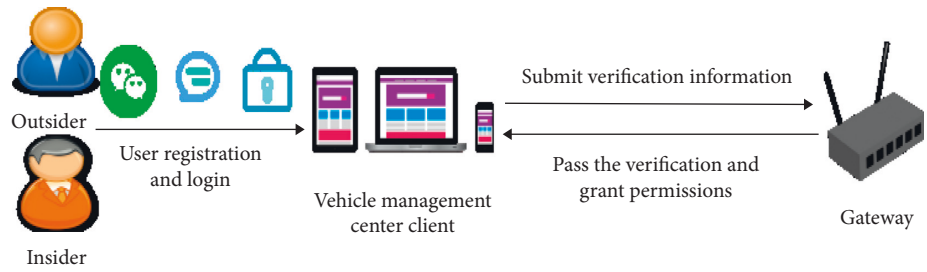

Figure 5: Client authentication.

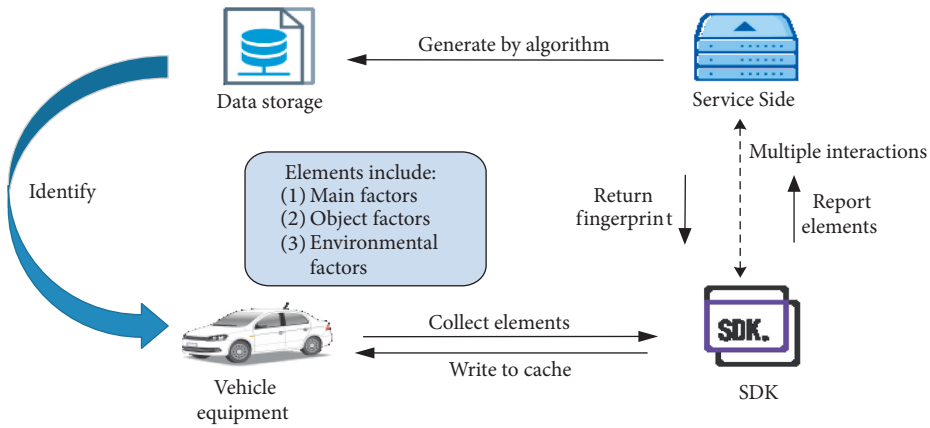

Figure 6: Device fingerprint extraction.

(3) API Certification Pass Rate. The use of API gateway can reduce the attack surface and concentrate resource advantages. The API gateway is based on a defense-in-depth strategy and has the function of authentication. Even if the attacker breaks the API gateway, it still needs to further break the internal service authentication to enter a single service. Next, the microisolation test of the system will be carried out on the three vehicles to verify the proxy and hiding conditions applied by different modules of the system after the installation of the access gateway plug-in, as shown in Figure 7. In the specific test of the system, the API gateway of vehicle deployment is verified, the specific steps of the implementation phase are evaluated, and the verification and call success rate are taken as key evaluation values. Three vehicles are verified by experiment in parallel. Due to the different situations of vehicle API verification and call, three vehicles will produce different trust values, which will be used as the basis for subsequent trust evaluation.

(4) SPA Packet Transmission Acceptance Rate of SDP Architecture. After completed the microisolation test, the next step is to validate the SPA single-pack authorization for the three vehicles. The client carries the encrypted SPA packet and sends an access request to the gateway. The gateway decrypts the packet using the key provided by the controller and cross-checks the information in the decrypted packet with the information it receives from the controller to determine whether the client can access the packet, as shown in Figure 8. After the vehicles have completed the SPA single package authorization, the trust evaluation is conducted based on whether the SPA package is sent successfully and whether the certificate verification is passed.

When the device ed_i conducts identity authentication, it needs to conduct identity authentication at the edge computing layer.

By sending authentication requests to node es_1 of the edge computing layer, the corresponding key is obtained from PKG and applied to the key communication of the session. The request sent by the device contains the identity of the device and the node of the edge layer. The SM2 signature algorithm is used to calculate the corresponding digital signature (h, s) by using the private key of the device.

$$ed_i \longrightarrow es_1: \text{AccessReq} \,\|\, N_1 \|\, ed_i \|\, es_1 \|\, h \|\, S. \tag{1}$$

AccessReq is the authentication request when the device accesses, and N_1 is a random number.

After receiving the authentication request of the terminal device, the edge computing layer uses the SM2 signature algorithm to sign and authenticate it. After verification, the edge computing layer node saves the identity information of the terminal device to the authentication list and gives feedback of the encrypted authentication information to the terminal device node. First of all, the value of the Q_D element in group G_1 is calculated according to formula (2), and the Cipher values in group G_1 are calculated according to the generated random number r. Ciphers are the ciphertext and $r \in [1, N-1]$, the encapsulated key Key is calculated by KDF according to formula (3), and the key value is the shared key of the edge layer and the terminal device:

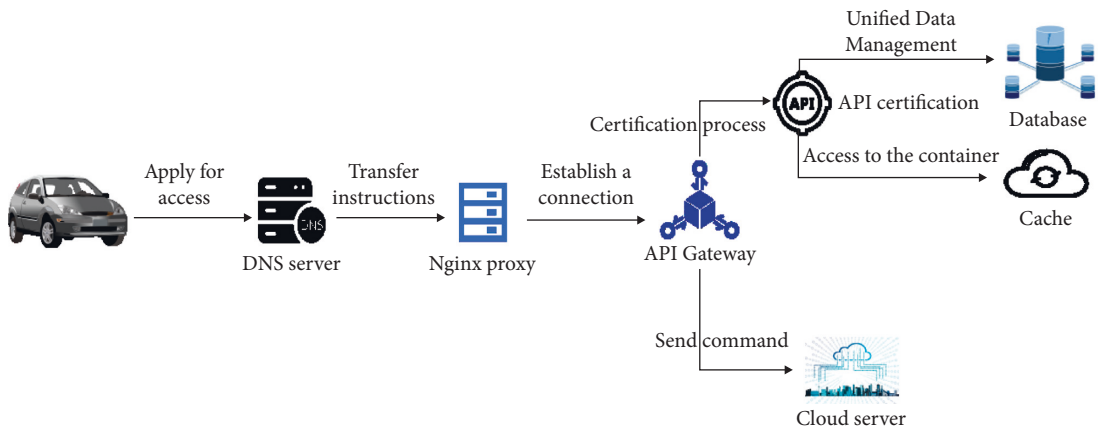

Figure 7: API gateway authentication.

