World Electric Vehicle Journal

MDPI

Article

Design of a Data Security Access Control Algorithm for the Electric Vehicle Internet of Vehicles Based on Blockchain Technology

Jia Miao

Department of Vehicle Engineering, Vocational and Technical College of Inner Mongolia Agricultural University, Baotou 014100, China; miaojia_19881026@163.com

Abstract: The data transmission in the vehicle network is easily interfered with by the outside world, which makes the security of data access difficult to provide in order to meet the actual needs. Therefore, a data security access control algorithm for an electric vehicle network based on blockchain technology is proposed. Using the double-chain architecture of anallliance chain-private chain in a blockchain, the distributed database of data communication for vehicle networking is constructed. In the process of vehicle network communication, the longshort-term memory neural network is introduced to analyze the risk of communication behavior. A generator and discriminator are used to avoid communication risk behavior and realize secure access to data. The experimental results show that the success rate of data tampering is lower than 0.09 when this design method is used to deal with external intrusion, and it has high security.

Keywords: blockchain technology; generate countermeasure network; attribute matching

Citation: Miao, J. Design of a Data Security Access Control Algorithm for the Electric Vehicle Internet of Vehicles Based on Blockchain Technology. *World Electr. Veh. J.* **2022**, *13*, 111. https://doi.org/10.3390/wevj13070111

Academic Editors: Kai Liu, Jiangbo Wang and Wei Fan

Received: 17 May 2022
Accepted: 22 June 2022
Published: 23 June 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Copyright: © 2022 by the author. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

1. Introduction

The Internet of vehicles adopts various mature communication technologies, such as can bus, LIN bus, mobile cellular communication, Bluetooth technology, WiFi, etc.; at the same time, it also formulates some special standard protocols, such as special short-range communication standard and lte-v2x. The whole vehicle networking system mainly consists of vehicle communication, vehicle-to-vehicle communication, vehicle-to-person communication, vehicle-to-road communication, and vehicle-to-cloud communication [1]. Among these, vehicle to vehicle communication refers to the communication through on-board units, which is the focus of this study. The communication technologies adopted include lte-v2x, dedicated short range communication (DSRC), etc. [2]. The on-board unit can collect the position, speed, direction, and vehicle status of surrounding vehicles in real time, and can also realize the interaction of short messages, pictures, audio, and video. In the dynamic and open network environment of the Internet of vehicles, the access behavior of nodes usually presents volatility due to the vulnerability of the nodes. Volatility refers to the fact that the access behavior of the Internet of vehicles nodes changes with time. For example, the behavior of vehicle nodes is normal for a certain period of time, but they are easily controlled by attackers, resulting in the attack behavior of eavesdropping and tampering with system information resources [3–5]. However, most of the current access control mechanisms are static, such as the role-based access control (RBAC) mechanism. Once a node has access to an information resource, it will always have it, and it cannot be adjusted dynamically. Therefore, when the node is attacked during access, the system cannot protect the system information resources by adjusting the access rights of the node in time. Therefore, only by starting from the historical communication behavior of the node, accurately predicting the risk of the node through the historical

communication behavior data, and taking this as the basis for controlling the access authority of the node, so as to realize the dynamic access control mechanism, can we improve the integrity, confidentiality, and availability of information when sharing information resources of the Internet of vehicles.

Therefore, Ren Tiaojuan designed the research on the data security communication model of the Internet of vehicles nodes based on a blockchain [6]. Considering the real-time performance of the Internet of vehicles data and the mobility of vehicle nodes, she designed the block structure and packet format of ordinary data and emergency data, and proposed a node authentication scheme based on a cloud server and a blockchain to solve the problems of user authentication and privacy. Then, on the basis of the practical Byzantine fault tolerance (pbft) consensus mechanism, an improved dynamic pbft mechanism is proposed The evaluation of the DSCM (digital speckle correlation method) model effectively improves the security of data communication of networking nodes, but the efficiency of data communication is low. Wu Guangfu et al. Proposed the secure storage method of Internet of vehicles data considering the hybrid architecture ofblockchain and cloud edge computing [7], and adopted the dual chain decentralized storage structure of an alliance chain private chain to ensure the security of communication data.An identity based digital signcryption algorithm and a ring signature scheme, based on discrete central binomial distribution, are used to solve the security problem in the process of communication. A practical Byzantine fault tolerance mechanism (drpbft), based on dynamic layering and reputation value evaluation, is proposed, and the edge computing technology is combined with cloud computing technology. This method can effectively reduce the delay, but the data access security of the Internet of vehicles is poor. Fan et al. [8] put forward a data sharing model for car networking based on a blockchain, which takes vehicles with limited computing power as all nodes to build a blockchain, and the cost is too high; Oham et al. [9] put forward a data storage scheme for car networking based on a blockchain. This scheme realizes the access control of the data on the chain by partition, and the access control is relatively limited, so it is difficult to meet the multi-entity and multi-role flexible access control requirements of car networking.

In summary, the existing research cannotrealize the effective access control of the data in the blockchain, and the traditional method to realize the access control of the data in the Internet of vehicles has the disadvantage of complicated strategy and high computational cost. To this end, a data security access control algorithm of electric vehicle networking based on blockchain technology is proposed, which can effectively improve the poor data access security of vehicle networking and improve the efficiency of data communication. In this paper, an access control strategy generation method based on data attribute features is designed. By using the double chain architecture of a blockchain alliance chain and a private chain to establish distributed database, the complexity of the access control strategy can be simplified, the calculation and transmission overhead can be reduced, and effective data sharing can be realized. The relationship between attribute permissions of data access roles can be mined by using a long-short memory neural network, and the multi-entity and multi-role access requirements of thevehicle network arenacan be realized. Generators and discriminators can be used to avoid communication risk behaviors.

2. Blockchain Technology

2.1. Design of Data Security Access Tree Structure of Internet of Vehicles

The block in the blockchain is composed of a block header and a block body. The block header includes the hash of the previous block and the root of the Merkle tree. The Merkle tree records a large amount of complex data: the leaf node records the data, and the root node only needs a partial hash to judge the data location and whether the data has been artificially changed [10–12].

