Hindawi
Security and Communication Networks
Volume 2023, Article ID 9839245, 1 page
https://doi.org/10.1155/2023/9839245

Retraction

Retracted: Blockchain-Based Dangerous Driving Map Data Cognitive Model in 5G-V2X for Smart City Security

Security and Communication Networks

Received 31 January 2023; Accepted 31 January 2023; Published 7 February 2023

Security and Communication Networks has retracted the article titled "Blockchain-Based Dangerous Driving Map Data Cognitive Model in 5G-V2X for Smart City Security" [1] due to concerns that the peer review process has been compromised.

Following an investigation conducted by the Hindawi Research Integrity team [2], significant concerns were identified with the peer reviewers assigned to this article; the investigation has concluded that the peer review process was compromised. We therefore can no longer trust the peer review process, and the article is being retracted with the agreement of the Editorial Board.

The authors do not agree to the retraction.

References

[1] K. Chen, C. Xu, H. Liu, P. Wang, and Z. Chen, "Blockchain-Based Dangerous Driving Map Data Cognitive Model in 5G-V2X for Smart City Security," *Security and Communication Networks*, vol. 2022, Article ID 8922289, 10 pages, 2022.

[2] L. Ferguson, "Advancing Research Integrity Collaboratively and with Vigour," 2022, https://www.hindawi.com/post/advancing-research-integrity-collaboratively-and-vigour/.

Hindawi
Security and Communication Networks
Volume 2022, Article ID 8922289, 10 pages
https://doi.org/10.1155/2022/8922289

Research Article

Blockchain-Based Dangerous Driving Map Data Cognitive Model in 5G-V2X for Smart City Security

Kai Chen,[1] **Cheng Xu**,[1] **Hongzhe Liu**,[1,2] **Pengfei Wang**,[3] **and Ziyi Chen**[1,3]

[1]*Beijing Key Laboratory of Information Service Engineering, College of Robotics, Beijing Union University, Beijing, China*
[2]*Beijing Key Laboratory of Traffic Data Analysis and Mining, Beijing Jiaotong University, Beijing, China*
[3]*Communication and Information Center of Ministry of Emergency Management of the People's Republic of China, Beijing, China*

Correspondence should be addressed to Hongzhe Liu; liuhongzhe@buu.edu.cn

Received 18 January 2022; Revised 18 February 2022; Accepted 23 February 2022; Published 14 April 2022

Academic Editor: Muhammad Arif

The development of 5G network communication has brought technological innovation to smart city communication, making the realization of V2X (vehicle to everything) technology possible. Vehicles wirelessly communicate with other vehicles, sensors, pedestrians, and roadside units, raising data security issues while driving. In order to ensure driving safety, the risk map cognitive model is established with the help of blockchain technology. In this model, the key map data and personal privacy information are encrypted and uploaded to form a blockchain, and the smart contract technology is used for automatic script processing. Then, according to different risk scenarios, cognitive learning is carried out for different risk levels, the cognitive results and corresponding operations are fed back to the intelligent vehicle, and these operations ensure the safe operation of the vehicle according to the intelligent vehicle. Finally, the feasibility of the model was verified by comparing different dangerous scenarios. The experimental results show that this risk cognition model can cognize the data of the intelligent vehicle according to different danger scenarios, and the model can transmit acceleration, deceleration, braking, and other behaviors to the intelligent vehicle to ensure smart city driving safety.

1. Introduction

The rapid increase in the number of vehicles has posed a severe challenge to the existing transportation system. For example, traffic congestion and traffic accidents are frequent, which seriously threaten people's life and property safety. The internet of vehicles [1] is an effective way to solve the above problems. By establishing communication between vehicles and between vehicles and network facilities, vehicles can adequately obtain traffic environment information and make driving decisions in advance, thus improving traffic safety and efficiency. However, if data related to connected vehicle driving that is stolen or tampered with, the result can directly lead to loss of property or life. How to prevent vehicle information from being modified on the internet of vehicles [2] is an extremely important part of intelligent driving [3].

Moreover, not only vehicles are intelligent, but all things around us are gradually intelligent. We will live in a smart city [4] full of convenience. In recent years, the development of 5G technology has promoted the transformation of the communication data transmission industry and also played a major role in the field of the internet of vehicles. The emerging 5G-V2X and blockchain [5–8] technology intelligently connects road units in the vehicle road environment, making it easier to build a safe vehicle network platform.

Blockchain is a decentralized technology. Blockchain technology includes five features: distributed database, peer-to-peer transmission, anonymity, irreversibility of records, and computing logic. It can effectively analyze and identify the credibility of data added to blocks to ensure that the data are credible, available, and traceable. The risk cognition model designed in this study establishes trust cognitive for the transmitted data [9], and the model processes the data with the

decentralized technology of blockchain for the network. Specific map data are collected for a single vehicle and uploaded it to the blockchain, and the risk cognition of different dangerous situations encountered in the operation process of the vehicle is carried out. Data tampering is effectively avoided through the smart contract [10] program automatically executed. The input-output model is built through the universal set theory [11] to improve the expansion and applicability of the model. The smart contracts are decentralized trusted environments that are primarily used to establish trust in blockchain technology. The smart contract is similar to a paper contract. Both parties make a contract and deploy and execute it through a computer. It will be triggered when both parties meet the conditions specified in the contract during the transaction.