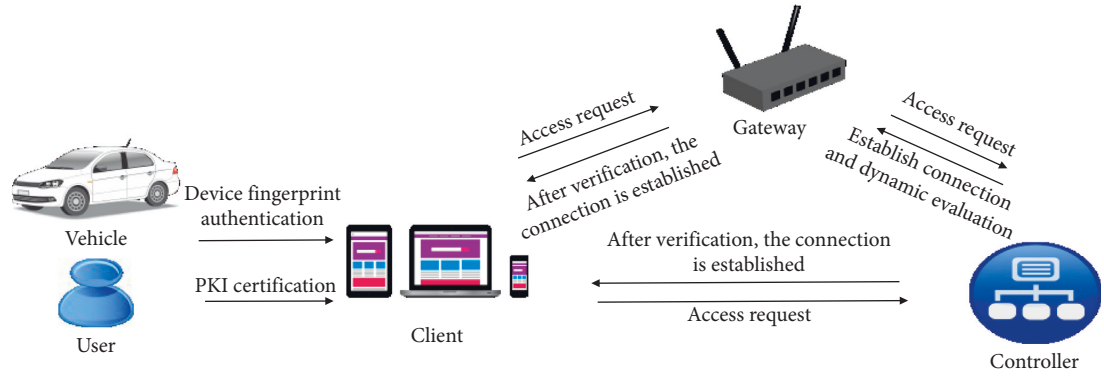

Figure 8: Single-packet authorization process.

$$\begin{aligned} \mathrm{QD} &= [H_1(\mathrm{ed}_i \| \mathrm{hid}, N)]P_1 + P_{\mathrm{pub}-e}, \\ \mathrm{Key} &= \mathrm{KDF}\left(\mathrm{Cipher} \left\| \left(P_{\mathrm{pub}-e}, P2\right) \right\| D, \mathrm{Klen}\right), \\ \mathrm{es}_1 &\longrightarrow \mathrm{ed}_i\colon \mathrm{AccessRsp} \| \mathrm{es}_1 \| \mathrm{Cipher} \| h \| S, \end{aligned} \tag{2}$$

where klen is the key length and AccessRSP requests response identification.

After receiving the response package of the edge layer node, the edge terminal device parses the received Cipher to obtain the corresponding key Key. First, it needs to determine whether the Cipher belongs to the element in G_1. If not, the input is 0; otherwise, w' in G_T is calculated according to formula (5). Then, SM2 converts the data into a bitstream to calculate the Key of the response:

$$\begin{aligned} w &= e\left(\mathrm{Cipher}, d_{\mathrm{ed}_1}\right), \\ \mathrm{Key} &= \mathrm{KDF}\left(\mathrm{Cipher} \| w' \| \mathrm{ed}_i, \mathrm{klen}\right), \\ \mathrm{ed}_i &\longrightarrow \mathrm{es}_1\colon \mathrm{AccessAck} \| \mathrm{key}\left(\mathrm{ed}_i \| \mathrm{es}_1\right), \end{aligned} \tag{3}$$

where AccessAck confirms the response and d_{ed1} is the private key of the terminal.

In summary, if the obtained key is 0, the identity authentication fails; otherwise, the identity authentication of the device is successful, and the identity of the device is saved to the node of the computing layer.

After evaluating CA's certificate level and verifying device identity, with the traceable and tamper-free feature of the blockchain network, we record all identity fingerprints, digital certificates, and verification information and save them in the block. By using a smart contract, automatic verification can be realized when the next device is accessed. However, if the node's trust value falls below the threshold or is deemed to be a malicious node, the smart contract will remove the digital certificate of the Internet of Vehicles users from the list. At the same time, the zero-trust system will also conduct historical behavior evaluations. The zero-trust trust evaluation engine will continuously collect the behavior characteristics of the vehicle and judge whether the vehicle node is a malicious node in combination with the historical behavior. It is an important factor in the evaluation of vehicle trust level. In this process, all noncompliance and malicious operations will be recorded in the blockchain network and will be used in the evaluation of the next cycle as a reference.

So far, we have completed some tasks of the engine in terms of trust evaluation in the zero-trust system. Next, we will proceed with the work of the access control engine. In the process of trust evaluation, since the degree of trust between vehicles is not a white and black exclusive relationship, it cannot be mechanically divided into trust and distrust. For example, the trust between vehicles can be described as "complete trust," "general trust," "neutrality," "general distrust," and "complete distrust." These trust

descriptions can be used as the evaluation set of fuzzy evaluation process $D = \{$complete trust, general trust, neutrality, general distrust, complete distrust$\}$. The cloud platform will set different access permissions according to the evaluation level of the vehicle. The higher the trust level of the node, the higher the permissions can be obtained.

