electronics

MDPI

Article

Access Control Strategy for the Internet of Vehicles Based on Blockchain and Edge Computing

Leixiao Li [1,2,3], Jianxiong Wan [1,2,3] and Chuyi Liu [1,2,3,*]

[1] College of Data Science and Applicatioon, Inner Mongolia University of Technology, Hohhot 010062, China; lileixiao@imut.edu.cn (L.L.); jxwan@imut.edu.cn (J.W.)
[2] Inner Mongolia Autonomous Region Engineering, Technology Research Center of Big Data Based Software Service, Hohhot 010062, China
[3] Research Center of Large-Scale Energy Storage Technologies, Hohhot 010062, China
* Correspondence: lcy@imut.edu.cn

Abstract: Data stored in the Internet of Vehicles (IoV) face problems with ease of tampering, easy disclosure and single access control. Based on this problem, we propose an access control scheme for the IoV based on blockchain, trust values and weighted attribute-based encryption, called the Blockchain Trust and Weighted Attribute-Based Access Control Strategy (BTWACS). First, we utilize both local and global blockchains to jointly maintain the generation, verification and storage of blocks, achieving distributed data storage and ensuring that data cannot arbitrarily be tampered with. Local blockchain mainly uses Road Side Unit (RSU) technology to calculate trust values, while global blockchain is mainly responsible for data storage and access policy selection. Secondly, we design a blockchain-based trust evaluation scheme called Blockchain-Based Trust Evaluation (BBTE). In this evaluation scheme, the trust value of the vehicle node is based on four factors: initial trust, historical experience trust, recommendation trust and RSU observation trust. CRITIC is used to determine the optimal weights of four factors to obtain the trust value. Then, we use the Network Simulator version 3 (NS3) to verify the security and accuracy of BBTE, improving the recognition accuracy and detection rate of malicious vehicle nodes. Finally, by mining the association relationships between attribute permissions among various roles, we construct a hierarchical access control strategy based on weight and trust, and further optimize the access strategy through pruning techniques. The experiment results indicate that this scheme can effectively respond to gray hole attacks, defamation attacks and collusion attacks from other vehicle nodes. This method can effectively reduce the computing and transmission costs of vehicles and meet the access requirements of multiple entities and roles in the IoV.

Keywords: Internet of Vehicles; blockchain; edge computing; trust computing; access control; malicious attacks; attributes based on encryption

Citation: Li, L.; Wan, J.; Liu, C. Access Control Strategy for the Internet of Vehicles Based on Blockchain and Edge Computing. *Electronics* **2023**, *12*, 4057. https://doi.org/10.3390/electronics12194057

Academic Editor: Jianer Zhou

Received: 13 August 2023
Revised: 25 September 2023
Accepted: 25 September 2023
Published: 27 September 2023

1. Introduction

The Internet of Vehicles (IoV) uses wireless communication technology to share information between vehicles, which helps to achieve automatic driving and maintain traffic safety [1,2]. IoV uses Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) for communication [3]. The interactive information mainly includes road congestion, moving tracks, traffic accidents and entertainment consultation to create a safe and comfortable driving environment [4]. In order to prevent criminals from eavesdropping on and tampering with information, which may endanger the traffic system, information interaction must ensure the integrity and security of data, otherwise the system is vulnerable to malicious attacks, including replay, camouflage, message tampering attacks, etc. [5]. Therefore, the information resources in the IoV must be controlled to prevent unauthorized access and ensure the safe sharing of information resources. The goal of this paper is to build a more effective access control scheme to improve the security of IoV's information sharing.

Due to the widespread distribution and mobility of vehicles, it is difficult to expand the current centralized cloud model of the IoV system through a large number of weak devices, and it is difficult to meet the flexible access control requirements of multiple entities and roles in IoV [6]. In addition, the communication distance between IoV devices and the cloud is relatively long, which may consume a lot of bandwidth, time and energy. Cloud servers are the bottleneck of the current IoV network. A centralized server has a defect of single point failure, that is, a server failure will disrupt the entire network. On the other hand, blockchain is characterized by having distributed storage and being tamper proof, which can allow the realization of a trusted decentralized environment and provide a system with tamper resistance, traceability, fault tolerance and automatic execution strategies [7]. Thus, we utilize local blockchains (maintained by Road Side Units) [8] and global blockchains (maintained by trusted centers) to build an IoV network environment, with the goal of promoting secure access control for IoV and jointly addressing key challenges.

We proposed the Blockchain Trust and Weighted Attribute-Based Access Control Strategy (BTWACS) for controlling the access of IoV based on secure access. A trust evaluation mechanism, Blockchain-Based Trust Evaluation (BBTE), is introduced. BBTE takes into account four factors—initial trust, historical experience trust, recommendation trust and RSU observation trust—and is more comprehensive and efficient. It improves the accuracy and speed of identification of malicious nodes. A simulation environment is constructed to test the performance of the algorithm and compare it to other algorithms.

In sum, the main contributions of this paper are threefold:

- We propose BBTE, a trust evaluation mechanism that can identify malicious nodes faster and more accurately than other mechanisms.
- We propose the BTWACS, an IoV networking access control strategy that can make the communication process between nodes in the IoV safer, faster and more efficient.
- Extensive simulation studies are conducted to evaluate the effectiveness of the proposed strategy. Numerical results show that our strategy outperforms existing algorithms in terms of encryption and decryption efficiency and in the size of cipher-text.

The rest of the paper is organized as follows. Section 2 reviews the related literature. Section 3 describes the proposed trust evaluation method, BBTE. Section 4 presents the IoV access control strategy, the BTWACS. Section 5 details the experiment and the numerical studies. Section 6 concludes the paper.

2. Related Work

2.1. The Application of Blockchain in the Access Control of the IoV

The blockchain's own traceability, tamper-proof ability and anonymity, as well as other characteristics, can serve as a trusted third party in the access control of the IoV. Blockchain provides trusted computing and storage. It can not only store important data but can also use its computing power for access control decisions. The combination of blockchain technology and the IoV has become one of the current main research fields.

Since the 1970s, many access control methods have been implemented, such as Role-Based Access Control (RBAC) [9,10], Attributes-Based Access Control (ABAC) [11], Capability-Based Access Control (CapBAC) [12], etc. RBAC is a static model, which makes it difficult to adapt to frequent changes in IoV devices. For example, Cruz et al. [13] implemented role-based access control through smart contracts, but it required the maintenance of a large number of roles and authorization relationships, resulting in a heavy workload for administrators. Liu et al. [14] proposed ABAC for on-chain data, constructing a hierarchical access control strategy based on multiple attributes, implementing weighted attribute-based encryption and simplifying the complexity of access control strategies. However, without the trust evaluation of vehicle nodes, it is impossible to control the credibility of vehicles. Nakamura et al. [15] proposed CapBAC and used Ethereum smart contracts to store and manage capability tokens, which are special data structures for maintaining user-allowed actions for specific resources. But BAC focuses more on solving the dynamic network topology problem of IoV. These schemes lack evaluation abilities for malicious

nodes and for the consideration of the reliability of on-chain data; attackers may send false or incorrect information. Thus, the reliability and security of data cannot be guaranteed.

2.2. Trust Computing

The IoV has high dynamism, and messages propagate between adjacent moving vehicles, making it susceptible to malicious attacks and security threats. Malicious vehicle nodes sending false or incorrect information in information exchange may lead to traffic congestion, even traffic accidents, and may threaten the safety of car owners' lives and property. To ensure the safe transmission of data between vehicle nodes and enable vehicle owners to make correct decisions based on reliable information, it is necessary to evaluate the trust of communication objects before exchanging messages between vehicles to ensure the reliability of information.