This study makes two main contributions: (1) established the network data encryption based on blockchain technology platform, the platform ensures the safety of the users' personal information and vehicle running data using smart contracts set up an automatic program, and the platform connects the data generated in the process of vehicle operation information chain to the blockchain. According to the results, a smart contract anonymous system is established, and the data are ensured to be trusted. (2) Risk rating model for intelligent vehicle map data interaction is established. This model evaluates two kinds of road environment, namely, network attack and dangerous road. When the vehicle data evaluation value reaches the risk level, it gives the vehicle to return to slow down, stop, and other safety instructions.

The rest of this study is organized as follows: the second chapter discusses the relevant technology of the smart contract dangerous driving model. Then, the third chapter designs and analyzes the dangerous driving map cognitive model. The fourth chapter is the specific experimental results and experimental analysis. Finally, a brief conclusion and an outlook to future work are given in the fifth chapter.

2. Related Work

The application of the internet of vehicles is becoming more and more common, but its network security situation is becoming increasingly severe [12]. There are many problems in data security on the internet of vehicles, and there have been many attempts and research results. Literature [13] proposes an authentication and secure data transmission algorithm, using promising and developing blockchain technology in the framework of the internet of vehicles, to ensure true information communication between nodes. Literature [14] proposes a new vehicle information system architecture based on blockchain technology to maintain consistency among distributed service providers, thus ensuring data integrity, vehicle authentication, privacy protection, and seamless access control. This decentralized blockchain framework is particularly suited to managing large-scale IoV data. By adopting the proposed local caching strategy, a long transaction time limit can be avoided.

2.1. V2X with Blockchain. Recently, a lot of work has been performed on the integration of V2X and blockchain technologies. Literature [15] proposed a joint cluster and blockchain scheme for real-time information security transmission to prevent some vehicles from sending malicious messages to disrupt traffic order at C-V2X network intersections. The scheme keeps the dynamic stability of the cluster by updating the trust value of the vehicle nodes so as to improve the real time and accuracy of information transmission. In addition, blockchain technology is used to establish a vehicle trust management mechanism in C-V2X to avoid malicious tampering with vehicle information in the process of information sharing and to ensure the security of vehicle information communication. Literature [16] proposed a game theory method to balance the load of mining clusters while maintaining fairness between unloading vehicles. The purpose of this study is to solve the unloading mining task in the cellular V2X network by using finite channel block length transmission to meet the requirement of low delay of vehicle. Literature [17] designs a blockchain-based secure data processing advantage framework that envisages a V2X environment, including an optimal container-based data processing scheme and a blockchain-based data integrity management scheme, aiming to minimize link interruptions and reduce delays. Literature [18] proposes a decentralized V2X (D-V2X) method, this method does not require any trusted authority, and it can be on any communication protocol implementation, mainly using intelligent build processing mechanism for a decentralized management contract, complete the road infrastructure, signal components, and modernize transportation management system.

2.2. On-Chain Authentication Model for Data Privacy Information. Information and data communication are the most important part of the internet of vehicles. Efficient communication between nodes can prevent many disasters. In order to prevent malicious activities, such as tampering with emergency messages or sending false information, it is very important to have only authenticated nodes [19] in the network. Literature [20] proposes an edge trust management scheme, and the scheme uses Ethernet blockchain, an open-source platform, to establish a decentralized trust management platform. All response units work in a distributed manner to maintain a consistent vehicle trust database and enhance reliability, availability, and consistency. The trust mechanism is established between vehicles to judge the accuracy of the data transmitted by vehicles each time, and the mechanism avoids accidents caused by the application of wrong information.

Literature [21] proposed an anonymous address management scheme, in which the control of personal data was decentralized, authority controller (AC) managed the encrypted address, and resource service (RS) managed the decrypted private key. However, neither party obtained the real address, and only after authorized third party (TP) access, TP submitted the encrypted address to RS and decrypted the address. Only in this way can the real address be obtained and the data request of TP be executed, to realize the effective protection of personal data.

2.3. Smart Contract Risk Analysis Model. The internet of vehicles has established intelligent transportation applications. Due to the openness of wireless communication, the integrity, confidentiality, and availability of transmission information resources are easily damaged by illegal access, which threatens the security of related IoV applications. Literature [22] proposed a privacy-protecting vehicle data aggregation scheme to protect data privacy and the unlikability between participating vehicles and perceptual data. In addition, two protocols are designed to protect data privacy and achieve fair returns for data providers. The proposed model realizes privacy protection, reliability, and fairness. Literature [23] uses the smart edge chain to achieve access control of IOV devices, and a Wasserstein composite GaN (WCGaN) was designed to improve the accuracy of the RPBAC model to solve the problems of gradient disappearance and mode collapse in the original GaN.

3. Risk Cognition Model Based on Smart Contract

Table 1 shows the custom parameter symbols used in this study and their corresponding meanings. (*A, B, F, J, D*) is a five-tuple theory, and it is the theoretical basis of our model. Then, λ is security parameters, and it is used to assess the value of risk. K_1, P_1, K_2, P_2, T, and *CTK* are variable parameters in the data encryption process. State means the cognitive state of the vehicle. *Rate_block* is the dependent variable in the cognitive process of the smart contract model. *Rate_block* is the matching degree of the corresponding transaction data transmitted from local data to the blockchain. A more detailed description will be given in the corresponding section below.

Each participant has a unique address, when a user is connected to drive the vehicle blockchain network, the users' personal information, vehicle data, vehicle environment information, and the base station network information into accurate position coordinates information. Then, this anonymous data are transferred to the model server through address matching, and the smart contract program processes the map data and conducts hazard assessments. When the network is attacked, the response command is issued. Smart contract transactions only show address interactions to ensure anonymity; at the same time, it gives users an interface to query their own data.

