IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 17, 2020, accepted March 16, 2020, date of publication March 19, 2020, date of current version March 31, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2981945

Secure Data Sharing and Customized Services for Intelligent Transportation Based on a Consortium Blockchain

DI WANG AND XIAOHONG ZHANG
School of Information Engineering Jiangxi University of Science and Technology, Ganzhou 341000, China

Corresponding author: Xiaohong Zhang (xiaohongzh@263.net)

This work was supported in part by the National Natural Science Foundation of China under Grant 51665019 and Grant 61763017, in part by the Scientific Research Plan Projects of Jiangxi Education Department under Grant GJJ150621, in part by the Natural Science Foundation of Jiangxi Province under Grant 20161BAB202053 and Grant 20161BAB206145, and in part by the Innovation Fund for Graduate Students in Jiangxi Province under Grant YC2017-S302.

ABSTRACT In view of the security risks and centralized structure of traditional intelligent transportation system, we propose a novel scheme of secure data sharing and customized services based on the consortium blockchain (DSCSCB). The ciphertext-policy attribute-based proxy re-encryption algorithm has the function of keyword searching by dividing the key into an attribute key and a search key, which not only solves the problem that proxy re-encryption algorithm cannot retrieve data, but also realizes data sharing and data forwarding. Moreover, the algorithm effectively controls the access permission of data, and provides a secure communication environment for the vehicular ad-hoc network (VANET). Service sectors, such as insurance companies, the traffic police and maintenance suppliers, obtain the corresponding ciphertext and then apply the smart contract to provide customized services for the onboard unit after decryption. Security analysis and performance evaluation demonstrate that our scheme not only meets the requirements of data sharing in the security and confidentiality, but also has obvious advantages in the overhead of computing and communication.

INDEX TERMS Consortium blockchain, data sharing, customized services, smart contract, intelligent transportation.

I. INTRODUCTION

With the improvement of living standards, vehicles have become an indispensable tool of transportation in our daily life. Intelligent transportation system [1], [2] combines various technologies such as sensors, wireless communication, and computer technology to establish a safe and efficient transportation network, and thus provides comfortable and convenient services for car owners. In recent years, with the development of Internet of Things (IoT) and Mobile Internet of Things (MIoT), the vehicular ad-hoc network (VANET) has become an important part of the intelligent transportation system, which has attracted extensive attention from numerous scholars and researchers [3].

The onboard unit in the VANET could detect and communicate with other onboard units, which means the onboard unit can receive and transmit information, so that other vehicles and management departments could obtain accurate real-time traffic data. In order to detect the integrity of data on two-way traffic roads, Aslam *et al.* [4] proposed a two-direction and time-based data verification scheme achieving safe transmission of traffic data. Although the scheme does not rely on complex and expensive public key infrastructure, it cannot resist man-in-the-middle attacks and collusion attacks. Therefore, Feng et al [5] proposed a data sharing scheme based on the cloud platform that can resist man-in-the-middle attack and collusion attacks. In addition, to prevent denial of service attacks, Hash problem based trust cluster cooperative authentication scheme [6] was proposed, which also reduced the overhead of pseudonym authentication. Recently, a data aggregation scheme based on fully homomorphic encryption [7] was used to protect the privacy of identity and location in information interaction. Compared with Paillier homomorphic encryption, the reference [7] improved the security and reduced computational burden, but it is inefficient. In general, the above schemes realize the sharing of traffic data, but there are still some challenges:

1) Threats to security and privacy: It is easy for an attacker to eavesdrop, tamper with, or forge data sent

The associate editor coordinating the review of this manuscript and approving it for publication was Jiafeng Xie.

by onboard units in an open wireless communication environment. Worse still, the leakage of privacy data will threaten the security and confidentiality of data. Once key information is tampered with, it will not only reduce traffic efficiency, but also threaten life safety.

2) Centralization: The traditional intelligent transportation system have a centralized structure, relying on a trusted third party. Once the central node is attacked, the security of the VANET will be threatened. In addition, the maintenance and construction of the central node requires plenty of financial and material resources.