Existing trust management methods evaluate the trust value of vehicle nodes based on collecting and analyzing a large amount of the node's historical behavior and other data. Due to the high mobility of vehicles in the IoV, the interaction between vehicles is transient, and it is necessary to quickly and accurately identify malicious nodes to prevent malicious attacks and spread false information in the network to avoid traffic accidents. The trust management mechanism can effectively identify the level of trust of nodes. The higher the trust value, the more trustworthy the messages published by nodes. Chen et al. [16] constructed a data-sharing system consisting of a double-layer blockchain. In order to prevent malicious nodes from spreading false messages, a reasonable trust evaluation scheme was designed that evaluates the service quality of different providers by combining negative and positive shared records. Kang et al. [17] proposed an IoV data-sharing system based on federated blockchain, which utilizes a three weight subjective logic model to accurately manage the trust values of vehicles. Vehicles choose the best data provider based on trust values to choose more reliable data sources and improve data credibility. At present, many research works have discussed the problem of node safety improvement in the IoV. In reference [18], Zhang et al. used the blockchain to define the IoV framework. In a complex vehicle environment, considering the trust characteristics of blockchain nodes and the number of consensus nodes, the authors achieved node consensus based on the Practical Byzantine Fault Tolerance (PBFT) [19] to ensure node security. In reference [20], Yang et al. proposed a decentralized trust management system for a vehicle network based on blockchain technology, deployed smart contracts [21] on the vehicle blockchain, calculated the trust value of related vehicles on a Road Side Unit (RSU) based on the Proof of Work (PoW) [22] and cooperated in maintaining and updating the trust blockchain to achieve secure data sharing.

However, the above trust models cannot effectively resist various malicious attacks in all cases. Access control mechanisms based on trust management are still a hot topic in current research.

2.3. Cipher-Text Policy Attribute-Based Encryption

Cipher-Text Policy Attribute-Based Encryption (CP-ABE) is an encryption technology with fine-grained access control. It associates cipher-text with access control policies and can decrypt cipher-text only when the attributes of the data visitor meet the access control policies. This technology can flexibly control the attribute set of data visitors by changing the access control strategy structure, which is particularly suitable for a network environment where IoV nodes move at high speed and the topology changes rapidly. However, the more attributes in the access control policy, the higher its complexity. The encryption and decryption cost increases linearly with the increase in policy complexity, which has the drawback of a high computational cost.

CP-ABE can be used to formulate access control policies, which is convenient and flexible and is considered an effective access control method. The key is related to the attribute set, and the cipher-text is related to the access structure. Only when the attribute

set matches the access structure can the cipher-text be successfully decrypted to plaintext, thereby achieving fine-grained access control for IoV data.

Porwal et al. adopted a combination of a CP-ABE scheme and a multi-chain platform to achieve easy and secure access control in an efficient, fine-grained, transparent and traceable manner [23]. However, the different types of entities in the IoV result in a large number of attributes involved in access policies, leading to a higher complexity of access control policies. Therefore, Liu et al. [14] proposed a weight-based access control strategy. It is different from that which Oham et al. [24] proposed, which divides regions based on the organization in advance, and is different from the density-based access strategy proposed by Kanumalli et al. [25]. The weight-based access control strategy does not require the identification of data visitors in advance and can flexibly formulate access control strategies. By mining the association of attribute permissions between different roles, it simplifies the complexity of access control policies and can access IoV data more efficiently.

3. Trust Evaluation Method

The purpose of trust assessment is to evaluate the trust value of vehicle nodes by collecting behavioral state information, and quickly and accurately identifying malicious vehicle nodes in the IoV. Using trust values as a basis for establishing communication, we can effectively respond to various attacks. BBTE comprehensively considers four core decision-making factors: initial trust, historical trust, recommendation trust and RSU observation trust. Next, we will introduce these four factors one by one.

3.1. Initial Trust

The vehicle stores some basic safety information in the Trusted Platform Module (TPM) [26], which includes the basic safety attributes of the vehicle, such as vehicle type, factory years, user information, digital certificates, etc. We can decompose the attribute information that affects vehicle safety performance into m indicators based on the system security strategy. The corresponding system security correlations are $S_i \in [0,1](i = 1,2,\ldots)$. We can then assign weights to them. The initial trust of the vehicle is

$$IT = \sum_{i=1}^{m} \omega_i s_i \tag{1}$$

The basic safety attributes of vehicles may change with movement. Therefore, to ensure the authenticity of basic safety attributes, the vehicle will periodically calculate and update its basic safety attributes through RSU. After being verified by the RSU, it is stored in a distributed manner on the blockchain built by the RSU.

3.2. Historical Trust

Historical trust, also known as experiential trust, is established based on the historical interaction records of both parties. Due to the dynamic real-time nature of IoV, the time period of interaction needs to be taken as the calculation factor. The calculation formula for node historical trust is as follows:

$$HT(i,j) = \sum_{i=1}^{m} \frac{2e^{-\Delta t_i/r} SF_i}{e^{\Delta t_i/r} + e^{-\Delta t_i/r}} ES_{ij} \tag{2}$$

where SF_i is the weight of information resources, which is based on the correlation between information resources and security; m is the number of historical interactions of vehicles i and j; $\triangle t_i$ is the difference between the current time and the access time; the larger the Δt_i, the smaller the weight; r is set according to the time unit; and ES_{ij} represents the trust evaluation of the message receiver j towards the sender i.

For the convenience of calculation, we set the total weight to 10. Because traffic safety is the most important attribute in the IoV, we classify and determine the weight according to the correlation between information and security. Therefore, the weight of strong safety

information is the highest, accounting for half of the total, set to 5. The weight of non-safety-related information is the lowest, set to 2, and the weight of safety-related information is in the middle, set to 3. The classification of information resources in the IoV is shown in Table 1.

Table 1. The classification of trust value weight.

Information Classification	Example	Weight
Strongly safety-related	Collision warning, emergency braking, vehicle out of control, anchoring	5
Safety-related	Emergency vehicle yield, double flash, whistle	3
Non-safety-related	ETC, location services, information services	2

3.3. Recommendation Trust

When there is less or even no information interaction between vehicle nodes, the node needs to collect multiple recommendation nodes to calculate recommendation trust. The criteria for determining credibility vary depending on the type of recommendation node. Therefore, according to the degree of association between recommendation nodes k and evaluation nodes i, we divide them into three categories and calculate their respective recommendation trust. CRITIC [27] is used to determine the optimal weight of various types of recommendation trust. It multiplies different recommendation trust values with corresponding weights, incoming plus and, namely, for the final recommendation trust value, TR_{ij}.

3.3.1. Direct Recommendation Trust

We define recommendation nodes k that have had direct interaction with evaluation nodes i as direct recommendation nodes. The trust value of evaluation nodes towards such recommended nodes TD_{ik} can be directly used as their relationship credibility. The direct recommended trust is calculated as follows:

$$TR^d(i,j) = \sum_{i=1}^{m} \frac{C_{ik}M_{ik}}{\sum_{k=1}^{m} C_{ik}M_{ik}} TD_{ik} \tag{3}$$

where C_{ik} refers to the trust level of the recommendation trust given by the evaluation node i to the recommendation node k, $C_{ik} \in [0,1]$; m refers to the number of direct recommendation nodes; and M_{ik} refers to the number of interactions between the node i and the direct recommendation node k.

3.3.2. Indirect Recommendation Trust

We define recommendation nodes k that have had indirect interaction with evaluation nodes i as indirect recommendation nodes. The traditional recommended trust model takes the trust value of the node as the weight, as shown in Equation (4).