The model encrypts the user data and asymmetrical vehicle operation data and automatically processes the data in the block through a smart contract script. The script stores the processed data results into a distributed ledger, and each user has a copy of the ledger, which is updated and published through the Hyperledger Fabric platform to realize information transfer.

As shown in Figure 1, the dangerous driving map cognitive model of vehicles consists of five tuples (*A, B, F, J, D*). *A* is the data at the input end of the model, specifically the user's personal information data, road condition map information, and the instruction information transmitted by the network base station. *B* is the model mapping environment, the vehicle information is encrypted to form a block, and the data information is linked to form a blockchain ledger through this process. *F* is the process of model data transformation, mainly including the following processes: The smart contract converts input data into hash data for transmission. Than the model converts the data into the risk coefficient of map environment data through weight operation. Finally the model converts the risk coefficient into the corresponding safety behavior instruction which returned to the vehicle. *J* is the satisfaction value of the model environment mapping, which determines the boundary range of the satisfaction value of the environment mapping. After processing by the smart contract script, the cognitive result data are linked up, and this satisfaction value is also used as the key weight of the mapping to participate in the next iteration cycle. *D* is a table that stores mappings between data. The model matches the vehicle state as safety, stability, and danger. The mapping relationship stores the speed, direction, stop, operation, and other control states of the vehicle in different states, and the model controls the vehicle by invoking this mapping.

Table 1: Relevant symbols and meanings used in this study.

A	Input
B	Mapping environment
F	Data transformation process
J	Mapping feedback satisfaction value
D	Table mapping
Λ	Security parameters
K_1, P_1	Local public key and private key
K_2, P_2	Server public key and private key
T	Encryption mapping
CTK	Ciphertext of key
State	Cognitive of state
Rate_block	Block recognition rate

Using the global set theory, the system model is defined in formula (1):

$$S = \left(A, B, F\left(\lambda, R^2, t\right), J, D\right). \tag{1}$$

We can see from equation (2) that an asymmetric encryption algorithm is used to encrypt and decrypt the data. The public key (*n, e*) is used to encrypt the plaintext *A*. In the formula, *n* and *e* are the public keys, and the encrypted ciphertext is *Y*:

$$A^e = B \,(\mathrm{mod}\, n). \tag{2}$$

The private key (*n, d*) is used to decrypt the ciphertext *Y*. In the formula, *n* and *d* are private keys, and the plaintext after decryption is *A*. The decryption formula is from formula (3):

$$B^d = A \,(\mathrm{mod}\, n). \tag{3}$$

The risk cognition uses the determination coefficient to make the fitting judgment on the model, and the estimation and prediction formula is given as formula (4):

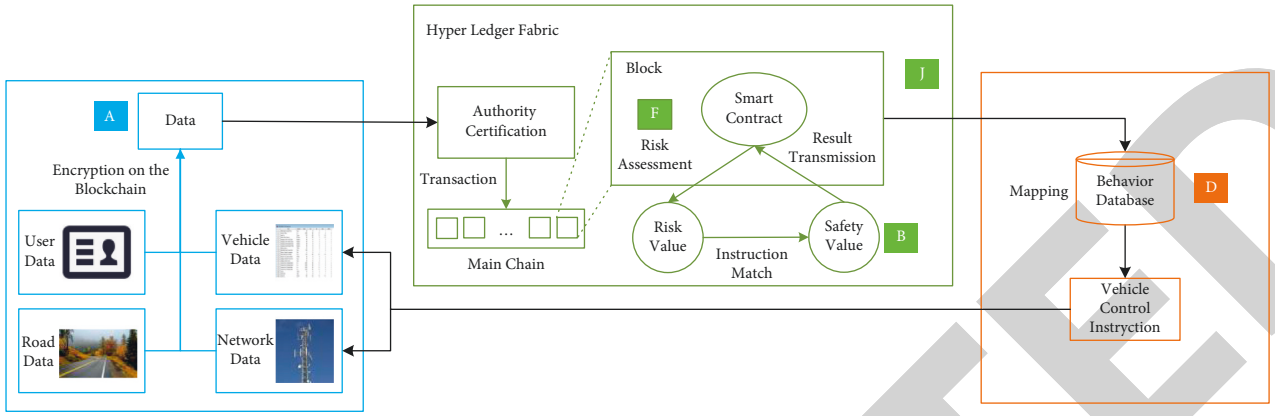

Figure 1: Vehicle dangerous driving cognition model.

$$\overline{y} = \frac{1}{n}\sum_{i=1}^{n}(y_i - \overline{y})^2, \tag{4}$$

$$\begin{aligned} R^2 &= 1 - \frac{SS_{\text{res}}}{SS_{\text{tot}}} \\ &= 1 - \frac{\sum (y_i - f_i)^2}{\sum (y_i - \overline{y})^2}, \end{aligned} \tag{5}$$

$$\text{risk} = F\left(\lambda, R^2, t\right). \tag{6}$$

The risk value in vehicle operation is calculated by formulas (5) and (6), where y_i is the real behavior data acquired during the operation of the vehicle, $\overline{y}$ represents the average value of the map information data collected in a certain period t, f_i represents the estimated data, SS_{res} is the error between the data and the average value, and SS_{tot} represents the error between the real data and the average value.