In a ciphertext policy attribute based encryption (CP-ABE) scheme, a tree data structure is used to make the encryption key of the data invisible. The data in the leaf node of the structure are attributes and attribute values, which are uploaded by the program formulated by the maker. The parent node passes invisible secret values to the leaf node. If the data requester wants to obtain the secret, it must match its own attributes with the corresponding attributes in the node. A non-leaf node is actually a threshold node [13]. The attributes of the data requester should at least meet the minimum threshold of the corresponding attributes under the node. For example, as shown in Figure 1, the number of child nodes of this node is 5 and the threshold is 3/5. In other words, to decrypt this secret, it conforms to two attributes in leaf nodes A, B, and C of the left subtree of the root node, or conforms to the attributes in leaf nodes D and F of the right subtree of the root node. If only one attribute on the left and right sides matches, it cannot be decrypted. To ensure that it can be decrypted, it must match the attributes in at least three child nodes.

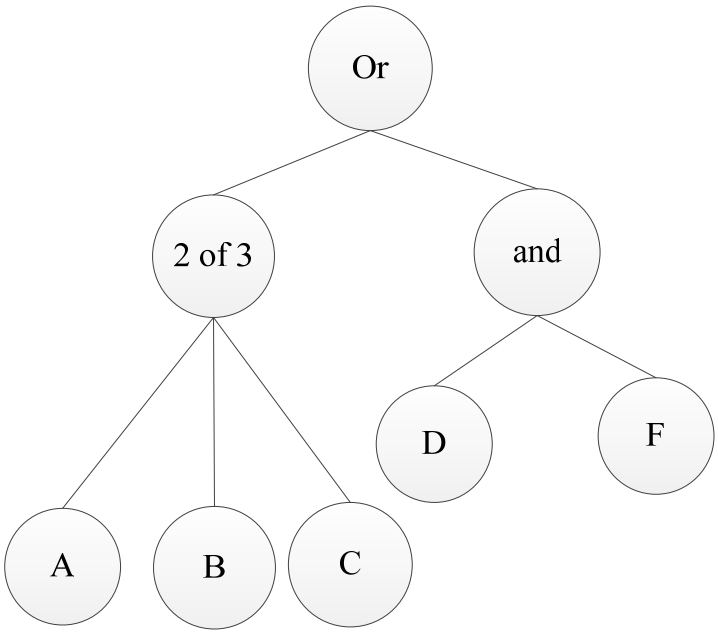


Figure 1. Accesstree structure.

2.2. Blockchain Structure

Blockchains connect blocks together in chronological order using block hash values. A block is composed of a block header and a block body. The block header contains the hash value, timestamp, and other information of the previous block.

Transaction data: it depends on the applicable services of the blockchain.

Hash value: when the transaction is executed, it has been hashed into a code and then broadcast to each node in the network. The blockchain uses the Merkle tree structure to generate the final hash value, which is then recorded in the block header. By using the Merkle tree to store data, data transmission and computing resources can be greatly reduced [14].

Timestamp: records the generation time of the block.

Other information: including the block signature, a random number, or other user-defined data [15].

Blockchains can be roughly categorized into public chains, alliance chains, and private chains. The Table 1 compares the three types of blockchains.

(1) Public chain: in the public chain, each node can check the transaction and verify it, or participate in the process of reaching a consensus, e.g., Bitcoin and Ethereum.

(2) Alliance chain: in the alliance chain, some nodes have pre-selected permissions, which are usually enterprise to enterprise partnerships. The data recorded in the blockchain can be open or private, which can be regarded as partial decentralization, e.g., Hyperledger and r3cev [16–19].
(3) Private chain: in the private chain, nodes will be restricted. Not all nodes can participate in the blockchain. Nodes boast strict permission management for data access.

Table 1. Comparison of blockchains.

Characteristic	Public Chain	Alliance Chain	Private Chain
Decentralization	Completely	Part	Part
Immutability	Immutable	Partially variable	Variable
Non repudiation	Cannotrefuse	Partial rejection	Can refuse
Transparency	Transparent	Partially transparent	Opaque
Traceability	Traceable	Partially traceable	Traceable
Scalability	Poor	Good	Superior
Flexibility	Poor	Good	Superior
Ask for permission	No need	Need	Need
Consensus algorithm	PoW	PoS Ripple PBFT	PoA

In this paper, the alliance chain-private chain double-chain structure is adopted, ordinary vehicle nodes are added to the alliance chain, and special vehicle nodes are used to form private chains. This structure will give more preferential treatment to special vehicle nodes on the basis of ensuring the normal demand of ordinary vehicles.

3. Design of Data Security Access Control Algorithm for Electric Vehicle Internet of Vehicles Based on Blockchain Technology

3.1. Composition of Electric Vehicle Networking System

The structure of the vehicle safety communication system based on a blockchain consists of four parts: certification authority (CA), law enforcement agency (LEA), roadside unit (RSU), and vehicle, as shown in Figure 2.

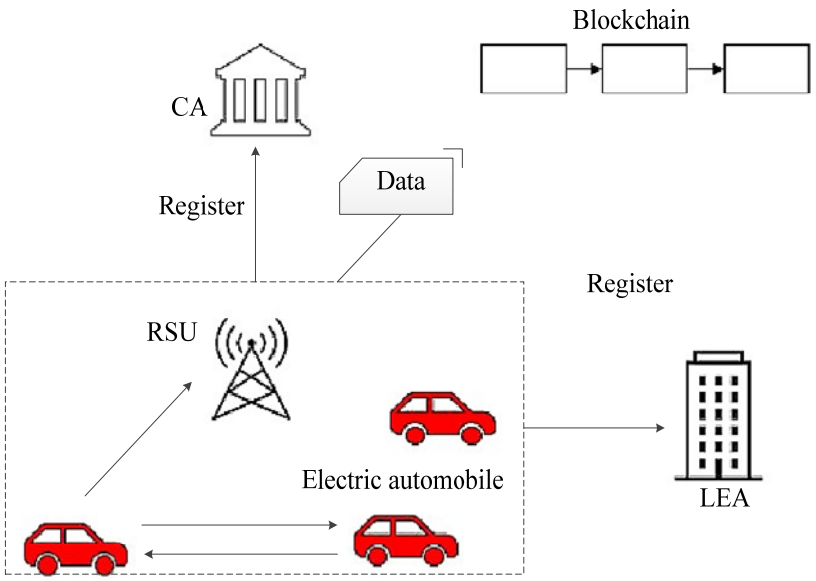


Figure 2. Electric vehicle networking system model.