The main factors that affect the evaluation are considered to determine the fuzzy evaluation process factor set $U = \{$client authentication pass rate, fingerprint authentication pass rate, API authentication success rate, SPA packet transmission-reception rate$\}$. At the same time, according to the importance of the evaluation index of each factor in the factor set, the weight is calculated by the Delphi method, and the weight distribution set $W = \{0.4, 0.2, 0.2, 0.2\}$ is obtained. The cloud server will access and operate the device according to the evaluation level. In the process of data transmission, we will use SM2 to encrypt data to further ensure the safety and integrity of data transmission. Suppose the threshold of different permissions is V_n, $5 > V_n \geq 0$, the access control engine divides the security levels of device into five levels: complete trust $(5 > X \geq 4)$, general trust $(4 > X \geq 3)$, neutrality$(3 > X \geq 2)$, general distrust $(2 > X \geq 1)$, and complete distrust $(1 > X \geq 0)$, as listed in Table 1.

The zero-trust architecture will conduct a real-time evaluation of vehicle nodes, combined with the above four passing rates and the historical behavior of vehicles, and calculate the trust value X in the process of operation. The fuzzy mapping of several attributes of vehicle trust evaluation on the evaluation set is carried out to obtain the comprehensive evaluation matrix R. The proportion of each weight factor in each evaluation is obtained by calculating the vector $T = W * R$. Finally, the trust value X is calculated. The calculation formula is as follows:

$$X = T \times \begin{pmatrix} \frac{V0 + V1}{2} \\ \frac{V1 + V2}{2} \\ \frac{V2 + V3}{2} \\ \frac{V3 + V4}{2} \\ \frac{V4 + V5}{2} \end{pmatrix}. \tag{4}$$

Within a monitoring cycle T, we will continuously evaluate the operating performance of the vehicle terminal, which is evaluated for n times in total, and obtain a series of trust values $X_1, X_2, \ldots, X_n$.

Assuming that the initial user's trust value is X_0, $X_0 > V_n$, the vehicle terminal obtains the corresponding access and operation permissions; otherwise, the operation is blocked.

Calculate the variance $\sigma(X)^2$ of the trust value of each step within m cycles and take the mean value of the variance $\sigma(X)^2$. If $\overline{\sigma}^2 > \sigma(X)^2$, the user's access level will be lowered. At this time, the user trust value is changed from X_m to the low-level permission until it is reduced to 0, and the user is forbidden to access.

If $\overline{\sigma}^2 < \sigma(X)^2$, the user's access level will be increased, and the user's X_m trust value will change to a higher level of authority. The longer the operation cycle is, the more obvious the change of the trust value will be.

In the evaluation process of the convolutional neural network, the two classification authentication model is established to analyze the authentication results of users and vehicles. The results listed in Table 2 usually appear in the identification.

TP indicates the number of samples, in which all positive samples are classified correctly in the result. TN indicates the number of samples, in which all negative samples are classified correctly in the result. FN represents the number of samples, in which all positive samples are classified incorrectly in the result. FP indicates the number of samples, in which all negative samples are classified incorrectly in the result.

We used three indicators to assist in the analysis: precision, recall, and F1 score. We hope to obtain the comprehensive performance of the classifier in all categories. Therefore, it mainly focuses on the microaveraging F1 value as the measurement standard; that is, it calculates TP, FP, and FN for each group in the category set and completes the cumulative calculation of P, R, and F1. Their calculation formula is as follows:

$$\begin{aligned} \text{Precision} &= \frac{\text{TP}}{(\text{TP} + \text{FP})}, \\ \text{Recall} &= \frac{\text{TP}}{(\text{TP} + \text{FN})}, \\ F_1 &= \frac{2 \times \text{precision} \times \text{racall}}{\text{precision} + \text{recall}}. \end{aligned} \tag{5}$$

Under different thresholds, the accuracy rate and recall rate are often negatively correlated. In order to balance the overall evaluation effect of the two, the F1 score is calculated as the harmonic average of the two.

In the evaluation, we first need to find the weight convergence point of the CNN and then calculate the trust value of vehicle nodes with different trust levels. With the learning function of CNN, the weight convergence point is taken as an evaluation point. Once the network trust value to be classified is inputted at the input end, the weight coefficient in the network will be determined and finally reach the stable state after a process from initial to steady-state convergence. The trust level of vehicle nodes is the corresponding classification level. The specific CNN evaluation algorithm is as follows:

The trust value of the vehicle node to be rated is taken as the input value, and the predicted trust level of the vehicle node is taken as the output value. The CNN model will obtain the trust value of the sample vehicle node in the Internet of Vehicles.

Table 1: Vehicle rating level and authority.

Level	Estimation scale	Authorization
1	Complete trust	Vehicles and users can access, edit all data, and modify cloud facilities
2	General trust	Vehicles and users can access and edit all data
3	Neutrality	Vehicles and users can access all data
4	General distrust	Vehicles and users can access some data
5	Complete distrust	Refuse to provide service

Table 2: Classification results of binary classification model.

	Postive forecast	Negative forecast
True positives	TP (true positives)	FN (false negatives)
True negatives	FP (false positives)	TN (true negatives)

First, the model finds the convergence point through the given sample of node trust level. According to the set trust value rating rules, it matches the trust value levels of vehicle nodes treated separately and classified. Then, it creates a convolutional neural network (CNN) and sets the initial state value of the neural network. It takes the trust value of each node to be rated as the input value of CNN. Finally, the CNN obtains evaluation points through self-study convergence and predicts the obtained trust level of vehicle nodes.