3.1. Data Information Is Anonymously Connected to the Blockchain. The anonymous upper chain structure of information data is shown in Figure 2. First, initialization is carried out, in which the security parameter λ is the input, and a pair of encryption and decryption public and private keys are generated by the local vehicle and the server, respectively. The server public key is obtained during message transmission, and then, the information is asymmetric encrypted by using the Elliptic Curve Digital Signature Encryption Algorithm (ECDSA). After the information is transmitted, the private key is, respectively, used to decrypt the information to ensure the security of the information transmission. The local generation key of the vehicle is K_1, P_1, and the server generates the key to K_2, P_2. The public key of the server is K_2 for local encryption through the asymmetric encryption algorithm, and the server uses the private key P_2 for decryption after transmission. Similarly, the data returned by the server are K_1 for encryption, and the local private key P_1 is for decryption.

Map data anonymous encryption process is shown in algorithm 1. When the system performs information up-chain behavior, it first compares the value of λ, and the data up-chain behavior is carried out in the safe range of λ. λ is the security parameter, each time through the risk cognition to change its value, and if the network is attacked, the security parameter will be appropriately reduced. During message transmission, the server public key K_1 is obtained, and then, the public key K_1 and the established access policy T are used to encrypt to obtain the ciphertext CTK. Finally, there are visible public keys and encrypted ciphertext exposed in the blockchain network, and then, data transmission is carried out. The specific implementation process is as follows: the user will first judge whether there is registered information in the blockchain when using it. If not, a new uniquely identified blockchain network ID will be created, and a new block will be established according to the blockchain network ID. In a complete driving process, this ID will serve as the only certificate for the vehicle to connect to the network. User data privacy information and map information at a certain time are encapsulated and encrypted with ECDSA, and the server decrypts and reads the data information through the private key. If the network is attacked, the attacker can only obtain the public key and decrypt it without the inverse operation of the private key, which effectively prevents the data information loss caused by key leakage. After each encryption, the data information and the time stamp at the moment establish the data ID so that the same network can distinguish the map data information of different time slices. When adding blockchain network data in a loop, only a matching user ID is needed to save authentication time cost.

3.2. Hazard Cognition Model Process. As shown in Figure 3(a), it is the traditional data processing process of the internet of vehicles, and 3(b) is the risk assessment model based on blockchain. The traditional way of processing internet of vehicles data is that the vehicle accesses the vehicle data platform server through the client, in which the vehicle management service analyzes the transmitted data and returns the safe operation data. The operation analysis process is monitored by the company and supervised by the government to ensure its safety. Risk assessment model based on blockchain, the vehicles to encrypt the data transmission, connected to the blockchain, through

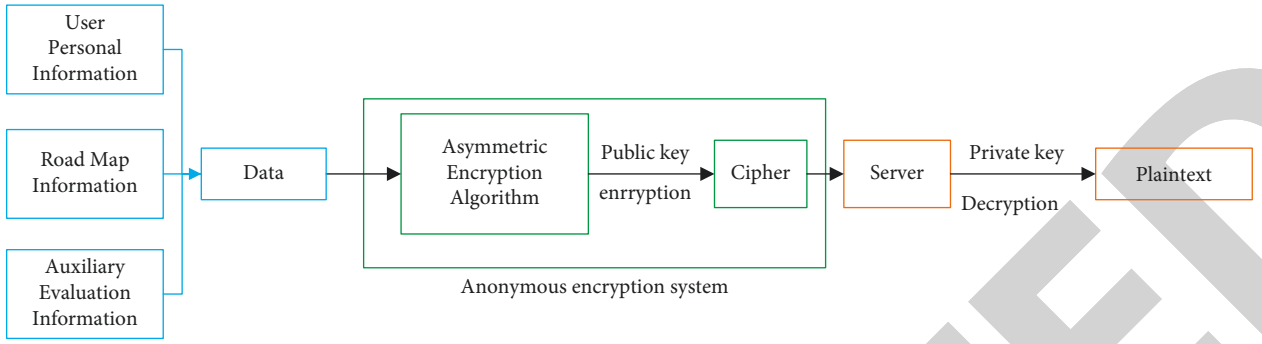

Figure 2: Anonymity of information on the chain structure diagram.

Input: λ,K_2, Person Information, Map Information
Output: The result of on-blockchain Y
(1) System executes:
(2) X_1 = person Information.ID
(3) X_2 = person Information + Map Information
(4) If X_1 is a new user then
(5) Add X_1 to Blockchain.ID
(6) Add X_2 id to Blockchain.Data.Id
(7) End if
(8) MData = EncryptedFile <— ECDSAencrypt (X_2, K_2, T)
(9) If X_1 is belong to Blockchain.ID
(10) Data < - (MData, K_2, T)
(11) Blockchain.Data = Blockchain.Data + Data
(12) End if
(13) Return true

Algorithm 1: Shows the process of map data anonymous encryption.