$$TR(i,j) = \sum_{k=1}^{m} TR(i,j)TR(k,j) \tag{4}$$

where $TR(i,j)$ indicates the trust value of node i towards node k. The higher the trust value, the more important its recommendations are. However, this mechanism ignores the possibility of collusive attacks and defamation attacks. If malicious nodes obtain high trust values through disguise, they will spread false information to normal nodes. TSMRP [28] uses the cosine similarity function to calculate the recommended trust value, but does not fully consider the difference between the information values. Based on this issue, we use the Pearson correlation coefficient to describe the difference between two views on the same question. The successful interaction score of vehicle node i on m nodes over a

period of time t is $[r_{a1}, r_{a2}, \cdots, r_{am}]$, and the scores of vehicle node k on these m nodes is $[r_{o1}, r_{o2}, \cdots, r_{om}]$. The similarity scores equation for node i to node k is

$$P(i,k) = \frac{\left|\sum_{j-1}^{m} r_{aj} r_{oj} - \sum_{j-1}^{m} r_{aj} \sum_{j-1}^{m} r_{oj}\right|}{\sqrt{\sum_{j-1}^{m} (r_{aj})^2 - \left(\sqrt{\sum_{j-1}^{m} r_{aj}}\right)^2} \sqrt{\sum_{j-1}^{m} (r_{oj})^2 - \left(\sqrt{\sum_{j-1}^{m} r_{oj}}\right)^2}} \tag{5}$$

where the higher the value, the higher the score similarity between the two nodes, which means that when the score to other nodes in the network is more consistent, the calculation of indirect recommendation trust is as follows:

$$TR^{in}(i,j) = \sum_{k=1}^{m} p(i,k) TR(k,j) \tag{6}$$

3.3.3. Strange Recommendation Trust

We define recommendation nodes k that do not have interactions with evaluation nodes i as strange recommendation nodes. The evaluation trust level of the evaluation node towards this type of recommendation node is tru_i. We introduce feedback satisfaction FC_i to prevent defamation attacks, $FC_i \in [0,1]$. If $FC_i < 0.5$, the recommendation node is considered untrusted, and its recommendation trust will be discarded; otherwise, it is considered to be reliable. The filtered recommended trust set $B = [tru_1, tru_2, \cdots, tru_N]$. The strange recommendation trust is calculated as follows:

$$TR^{u}(i,j) = \frac{\sum_{i=1}^{N} tru_i}{N} \tag{7}$$

3.3.4. Final Recommendation Trust

TSMRP [28] used the fuzzy analytic hierarchy process based on the Entropy Method to determine the optimal weight of three types of recommendation trust but did not consider the correlations between data. We use CRITIC to determine the optimal weight. CRITIC is a better objective weighting method, which is calculated based on the volatility of data or the correlations between data [27]. n represents the number of vehicle node samples, and m represents the number of evaluation indicators of recommended trust. As above, the evaluation indicators of recommendation trust in this paper are direct, indirect and strange recommendation trust, that is, $m = 3$, forming the original indicator data matrix, as follows:

$$X = \begin{pmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{m1} & \cdots & x_{mn} \end{pmatrix} \tag{8}$$

where x_{ij} represents the numerical value of the ith sample for the jth evaluation indicator.

1. Dimensionless Processing

To eliminate the impact of different dimensions on the evaluation results, it is necessary to perform dimensionless processing on each indicator. The larger the value of the indicator used the better (using positive indicators).

$$\hat{X}_{ij} = \frac{x_j - x_{min}}{x_{max} - x_{min}} \tag{9}$$

2. Indicator Variability

The fluctuation of the internal values of each indicator is represented in the form of standard deviation. The larger the standard deviation, the stronger the evaluation strength of the indicator itself, and the indicator should be assigned more weights:

$$\begin{cases} \overline{x}_j = \frac{1}{n}\sum\limits_{i=1}^{n} x_{ij} \\ s_j = \sqrt{\frac{\sum\limits_{i=1}^{n}\left(x_{ij}-\overline{x}_j\right)^2}{n-1}} \end{cases} \tag{10}$$

where s_j is the standard deviation of jth evaluation indicator.

3. Indicator Conflict

The correlation coefficient is used to represent the correlation between indicators. The stronger the correlation with other indicators, the less conflicting it is with other indicators. The more information it reflects, the more repetitively the evaluation content can be reflected. Therefore, the weight assigned to this indicator should be reduced:

$$R_j = \sum_{i=1}^{m}\left(1 - r_{ij}\right) \tag{11}$$

where r_{ij} is the correlation coefficient between evaluation indicators i and j.

4. Amount of Information

$$C_j = S_j \times R_j = S_j \sum_{i=1}^{m}\left(1 - r_{ij}\right) \tag{12}$$

The larger the value of C_j, the greater the role of the jth evaluation indicator in the entire evaluation indicator system, and more weights should be assigned to it.

5. Weight

$$\omega_j = \frac{C_j}{\sum_{j=1}^{m} C_j} \tag{13}$$

We can calculate the weight assigned to each evaluation indicator through the method of weighted summation. From this, we can obtain the weights of direct, indirect and strange recommendation trust, ω_1, ω_2 *and* ω_3, respectively. The total recommendation trust is calculated as follows:

$$TR_{i,j} = \omega_1 TR_{i,j}^{d} + \omega_2 TR_{i,j}^{in} + \omega_3 TR_{i,j}^{u} \tag{14}$$

3.4. RSU Observation Trust

RSUs can act as observers to detect the behavior status of vehicles for trust evaluation and can transmit vehicle trust in real-time between RSUs. The relevant trust attributes of a vehicle are $\lambda_i = [\lambda_1, \lambda_2, \cdots, \lambda_k]$. Different trust attributes play different roles in credibility calculation, so it is necessary to assign different trust weights to each trust attribute, which can be expressed as $\varphi_i = [\varphi_1, \varphi_2, \cdots, \varphi_k]$, $\sum_{i=1}^{k} \varphi_i = 1$. The observation trust of a vehicle is

$$RT_i = \sum_{i=1}^{k} \varphi_i \lambda_i \tag{15}$$

RSUs are usually semi-trusted because they are distributed on the road without any strong security measures and are vulnerable to attacks from attackers. To ensure the authenticity and credibility of the RSUs, we conduct positive and negative evaluations on the RSUs to obtain a set of trusted RSUs, and then give a true and credible recommended

trust value of the RSU according to the RSU stage trust and the latest trust value of the RSU. a^+ is a positive rating given by the vehicle to the RSU, and a^- is a negative rating. θ_n is the trust judgment for the nth RSU:

$$\theta_i = \frac{\theta_1 a^+ - \theta_2 a^-}{a^+ + a^-} \tag{16}$$

$\theta_n = [-1, 1]$, θ_1 and θ_2 are the weights of a^+ and a^-, respectively.

$$\theta_1 = \frac{F(a^+)}{F(a^+) + F(a^-)} \tag{17}$$

$$\theta_2 = \frac{F(a^1)}{F(a^+) + F(a^-)} \tag{18}$$

where $F(*)$ is the sensitivity to scoring. From Equation (16), it can be seen that the ratios of negative scores and different $F(*)$ will both affect the trend of θ_n changes. According to the consideration of time complexity and space complexity, within the range of error selection, $F(x) = x$, $F(x) = x^2$, $F(x) = x^3$, $F(x) = x^4$, $F(x) = e^x$ and $F(x) = e^{2x}$ are used to evaluate the impact of $F(*)$ on θ_n, as shown in Figure 1. When the negative score ratio is less than 50%, $F(x) = x^4$ is higher than other functions. This proves that a small proportion of the negative score has a small impact on the evaluation results, which is consistent with the evaluation results of most vehicles.

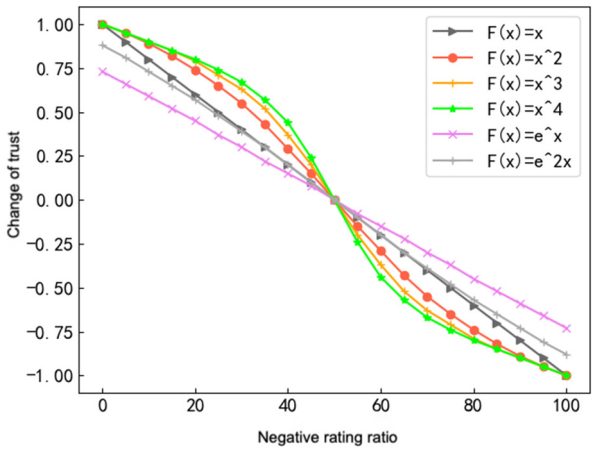


Figure 1. Changes in trust with the ratio of negative ratings under the $F(*)$.

.

Therefore, we choose $F(x) = x^4$ to control the change of trust θ_n in RSU. When the trust level of RSU is lower than the lower limit, it is considered untrustworthy. For the next moment, the RSU is removed from the trusted set and does not need to be recognized again, which improves the efficiency. From the vehicle entering the nearby RSU communication range until its exit, the RSU observes the behavior status of the vehicle and calculates the phase trust value of the vehicle and uploads it to the blockchain constructed by the RSU to update the trust value list, as shown in Table 2.