Law enforcement agencies: the main work of law enforcement agencies includes vehicle registration, authorizing issuing agencies to issue communication certificates to trusted vehicles, assigning pseudonyms to vehicles, monitoring vehicle behavior, and assigning rights and interests to communication vehicles.

Certification authority: the functions of the certification authority include RSU registration and certificate issuance, as well as digitally signing legal vehicles.

Roadside unit (RSU): The RSU manages vehicle communication within the communication range and verifies the authenticity of the message after receiving the message sent by the vehicle.

Vehicle: the vehicle is the communication subject, and here, the message is verified again. At the same time, vehicles also monitor each other to prevent vehicles from tampering with and forging messages.

The Merkle tree is adopted in the blockchain to help verify the existence of transactions. The value of the leaf node is the hash value of the unit data, and the value of the non-leaf node is the hash value of its left and right child nodes. Each transaction in the tree can be deleted directly, and only the hash value of the transaction is retained to reduce the amount of data [20–23]. Moreover, it will not change the password security and integrity of the block. Hash set Hash = {Hash56, Hash78, Hash14, Hash18} is sufficient to prove that TX5 exists in CMT. The verifier can prove the existence of TX5 by comparing the root hash value obtained from the hash set with the known root hash value. Figure 3 is the process of verifying whether TX5 exists.

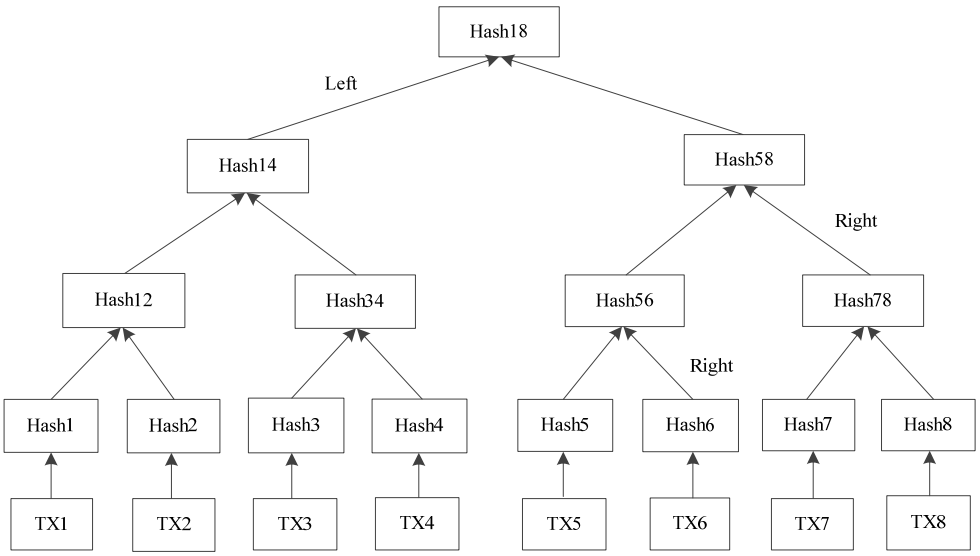


Figure 3. Verifying transaction existence.

During V2V communication, there are two transmission mechanisms, unicast or multicast, and only vehicles are allowed to participate. The information transmitted in V2 usually includes speed, direction, and traffic congestion data. In the case of sexual communication, the information sent by a certain vehicle can only be decrypted and read by a specific vehicle. In order to ensure the reliability of data, the sender needs to sign the information digitally, while the receiver needs to carry out relevant verification. After the data is confirmed to be true and valid, the receiving vehicle will analyze the data in time, and then assist the driver in driving according to the analysis results, so as to ensure the driver's personal safety. In the Internet of vehicles, RSU exists as a fixed point, and V2R can only be carried out when the vehicle enters the fixed wireless communication range of a certain RSU. Because RSUs use wired communication, there are not many restrictions on using wireless communication. In order to ensure that special vehicles can perform

their tasks better, ordinary vehicles can communicate with them only when special vehicles take the initiative to send communication requests to ordinary vehicles, and vice versa.

3.2. Data Risk Forecast Model of Electric Vehicle Internet of Vehicles Based on a Generated Countermeasure Network

To realize decentralized data storage based on a blockchain, a one-to-many data sharing scheme is designed to meet the needs of multi-entity access in the Internet of vehicles, so as to ensure the confidentiality of data. In order to ensure the integrity and availability of data, valid data cannot be tamperedwith or deleted by potential entities or malicious attackers. In order to adapt to the Internet of vehicles data access scenario, secure, efficient, and flexible sharing should be ensured under the requirements of complex access sets and diversified access subjects. The process of data sharing in a blockchain is based on this [24,25]. The attack types of Internet of vehicles nodes include information tampering attack, Sybil attack, packet replay attack, denial of service attack, etc. A feature extraction module is designed to extract the features from different attack behaviors combined with a VANET model, attack model, and application features affected by the attack. These behavior characteristics are as follows: received signal strength, packet sending volume, packet receiving volume, packet delivery rate, packet loss rate, packet capture rate, packet conflict rate, packet retransmission rate, packet tampering rate, speed deviation, etc. Signal strength refers to the strength of data signals received by vehicles in the Internet of vehicles, which helps to improve the success rate of signal connection and the quality of information transmission. Packet sending/receiving capacity refers to the amount of information in the data packet every time data is sent/received. Packet delivery rate refers to the maximum number of network packets that the server can deliver per second. Packet loss rate refers to how many packets sent by the server are not received successfully. Packet capture rate refers to the maximum number of network packets that a vehicle can receive per second. Packet collision rate refers to the repair speed of packet collision formed when the transmitting vehicle transmits using the same resource (i.e., the same sub-channel and sub-frame) as another interfering vehicle. Packet retransmission rate refers to the maximum number of retransmissions per second after packet transmission is lost. Packet tampering rate refers to the speed of data tampering and repair caused by data packet interference. Speed deviation refers to the detected deviation of data packet transmission speed.

Experiments show that these features can distinguish different types of attack behaviors. Different attacks will cause different risks to the information resources of the Internet of vehicles. Therefore, this paper selects the above behavior characteristics of nodes for risk forecast.