4. Test

4.1. Experiment Environment. The computer platforms used for this test platform are Intel I7-8750H, 2.20 GHz CPU, 16 GB memory, 1 TB external memory, Ubuntu 20.04 operating system, and MySQL 8.0.22 database system. The blockchain system adopts hyperledger fabric architecture, the operating system is Ubuntu 20.04, the memory size is 8 GB, the development language is Java, and the blockchain type is federation chain. The vehicle model of the Internet of Vehicles system is BYD Tang 2021 automatic flagship model, the intelligent vehicle network system in the vehicle is DiLink intelligent system, CPU is 8-core 2.0 GHz processor, memory is 3 GB, external memory is 32 GB, the power system is 2.0 T 141 kW L4, maximum power is 141 kW, and maximum torque is 320 N·m.

The parameter settings are as follows: The input matrix is 80 by n. The number of convolutional filters is 80 and the number of convolution filter windows is 4. We choose a sigmoid function as a convolution layer activation function and set up 3 sampling layers. Then, we used a gradient descent method for parameter optimization and repeated training for 100 iterations.

The experimental environment of this study is listed in Table 3.

4.2. Computation and Evaluation. Through the above four steps, we have implemented the main experimental steps of zero trust. We will take the above four steps, that is, client authentication pass rate, fingerprint authentication pass rate, success rate of API certification, and SPA packet transmission receiving rate, as the four factors for fuzzy algorithm sets. According to the main influencing factors of each step, the weight of each step is reviewed by experts. From Tables 4–7, we describe the data distribution tables of the four evaluation indicators at each grade after rating evaluation of 100 tests.

First, the single factor evaluation is carried out, and the evaluation r_i of each factor is obtained through statistical data. We establish the fuzzy relationship between each evaluation index U_i and trust level D_i. Based on the actual test results of the three vehicles, we have obtained three evaluation matrices and then combined them with the weight set to calculate the trust value in an evaluation cycle:

$$R_1 = \begin{pmatrix} 0.82 & 0.13 & 0.03 & 0.02 & 0.00 \\ 0.7 & 0.1 & 0.15 & 0.04 & 0.01 \\ 0.6 & 0.23 & 0.1 & 0.04 & 0.03 \\ 0.48 & 0.21 & 0.13 & 0.10 & 0.08 \end{pmatrix},$$

$$R_2 = \begin{pmatrix} 0.85 & 0.05 & 0.05 & 0.03 & 0.02 \\ 0.75 & 0.08 & 0.08 & 0.05 & 0.04 \\ 0.63 & 0.19 & 0.3 & 0.08 & 0.07 \\ 0.54 & 0.05 & 0.12 & 0.15 & 0.14 \end{pmatrix}, \quad (6)$$

$$R_3 = \begin{pmatrix} 0.82 & 0.11 & 0.05 & 0.02 & 0.00 \\ 0.73 & 0.12 & 0.08 & 0.05 & 0.02 \\ 0.58 & 0.15 & 0.12 & 0.09 & 0.06 \\ 0.52 & 0.17 & 0.08 & 0.13 & 0.1 \end{pmatrix}.$$

By multiplying the evaluation matrix R_i of the three cars with the weight vector $W = \{W_1(0.4), W_2(0.2), W_3(0.2), W_4(0.2)\}$, the fuzzy evaluation T_i can be obtained:

$$\text{Vehicle 1 } T_1 = (0.684 \quad 0.160 \quad 0.088 \quad 0.044 \quad 0.024), \quad (7)$$

$$\text{Vehicle 2 } T_2 = (0.724 \quad 0.084 \quad 0.066 \quad 0.068 \quad 0.058), \quad (8)$$

$$\text{Vehicle 3 } T_3 = (0.694 \quad 0.132 \quad 0.076 \quad 0.062 \quad 0.036). \quad (9)$$

Table 3: System configuration parameters.

Configuration items	Computer system	Configuration items	Blockchain system
CPU	Intel i7-8750H, 2.20 GHz	Name	Hyperledger fabric
MEM	16.00 GB	Operating system	Ubuntu 20.04 TLS
SSD	1 TB	MEM	8 GB
Operating system and version number	Ubuntu 20.04	Development language	Java
Database system and version number	Mysql 8.0.22	Types of chain	League chain

Table 4: Grade distribution of client authentication pass rate.

Vehicle	Complete trust	General trust	Neutrality	General distrust	Complete distrust
Vehicle 1	82	13	3	2	0
Vehicle 2	85	5	5	3	2
Vehicle 3	82	11	5	2	0

Table 5: Grade distribution of fingerprint certification pass rate.

Vehicle	Complete trust	General trust	Neutrality	General distrust	Complete distrust
Vehicle 1	70	10	6	4	0
Vehicle 2	75	8	8	4	4
Vehicle 3	73	12	8	5	2

Table 6: Grade distribution of API certification pass rate.

Vehicle	Complete trust	General trust	Neutrality	General distrust	Complete distrust
Vehicle 1	60	23	10	4	3
Vehicle 2	63	19	3	8	7
Vehicle 3	58	15	12	9	6

Table 7: Grade distribution of SPA packet delivery acceptance rate evaluation.

Vehicle	Complete trust	General trust	Neutrality	General distrust	Complete distrust
Vehicle 1	48	21	13	10	8
Vehicle 2	54	5	12	15	14
Vehicle 3	52	17	8	13	10

Finally, we will calculate the comprehensive evaluation matrix X.

$$X_1 = T_1 * R_1 = 3.936 \quad X_2 = T_2 * R_2 = 3.848 \quad X_3 = T_3 * R_3 = 3.886. \tag{10}$$

According to the scores, we can conclude that the scores of the three cars are between 3.5 and 4. According to the permission set, the three cars will obtain the general trust level, that is, the vehicle and the user can access and edit all the data. Through many experiments, we get the scores of the three cars, as shown in Figure 9.