Therefore, it is urgent to design a secure data sharing scheme. Attribute-based encryption is an emerging technology to achieve data access control and secure data sharing [8]. Extended file hierarchy access control scheme with ciphertext-polity attribute-based encryption [9] was proposed for big companies with different hierarchical departments, which implemented encryption for multiple files on the same access level. In order to reduce the storage space occupied by the ciphertext and computational overhead, the attribute-based encryption algorithm with keyword search, outsourcing decryption, and outsourcing key distribution [10] was proposed, but it cannot achieve user revocation and attribute revocation. Therefore, Li *et al.* [11] proposed the ciphertext-policy attribute-based encryption with efficient user revocation by introducing the concept of user groups. Later, the issue that the attribute revocation was solved by exploiting the concept of attribute groups [12]. To prevent the insecure problems caused by the random oracle model, Ge *et al.* [13] proposed a key-policy attribute-based proxy re-encryption without random oracles, which improved security via improving the re-encryption key query and re-encryption query. Later, an attribute-based proxy re-encryption and its adaptive security model [14] were proposed and proved against chosen-ciphertext attack secure in the adaptive model without random oracles. A novel revocable identity-based broadcast proxy re-encryption [15] was not only semantically secure in the random model, but also allowed the proxy to revoke a set of delegates from the re-encryption key.

To provide a secure and trusted communication environment for intelligent transportation systems, Yang *et al.* [16] proposed a lightweight anonymous authentication scheme that can track malicious vehicles sending false information and revoke their identities. Additionally, a privacy protection scheme [17] used source authentication to prevent the attackers from impersonating the legitimate node, which utilized the cloud server to verify part of the ciphertext without decrypting and filtered out the invalid traffic information. In order to reduce the communication overhead and the possibility of roadside unit collusion, Ni et al [18] used the Bloom filter to provide drivers with privacy protection parking navigation services, including identity authentication, request authentication and driving guidance. Kumar *et al.* [19] used elliptic curve encryption algorithm and end-to-end authentication to protect the confidentiality of road information, and took advantage of sandboxing method to improve the security of data. Although the performance of this scheme is better than other schemes, the computing cost increases linearly with the size of data. The Secure Signcryption Authentication Protocol [20] was used for authentication, which can resist impersonation attacks, sybil attacks, man-in-the-middle attacks and other network attacks. In order to solve the problem that certificate revocation lists need to occupy a large amount of network resources, the semi-trust authentication scheme [21] combined key distribution and certificateless signature, which not only improved the efficiency of message verification, but also reduced a lot of storage space. The above schemes improve the confidentiality and security of data to some extent, but the centralized structure in intelligent transportation still exists.

In recent years, there has been a global upsurge in blockchain research, which has attracted numerous scholars to combine blockchain with the VANET [22]. Subsequently, Kang *et al.* [23] used blockchain technology to achieve secure data sharing in the vehicular edge network, and applied a three-weight subjective logic model to improve the quality of shared data. Furthermore, in order to ensure the security of access data, the blockchain-based distributed architecture [24] applied a variable public key to protect the privacy of the onboard unit and prevent location tracking. Yang *et al.* [25] proposed the Proof-of-even consensus to verify the validity of traffic events and fed back the correctness of traffic events. Cebe *et al.* [26] proposed a lightweight license blockchain for traffic accident forensics and forensic analysis, which is convenient for solving traffic disputes efficiently and quickly. Cheng *et al.* [27] proposed a semi-centralized traffic signal regulation mode based on blockchain, which regulates traffic signal lights according to the dynamic properties of vehicles, which is not affected by the environment and equipment installation, and has better effects in the environment with sparse traffic flow. Jin *et al.* [28] proposed a charging mechanism for electric taxis based on the consortium blockchain, which improved the flexibility of charging services and effectively solved the monopoly problem of charging operators' charging information.

Different from the existing schemes, we propose a secure data sharing and customized services based on the consortium blockchain (DSCSCB). The onboard unit sends the ciphertext to the roadside unit, and the verification node verifies the ciphertext by the Ripple consensus. After the verification is successful, the ciphertext is packaged to generate the block, and then the block is connected to the blockchain. The onboard unit sends a search service request to the smart contract, the corresponding ciphertext is sent to the service sector according to the keyword searched by the onboard unit. The service sector decrypts and obtains the plaintext to provide customized services for the onboard unit. If the service department sends a search service request to the smart contract, the corresponding ciphertext is converted to re-encrypted ciphertext, which is sent to the relevant service departments according to the keywords searched by

the service sector. The service sectors cooperate with each other to provide more efficient and convenient services for the onboard unit. In summary, the main contributions of this paper are as follows:

1) We use the decentralization of the consortium blockchain to break the data centralized management of traditional intelligent transportation, prevent single point collapse and data monopoly, and realize the data sharing without the third-party intermediary. Service sectors apply smart contracts to provide multi-dimensional and customized services for onboard units, not limited to the single-dimensional service.
2) Attribute-based proxy re-encryption algorithm is proposed to implement keyword retrieval and proxy re-encryption. According to keywords and attribute sets, data access permissions are controlled, which prevents collusion attacks and achieves secure and trusted data sharing.
3) Security analysis and performance evaluation demonstrate that DSCSCB not only meets the security requirements of data sharing, but also has more advantages than other schemes in term of computational overhead and communication overhead. Therefore, DSCSCB is suitable for secure data sharing and customized services for intelligent transportation.

The structure of this paper is organized as follows. Section II introduces the technical preliminaries, mainly including blockchain, bilinear mapping and encryption algorithm. Section III details the proposed system framework. Sections IV and V describe secure data sharing algorithm and customized services respectively. Section VI analyzes the security of proposed scheme and evaluates its performance. Finally, we conclude this paper in Section VII.

II. PRELIMINARIES

A. BLOCKCHAIN

The blockchain is a distributed ledger that originated from Bitcoin [29] proposed by Nakamoto in 2008. With the rise of digital currencies such as Bitcoin, blockchain has become a new technology that is decentralized, secure, credible, non-tamperable and traceable. Consensus mechanism is used to generate the block. Asymmetric encryption and chain structure can prevent data in blocks from being tampered with. What's more, smart contracts change traditional contract formulation and fulfillment methods.

According to the nodes participating in the consensus, blockchain is divided into the private blockchain, public blockchain and consortium blockchain. Only a few nodes in the private blockchain have write permissions and read permissions, and the speed of reaching a consensus is fast, but it is difficult for private blockchain to realize data sharing. The public blockchain is completely decentralized, allowing all nodes in the network to participate in the consensus, so the demerit is that it takes an awfully long time to verify and update data. However, the pre-selected nodes in the consortium blockchain verify and record data, which speeds up the generation of blocks and the nodes reach a consensus faster.

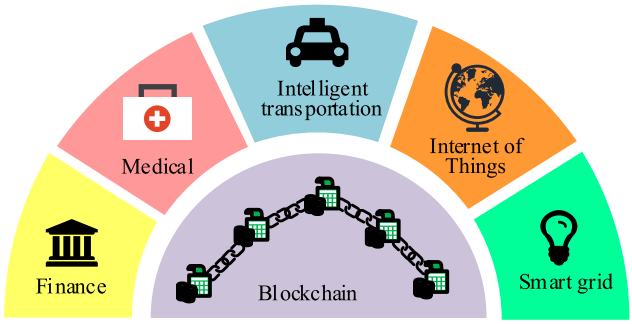

FIGURE 1. Application scenarios of blockchain.

Recently, blockchain has attracted great attention from the government, investment companies and scientific research institutions. It has been widely used in medical, Internet of Things and other fields, as shown in Figure 1. Xu *et al.* [30] proposed a healthchain based on the patient medical data to control and management of electronic health records, avoid leakage of sensitive data, and enhance privacy protection of user. Zhang *et al.* used priority and cryptocurrency to encourage electric vehicle users to use renewable energy, which solved the problem of mismatch between supply and demand of renewable resources [31]. Lei et al [32] proposed an efficient and practical dynamic key management scheme, which simplifies the key transmission process, and makes key management easy to deploy and expand. In addition, some scholars have applied blockchain to intelligent transportation. Zhang et al [33] proposed a secure data sharing system for the Internet of vehicles based on the blockchain, which employs the fragmentation technology to improve the scalability of the network and generate auxiliary blockchain to manage the data of different entities. Adaptive traffic signal control mechanism based on the consortium blockchain [34], which dynamically regulates the period of traffic signal according to the road information sent by vehicles, reduces waiting time and alleviates traffic congestion. Therefore, the emergence of blockchain brings new opportunities for intelligent transportation.

B. BILINEAR PAIRING

G_1 and G_2 are multiplicative cyclic groups with prime orders p. g is the generator of G_1. Bilinear pairing [35] $e : G_1 \times G_1 \rightarrow G_2$ satisfies the following properties.