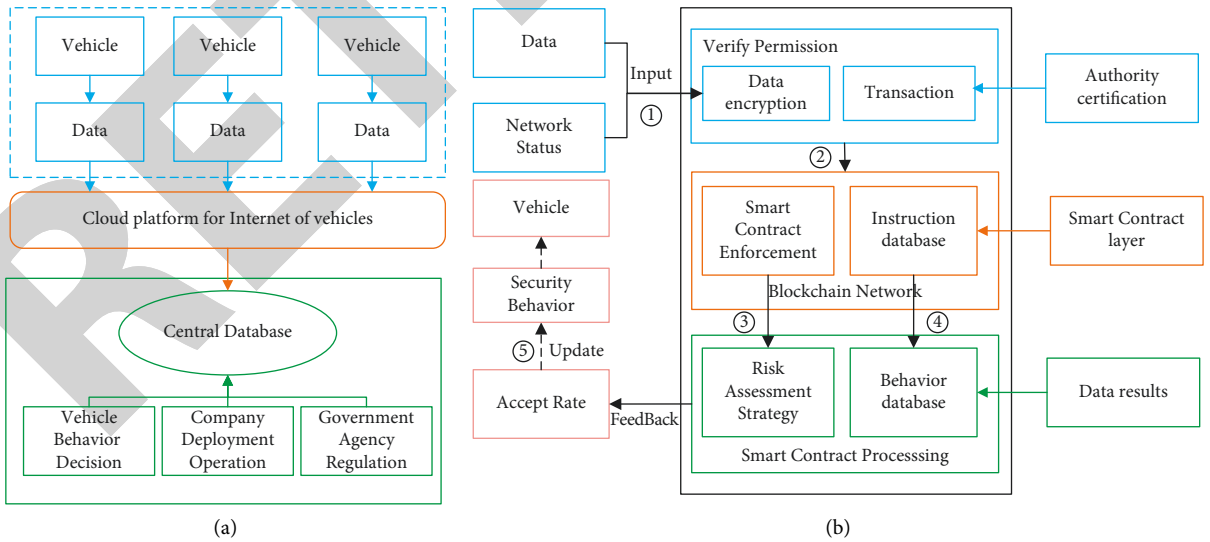

Figure 3: Comparison between traditional vehicle network validation model and risk assessment model. (a) Traditional data transmission model of internet vehicles. (b) Risk assessment model based on blockchain.

the deployment of intelligent contract evaluation analysis, is the main purpose of an intelligent contract according to different input data to judge the security of the network, data analysis, and get the current network risk value, according to the different risk-return value matching behavior database security operations.

```
Input: Blockchain.Data, P2
Output: Risk R, Network attack status attack
(1) ECDSADencrypt(Blockchain. Data, P2, T)
(2) for each Blockchain.Data do
(3) Change rate_Block = Blockchain.Data/Old data
(4) If the rate_block >0.5 then
(5)       If is tampered by communities
(6)           State = 0
(7)    End if
(8)    State = 1
(9) End if
(10) State = 0
(11) If the state = 0 then
(12) R= (Weather, road, speed, vehicle condition) × weight
(13)          Risk = state + R
(14) End if
(15) Return Risk, state
```

Algorithm 2: The execution process of smart contract.

There are two risk cognition modes in this model. The first one is that the vehicle is about to be in a dangerous driving state, and the obtained map information reveals that the vehicle is about to encounter danger. The second is that the information is tampered with during the process of the received map information being linked, which is caused by the network attacker attacking the blockchain. Blockchain has the characteristics of decentralization, and there is no centralized database modification method. If you want to modify the blockchain information, it needs to vote by the whole network nodes, it means attack most nodes in the whole network, and it costs heavy computational power. The automatically executed smart contract script regularly compares the on-chain data and information, compares the data processed by the previous model with the current data on nodes, and calculates the node modification rate. If the node modification rate is too high, it will be considered dangerous.

Algorithm 2 describes the process of contract execution. The input parameter is the encrypted data of vehicles that received in smart contract transaction, then the smart contract decrypts data to the plaintext through private key P2 and sends it to the neighboring node for consensus verification. Different nodes synchronously store vehicle data for transactions on the blockchain. The consensus algorithm supports node fault tolerance. If a transaction is not forwarded by the node after being sent, it is considered that a fault has occurred. In unit time, the failure rate of the network is too high, which means that there may be a large number of discredited nodes in the network. At this time, the model is assessed as a dangerous state. Finally, in the process of forming block detection nodes, the voting nodes are verified. Check whether the voting node in the system has a certificate issued by the system and has high reliability. Once a large number of nodes without certificates in the network request voting verification, it means that they are attacked, and the update status is dangerous. If the up-chain encryption process is deemed safe, the risk prediction is made for the data. According to the established prediction model, the weight of different input data is different, and then, the risk value of the map information is calculated by the method. Finally, according to the data status and cognitive value mapping, it is transferred to the local vehicle control.

3.3. Hazard Cognition Mapping Process. Algorithm 3, according to the smart numerical R contract process access to dangerous and network attack, from blockchain network access to the map information of the vehicle, according to the risk value and state of cyber-attacks, according to Table 2 mapping to convert the data for vehicle executable instruction, to ECDSA encrypted transmission of data, the local private key P_1 will be provided to decrypt data. The weight calculation cognitive data update the safety parameter λ, and the vehicle control is performed based on the returned vehicle behavior data.

4. Experimental Process and Results

4.1. Node Communication Mode. In the model experiment part, Hyperledger Fabric is used to build the blockchain platform, and the traditional PoW consensus protocol is not used, which reduces the waste of power caused by mining caused by consensus execution. The use of cryptocurrency will reduce the risk of the system. The practical Byzantine fault tolerance (PBFT) consensus is used in the test experiment at this stage. The performance and throughput are guaranteed under the premise of ensuring user data privacy. During the experimental testing phase, we completed the deployment of the private chain on the Fabric platform, and it needs to be authorized by the designated node before joining the node. PBFT uses cryptographic algorithms to ensure that message transmission between nodes is immutable. Encryption is used to prevent network attacks and detect corrupted messages. The transmitted message contains the public key signature, message validation code, and

Input: R,K
Input: Network attack status:Attack, Blockchain.Data.Id
Output: λ, action
(1) Get R from smart contract
(2) Ndata < -Blockchain.Data
(3) If $R \geq 0.4$ do
(4) Action = Change (λ, Ndata)
(5) Data = Ndata + Action
(6) $\text{ECDSA}_{\text{Encrypt}}$(Data, K_1, T)
(7) End if
(8) Data = $\text{ECDSA}_{\text{Dencrypt}}$(Blockchain.Data, P_1, T)
(9) λ = Update (Data)×weight
(10) Return directives, λ

Algorithm 3: Three hazard cognition mapping.