In the first few cycles, as the number of tests increases, the trust value of the three vehicles also increases continuously. In the process of multiple visits, according to the dynamic engine detection, there is no malicious operation. Therefore, the trust value of vehicle 1 rises steadily, and the rise slows down gradually after reaching a relatively high level of trust. In terms of vehicle 2, when the initial access conforms to the access the specification, the trust value rises slowly. But after 3 times detection, due to the malicious operation, in the subsequent trust value tests, vehicle 2 keeps falling and the access right it has gained also lowers. If subsequent vehicle 2 does not change its behavior, it will eventually reduce to trust level 1 and the system will cease to serve it; when it comes to vehicle 3, to begin with, its trust value is rising and we can see at this time, there is

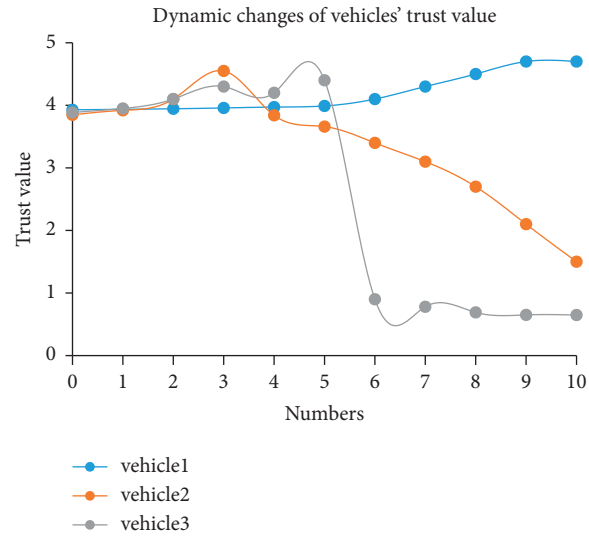

Figure 9: Dynamic changes of vehicles' trust value.

no malicious operation in the process of access. However, after 5 times detection, it is identified as malicious nodes. Thanks to its great harmfulness, it is detected by the dynamic detection engine immediately and has directly reduced to the trust level 1and refused to continue to provide service for the vehicle. Thus, this model can accurately describe the behavior of vehicles and quickly identify malicious nodes.

In the test of dynamic evaluation engine, trust values of three vehicles will be updated once every cycle, and the size of trust values will affect the access rights of vehicles. Client authentication and device fingerprint authentication will determine whether the users can register normally and enter the Internet of Vehicles system. API gateway authentication and single-packet authentication access will identify whether malicious operations will occur during the user's access. For normal users, their trust value will finally reach a higher score range. At this moment, they can access and edit all data. For malicious nodes, the trust value will change rapidly. For example, the vehicles are suddenly controlled to attack the systems, resulting in the loss of system files or a system crash. In this case, the nodes will be forcibly disabled from access.

Finally, we use relevant data sets to conduct experiments on the convolutional neural network (CNN) model. The experiment consists of two levels: the first level is the input feature dimension analysis to analyze the accuracy of the classification of the trust level of vehicle nodes and the second level is to compare the accuracy of the algorithm under different noise ratios.

Let X_i be the internal state of a neuron node constituting the neural network, Y_i be the trust level of the input vehicle, and W be the weight of the connection from X_i to Y_i. If B_i is the external input signal (in some states, the neuron node Z_i can be controlled to keep it in a certain state), then its formal description is as follows:

The input Y_i of the trust node can be expressed as the measured value of the behavior attributes, and the influence of each behavior attribute of the users' trust value can be expressed by the weight W.

In order to deal with vehicle features of different dimensions, we define the maximum vehicle dimension as 80, and the dimensions less than the maximum length are filled with zero vectors. A stochastic gradient descent algorithm is used for model parameters. The outputs of each convolution layer and full connection layer in the model are connected to the ReLU activation function. The outputs of the last full connection layer are classified by SoftMax, and dropout is used to prevent overfitting. Comparative experiments are conducted on data sets in different fields to verify the accuracy of trust level assessment of the test model on data sets. Before and after adding the trust level tendency dimension, the accuracy of user trust level classification was analyzed. The experimental results are shown in Figure 10. It can be seen that when more feature attributes are used to participate in the convolution calculation, the classification accuracy of trust level will be significantly improved. However, with the increase of attributes, the classification accuracy does not necessarily increase together. The improper selection of feature attributes will reduce the accuracy of classification.

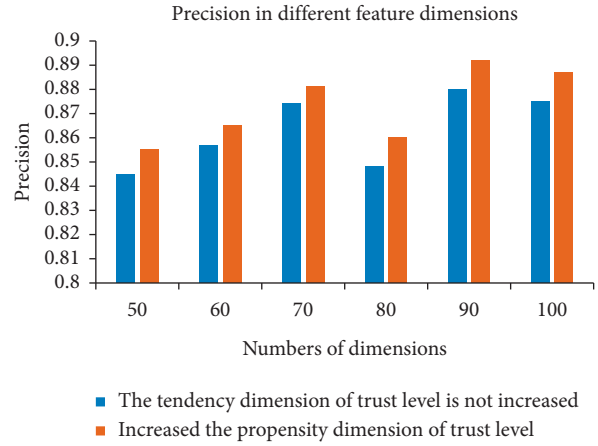

Figure 10: Precision in different feature dimensions.