Table 2. RSU trust value update list.

RSU_{ID}	Stage Trust Value	Latest Trust Values	Time Period
RSU_1	RT_{D1}	RT_{R1}	$t_1 \sim t_2$
RSU_2	RT_{D2}	RT_{R2}	$t_2 \sim t_3$
...	...	...	...
RSU_n	RT_{Dn}	RT_{Rn}	$t_n \sim t_{n+1}$

The RSU observation trust value of the updated target node is calculated as follows:

$$RT_{Rn} = RT_{R(n-1)} + \frac{RT_{Dn} - RT_{D(n-1)}}{RT_{Dn} + RT_{D(n-1)}} \tag{19}$$

When the vehicle approaches the RSU, calculate the trust value for each behavior attribute of the vehicle using Equation (15), and then calculate the latest trust value RT_i according to Equation (19).

In summary, the initial trust value, historical trust value, recommended trust value and RSU observation trust value of the vehicle node are calculated. CRITIC is used again to determine the optimal weights of the four trust decision factors. At this point, the number of evaluation indicators $m = 4$, and the corresponding weight is obtained as $\varphi_i = \left[{\varphi_i}^{(1)}, {\varphi_i}^{(2)}, {\varphi_i}^{(3)}, {\varphi_i}^{(4)}\right]$. The overall trust value is calculated as follows:

$$Tr_i = {\varphi_i}^{(1)} IT_i + {\varphi_i}^{(2)} HT_i + {\varphi_i}^{(3)} TR_i + {\varphi_i}^{(4)} RT_i \tag{20}$$

4. BTWACS

Different types of entities in the IoV introduce more attributes involved in access policies, which leads to a higher complexity of access control strategy. The cost of encryption and decryption increases linearly with the complexity of the strategy, resulting in additional computational overhead for the vehicle. By mining the association of attribute permissions between different roles and simplifying the complexity of the access control strategy, the IoV system can achieve more efficient data access. Therefore, based on the advantages and disadvantages of current IoV access control models, we have designed a hierarchical access control strategy based on blockchain, trust and weighted attributes called the BTWACS.

The immutability of blockchain can provide more secure data protection for the system and increase its security. The evaluation mechanism based on trust values can achieve a reliable judgment of entities, improve the recognition rate of malicious nodes and thus improve the stability of the system. The hierarchical control of weighted attributes represents similar attributes through inclusion relationships through hierarchical division, simplifying the number of attributes and reducing computational and transmission costs, thereby improving system efficiency.

4.1. An IoV Network Model Based on Blockchain

The overall framework of the IoV network model based on blockchain is shown in Figure 2 and mainly includes five parts: (1) The Trusted Center (TC) is responsible for managing attributes and distributing keys. (2) The vehicle perceives data through the onboard unit and communicates with the RSU. (3) The RSU has storage space and good computing capabilities. Its main functions include communicating with vehicles, receiving uploaded data, calculating vehicle trust values, encrypting data and generating, verifying and storing blocks. (4) Global blockchain is built in the cloud, and its main functions include communication with RSUs and distributed storage of access policies and data uploaded. Decryption verification is required when accessing data. (5) Data visitors mainly refer to entities under IoV, such as insurance companies, traffic law enforcement agencies and car owners.

This model deploys smart contracts on the edge layer and network layer of the blockchain and achieves node consensus based on the Byzantine fault-tolerant algorithm to ensure the security of the blockchain nodes.

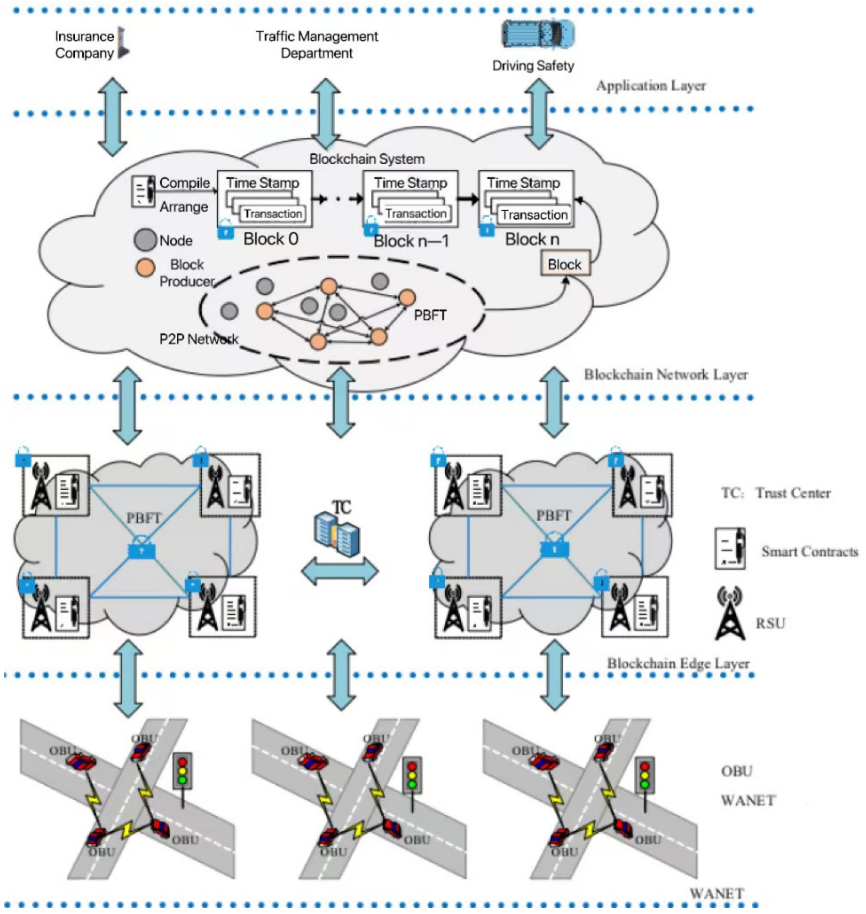


Figure 2. Overall framework of the IoV network model based on blockchain.

4.2. Access Control Policy

Trust assessments are mainly aimed at vehicles in the IoV, such as taxis, trucks, regular private cars and buses. Police vehicles, such as police cars and fire trucks, have higher-level user permissions and do not require trust assessment, and can access all shared data in the IoV. For example, when a vehicle encounters a traffic accident, it will upload the perceived data to the blockchain, which will be accessed by different entities. Traffic law enforcement departments use these data to investigate the cause of accidents and determine liability, while insurance companies use these data as the basis for claims and other car owners will use the data to replan their driving routes to avoid traffic congestion.

To avoid complex access control strategies that increase vehicle overhead, we design a weighted hierarchical access control strategy. The access permissions for data are not only divided by the attributes of vehicle type, the department to which the vehicle belongs and the position of the vehicle driver, but are also related to the trust attributes of the vehicle. Therefore, we also need to consider this attribute when dividing access permissions in order to achieve the trusted judgment of entities. Due to the numerous attributes contained by vehicle drivers, directly designing attribute-based access control strategies is highly complex. We intend to classify attributes into weighted hierarchies. For example, the relationship between job attributes in the truck transportation business department is truck driver$\subset$team leader$\subset$team leader$\subset$team manager. We assign weights to the attributes after hierarchical division and use the weighted attributes to represent similar attributes with continuous inclusion relationships in access permissions in the attribute set in order to simplify the number of attributes in access control policies and reduce the required computational and transmission costs, thereby improving encryption efficiency and ciphertext transmission rate.

Finally, we develop a hierarchical access control strategy through Algorithm 1.

Algorithm 1 BTWACS access control Strategy

Input: $AttrSet_i$, $Credit_i$

Output: Access Control Policy $\boldsymbol{T}$

1: Each entity is assigned different trust values: $Credit_i \in C$ (set trust threshold ***trust***). If entity is a vehicle, if $Credit_i >$ ***trust***, $AttrFlag_i = 1$, otherwise $AttrFlag_i = 0$. If the entity is the traffic management department, traffic law enforcement department or insurance company, $AttrFlag_i = 1$.