Table 2: Hazardous behavior mapping.

Risk value	State	Acceleration	Behavior
0–0.2	Start	$a = +s/v$	Speed up
0.2–0.4	Normal	$a = 0$	Keep
0.4–0.6	Wave	$a = \pm s/v$	Speed up/slow down
0.6–0.8	Hazards	$a = -s/v$	Slow down
0.8–1	Dangerous	$a = -\max$	Brake

message digest generated by the hash function. If there are n nodes in the system, the maximum number of evil/failure nodes that the system can tolerate is (N-1)/3. Evil nodes cannot respond or respond to wrong information to ensure the stability and security of the system. Under the consensus mechanism PBFT model, a master node is first selected to have the billing right, and other nodes are used as backup nodes. All nodes in the system communicate with each other and eventually reach a consensus based on the principle of majority rule. If the billing node misbehaves, other nodes will band together to replace the billing node. The model then diffuses the modified blockchain to the participating nodes of the network through the gPRC messaging mechanism. Two-thirds of the nodes agree that the message is true. The gPRC communication mechanism in the blockchain diffuses messages in this blockchain to other participant nodes. When the data are transmitted, the node transmitting the data acts as the client and the other nodes act as the server, and the data of the vehicle node are transmitted through the http protocol, which will save electricity and space through gPRC.

4.2. Data Up-Chaining and Throughput Performance Comparison. Vehicle users apply for joining node authority through Fabric and then save node ID and relevant personal and vehicle information for vehicle registration. Then, the model collects the road pictures through the on-board camera and classifies the road pictures by the deep learning algorithm. At the same time, the road environment information and obstacle information are determined by the lidar, and the positioning data are obtained by combining with the inertial navigation system to accurately locate the vehicle.

As can be seen from Figure 4, it compares the transaction speed of 1, 10, 50, and 100 peers to determine throughput. For different cognitive transactions, the average throughput of different miners is as follows: with the increase in the number of joined miners, the number of nodes in the blockchain network that need to forward updated information increases, and the higher number of nodes causes a decrease in the throughput of the network cognitive model. By comparing 1,000 cognitive transactions executed by a single peer, it can be seen that as the number of cognitive transactions increases, the throughput growth rate will also decrease. Thus, as the number of blockchain construction transactions increases, the average throughput of the blockchain network will become constant.

4.3. Hazard Scenario Prediction Process and Results. After the vehicle data node is transmitted to the base station node, the intelligent contract code is executed to evaluate the risk value of the data, the mapping relationship is established according to the mapping part of the global centralized table, and the corresponding safe operation is found according to the value. Finally, the acceleration, deceleration, and parking activities are realized according to the safe operation.

In the experiment, the tool Simulink of MATLAB was used to create virtual vehicles, and cars, trucks, and buses were used for comparative experiments. The fixed map scene was selected to carry out normal vehicle operation, and the time and model cognitive results were recorded. Then, the scene is simulated and predicted. Scenario 1: the network is attacked, in the process of vehicle running blockchain network access to calculate force higher equipment to cognize the vehicle to calculate force attack, and high