- Bilinearity: for $\forall P, Q \in G_1$ and $r, s \in Z_p^*$, $e(P^r, Q^s) = e(P, Q)^{rs}$.
- Computability: for $\forall P, Q \in G_1$ bilinear pairing $e(P, Q)$ can be effectively calculated.
- Non-degeneracy: $e(P, Q) \neq 1$ for $\forall P, Q \in G_1$.

C. LINEAR INTEGER SECRET SHARING

Suppose $M_c \in Z^{1\times 1}$ represents the single element matrix $M_c = [1]$ and $a_i \in Z^k$ denotes the elements of the first

column of the multi-element matrix $M_i \in Z^{k_i \times v_i}$. $F_i \in Z^{k_i \times (v_i - 1)}$ represents all the columns in M_i except the first column. The linear integer secret sharing (LISS) [36] matrix constructed with the access policy has the following properties.

- Each attribute i of the access policy R is expressed by M_i.
- Suppose N_1 and N_2 represent matrices $M_1 \in Z^{k_1 \times v_1}$ and $M_2 \in Z^{k_2 \times v_2}$, respectively. Any logic OR operation is $N = N_1 \cup N_2$, then N can be denoted as $M_{or} \in Z^{(k_1+k_2)\times(v_1+v_2-1)}$, where the first column of M_{or} is the result of cascading a_1 and a_2, the next $(v_1 - 1)$ columns of M_{or} is the result of cascading the vectors in F_1 with k_2 zeros. The last $(v_2 - 1)$ columns of M_{or} is the result of cascading k_1 zeros and vectors in F_2. M_{or} can be expressed as

$$M_{or} = \begin{bmatrix} a_1 & F_1 & 0 \\ a_2 & 0 & F_2 \end{bmatrix} \tag{1}$$

- Suppose N_3 and N_4 represent matrices $M_3 \in Z^{k_3 \times v_3}$ and $M_4 \in Z^{k_4 \times v_4}$, respectively. Any logic AND operation is $N' = N_3 \cap N_4$, then N' can be denoted as $M_{and} \in Z^{(k_3+k_4)\times(v_3+v_4)}$, where the first column of M_{and} is the result of cascading a_3 and k_4 zeros, the second column of M_{and} is the result of cascading a_3 and a_4, the next $(v_3 - 1)$ columns of M_{and} is the result of cascading the vectors of F_3 with k_4 zeros. The last $(v_4 - 1)$ columns of M_{and} is the result of cascading k_3 zeros with vectors in F_4. M_{and} can be expressed as

$$M_{and} = \begin{bmatrix} a_3 & a_3 & F_3 & 0 \\ 0 & a_4 & 0 & F_4 \end{bmatrix} \tag{2}$$

D. ATTRIBUTE-BASED PROXY RE-ENCRYPTION

The concept of proxy re-encryption was first proposed by Blaze *et al.* [37] in 1998 and was not formally defined until 2006. Proxy re-encryption means that the proxy converts the ciphertext into a ciphertext that the visitor can decrypt, while the proxy cannot obtain any plaintext. The attribute-based proxy re-encryption algorithm [38] only allows users who satisfy the access structure to decrypt data, mainly including the following seven algorithms:

- *Setup* is the system initialization algorithm. It takes as input a security parameter λ and the attribute set X. It outputs the system parameters *Sparams*, a master key *MSK* and the system public key *SPK*. Expose *Sparams* and *SPK* public, but keep *MSK* secret. The system initialization algorithm can be expressed as $Setup(\lambda, X) \rightarrow (Sparams, MSK, SPK)$.
- *KeyGen* is the key generation algorithm. Given the system parameters *Sparams*, the master key *MSK*, the system public key *SPK*, and the attribute set $S_C \subseteq X$ of the user Cindy, the private key SK_C and public key PK_C of Cindy are generated. The key generation algorithm can be described as $KeyGen(Sparams, MSK, SPK, S_C) \rightarrow (SK_C, PK_C)$.
- *Enc* is the data encryption algorithm. The ciphertext C is generated by the system parameters *Sparams*, Cindy's public key PK_C, the access structure (M, ρ), and plaintext m. The encryption algorithm can be expressed as $Enc(Sparams, PK_C, (M, \rho), m) \rightarrow C$.
- Re*KeyGen* is the re-encryption key generation algorithm. Suppose Cindy is the data owner and Nancy is the data visitor. Input the system parameters *Sparams*, a new access structure (M', ρ'), Cindy's private key SK_C and her attribute set S_C, and Nancy's public key PK_N. Output the re-encryption key $RK_{C\rightarrow N}$, that is, $ReKeyGen(Sparams, (M', \rho'), SK_C, S_C, PK_N) \rightarrow RK_{C\rightarrow N}$.
- Re*Enc* is a re-encryption algorithm. The re-encrypted ciphertext C' is generated by the system parameters *Sparams*, the system public key *SPK*, the re-encryption key $RK_{C\rightarrow N}$, and the ciphertext C. The re-encryption algorithm can be represented by $ReEnc(Sparams, SPK, RK_{C\rightarrow N}, C) \rightarrow C'$.
- *Dec* is the ciphertext decryption algorithm. Taking as input the system public key *SPK*, Cindy's private key SK_C, and the ciphertext C, the algorithm outputs the plaintext m, that is, $Dec(SPK, SK_C, C) \rightarrow m$.
- Re*Dec* is a re-encrypted ciphertext decryption algorithm. Nancy's private key SK_C is used to decrypt the re-encrypted ciphertext C' to get the plaintext m, that is, $ReDec(SK_N, C') \rightarrow m$.

III. PROPOSED SYSTEM FRAMEWORK

DSCSCB can not only realize secure data sharing but also provide customized services for onboard units, the system framework of which is shown in Figure 2. It mainly includes the onboard unit, roadside unit, consortium blockchain, trusted authority, consensus mechanism, smart contract and service sector. The detailed definition of each entity is as follows.

A. ONBOARD UNIT

The structure of the onboard unit is shown in Figure 3. The onboard unit (*OBU*) is equipped with a communication module, a sensor, a memory unit, an embedded computer, etc. Among them, the sensor is used to collect driving data of the vehicle, such as speed, mileage, working status of automobile parts, etc., and sends them to the *OBU*. The *OBU* integrates driving data to form plaintext, then the plaintext and the access structure are encrypted to generate the ciphertext, which is sent to the *RSU* by dedicated short-range communication [39]. Once an *OBU* is produced, a unique identity is assigned to it. The *OBU* as the data owner is responsible for encrypting the plaintext and preseting the access structure of the data. The service sector can access data only if the access policy is met.

B. ROADSIDE UNIT

Compared with the *OBU*, the *RSU* has stronger computing power and larger storage. The *RSU* is generally installed on