2: For each attribute$AttrSet_i \in U$, perform:

3: Classification attributes according to entity, vehicle type, department and position, and obtain $\boldsymbol{M}$ types of attributes $S = \{S_A, S_B, S_C, \cdots, S_M\}$;

4: $Classify(AttrSet_i) \rightarrow S_i$;

5: End.

6: Sort attributes based on access permissions. If there is an inclusion relationship between access permissions of similar attributes, that is, $S_{i,1} \subset S_{i,2} \subset S_{i,3} \subset \cdots \subset S_{i,N}$, weight them.

7: For $i = 1$ to M perform;

8: For $j = 1$ to N perform;

9: $S_{i,j}.\omega = j//\omega$ starting from 1;

10: End.

11: End.

12: For $i = 1$ to $AttrSet.length$ perform:

//Using weighted attributes to represent similar attributes with continuous inclusion relationships in access permissions in attribute sets.

13: if $S_{i,1} \subset S_{i,2} \subset S_{i,3} \subset \cdots \subset S_{i,M}$ in Staff, perform:

14: $S_{i,j}.\omega = m$, $S_{i,j} \rightarrow S_i : \omega_i$, $j \in [1, m]$;

15: End.

16: Use OR to connect different entities, and AND to connect different department and position attributes and trust values under the same entity.

17:$T = (Car_A\ AND\ (CarType_A \cdots OR \cdots)\ AND\ AttrFlag_A)\ OR$
$(Entity_B\ AND\ (Department_B \cdots OR \cdots)\ AND\ (S_B : \omega_1 \cdots OR \cdots)\ AND\ AttrFlag_B)\ OR$
$(Entity_C\ AND\ (Department_C \cdots OR \cdots)\ AND\ (S_C : \omega_2 \cdots OR \cdots)\ AND\ AttrFlag_C)\ OR \cdots$

The algorithm input is attribute sets and vehicle trust value sets defined by different entities, vehicle types, departments and positions, and output is the formulated hierarchical access control strategy T. According to entity, vehicle type, department and position, attributes are divided into different types of attribute: $S = \{S_A, S_B, S_C, \cdots, S_M\}$. If there is an inclusion relationship between access permissions for the same type of attribute, that is, $S_{i,1} \subset S_{i,2} \subset S_{i,3} \subset \cdots \subset S_{i,N}$, assign weight ω to them, increasing from 1, and then traverse. If there are continuous job attributes under the same physical department, replace these attributes with $S_i : \omega_i$. Use OR to connect different entities, and AND to connect different departments, job attributes and trust values under the same entity to generate hierarchical access control policies T. The structure of the access control policy is shown in Figure 3, where the attributes in the policy T are reduced to the $1/m$ of total attributes. However, the composition of data visitor attribute sets is complex, and there may be a risk of attribute redundancy. Therefore, we need to prune and optimize to obtain the final access control strategy T_a according to Algorithm 2.

Algorithm 2 BTWACS pruning

Input: Access Control Policy $\boldsymbol{T}$, *parameter* α

Output: Pruned Tree T_α

1: Calculate the empirical entropy of each node.

2: Recursively retract upwards from the leaf nodes of the tree.

3: The whole tree of a group of leaf nodes before and after retracting to its parent node is T_a and T_b, respectively. Calculate the loss function of T_a and T_b by (21) to obtain $Loss_\alpha$ (T_a) and $Loss_\alpha$ (T_b), respectively. If $Loss_\alpha$ (T_a) $\geq Loss_\alpha$ (T_b), then prune. Then, merge and reorganize the attribute sets in the leaf nodes, and retract them upwards to replace the parent node and become the new leaf node.

4: Return to 2 until it cannot continue, and obtain the subtree with the smallest loss function T_α.

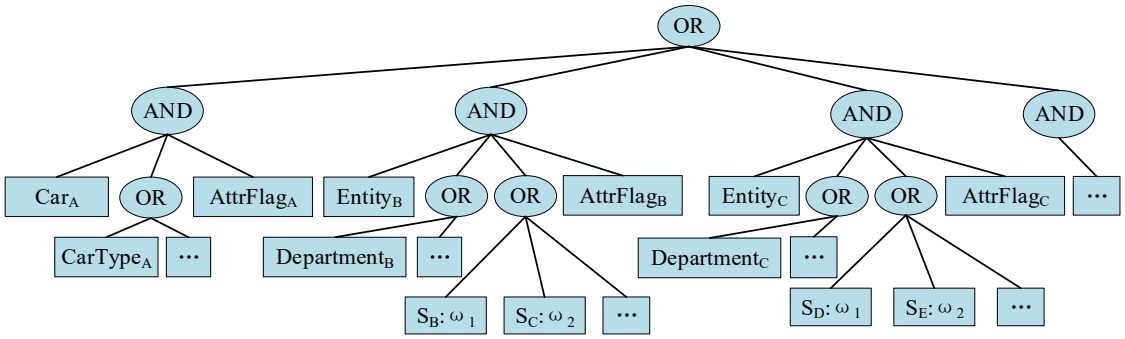


Figure 3. Access control policy.

Let the number of leaf nodes of the tree be $|T|$, with m as the leaf node of the tree T. The leaf node has N_m sample points, where the number of sample points of class k is N_{mk}, $E_m(T)$ is the empirical entropy on the leaf node m and $\alpha > 0$, and then the tree's loss function can be defined as:

$$Loss_\alpha(T) = \sum_{m=1}^{|T|} N_m E_m(T) + \alpha|T| \tag{21}$$

where the empirical entropy is

$$E_m(T) = -\sum_k \frac{N_{mk}}{N_m} log \frac{N_{mk}}{N_m} \tag{22}$$

4.3. Attribute-Based Encryption

The attribute-based encryption algorithm mainly consists of four parts: system initialization, generating user keys, generating encrypted files and decrypting.

4.3.1. System Initialization

The inputs of the system are the safety parameter γ and the attribute set U, and γ is publicly available. The output of the system is the public key PK and master key MSK. There is a bilinear group G_1 with prime P as the order, where g is the generator of G_1 and Z_p is the multiplication group of integer module P. This performs bilinear pairing operations $e : G_1 \times G_1 \to G_r$. We can generate the hash function $H : \{0,1\}^* \to G_1$ and attribute set $U = \{\alpha_1, \alpha_2, \alpha_3, \cdots, \alpha_n\}$, assign weighted attributes $\{s|s \in s_i\}$ to entities, select random number $\alpha, \beta \in Z_p$ and calculate $e(g,g)^\alpha$ and g^β.

The generated public key PK and master key MSK are as follows:

$$PK = \left\{ G_1, g, g^\beta, e(g,g)^\alpha \right\} \tag{23}$$

$$MSK = g^\alpha \tag{24}$$

4.3.2. Generating User Keys

$Keygen(MSK, S, Tr)$ is a key SK that uses master key MSK, a group of weighted attributes S and trust value Tr as the input, and whose output is related to S and Tr. We can choose $t \in Z_p$ randomly, and every weighted attribute $i \in S$ has a weighted value ω_i. For each attribute i in the attribute set, calculate $D_i = H(i)^{\omega,t}$ and generate the key for data visitors as SK:

$$SK = \left\{ D = g^\alpha g^{\beta t}, g^t, \{D_i\}_{i \in S}, Tr \right\} \tag{25}$$

4.3.3. Encryption

In order to ensure the confidentiality and security of data and achieve effective access control effects, we adopt a hybrid encryption mechanism. Advanced Encryption Standard (AES) is used to encrypt data, and CP-ABE (See Section 2.3 for details) is used to encrypt symmetric keys and embed the encrypted data and symmetric keys into access control policies. The mechanism of mixing symmetric encryption AES and asymmetric encryption (CP-ABE) ensures the confidentiality of the data.