Based on the idea of generating a countermeasure network, the risk forecast problem of electric vehicle networking nodes is transformed into the generation problem of behavior sequence in the generation countermeasure network [26,27]. Let the behavior sequence of nodes be $B = \{B_1, B_2, ..., B_n\}$, where B is the set of overall behavior sequences of nodes, $B_i (i = 1, 2, ..., n)$ is the behavior sequence at a certain time, so that $B_i = \{b_{i1}, b_{i2}, ..., b_{im} | risk_i\}$ contains m behavior attributes, such as b_{i1} is the amount of data sent, b_{i2} is the amount of data received, and $|risk_i$ is the risk level. Given the real historical communication behavior sequence $B = \{B_1, B_2, ..., B_{t-1}\}$, a new behavior sequence $B_t' = \{b_{t1}', b_{t2}', ..., b_{tm}' | risk_t'\}$ can be generated by generating model G, where $risk_t'$ is the forecasted risk level.

According to the historical communication behavior data of the nodes, we learn the probability distribution of the node risk, so as to predict the risk of nodes in the future. Figure 4 shows the structure of the GAN model, in which the goal of G is to learn the

data distribution of the historical communication behavior of the nodes, and to generate new behavior sequences as accurately as possible to deceive the discrimination model, while the goal of D is to distinguish the probability that the input data is a real sample as accurately as possible.

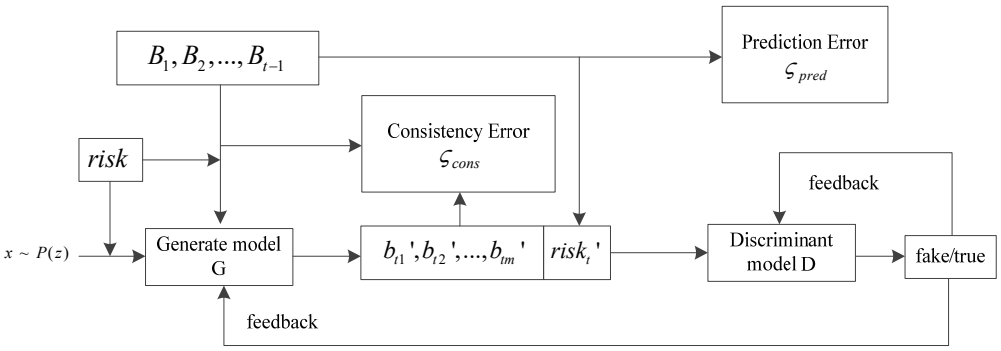


Figure 4. GAN model structure.

$$\min_G \max_D V(D,G) = E_{x \sim P_{data(b)}}[\log D(b \mid risk)] + E_{x \sim P_z(z)}[\log(1 - D(G(z; risk))] \quad (1)$$

Equation (1) is the objective function of GAN, and models G and D are trained alternately, so as to improve the generation ability of the generation model and the discrimination ability of the discrimination model. The training process of GAN is as follows: fix the parameters of D and minimize the expectation of $\log(1-D)(G(z \mid risk))$ by adjusting the parameters of the generation model G; Fix the parameters of G and maximize the expectation of $\log D((b \mid risk)) + \log(1 - DG(z \mid risk))$ by adjusting the parameters of discriminant model D. this process can be attributed to the "binary minimax game" process of G and D. Finally, G and D will converge to the Nash equilibrium state. At this time, D cannot distinguish the probability that the input data is the real behavior sequence, indicating that the generated model can well fit the behavior distribution of the nodes, that is, it can accurately predict the risk of the nodes.

A recurrent neural network (RNN) can be used to process sequential data. The difference between RNN and other neural networks is that RNN records and learns the historical information of sequential data through periodically connected hidden layer nodes. However, RNN will have problems when dealing with time series in a long distance. Because the calculation of the connection between long-distance nodes will involve multiple multiplication of the Jacobian matrix, the phenomenon of gradient disappearance easily occurs, which means that the network has difficulties in retaining the sequence information with a long interval, and a long short-term memory (LSTM) network can solve this problem well. LSTM is an improved RNN. In order to overcome the gradient disappearance problem of RNN, LSTM redesigns the memory unit on the basis of RNN. Its structure is shown in Figure 5, which makes it more suitable for processing and predicting data with a long interval in the time series. Therefore, this paper designs and generates a model based on LSTM.

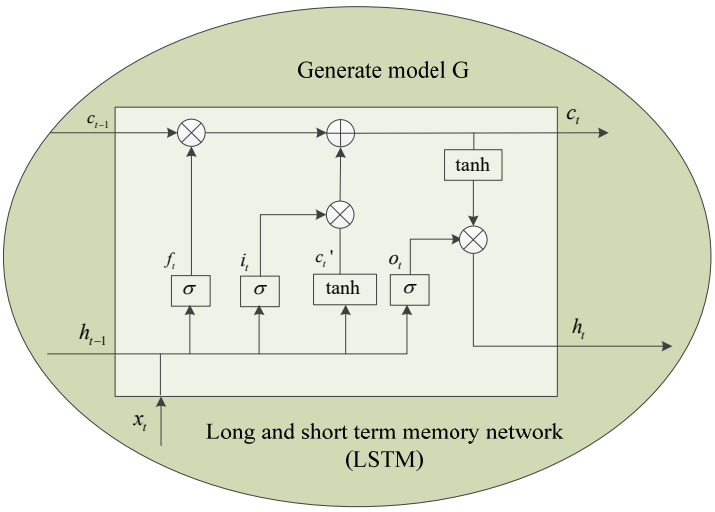


Figure 5. LSTM network structure.

Each LSTM memory cell contains three control gates, including input gate i_t, output gate o_t and forgetting gate f_t. The input value of LSTM at time t is x_t, the output value is h_t, the memory state is c_t', and the memory unit is updated as follows:

Calculation of forgetting gate f_t. f_t depends on how much information is forgotten from the memory unit, which is determined by x_t of time t and $t-1$ time h_{t-1}. The calculation formula of f_t is:

$$f_t = \sigma(w_{hf} h_{t-1} + w_{xf} x_t + b_f) \tag{2}$$

In Equation (2): w is the weight matrix, and its subscript is the weight correlation term, where w_{hf} is the weight matrix from the hidden layer to the forgetting gate at time t, w_{xf} is the weight matrix from the input layer to the forgetting gate at time t, b_f is the offset, and σ refers to the sigmoid activation function.