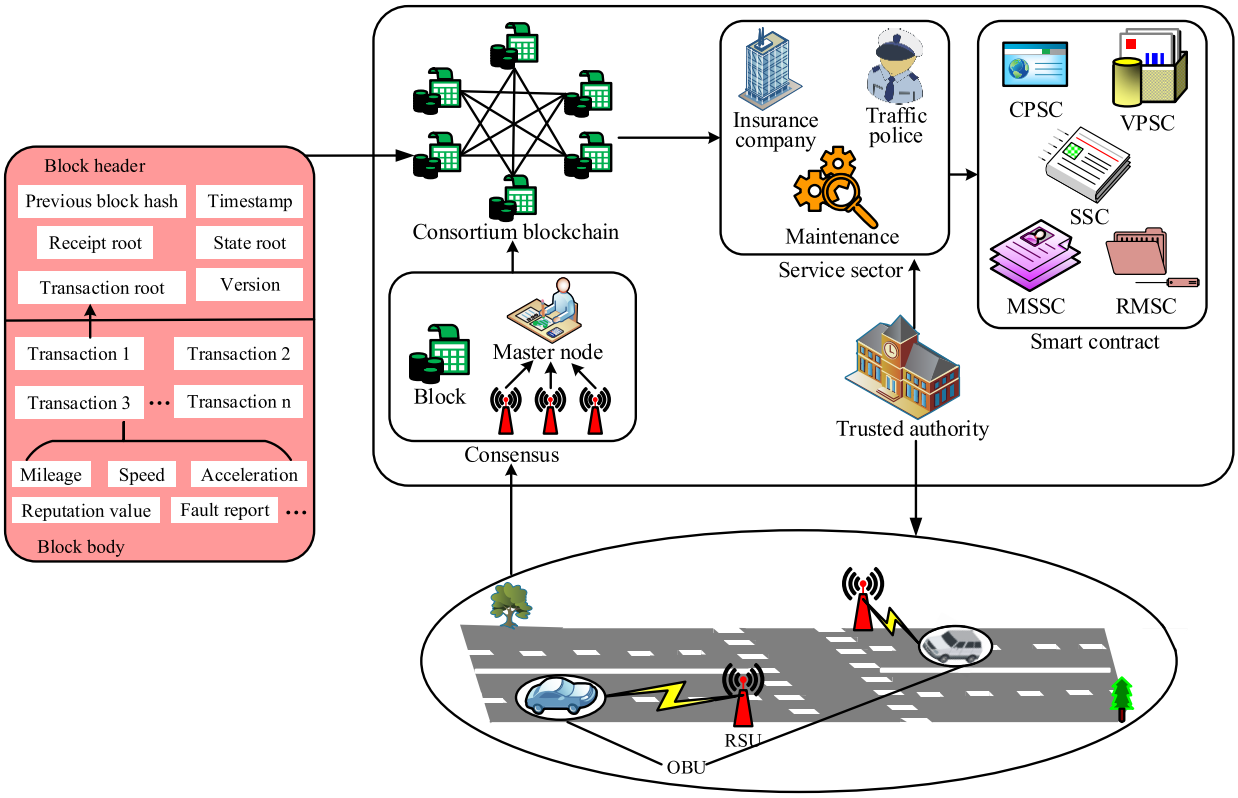

FIGURE 2. DSCSCB system framework.

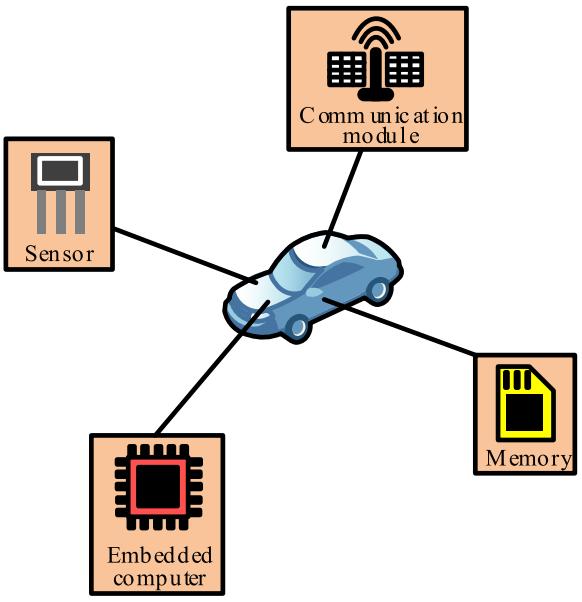

FIGURE 3. The structure of the onboard unit.

both sides of the road every kilometer or even shorter distance to ensure a high quality communication environment even in a traffic congestion. The *RSU* communicates with the *OBU* through a wireless network, whereas it communicates with other *RSUs* through a wire network. The *RSU* is required to be registered in the blockchain with identity when it is used. The *RSU* with better performance is pre-selected as an accounting node to verify traffic data sent by the *OBU*.

C. TRUSTED AUTHORITY

It is assumed that the trusted authority (*TA*) has strong computing power and huge storage space in the whole network, which is secure and hard to be captured. *TA* is mainly responsible for generating the system parameters, the master key, private keys, search keys and re-encryption keys.

D. CONSORTIUM BLOCKCHAIN

For more secure data sharing and less network overhead, it is appropriate to adopt the consortium blockchain. The block body of the consortium blockchain mainly records the location, speed, reputation value and other data. The receipt root in the block head stores customized services provided by the service sector. For example, the insurance contract specially formulated by the insurance company according to the driving style of the owner. The transaction root mainly records the driving data of the *OBU*, such as acceleration, mileage, etc. As for the status root, it saves the overall status of the service sector. For instance, data accessed by the service sector.

E. CONSENSUS MECHANISM

In this paper, Ripple Consensus is used to verify the data and each *RSU* is a verification node. Nodes with better performance (more computing power and better hardware

and software environment) are selected from the verification nodes to join the master node list. The *RSU* stores the data sent by the *OBU* to the local buffer pool, and then the local data is aggregated and sent to the master node for verifying. Master nodes verify the data and send the result to the *RSU*. The data confirmed by more than 80 percent of the master nodes is packaged into blocks, which are then connected to the consortium blockchain.