$Encrypt(PK, CK, M, T)$: Input the public key PK, plain text M, symmetric key CK and access control strategy T. Output the cipher-text CT. Choose the polynomial f_x for each node x in T. Choose a $d_x = k_x - 1$ degree polynomial for each node in T. From the root node R, $f_R(0) = s\left(s \in Z_p\right)$, s is random. For leaf node x, set $f_x(0) = f_{parent(x)}(index(x))$ and choose an f_x defined by d_x randomly. Every leaf node stands for a weighted attribute. ω_i is the smallest weight for each leaf node. Calculate $C = M{\cdot}e(g,g)^{\alpha s}$, $C_0 = g^s$. Make s a secret and split it along the tree. The corresponding secret sharding for the leaf node attribute i is $f_x(0)$. Calculate $C_i = H(i)^{-\omega_i s} \prod_{z \in S_i} g^{\gamma_z}$, $C_T = g^{f_x(0)}$.

$$CT = \left\{T, C, C_0, C_T, \left\{C_i\right\}_{i \in [1,n]}\right\} \tag{26}$$

4.3.4. Decryption

After the data requester obtains access permissions, AES is used to decrypt the data resources and CP-ABE is used to verify the legitimacy of the user. Only when the trust values and attribute sets match the access policy can the cipher-text be successfully decrypted to obtain plaintext, thus achieving fine-grained access control of the IoV data.

Only when the attribute set S and the trust value Tr of the key satisfies the T policy of the cipher-text access tree can the cipher-text be decrypted. Calculate $TP_x = MSK{\cdot}H{\cdot}\prod_{z \in S_x} g^{\gamma_z}$. Starting from the root node, perform recursive calculations. The partition of each sub node can be exponentially calculated based on the Lagrange difference factor, and then the multiplication operation can be performed. Construct decryption components as follows:

$$e(g,g)^{\alpha s} = \frac{e(P_x, C_0)}{e(C_T, C_i)} = \frac{e(P_x, C_0)}{e\left(g^{f_x(0)}, H{\cdot}\prod_{z \in S_x} g^{\gamma_z}\right)} = \frac{e\left(g^{\alpha}{\cdot}H{\cdot}\prod_{z \in S_x} g^{\gamma_z}, g^s\right)}{e\left(g^{f_x(0)}, H{\cdot}\prod_{z \in S_x} g^{\gamma_z}\right)} \tag{27}$$

We can then obtain plain text M through $M = \frac{C}{e(g,g)^{\alpha s}}$.

5. Experimental Results and Analysis

We use OpenStreetMap to construct a map of real traffic scenes and combine it with network simulators NS3 and Simulation of Urban MObility (SUMO) to simulate the motion trajectory of mobile vehicle nodes and the IoV environment of connected vehicles.

In the simulation environment, when vehicle A encounters an accident while driving, the program runs as follows: Firstly, the vehicle senses and generates access data M. Secondly, we can call Algorithm 1 to input the attribute set of the access object and the evaluated trust value, and then call Algorithm 2 to remove redundant attributes, and finally output access control policy T. Finally, the vehicle encrypts data using the access control strategy and uploads cipher-text to the blockchain network layer. After reaching node consensus based on the improved PBFT algorithm, the data are stored in the blockchain.

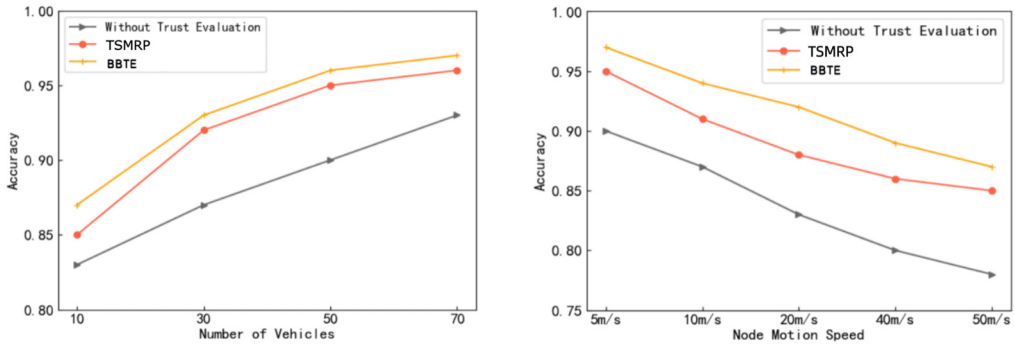
We validate the security and performance of the BTWACS and compare it to other access control methods. The simulation parameters are shown in Table 3.

Table 3. Parameter settings.

Parameter	Value
Scene	City street
Speed of vehicles	(5–50) m/s
Vehicle density within RSU	(10–70)
Communication range	0~300 m
OBU configuration	1.5 Ghz, 4 core CPU
RSU configuration	1.8 Ghz, 4 core CPU, 237 G hard disk

5.1. Safety Analysis

In order to ensure timely and reliable information exchange between vehicles, it is necessary to improve the recognition of malicious nodes, that is, to improve the recognition accuracy of untrusted nodes. We simulate and compare BBTE to TSMRP [28] and the scheme without trust evaluation, and the experimental results are shown in Figure 4. Figure 4a shows the accuracy of identifying malicious nodes with different node densities. Figure 4b shows the accuracy of identifying malicious nodes at different vehicle speeds.



(**a**) (**b**)

Figure 4. Comparison of accuracy in identifying malicious nodes. (**a**) Identification accuracy of malicious nodes with different node densities; (**b**) identification accuracy of malicious nodes at different vehicle speeds.

As shown in Figure 4, a higher density of vehicle nodes, higher recognition accuracy and faster vehicle speed result in a decrease in the recognition accuracy of malicious nodes. TSMRP [28] combines direct trust and indirect trust to improve the accuracy of identifying malicious vehicle nodes but neglects the collection and calculation of vehicle experience trust and behavior observation information. BBTE combines direct trust, indirect trust, historical experience trust and behavioral observation trust, and the recognition accuracy of the BBTE is higher than the other two models.

This experiment simulates and implements a network using gray hole attack, on/off attack and defamation attack. BBTE is compared to trust models ART [29], CAT [30] and TSMRP [28] using the malicious node detection rate and malicious node recognition accuracy as two evaluation indicators. The accuracy of malicious nodes and the ratio of the real malicious nodes identify to the identified malicious nodes, as well as the detection rate of malicious nodes and the ratio of the identified real malicious nodes to the total number of malicious nodes are all used. We set the total number of nodes to 100, and the number of malicious nodes to 10, 20 and 30, respectively. The network attack scenario settings are shown in Table 4.

Table 4. Network attack scenario settings.

Attack Type	Description
Gray hole attack	50% probability of malicious packet loss.
On-off attack	Normal forwarding first, followed by mali-cious packet loss, alternating for a period of 30 seconds.
Defamation attack	In the process of trust recommendation, reduce the trust value of honest nodes and increased the trust value of untrusted nodes.

The comparison between the recognition accuracy and detection rate of malicious nodes under different attacks is shown in Figures 5 and 6.

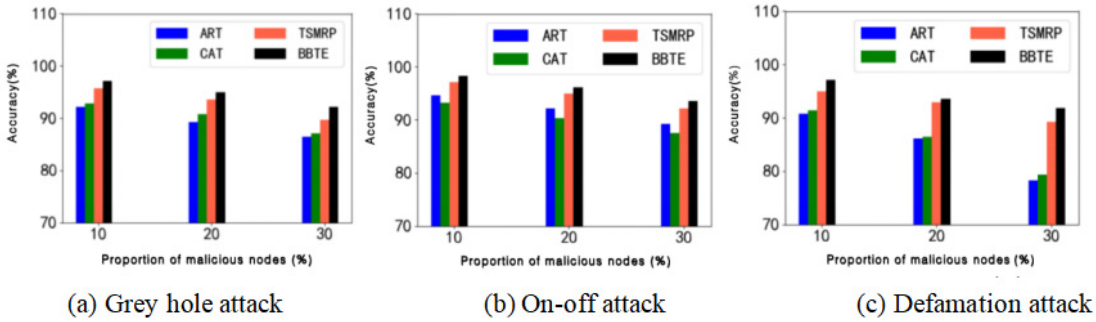


Figure 5. Comparison of malicious node identification accuracy under different attacks.