Input gate i_t. i_t is how much data is currently input to the memory unit, which is determined by x_t at time t and h_{t-1} at time $t-1$. The calculation formula of i_t is:

$$i_t = \sigma(w_{hi} h_{t-1} + w_{xi} x_t + b_i) \tag{3}$$

In Equation (3), w_{hi} is the weight matrix from the hidden layer to the input gate at time t, and w_{xi} is the weight matrix from the input layer to the input gate at time t.

Calculation of candidate state c_t' of memory unit. c_t' is determined by the input value x_t at time t and h_{t-1} at time $t-1$. The calculation formula of c_t' is:

$$c_t' = \tanh(w_{hc}' h_{t-1} + w_{xc}' \cdot x_t + b_c) \tag{4}$$

In Equation (4), w_{hc}' is the weight matrix from the hidden layer to the candidate state at time t, and w_{xc}' is the weight matrix from the input layer to the candidate state at time t.

Update calculation of memory unit status value c_t. c_{t-1} and c_t' are adjusted by i_t and f_t to update c_t. The updated calculation formula of c_t is:

$$c_t = f_t \times c_{t-1} + i_t \times c_t' \tag{5}$$

Calculation of output gate o_t. o_t is used to control the output of c_t, which is jointly determined by t time x_t and $t-1$ time h_{t-1}. The calculation formula of o_t is

$$o_t = \sigma(w_{ho} h_{t-1} + w_{xo} x_t + b_o) \tag{6}$$

In Equation (6), w_{ho} is the weight matrix from the hidden layer to the output gate at time t, and w_{xo} is the weight matrix from the input layer to the output gate at time t.

Calculation of hidden layer output value h_t. h_t is determined by t time o_t and c_t. The calculation formula of h_t is

$$h_t = o_t \times \tanh(c_t) \tag{7}$$

LSTM records the information transmitted over time by adding a memory unit on the basis of RNN. In the process of information transmission, LSTM adds or deletes the information in the memory state. The addition or deletion of information is controlled by the door structure. The LSTM updates the memory state according to the data of the forgetting gate and the input gate. The updated memory state is composed of the memory state information of the previous time and the newly generated information of the current input. Finally, the hidden state is output according to the updated memory state.

Using the LSTM model, the vehicle communication behavior in the vehicle network is taken as the initial data input, and after model processing, the communication characteristics are output, including the received signal strength, packet sending capacity, packet receiving capacity, packet delivery rate, packet loss rate, packet capture rate, packet collision rate, packet retransmission rate, packet tampering rate, speed deviation, etc. Next, compare the above communication characteristics of the vehicle with its own historical transmission information, so as to verify the risk of the communication process, determine the risk level, and realize the data risk prediction of the vehicle network.

3.3. Internet of Vehicles Data Access Security Optimization

The probability distributions of different modes are covered by using multiple generators. A network architecture using multiple generation models is proposed. Each generation model cooperates and complements to learn the sample distribution that cannot be covered by a single generation model, so as to enhance the fitting ability of the generation model to the real data, reduce the possibility of pattern collapse, and improve the convergence speed and learning efficiency of Gan, to a certain extent. The generator and the discriminator are game relations, which are optimized together during the training process. The goal of training is to enable the generator to accurately fit the data distribution of real samples. In fact, because the learning ability of a single generated model is limited, it can only fit part of the real data distribution, resulting in the lack of some models, that is, the collapse of models, resulting in the redundancy of training results and poor forecast accuracy. Through the analysis of the real behavior data of the Internet of vehicles nodes, it is found that there are great differences between different modes, such as the packet delivery rate and packet tampering rate of different attack behaviors. Based on the above analysis, this paper uses two (or more) generators and a discriminator. In order to cooperate with each other, each generator has the same input data and trains.

Given the set of k generators, the discriminator generates the softmax probability distribution on $k+1$ classes. $D_{j+1}(X)$ denotes the probability that the sample is in the real data distribution and the probability generated by the j-th generator, where $j \in \{1,...,k\}$. When learning θ_d, the cross entropy between the softmax output of the

discriminator and the Dirac delta distribution $\delta \in \{0,1\}^{k+1}$ is optimized. If the sample belongs to the j-th generator, then $\delta(j)=1$; otherwise $\delta(k+1)=1$. Therefore, the goal of the discriminator is to optimize its own parameter θ_d while keeping the parameter θ_g of the generator constant, and adjust it to:

$$\max_{\theta_d} E_{x\sim p} H(\delta, D(x;\theta_d)) \tag{8}$$

To identify the generators that generate false samples, the discriminator must learn to push different generators to different recognizable patterns, but the goal of each generator is still the same as that in the standard GAN. Therefore, the objective function of GAN is shown in Equation (9):

$$\min_G \max_D E_{x\sim P_d} \log D_{k+1}(x;\theta_d) + E_{x\sim P_z} \log(1 - D_{k+1}(G_i(z;\theta_g^i);\theta_d) \tag{9}$$

Combined with Equation (10), for the discriminator, given $x \sim p$ and the corresponding δ, the loss function is:

$$\varsigma_D = D_{k+1}(G_i(z;\theta_g^i);\theta_d) - D_{k+1}(x;\theta_d) \tag{10}$$

The gradient of the discriminator is calculated as:

$$\nabla_{\theta_d} = [D_{k+1}(G_i(z;\theta_g^i);\theta_d) - D_{k+1}(x;\theta_d)] \tag{11}$$

where $D_j(x;\theta_d)$ is the j-th parameter of $D(x;\theta_d)$, $\delta(j)=1$. Therefore, the optimization algorithm of the original GAN needs to be modified slightly, which can facilitate the training of different generators of GAN at the same time. The loss function of the i th generator is:

$$\varsigma_{G_i} = D_{k+1}(x;\theta_d) - D_{k+1}(G_i(z;\theta_g^i);\theta_d) \tag{12}$$

The gradient of the i th generator is calculated as:

$$\varsigma_{\theta_g^i} = [-D_{k+1}(G_i(z;\theta_g^i);\theta_d)] \tag{13}$$

The loss function of Equation (12) actually makes the generator form a combined model. When $P_d = \frac{1}{k}\sum_{i=1}^{k} P_{gi}$, each generator represents the combined component to achieve global optimization.