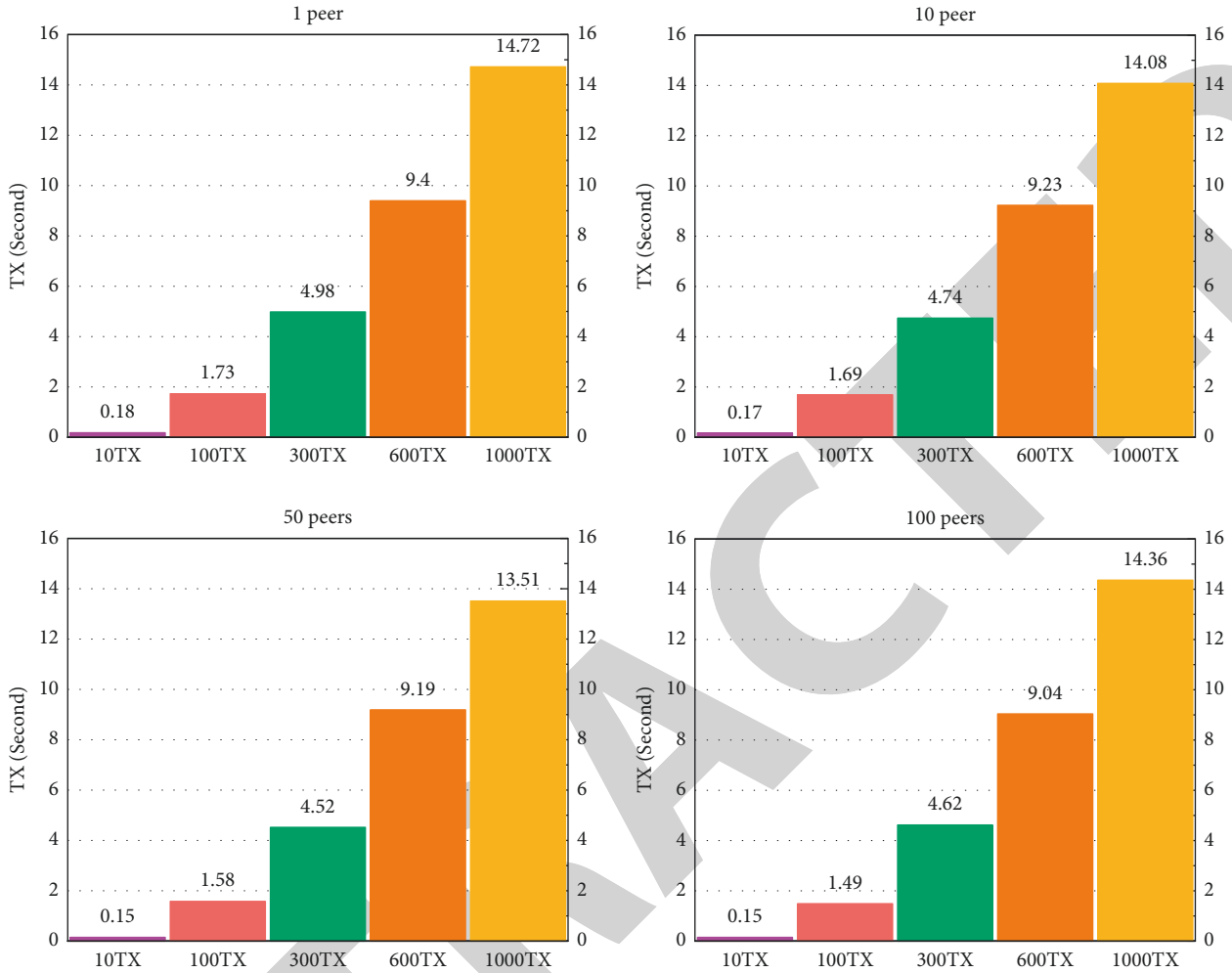

Figure 4: Throughput performance comparison under different peers.

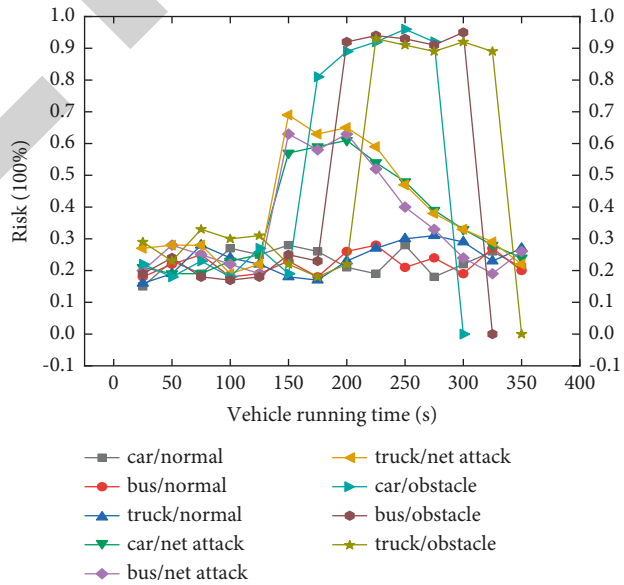

Figure 5: Diagram of the variation of hazard value over time under.

workforce that leads to a chain speed test vehicles will be blockchain cover to modify the data, through the network attack test model to cognize the effect. Scenario 2: it is the environmental hazardous state. Obstacles are added to the map of the normal operating environment of vehicles so that the vehicles can perceive the data of dangerous environment to test the cognitive effect of the model.Different dangerous situations in the same road section.

Figure 5 is the simulation of three types of vehicles in the risk value of different scene graph, and the change in the three types of vehicle curve trend is roughly the same. After the attack, the vehicle brake to avoid risk is the risk value is zero speed for the car is faster than the truck, the truck is faster than the bus, and the greater the reason for the quality of vehicle in large inertia, the time needed for the vehicle to slow down or brake is a bit long. According to the curve transformation comparison results, the risk value of the vehicle rapidly increases after the network attack, the risk value is judged as a dangerous state, and the vehicle stops running. The danger value of the vehicle in the obstacle situation increases. The vehicle state changes to the risk state, and the vehicle slows down to avoid the obstacle and returns to the normal state. The experimental results show that the model can make good prediction under different dangerous scenarios in the same road map and can cognize the network attack and environmental risk and avoid the risk.

5. Conclusions

In this study, a dangerous driving map cognitive model based on smart contract is proposed to predict and analyze the dangerous driving situation in the data interaction process of the internet of vehicles through malicious attacks. The model mainly recognizes the personal information and data generated by intelligent vehicles in the process of driving. Smart contract technology can not only ensure the security of data transmission and prevent data from being tampered with but also prevent network attacks and illegal tampering. The accuracy of data is ensured through the up-chain transmission of data, and the risk cognition model carries out cognitive assessment on the transmitted data. In the process of data transmission, the intelligent car can conduct emergency treatment under the influence of road and network dangers and ultimately ensure the safety of data. The intelligent contract is constructed into independent modules by applying general set theory to the design model. There are only data input and output between models. New functions can be established by modifying independent modules through design, which enhances the universality and robustness of the model. In this study, there is only a little way to map data in a single vehicle to carry on the risk cognition, and no multivehicle cognitive model is set up. In the future work, we try to access more intelligent vehicle cognition, and at the same time, using machine learning algorithm optimizes the risk cognition, through the design algorithm for the vehicle that can adaptively map to cognize different dangerous situation forecast road environment.

Data Availability

The datasets used and/or analyzed during the current study are available from the corresponding author on reasonable request.