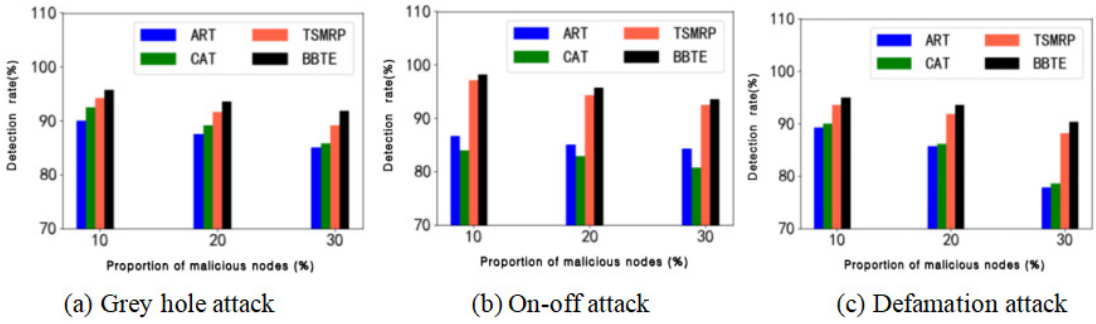


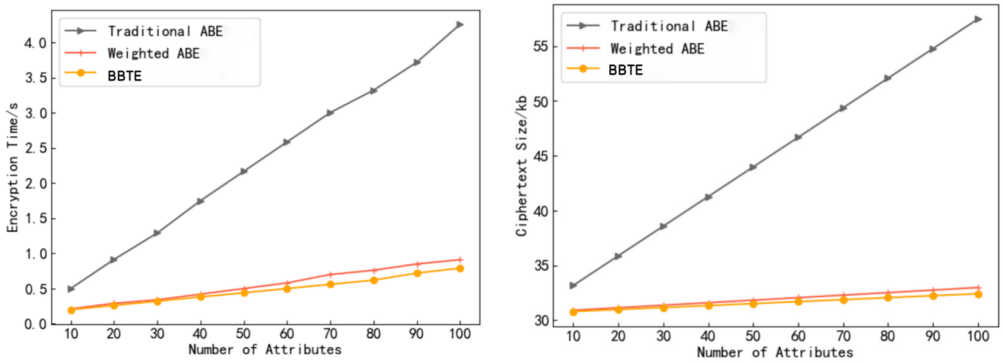
Figure 6. Comparison of malicious node identification detection rate under different attacks.

It can be seen from Figures 5 and 6 that CAT focuses on vehicle behavior detection and does not give enough consideration to historical experience trust and other vehicle recommendation trust information. ART relies on indirect trust and ignores the collection and calculation of direct trust. Neither ART nor CAT can effectively respond to temporal attacks. TSMRP combines direct trust and indirect trust and proposes a feedback mechanism to deal with temporal attacks but lacks consideration for the collection and calculation of vehicle experience trust and behavior observation information. BBTE combines direct trust, indirect trust, historical experience trust and behavioral observation trust, resulting in higher accuracy in trust calculation. Therefore, the recognition accuracy and the detection rate of BBTE are higher than the other three models.

5.2. Performance Analysis

The Trust Evaluation Method ensures the security and reliability of information transmission by judging the credibility of vehicle nodes and achieves the secure access control of data. We used the Java Pairing-Based Cryptography (JPBC) Library to perform comparative experiments on traditional CP-ABE [31], weighted CP-ABE [14] and BBTE. The number of attributes set in the experiment increases gradually from 1 to 100. In the access control strategy without pruning and restructuring, each attribute class contains an average of five

attributes. After optimization, each attribute class contains an average of six attributes. The experimental results are shown in Figure 7. Figure 7a shows the change trend in encryption time with the number of attributes, and Figure 7b shows the change trend in cipher-text size with the number of attributes.



(**a**) (**b**)

Figure 7. Comparison of encryption efficiency. (**a**) Encryption efficiency of vehicles; (**b**) cipher-text transmission size.

Calculation cost: As shown in Figure 7a, when the number of attributes is 100, the traditional CP-ABE encryption time takes about 4.26 s. Weighted CP-ABE constructs an access control policy by introducing weights, and the number of attributes can be reduced to 1/5, that is, the number of attributes in the policy is only 20, and the encryption time is reduced to about 0.91 s. In BBTE, not only are weights introduced to construct access control policies but trust value attributes are also introduced to improve the security of communication and interaction between vehicle nodes. After pruning optimization, redundant attributes are removed, resulting in an average of six attributes per attribute class. The encryption time is reduced to about 0.79 s, greatly reducing the complexity of the policy and significantly reducing computational overhead.

Transmission overhead: As shown in Figure 7b, when encrypting 100 attributes, the traditional CP-ABE cipher-text size is 57.5 kb. Weighted CP-ABE constructs an access control policy by introducing weights, and the number of attributes can be reduced to 1/5, which means that the policy only has 20 attributes and the cipher-text size is 33 kb. In BBTE, not only are weights introduced to construct access control policies but trust value attributes are also introduced to improve the security of communication and interaction between vehicle nodes. After pruning optimization, redundant attributes are removed, resulting in an average of six attributes per attribute class, reducing the cipher-text size to approximately 32.4 kb and reducing the transmission cost of vehicle data transmission to the blockchain network layer.

Weighted CP-ABE introduces weight to formulate hierarchical access strategies but does not consider factors such as entity trust values and attribute redundancy. BBTE adds trusted judgments to entities to further ensure secure access control effects and effectively reduces the complexity of access policies through pruning technology, saving computational costs.

6. Conclusions

In traditional IoV, data are easy to tamper with and leak. The BTWACS access control strategy achieves decentralized data security storage and access. This scheme evaluates the trustworthiness of accessing entities and introduces attribute-based encryption to achieve the flexible access control of on-chain data, ensuring the confidentiality and integrity of message transmission. It constructs a hierarchical access control strategy based on weight and trust by mining the association relationships between attribute permissions among various roles, and further optimizes the access strategy through pruning techniques. We evaluate the trust value to improve the security and efficiency of node interaction, and

the results show that this scheme can effectively respond to gray hole attacks, defamation attacks and collusion attacks from other vehicle nodes. This method can effectively reduce the computing and transmission costs of vehicles and meet the access requirements of multiple entities and roles in the IoV.

It improves the communication performance of the IoV, enhances the security of the network and creates a safe and comfortable transportation environment. The algorithm improves the trust evaluation mechanism in blockchain technology, making it more efficient and accurate, and has a promoting effect on the development of blockchain technology. It is an application of blockchain technology in the actual IoT scenario IoV and is a good example of the practical application of blockchain. It is beneficial for the materialization and application of blockchain technology to play a role in real life.

We utilize the BTWACS to control the credibility of entities, ensuring the security of information transmission and avoiding security issues such as malicious attacks and data leakage. However, there is a lack of incentive mechanisms to promote the participation of selfish vehicle nodes. Moreover, although we preliminarily implement the attribute-based access control strategy, we still lack in-depth research on policy updates and the attribute revocation of on-chain data.

In future research, we will continue to conduct in-depth research on the policy update and attribute revocation of the data on the chain for the selfish vehicle node incentive problem, and further improve the access control effect of the IoV on the premise of ensuring data security and reliability.

Author Contributions: Conceptualization, L.L.; methodology, J.W.; formal analysis, L.L.; data curation, J.W.; writing—original draft preparation, C.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded in part by the scientific research project of the National Natural Science Foundation of China (62362055), the Inner Mongolia Autonomous Region Key R&D and Achievement Transformation Program Project (2022YFSJ0013, 2023YFHH0052), the Research Program for Young Talents of Inner Mongolia Colleges (NJYT22084, NJYT23055), the Natural Science Foundation of Inner Mongolia (2023MS06008), the Key Research & Development Program of Erdos (YF20232328), the Scientific Research Program for Inner Mongolia Colleges (JY20220061, JY20230119, JY20230019), and the Basic Scientific Research Expenses Program of Universities directly under Inner Mongolia Autonomous Region (JY20220078, 2022ZY0169).

Data Availability Statement: Due to the nature of this research, participants of this study did not agree for their data to be shared publicly, so supporting data is not available.