In summary, this paper proposes a Wasserstein distance-based combined generative adversarial network (wcgan), which solves the problem of gradient disappearance by modifying the loss function, and solves the problem of pattern collapse by designing a multi generator combination, Therefore, it can improve the convergence speed and reduce the training time, while ensuring the accuracy of the node risk forecast model based on the generated countermeasure network.

4. Experiment

4.1. Experimental Scheme

To validate the feasibility of the proposed data security access control algorithm, a simulation environment is built through docker technology for corresponding testing. The specific test hardware parameters are shown in Table 2.

Table 2. Hardware environment.

Hardware	Number of CPU Cores	Dominant Frequency	Framework	Memory	Hard Disk
parameter	20	3100 MHz	x86	64GB	8T

Using docker technology to build the simulation environment can effectively use the computing resources of the hardware. Because the container of the docker is lighter than the traditional virtualization technology, we can create enough node containers for simulation in a single machine environment, and each container is isolated from the others. In the simulation, the docker container nodes are divided into two types: RSU node and OBU node. The RSU node undertakes more tasks than the OBU node, including block storage, block coding, block verification, and other tasks, while the OBU node is only responsible for receiving information from other vehicles. In addition, a container node is used as the master node to coordinate and monitor the global nodes. The specific node list is shown in Table 3.

Table 3. Network node types.

Node Name	Node Function	Number of Nodes
Main	Block generation	Node monitoring 1
RSU	Block coding and block storage	Multiple
OBU	Block verification	Multiple

In the simulation, all programs are pre coded into a docker image through DockerCompose. Docker Compose runs the configuration script to uniformly arrange the image. At the beginning of the simulation, the master node container will be run to simulate the consensus process in the blockchain network to generate new blocks. Then, multiple RSU containers will be started to obtain the master node information through the config file and connect to the master node. After receiving the master node's blocks, the block coding service will be started to encode and compress the blocks. Finally, the OBU container is started, and it sends a random request to the RSU node to test various performance indicators. In the experiment, the number of RSU nodes and OBU nodes will be dynamically increased to evaluate the performance changes in the algorithm. The specific network topology diagram is shown in Figure 6.

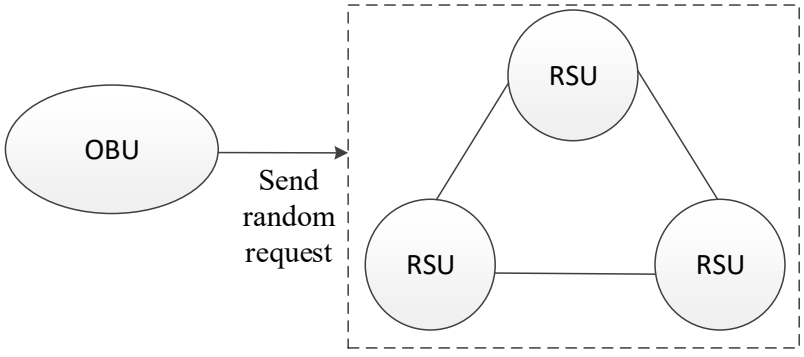


Figure 6. Network topology.

4.2. Experimental Result

4.2.1. Time Cost of Private Vehicle Encryption

The host processor of this experiment is 3.4GHz, the memory is 8 g, and the operating system is Windows operating system. Compared with the methods in reference [6] and reference [7], this method performs encryption with the same ciphertext length. The time cost for simulating private vehicles is shown in Figure 7.

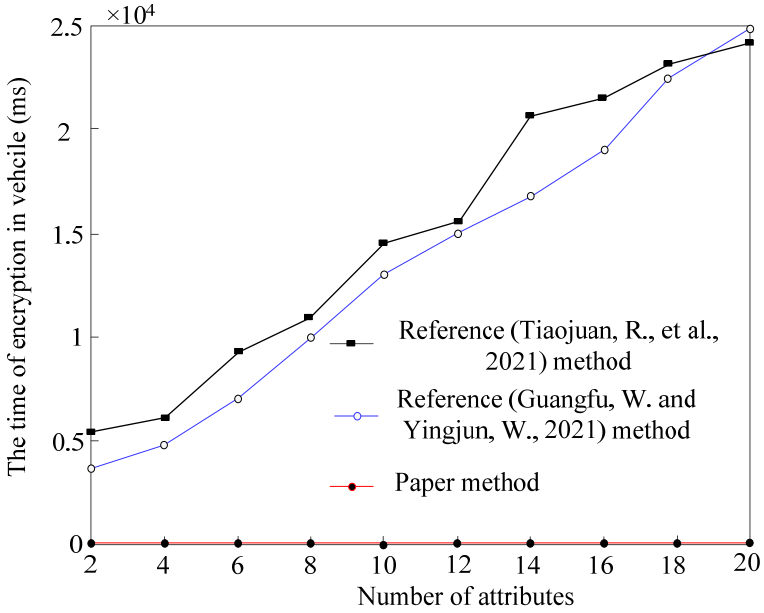


Figure 7. Time cost of private vehicle encryption under different methods.

Compared with the two traditional methods, the encryption time for private vehicles is greatly reduced. This is because the private vehicle in this method only needs to encrypt the symmetric key once, and other encryption processes and judgment processes are completed with the assistance of other entities. Therefore, the computational cost of private vehicle encryption in this method is very small, and it always maintains a horizontal straight line with the increase in the number of attributes.

4.2.2. Data Access Security of Electric Vehicle Internet of Vehicles

To verify the security of the EV Internet of vehicles data access under different methods, 10 dB~100 dB intensity noise is added in the experiment, and the tampering probability of the EV Internet of vehicles data under different methods is calculated. The results are shown in Figure 8.