Therefore, when we select the dimension of 80, the accuracy rate fluctuates to some extent. When the dimension of trust level tendency is added, the accuracy of the model calculation increases significantly compared with that without the dimension of trust level tendency, and the best effect of this experiment is achieved when the dimension is increased to 90. To solve the problem that the accuracy decreases when the dimension of feature attributes increases, we add noise value to trust classification to compare the performance of classification algorithms. As shown in Figure 11, the classified noise ratios of 20%, 30%, 40%, 50%, 60%, 70%, and 80% were respectively taken as four analysis environments. The results show that when the noise ratio is relatively small, the model has good accuracy, and when the noise ratio increases, the classification accuracy of the algorithm tends to decrease.

By using the CNN model proposed in this study, the predicted trust level by the CNN model is compared with the trust level obtained by zero-trust evaluation. We find that the result is basically consistent. We put the number of pass rates about client authentication, fingerprint identification authentication, API authentication, SPA packet acceptance, and other attributes of the vehicle into the CNN model. The corresponding trust level is obtained through self learning, which indicates that the model constructed in this study can extract key feature values and transform them into higher-level features through learning. The comparison results of trust level output are listed in Table 8.

Through the evaluation of the above CNN model, we find that the accuracy of CNN model is not only affected by the weights of different vehicle characteristics but also affected by the noise ratio. In order to improve the prediction accuracy of CNN model, the vehicle characteristic attributes should not be set too much. The horizontal dimension should be kept at 75, and the noise ratio should be set at 20%, so that the prediction accuracy can be higher.

5. Analysis

5.1. Security. After the CA certificate and identity fingerprint generated by PKI are authenticated, the data are stored in the blockchain through the consensus mechanism. The trust evaluation engine will evaluate the certificate level and

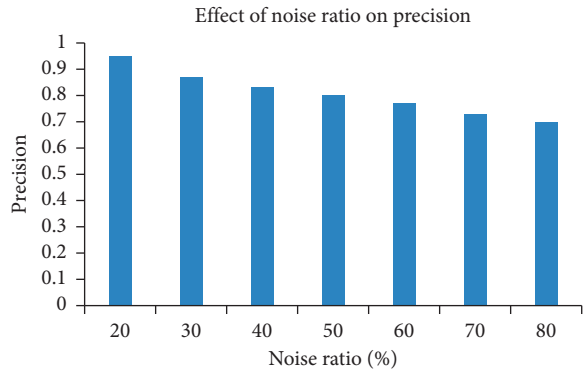

Figure 11: Effect of noise ratio on precision.

Table 8: The comparison results of trust level output.

Vehicle	Trust level output	Predicted output	Deviation rate (%)
Vehicle 1	3.936	3.91	0.66
Vehicle 2	3.848	3.81	0.99
Vehicle 3	3.886	3.85	0.93

historical behavior and convert them into relevant trust values. If the client wants to send data, it needs to be managed and verified through the API gateway. At this time, the client needs to be authorized by the controller to establish an MTLs connection and then requests the gateway to establish a connection. The gateway decrypts the data according to the key obtained from the control end. After the authentication succeeds, the client establishes a connection with the gateway to transmit data packets. The success rate of data transmission and the pass rate of certificate verification by the gateway and controller are converted into corresponding trust values for calculation. According to the size of the trust value, the trust level is determined and the corresponding service permissions are obtained. The access authority of the vehicle is modified by periodically updating the trust value to ensure the minimum access authority of the vehicle.

5.2. Confidentiality. In the Internet of Vehicles system, the session key is negotiated between the cloud server and the vehicle using the SM2 key negotiation algorithm to complete the secure transmission of sensitive data. In the Internet of Vehicles system, the ECS invokes the server cipher machine and uses SM4 and HMAC-SM3 algorithms to protect the confidentiality and integrity of user data and authentication data. At the same time, the vehicle calls the vehicle password module and uses SM4 and HMAC-SM3 algorithms to protect the confidentiality of key data such as identity authentication data, vehicle acquisition, and control data.

5.3. Attacks Defense

5.3.1. Switch Attack. In the process of evaluation of the Internet of Vehicles terminal nodes, if the attacker keeps performing well for a period to accumulate trust value, then it will reach a high trust level. Then, if it suddenly launches an attack, and then it will return to the state of good performance again. In this experiment, under the dual action of zero-trust historical trust record evaluation and incentive mechanism, the switch attack will be effectively suppressed. When the attacker carries out a switch attack, this malicious behavior will be recorded and uploaded to the blockchain network as a record of historical trust evaluation. Besides, users' trust will also decline rapidly. For those with malicious behaviors, if they want to increase their trust value again, then they will find that it grows at a very slow rate.

5.3.2. Novice Attack. Some attackers eliminate the historical interaction records badly and regain the trust of other Internet of Vehicles terminal nodes by registering new user identity information, thus launching attacks again in the network. Such attacks occur when malicious nodes can easily register as new vehicle terminal nodes. Aiming at the characteristics of novice attackers, we can use two-factor authentication, namely, fingerprint authentication for the vehicle and PKI authentication for the user to improve the difficulty of initial authentication. At the same time, the trust evaluation engine is used to render less trust value to the users who have passed the two-factor authentication. Only when they continue to perform trusted operations and other vehicle terminal nodes authenticate them with trust, the trust value can be gradually increased to become a trusted vehicle terminal node.

5.3.3. Replay Attack. Through the use of port knockout technology, the port for the communication of authentication information is closed, and the default discard firewall policy is dynamically reconfigured to allow access to services that would otherwise be blocked. Through this mechanism, remote users can be authenticated before granting access to services such as SSH daemon. On the SPA server system, fwknopd will sniff the replayed SPA packet and compare the SHA-256 summary of this packet with the SHA-256 summary of all previously seen and correctly decrypted SPA packets. If there is a match, fwknopd knows that a replay attack has been made. In this case, fwknopd generates a warning through syslog and does not grant access to the attacker to stop the replay attack.