Conflicts of Interest: The authors declare that they have no conflict of interest to report regarding the present study.

References

1. Yu, B.; Bai, F. PYRAMID: Probabilistic Content Reconciliation and Prioritization for V2V Communications. *IEEE Trans. Veh. Technol.* **2018**, *67*, 6615–6626. [CrossRef]
2. Cheng, X.; Zhang, R.; Chen, S.; Li, J.; Yang, L.; Zhang, H. 5G enabled vehicular communications and networking. Wireless Communication over ZigBee for Automotive Inclination Measurement. *China Commun.* **2018**, *15*, 3–6. [CrossRef]
3. Lyamin, N.; Kleyko, D.; Delooz, Q.; Vinel, A. AI-Based Malicious Network Traffic Detection in VANETs. *IEEE Netw.* **2018**, *32*, 15–21. [CrossRef]
4. Khelifi, H.; Luo, S.; Nour, B.; Moungla, H.; Faheem, Y.; Hussain, R.; Ksentini, A. Named Data Networking in Vehicular Ad hoc Networks: State-of-the-Art and Challenges. *IEEE Commun. Surv. Tutor.* **2020**, *20*, 320–351. [CrossRef]
5. Zhao, L.; Li, X.; Gu, B.; Zhou, Z.; Mumtaz, S.; Frascolla, V.; Gacanin, H.; Ashraf, M.I.; Rodriguez, J.; Yang, M.; et al. Vehicular Communications: Standardization and Open Issues. *IEEE Commun. Stand. Mag.* **2019**, *2*, 74–80. [CrossRef]
6. Sharma, S.; Sharma, A.; Goel, T.; Deoli, R.; Mohan, S. Smart Home Gardening Management System: A Cloud-Based Internet-of-Things (IoT) Application in VANET. In Proceedings of the 2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kharagpur, India, 1–3 July 2020; pp. 1–5.
7. Liu, A.; Du, X.; Wang, N.; Li, S. Research progress of blockchain technology and its application in information security. *Ruan Jian Xue Bao/J. Softw.* **2018**, *29*, 2092–2115. (In Chinese)

8. Qazi, F.; Khan, F.H. Enhancing the security of vehicle to road side unit (RSU) communication with key generation and advanced encryption procedure in vehicular ad-hoc network (VANET). *Indian J. Sci. Technol.* **2017**, *10*, 36. [CrossRef]
9. Lee, T.; Moon, S.H.; Jang, J. Data encryption method using CP-ABE with symmetric key algorithm in blockchain network. In Proceedings of the 2021 International Conference on Information and Communication Technology Convergence (ICTC), Jeju Island, Republic of Korea, 20–22 October 2021; pp. 1371–1373.
10. Blundo, C.; Cimato, S.; Siniscalchi, L. Managing Constraints in Role Based Access Control. *IEEE Access* **2020**, *8*, 140497–140511. [CrossRef]
11. Xue, Y.; Xue, K.; Gai, N.; Hong, J.; Wei, D.S.; Hong, P. An Attribute-Based Controlled Collaborative Access Control Scheme for Public Cloud Storage. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 2927–2942. [CrossRef]
12. Ahamed, J.; Khan, F. An Enhanced Context-aware Capability-based Access Control Model for the Internet of Things in Healthcare. In Proceedings of the 2019 Sixth HCT Information Technology Trends (ITT), Ras Al Khaimah, United Arab Emirates, 20–21 November 2019; pp. 126–131.
13. Cruz, J.P.; Kaji, Y.; Yanai, N. RBAC-SC: Role-based access control using smart contract. *IEEE Access* **2018**, *6*, 12240–12251. [CrossRef]
14. Liu, X.; Yin, Y.; Chen, W.; Xia, Y.; Xu, J.; Han, L. Data security sharing scheme of Internet of vehicles based on blockchain. *J. Zhejiang Univ. (Eng. Ed.)* **2021**, *55*, 957–965. (In Chinese)
15. Nakamura, Y.; Zhang, Y.; Sasabe, M.; Kasahara, S. Capability-Based Access Control for the Internet of Things: An Ethereum Blockchain-Based Scheme. In Proceedings of the GLOBECOM 2019—2019 IEEE Global Communications Conference, Waikoloa, HI, USA, 9–13 December 2019; pp. 1–6.
16. Chen, C.; Wang, C.; Qiu, T.; Lv, N.; Pei, Q. A Secure Content Sharing Scheme based on Consortium Bolckchain in Vehicular Named Data Networks. *IEEE Trans. Ind. Inform.* **2019**, *16*, 3278–3289. [CrossRef]
17. Kang, J.; Yu, R.; Huang, X.; Wu, M.; Maharjan, S.; Xie, S.; Zhang, Y. Blockchain for secure and efficient data sharing in vehicular edge computing and networks. *IEEE Internet Things J.* **2018**, *6*, 4660–4670. [CrossRef]
18. Zhang, D.; Yu, F.R.; Yang, R. Blockchain-Based Distributed Software-defined Vehicular Networks: A Dueling Deep Q-Learning Approach. *IEEE Trans. Cogn. Commun. Netw.* **2019**, *5*, 1086–1100. [CrossRef]
19. Gu, W.; Li, J.; Tang, Z. A Survey on Consensus Mechanisms for Blockchain Technology. In Proceedings of the 2021 International Conference on Artificial Intelligence, Big Data and Algorithms (CAIBDA), Xi'an, China, 28–30 May 2021; pp. 46–49.
20. Yang, Z.; Yang, K.; Lei, L.; Zheng, K.; Leung, V.C.M. Blockchain-Based Decentralized Trust Management in Vehicular Networks. *IEEE Internet Things J.* **2019**, *6*, 1495–1505. [CrossRef]
21. Abuhashim, A.; Tan, C.C. Smart Contract Designs on Blockchain Applications. In Proceedings of the 2020 IEEE Symposium on Computers and Communications (ISCC), Rennes, France, 7–10 July 2020; pp. 15–26.
22. Wang, W.; Hoang, D.T.; Hu, P.; Xiong, Z.; Niyato, D.; Wang, P.; Wen, Y.; Kim, D.I. A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. *IEEE Access* **2019**, *7*, 22328–22370. [CrossRef]
23. Porwal, S.; Mittal, S. Design of Concurrent cipher-text Policy-Attribute Based Encryption Library for Multilevel Access of Encrypted Data. In Proceedings of the 2018 Fifth International Conference on Parallel, Distributed and Grid Computing (PDGC), Solan, India, 20–22 December 2018; pp. 42–47.
24. 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 2018–3 August 2018.
25. Kanumalli, S.S.; Ch, A.; Murty, P.S.R.C. Secure V2V communication in IoV using IBE and PKI based hybrid approach. *Int. J. Adv. Comput. Sci. Appl. (IJACSA)* **2020**, *11*, 466–472. [CrossRef]
26. Liu, Y.; Wang, Y.; Chang, G. Efficient Privacy-Preserving Dual Authentication and Key Agreement Scheme for Secure V2V Communications in an IoV Paradigm. *IEEE Trans. Intell. Transp. Syst.* **2017**, *18*, 2740–2749. [CrossRef]
27. Diakoulaki, D.; Mavrotas, G.; Papayannakis, L. Determining objective weights in multiple criteria problems: The CRITIC method. *Comput. Oper. Res.* **1995**, *22*, 763–770. [CrossRef]
28. Xia, H.; Zhang, S.; Sun, Y.; Xiao, F.; Li, Y.; Cheng, X. Design of Trust-Based Secure Multicast Routing Protocol in VANETs. *J. Comput. Sci.* **2019**, *42*, 961–979. (In Chinese)
29. Li, W.; Song, H. ART: An Attack-Resistant Trust Management Scheme for Securing Vehicular Ad Hoc Networks. *IEEE Trans. Intell. Transp. Syst.* **2016**, *17*, 960–969. [CrossRef]
30. Raghu, V.; Barnwal, R.P.; Ghosh, S.K. CAT: Consensus-assisted trust estimation of MDS-equipped collaborators in vehicular ad-hoc network. *Veh. Commun.* **2015**, *2*, 150–157.
31. 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. [CrossRef]