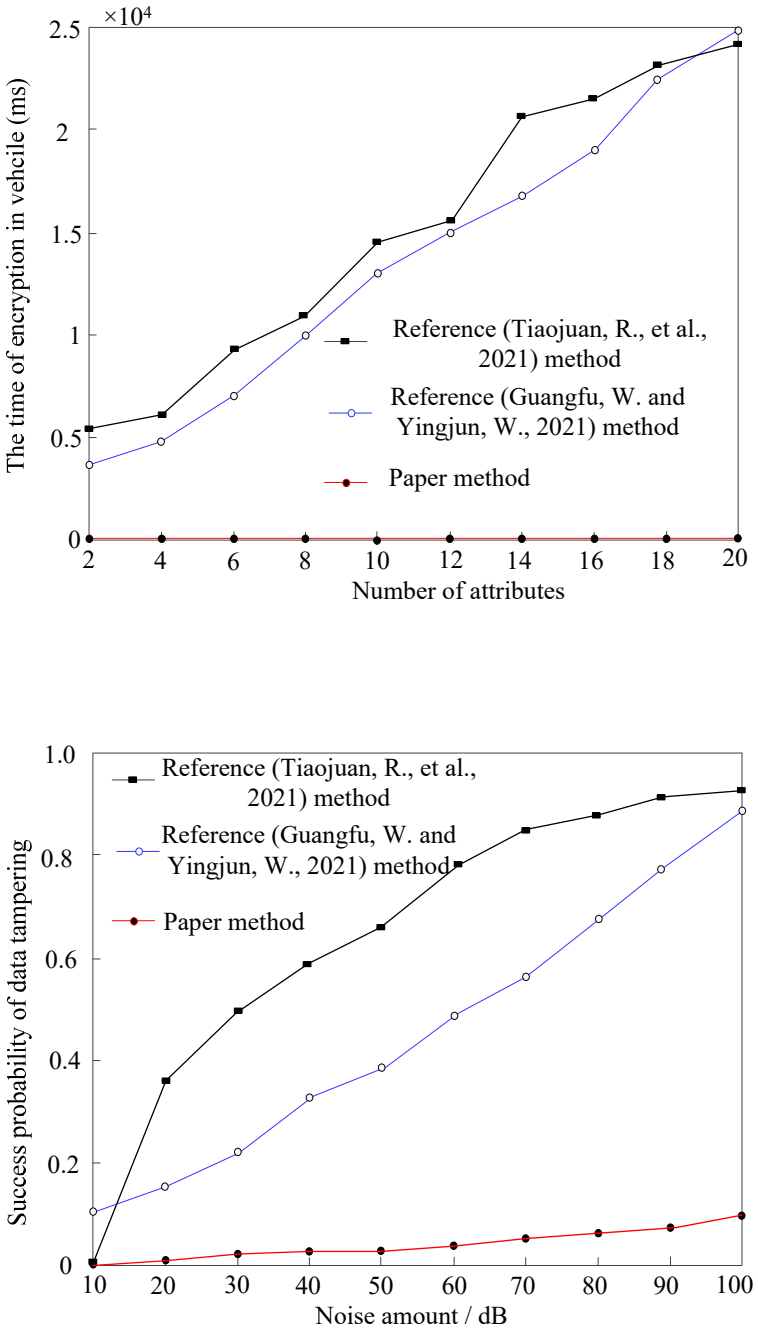


Figure 8. Success probability of data tampering by different methods.

Figure 8 shows that when the noise is 20 dB, the success probability of vehicle networking data tampering of the method used in reference [6] is 0.37, the success probability of vehicle networking data tampering of the method used in reference [7] is 0.15, and the success probability of vehicle networking data tampering of this method is 0.06. When the amount of noise is 80 dB, the success probability of vehicle networking data tampering of the reference [6] method is 0.88, the success probability of vehicle networking data tampering method of reference [7] is 0.70, and the success probability of vehicle networking data tampering of this method is 0.09. The success probability of data tampering of the Internet of vehicles in this method is far lower than that of other methods, which shows that the data access security of the Internet of vehicles of electric vehicles in this method

is high. This is because this method uses blockchain technology to realize the attribute matching of sub nodes, which effectively reduces the success probability of data tampering of the Internet of vehicles.

To test the consensus efficiency, a car is regarded as a block, and the consensus time of different blocks is tested. The trend of consensus time with the number of nodes is shown in Figure 9. By analyzing Figure 9, it can be found that when the number of nodes reaches 50, the consensus time is nearly 60 s, and the consensus time increases linearly with the number of nodes. Under different numbers of nodes, the consensus time is always lower than in other methods. This is because the consensus process of this method is based on convolution neural network calculation, which greatly reduces the amount of computation, making the verification of nodes faster and the consensus efficiency higher.

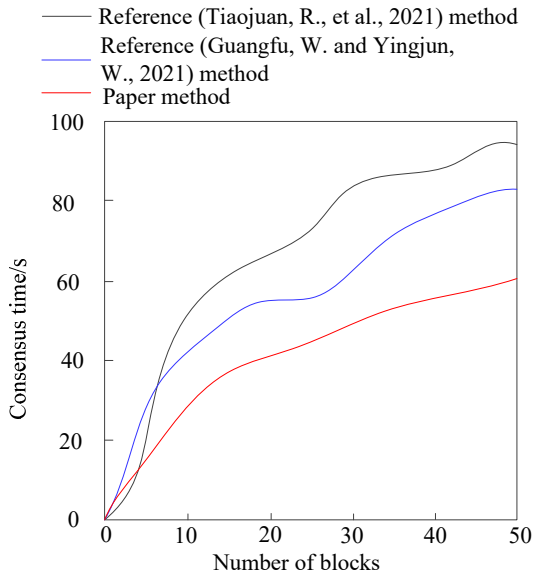


Figure 9. Success probability of data tampering by different methods.

5. Conclusions

In this study, a data security access control algorithm of the electric vehicle Internet of vehicles based on blockchain technology is proposed. The structure of the vehicle safety communication system is designed through blockchain technology, and the behavior characteristics of the electric vehicle Internet of things data are selected. Based on the idea of generating a confrontation network, the risk forecast model of electric vehicle Internet of vehicles data access is constructed, and the safety optimization of the Internet of vehicles data access is realized through a convolution neural network. The following conclusions are drawn:

(1) This method can greatly reduce the encryption time of private vehicles. This paper shows that this method of electric vehicle networking has high security.
(2) When the amount of noise is 80 dB, the success probability of vehicle networking data tampering in this method is 0.09; this shows that the data access security of electric vehicle networking based on this method is high.

Funding: This research received no external funding.