5.3.4. Internal Attacks. In the Internet of Vehicles, there are also internal threats, which are more difficult to defend against than the external attacks mentioned above. The internal threats in car networking include three basic types of attacks such as networking system damage, zero-trust framework intellectual property theft, and electronic fraud. The focus and difficulty of the internal defense of the system lie in the internal staff, so as to ensure the efficient work and concerted efforts of the internal staff, which is what we need to do. On the one hand, we focus on systematic innovation; on the other hand, we strengthen internal cooperation and communication among employees. Not only there must be a positive working atmosphere but also the relevant

management treaty. Insider threats can only be eradicated if everyone follows the rules.

5.4. Integrity. User's privacy information, device fingerprint, vehicle's trust value, punishment measures against malicious nodes, etc. will be uploaded to the blockchain in a specific data format. The participating organizations in the blockchain network can automatically update the distributed ledger through a unified consensus mechanism and algorithm, and there is no third-party centralized organization to participate. At the same time, the relevant principles of cryptography are used for data verification, and multiple private keys are used for access control. It ensures the security and nontamperability of users' data.

6. Conclusions

Aiming at the problems of easy disclosure of user data privacy in the Internet of Vehicles, we propose a data protection scheme for users in the Internet of Vehicles, which combines zero trust, blockchain, commercial cryptography, and other technologies in the Internet of Vehicles for the first time. It has achieved good results. The scheme relies on terminal environment analysis, trusted identity authentication, behavior model analysis, and other means to enhance the authentication ability and carries out minimum authorization and dynamic access control for the accessed vehicles, personnel, third-party enterprises, and institutions. It can effectively solve the security problems in the scenario of interconnection with people, vehicles, roads, and the cloud platform. It solves the risks encountered in data collection, data transmission, data use, data storage, data sharing, data destruction, and prevention of data leakage, data misuse, and abuse. The scheme protects the data security in the cloud platform of the Internet of Vehicles.

In view of the problems such as data loss and inadequate protection measures in data transmission of the Internet of Vehicles, we carry out PKI authentication and fingerprint identification as two-factor authentication for vehicles in the blockchain network. The SM series national secret algorithm is used for encryption and transmission, and the zero-trust evaluation engine and access control engine are used to realize identity authentication and authorization, improve the security and integrity of data transmission, and clarify the method of zero-trust system for vehicle networking data protection. Through the experiment of three vehicles, we tested the pass rate of identity authentication, the pass rate of fingerprint identification authentication, the success rate of API authentication, and the transmission and reception rate of SPA package and analyzed the change of trust value. The system can update the trust value of Internet of Vehicles devices in real time. By using the convolutional neural network to train the trust level of vehicle nodes, the set convolutional neural network can be trained to study the effectiveness of its application to the target, and the classification of user trust level in the convolutional neural network algorithm for specific applications can be determined quickly. Through the simulation of the influence of dimensions and weights of the four characteristic attributes of the vehicle on CNN identification performance, the specific dimension range of the characteristic attributes of vehicle nodes is determined.

This scheme has also some limitations. In the zero-trust framework, there are not enough vehicle nodes deployed to effectively simulate the huge Internet of Vehicles architecture in reality. Some representative nodes are selected in the scheme, which simplifies the workflow on the one hand and lacks sufficient data analysis on the other hand. In view of the limited number of selected nodes, we select some key nodes, increase the range of measurement data, and reduce the selection unit of experimental data.

Next, we will mainly conduct two aspects: one is to study the incentive measures of the trust evaluation model and the other is to conduct the system security and performance test targeted at the more complicated attack behaviors.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported in part by the Hainan Provincial Natural Science Foundation of China (grant no. 621RC508), Henan Key Laboratory of Network Cryptography Technology (grant no. LNCT2021-A16), the Science Project of Hainan University (grant no. KYQD(ZR)-21075), National Natural Science Foundation of China (grant no. 62162020), the Hainan Provincial Natural Science Foundation of China (grant no. 620RC563), the Hainan Province Science and Technology Special Fund (grant no. ZDYF2021GXJS216), and the Science Project of Hainan University (grant no. KYQD(ZR)20021).

References

[1] B. H. Li, *Secure Communication for Internet of Vehicles Based on Blockchain*, Doctoral Dissertation, Chongqing University of Posts and Telecommunications, Chongqing, China, 2019.

[2] Y. H. Zhou, Z. Q. Lv, Y. G. Yang, and W. Shi, "Data deposit management system basedon blockchain technology," *Netinfo Security*, vol. 19, no. 8, pp. 8–14, 2019.

[3] J. W. Jiang, Z. Hong, and Z. J. Chen, "Application of SM4 encryption algorithm in Internet of vehicles," *Computer Networks*, vol. 46, no. 3, pp. 58–60, 2020.

[4] K. Feng, W. Li, and J. Gong, "Analysis on the application status of cryptographic algorithms in Internet of vehicles," *China Information Security*, vol. 2019, no. 9, pp. 97–99, 2019.

[5] X. K. Chen, *Zero-knowledge Identity Authentication Technology for Internet of Vehicles Based on Consortium Blockchain*, PhD Dissertation, Zhejiang University of Science and Technology, Hangzhou, China, 2020.

[6] L. J. Zhang, Y. F. Zou, W. Z. Wang, Z. Jin, Y. Su, and H. Chen, "Resource allocation and trust computing for blockchain-

enabled edge computing system," *Computers & Security*, vol. 105, Article ID 102249, 2021.

[7] S. A. Mostafa, A. Mustapha, S. S. Gunasekaran et al., "An agent architecture for autonomous UAV flight control in object classification and recognition missions," *Soft Computing*, vol. 150, pp. 1–14, 2021.