F. SMART CONTRACT

The smart contract was first proposed by cryptographer Nick Szabo in 1994 [40], which means implementing contract terms by using computerized transaction protocols and user interfaces. Blockchain periodically traverses the trigger condition and the state of the smart contract. Once the trigger condition is met, the smart contract is invoked to control and manage the nodes in the blockchain. DSCSCB contains automatic claim and insurance pricing smart contract (CPSC), traffic violation penalty smart contract (VPSC), maintenance service smart contract (MSSC) and search service smart contract (SSC).

G. SERVICE SECTOR

1) THE INSURANCE COMPANY

Whenever a traffic accident happens, the car owner makes a claim on the insurance company and then pays the credit value to the CPSC address as a collateral to guarantee the solvency of the owner and avoid false requests. The insurance company obtains mileage, acceleration, vehicle speed, vehicle device status (such as brake pads, steering wheel control, engine, throttle control) and other related data from the blockchain according to the access policy. CPSC is utilized to traffic accident arbitration, evaluate insurance premiums, automatic claims and financial settlement. After the claim is completed, CPSC pays the insurance company the credit value as the service fee.

The insurance company has already established a database based on relevant data provided by the *OBU* and has made use of data analysis with CPSC to formulate customized insurance contracts for car owners with different driving style, thereby reducing the insurance cost. After the insurance contract has been made, the credit value will be paid as a reward to the onboard unit that provides data.

2) THE TRAFFIC POLICE

The traffic police obtains information such as the speed, position, and lane change of the vehicle and so on from the blockchain according to the access policy, and determines whether the driver complies with the traffic rules. Once the driver has violated the rules, the traffic police uses VPSC to deduct the *OBU*'s credit value and impose a fine. VPSC enhances drivers' awareness of complying with traffic rules, so it can effectively improves traffic safety.

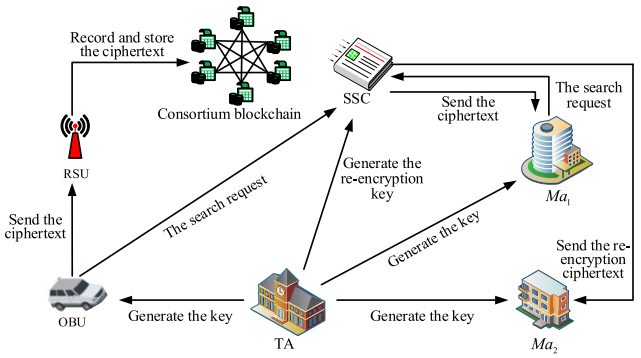

FIGURE 4. Secure data sharing.

3) THE VEHICLE MAINTENANCE

OBU submits a service request to the vehicle maintenance in case of *OBU* failure. The credit value is paid to MSSC address as a mortgage to ensure that the owner has the ability to pay the service fee and avoid false requests. After receiving the request, the vehicle maintenance obtains the working status data of vehicle components from the blockchain according to the access policy. The operation state of parts and equipment is analyzed and the vehicle maintenance system model is established to determine the cause of the *OBU* failure. Then, the vehicle maintenance uses the MSSC to develop a maintenance plan for the faulty *OBU*. After the *OBU* repair is completed, the MSSC pays the credit value as a service fee to the vehicle maintenance.

The vehicle maintenance obtains the relevant data of the *OBU* according to the access structure. Data analysis and the MSSC are used to formulate different vehicle maintenance plans. After the maintenance plans have been made, the credit value will be paid as a reward to the *OBU* that provides data.

IV. SECURE DATA SHARING

Take vehicle maintenance service as an example, as shown in Figure 4. Assume that *OBU* has failed, we want to carry out fault diagnosis and maintenance in the vehicle maintenance company within 3km of home. *OBU* encrypts relevant data such as the working status of vehicle components under $L_1 = \{within\ 3km\ \ away\ from\ home\}$ condition to generate the ciphertext and send the ciphertext to the *RSU*. The *RSU* node records the successfully verified ciphertext into the block, and then connects the block to the blockchain. The SSC searches for a vehicle maintenance Ma_1 that satisfies $L_1 = \{within\ \ 3km\ away\ from\ home\}$ and sends the ciphertext to it, so that Ma_1 can provide customized services for the *OBU*. If the maintenance level and conditions of Ma_1 can't solve the faults of *OBU* in the process of service, Ma_1 needs to cooperate with other maintenance companies that should meet th e condition $L_2 = \{Automobile\ Sales\ Servicshop\ 4S\}$. If Ma_2 satisfies the above conditions, SSC will convert the ciphertext under L_1 condition to the re-encrypted ciphertext under L_2 condition, so that Ma_2 can decrypt the re-encrypted ciphertext.