Data Availability Statement: All data generated or analysed during this study are included in this published article.

Conflicts of Interest: The authors declare no conflict of interests.

References

1. Meng, X.; Lv, J.; Ma, S. Applying improved K-means algorithm into official service vehicle networking environment and research. *SoftComput.* **2020**, *24*, 8355–8363.
2. Guo, X.; Aoki, T.; Lin, H.H. Model checking of in-vehicle networking systems with CAN and FlexRay. *J. Syst. Softw.* **2020**, *161*, 110461.1–110461.19.
3. Song, M.; Li, R.; Wu, B. Intelligent control method for traffic flow at urban intersection based on vehicle networking. *Int. J. Inf. Syst. Chang. Manag.* **2020**, *12*, 35–52.
4. Wang, X.; Qiu, P. A freight integer linear programming model under fog computing and its application in the optimization of vehicle networking deployment. *PLoS ONE* **2020**, *15*, e0239628.
5. Liu, Y.; Liu, C. Modeling analysis and algorithm optimization design of vehicle networking based on information transmission. *J. Phys. Conf. Ser.* **2021**, *1769*, 12072–12076.
6. Tiaojuan, R.; Jiaying, Z.; yourong, C.; Qiuxia, C.;Banteng, L. Research on data security communication model of Internet of vehicles nodes based on blockchain. *Automot. Technol.* **2021**, 52., 30–35.
7. Guangfu, W.; Yingjun, W. Secure storage and sharing scheme of Internet of vehicles data based on blockchain and cloud edge computing hybrid architecture. *Comput. Appl.* **2021**, *41*, 2885–2892.
8. Fan, K.; Pan, Q.; Zhang, K.; Bai, Y.; Sun, S.; Li, H.; Yang, Y. A secure and verifiable data sharing scheme based on blockchain in vehicular social networks. *IEEE Trans. Veh. Technol.* **2020**, *69*, 5826–5835.
9. Oham, C.; Jurdak, R.; Kanhere, S.S.; Dorri, A.; Jha, S. B-fica: blockchain based framework for auto-insurance claim and adjudication. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1171–1180.
10. Kim, H.J.; Choi, M.H.; Kim, M.H.; Lee, S. Development of an Ethernet-based heuristic time-sensitive networking scheduling algorithm for real-time in-vehicle data transmission. *Electronics* **2021**, *10*, 157–168.
11. Le, Q.; Jiang, K.; Zhang, F. Design of automatic detection system for vehicle networking communication abnormal data based on CAN bus. *Int. J. Inf. Commun. Technol.* **2020**, *16*, 123–136.
12. Rawat, D.B.; Doku, R.; Adebayo, A.; Bajracharya, C.; Kamhoua, C. Blockchain enabled named data networking for secure vehicle-to-everything communications. *IEEE Netw.* **2020**, *34*, 185–189.
13. Hou, R.; Zhou, S.; Cui, M.; Zhou, L.; Zeng, D.; Luo, J.; Ma, M. Data forwarding scheme for vehicle tracking in named data networking. *IEEE Trans. Veh. Technol.* **2021**, *70*, 6684–6695.
14. Shon, T. In-vehicle networking/autonomous vehicle security for Internet of things/vehicles. *Electronics* **2021**, *10*, 637–648.
15. Yang, M. Design of recognition and compensation system for vehicle communication signal based on vehicle networking. *Int. J. Veh. Inf. Commun. Syst.* **2020**, *5*, 187–196.
16. Luo, Q.; Zang, X.; Cai, X.; Gong, H.; Yuan, J.; Yang, J. Vehicle lane-changing safety pre-warning model under the environment of the vehicle networking. *Sustainability* **2021**, *13*, 5146–5162.
17. Liu, H.; Zhu, R.; Wang, J.; Xu, W. Blockchain-based key management and green routing scheme for vehicular named data networking. *Secur. Commun. Netw.* **2021**, *20*, 1–13.
18. Zhou, H.; Li, C.; Zhang, L.; Song, W. Attention-Aware Network and Multi-Loss Joint Training Method for Vehicle Re-Identification. In Proceedings of the 2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC), Chongqing, China, 12–14 June 2020.
19. Li, Y.; Xie, Y.Z.; Wang, Y.J.; Jiang H. Traffic anomaly detection method for vehicular ad-hoc networkflooding attack. *J. Nanjing Univ. Sci. Technol.* **2020**, *44*, 454–461.
20. Li, T.; Xie, Z.F. Advantages and security analysis of Internet of vehicles based on named data network. *Commun. Technol.* **2019**, *52*, 106–111.
21. Raissi, K.; Gouissem, B.B. Hybrid communication architecture in VANETs via named data network. *Int. J. Commun. Syst.* **2021**, *34*, 126–139.
22. Zhang, H.T. Threat suppression of vehicle network data transmission based on anonymous exchange algorithm. *Comput. Simul.* **2021**, *38*, 162–166.
23. Rana, M.M. IoT-based electric vehicle state estimation and control algorithms under cyber attacks. *IEEE Internet Things J.* **2019**, *7*, 874–881.
24. Aung, N.; Zhang, W.; Sultan, K.; Dhelim, S.; Ai, Y. Dynamic traffic congestion pricing and electric vehicle charging management system for the internet of vehicles in smart cities. *Digit. Commun. Netw.* **2021**, *7*, 492–504.
25. Yan, R.; Lin, C.; Zhang, W.F.; Chen, L.W.; Peng, K.N.Research on information security of users' electricity data including electric vehicle based on elliptic curve encryption. *Int. J. Distrib. Sens. Netw.* **2020**, *16*, 1550147720968458.
26. Iranmanesh, S.; Abkenar, F.S.; Jamalipour, A.; Raad, R. A heuristic distributed scheme to detect falsification of mobility patterns in internet of vehicles. *IEEE Internet Things J.* **2022**, *9*, 719–727. doi:10.1109/JIOT.2021.3085315.
27. Ye, J.; Guo, L.; Yang, B.; Li, F.; Du, L.; Guan, L.; Song, W. Cyber–physical security of powertrain systems in modern electric vehicles: Vulnerabilities, challenges, and future visions. *IEEE J. Emerg. Sel. Top. Power Electron.***2021**, *9*, 4639–4657. doi:10.1109/JESTPE.2020.3045667.