[8] M. Poongodi, M. Malviya, M. Hamdi, M. Mohammed, H. T. Rauf, and K. A. Al-Dhlan, "5G based Blockchain network for authentic and ethical keyword search engine," *IET Communications*, vol. 16, no. 5, pp. 442–448, 2021.

[9] S. Kumar, R. S. Raw, A. Bansal, M. A. Mohammed, P. Khuwuthyakorn, and O. Thinnukool, "3D location oriented routing in flying ad-hoc networks for information dissemination," *IEEE Access*, vol. 9, pp. 137083–137098, 2021.

[10] H. Xiong, C. J. Jin, M. Alazab et al., "On the design of blockchain-based ECDSA with fault-tolerant batch verication protocol for blockchain-enabled IoMT," *IEEE Journal of Biomedical and Health Informatics*, vol. 26, no. 5, pp. 1977–1986, 2022.

[11] T. Wang, Y. Quan, X. S. Shen, T. R. Gadekallu, W. Wang, and K. Dev, "A privacy-enhanced retrieval technology for the cloud-assisted Internet of things," *IEEE Transactions on Industrial Informatics*, vol. 18, no. 7, pp. 4981–4989, 2022.

[12] S. A. Mostafa, M. S. Ahmad, A. Mustapha, and M. A. Mohammed, "Formulating layered adjustable autonomy for unmanned aerial vehicles," *International Journal of Intelligent Computing and Cybernetics*, vol. 10, no. 4, pp. 430–450, 2017.

[13] L. Zhang, Z. Zhang, W. Wang, Z. Jin, Y. Su, and H. Chen, "Research on a covert communication model realized by using smart contracts in blockchain environment," *IEEE Systems Journal*, vol. 99, pp. 1–12, 2021.

[14] W. Z. Wang, H. Xu, M. Alazab, T. R. Gadekallu, Z. Han, and C. Su, "Blockchain-based reliable and efficient certificateless signature for IIoT devices," *IEEE Transactions on Industrial Informatics*, vol. 11, pp. 1551–3203, 2021.

[15] Z. T. Lian, W. Z. Wang, and C. H. Su, "COFEL: Communication-Efficient and Optimized Federated Learning with Local Differential Privacy," in *Proceedings of the IEEE ICC*, Montreal, Canada, June 2021.

[16] L. J. Zhang, M. H. Peng, W. Z. Wang, Z. Jin, Y. Su, and H. Chen, "Secure and efficient data storage and sharing scheme for blockchain-based mobile-edge computing," *Transactions on Emerging Telecommunications Technologies*, vol. 5, 2021.

[17] J. C. Song, Z. Y. Han, W. Z. Wang, J. Chen, and Y. Liu, "A new secure arrangement for privacy-preserving data collection," *Computer Standards & Interfaces*, vol. 80, Article ID 103582, 2021.

[18] N. M. Balamurugan, S. Mohan, M. Adimoolam, A. John, T. R. Gadekallu, and W. Wang, "DOA Tracking for seamless connectivity in beamformed IoT-based drones," *Computer Standards & Interfaces*, vol. 79, Article ID 103564, 2021.

[19] B. B. Wang, *Research on Vehicular Ad-Hoc NetworksMessage Authentication Scheme Based on Lliptic Curve*, Doctoral Dissertation, Northwest Normal University, Lanzhou, China, 2020.

[20] Y. Xie, X. Li, S. S. Zhang, and L. B. Wu, "An improved provable secure certificateless aggregation signature scheme for vehicular ad hoc NETworks," *Journal of Electronics and Information Technology*, vol. 42, no. 5, pp. 1125–1131, 2020.

[21] X. W. Li, D. Q. Yang, X. Zeng, X. W. Zhu, B. H. Chen, and Y. Q. Zhang, "Cross—domain authentication and the key agreement protocol in VANETs," *Journal of Xidian University*, vol. 48, no. 1, pp. 141–148, 2021.

[22] Y. Xin, X. Feng, and T. T. Li, "Position related lightweight Sybil detection approach in VANET," *Journal on Communications*, vol. 38, no. 4, pp. 110–119, 2017.

[23] Y. L. Shi and L. M. Wang, "Spatio temporal analysis based resist conspiracy Sybil attack detection in VANETs," *China Information World*, vol. 41, no. 9, pp. 2148–2161, 2018.

[24] L. Si, *Research on Authentication Scheme for Vehicle-Mounted Ad Hoc Network under Cloud Service Environment*, Doctoral Dissertation, Tiangong University, Tianjin, China, 2019.

[25] X. Y. Zhang, *Research on New Vehicular Network SecurityArchitecture and Privacy Protection Authentication Method*, Doctoral Dissertation, Anhui University, Hefei, China, 2020.

[26] J. Y. Zhang, *Research on Security Authentication and Privacy protection Mechanism of Vehicular Cloud Computing*, PhD Dissertation, Beijing Jiaotong University, P. R. China, 2018.

[27] W. W. Chen, L. Cao, and C. H. Shao, "Blockchain based efficient anonymous authentication scheme for IOV," *Journal of Computer Applications*, vol. 40, no. 10, pp. 2992–2999, 2020.

[28] Z. Y. Ma, *Research and Implementation of Distributed Trustscheme for Vehicular Ad Hoc Network Based on Blockchain*, Doctoral Dissertation, Nanjing University of Posts and Telecommunications, Nanjing, 2020.

[29] B. Xu, *Vehicle Attribute Recognition Based on Convolutional Neural Network*, Doctoral Dissertation, Beijing Institute of Technology, P. R. China, 2015.