Conflicts of Interest

The author(s) declare no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (grant nos. 62102033, 61871039, 62171042, 62006020, and 61906017), the Beijing Municipal Commission of Education Project (no.KM202111417001 and KM201911417001), the Collaborative Innovation Center for Visual Intelligence (grant no. CYXC2011), and the Academic Research Projects of Beijing Union University (no. BPHR2020DZ02, ZB10202003, ZK40202101, and ZK120202104).

References

[1] X. Yang and L. Zhong, "Identity authentication scheme based on vehicle behavior prediction in internet of vehicles," *Computer Engineering*, vol. 47, no. 1, pp. 129–138, 2021.

[2] F. Jameel, M. A. Javed, S. Zeadally, and R. Jäntti, "Efficient mining cluster selection for Blockchain-based cellular V2X communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, pp. 4064–4072, 2020.

[3] T. Cai, H. Lin, W. Chen, Z. Zheng, and Y. U. Yang, "Blockchain-enabled efficient IoT data incentive sharing scheme," *Journal of Software*, vol. 32, no. 4, pp. 953–972, 201.

[4] T. Liu, C. Xu, H. Liu, X. Li, and P. Wang, "A vehicle detection model based on 5G-V2X for smart city security perception," *Wireless Communications and Mobile Computing*, vol. 2021, 11 pages, Article ID 5237568, 2021.

[5] C. Xu, H. Wu, Y. Zhang, S. Dai, H. Liu, and J. Tian, "A real-time complex road AI perception based on 5G-V2X for smart city security," *Wireless Communications and Mobile Computing*, vol. 2022, 11 pages, Article ID 4405242, 2022.

[6] H. Huang, X. Chen, and J. Wang, "Blockchain-based multiple groups data sharing with anonymity and traceability," *Science China Information Sciences*, vol. 63, pp. 1–13, 2020.

[7] C. Xu, H. Wu, H. Liu, X. Li, L. Liu, and P. Wang, "An intelligent scheduling access privacy protection model of electric vehicle based on 5G-V2X," *Scientific Programming*, vol. 2021, 11 pages, Article ID 1198794, 2021.

[8] Y. Xu and Y. Huang, "Segment blockchain: a size reduced storage mechanism for blockchain," *IEEE Access*, vol. 8, pp. 17434–17441, 2020.

[9] Z. Zheng, J. Pan, and L. Cai, "Lightweight blockchain consensus protocols for vehicular social networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5736–5748, 2020.

[10] S. F. Wamba and M. M. Queiroz, "Blockchain in the operations and supply chain management: b," *International Journal of Information Management*, vol. 52, Article ID 102064, 2020.

[11] X. Li and R. Zhang, "Innovation research promots the development of key technologies in smart beijing," *Journal of Beijing Union University: Humanities and Social Sciences*, vol. 18, no. 3, pp. 1–10, 2020.

[12] B. Meng, J. Liu, Q. Liu, X. Wang, X. Zheng, and D. Wang, "Review of smart contract security," *Journal of Network and Information Security*, vol. 6, no. 3, pp. 1–13, 2020.

[13] Y. Sun, Y. Bi, Y. Han, and D. Xie, "Research on safe driving behavior of transportation vehicles based on vehicle network data mining," *Transactions on Emerging Telecommunications Technologies*, vol. 31, Article ID e3772, 2020.

[14] H. Zhang, R. Wang, W. Sun, and H. Zhao, "Mobility management for blockchain-based ultra-dense edge computing: a deep reinforcement learning approach," *IEEE Transactions on Wireless Communications*, vol. 20, no. 11, pp. 7346–7359, 2021.

[15] H. Xiao, W. Zhang, W. Li, A. T. Chronopoulos, and Z. Zhang, "Joint clustering and blockchain for real-time information security transmission at the crossroads in C-V2X networks," *IEEE Internet of Things Journal*, vol. 8, pp. 13926–13938, 2021.

[16] C. Xu, H. Luo, H. Bao, and P. Wang, "STEIM: a spatio-temporal event interaction model in V2X systems based on a time period and a raster map," *Mobile Information Systems*, vol. 2020, 20 pages, Article ID 1375426, 2020.

[17] G. S. Aujla, A. Singh, M. Singh, S. Sharma, N. Kumar, and K.-K. R. Choo, "BloCkEd: blockchain-based secure data processing framework in edge envisioned V2X environment," *IEEE Transactions on Vehicular Technology*, vol. 69, pp. 5850–5863, 2020.

[18] I. Agudo, M. Montenegro-Gómez, and J. Lopez, "A blockchain approach for decentralized V2X (D-V2X)," *IEEE Transactions on Vehicular Technology*, vol. 70, pp. 4001–4010, 2020.

[19] Z. Cui, X. Fei, S. Zhang et al., "A hybrid BlockChain-based identity authentication scheme for multi-WSN," *IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 241–251, 2020.

[20] P. K. Singh, R. Singh, S. K. Nandi, K. Z. Ghafoor, and D. B. Rawat, "Blockchain-based adaptive trust management in internet of vehicles using smart contract," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3616–3630, 2021.

[21] L. Ji, G. Zhang, and J. Yang, "Blockchain-based off-chain personal data protection scheme," *Computer Engineering*, vol. 47, no. 2, pp. 176–181+187, 2021.

[22] C. Zhang, L. Zhu, C. Xu, and K. Sharif, "PRVB: achieving privacy-preserving and reliable vehicular crowdsensing via blockchain oracle," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 1, pp. 831–843, 2020.

[23] Y. Liu, M. Xiao, S. Chen, F. Bai, J. Pan, and D. Zhang, "An intelligent edge-chain enabled access control mechanism for IoV," *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 12231–12241, 2021.