TABLE 1. Notation descriptions.

Notation	Definition
Sparams	System parameters
MSK	Master screte key
SK	Secret key
RK	Re-encryption key
X	Attribute set
S	User's attribute set
KW	Keyword set
(M, ρ)	Shared Permission
m	Plaintext
C	Ciphertext
$C^{'}$	Re-encrypted ciphertext

The process of secure data sharing is divided into two stages. The first stage is that the *OBU*, as the data owner, sends a search request to SSC, and SSC feedbacks retrieval results to the vehicle maintenance company Ma_1. The second stage is that maintenance company Ma_1, as the data owner, sends a search request to SSC, and SSC feeds search results back to maintenance company Ma_2.

In this paper, we propose a searchable attribute-based proxy re-encryption algorithm, which not only implements secure data sharing and keyword search, but also data forwarding. Table 1 is the symbol description involved in our scheme. Take the automobile maintenance as an example to describe our scheme in detail. The process of providing services by the insurance company and the traffic police is similar, and is not repeated here.

A. SYSTEM INITIALIZATION

G_1 and G_2 are two multiplicative cyclic groups with prime order p, g and g_1 are generators of G_1. There is a bilinear pairing $e : G_1 \times G_1 \rightarrow G_2$. Define message authentication function Y and six target collision resistance hash functions: $H_1 : \{0,1\}^{2k} \rightarrow Z_p^*$, $H_2 : G_2 \rightarrow \{0,1\}^{2k}$, $H_3, H_4, H_5 : \{0,1\}^* \rightarrow G_1$, $H_6 : \{0,1\}^k \rightarrow Z_p^*$. Random select $a, b \in Z_p^*$, input security parameter 1^λ and the attribute universe X, output the system parameters $Sparams = \left(e, p, g, g^a, e(g,g)^b, g_1, Y, H_1, H_2, H_3, H_4, H_5, H_6\right)$ and the master key $MSK = \left(g^b, a\right)$.

B. KEY GENERATION

Key generation includes private key generation and search key generation.

1) PRIVATE KEY GENERATION

Input system parameter *Sparams* and the user's attribute set $S \subseteq X$ with identity tag i, randomly select $c \in Z_p^*$, calculate $A = g^b g^{ac}$, $B = g^c$, and $D_x = \{H_3(x)^c\}_{\forall x \in S}$. Generate private key $SK = (A, B, D_x)$ for the user. *TA* stores (i, g^{ac}) in the local list.

2) SEARCH KEY GENERATION

When the user searches the keyword kw, d is randomly selected from Z_p^* to calculate $\varpi = g^d$. *TA* searches i in the local list after receiving (i, ϖ), and if i is in the local list, *TA* will generate a search key $SK' = g^{ac}\varpi^b$ for the keyword.

C. DATA ENCRYPTION

M in the access structure (M, ρ) is a matrix of $l \times n$. M_j represents the $j-th$ row vector of M, ρ is the row mapping of M. *OBU* randomly selects $\alpha \in \{0,1\}^k$ to calculate $s = H_1(m, \alpha)$. The vector $z = (s, z_2, z_3, \ldots, z_n)$ is selected from Z_p^* to share the secret index s, then randomly select $r_1, r_2, \ldots r_l \in Z_p^*$ and calculate

$$\begin{cases} U_1 = (m||\alpha) \oplus H_2(e(g,g)^{bs}),\ U_2 = g^s,\ U_3 = g_1^s \\ \left\{V_j = g^{a\eta_j} H_3(\rho(j))^{-r_j}\right\}_{j\in[l]} \\ \left\{W_j = g^{r_j}\right\}_{j\in[l]} \\ Z = (H_4(U_1, U_3, (V_j, W_j)_{j=1}^l, (M, \rho)))^s \end{cases} \tag{3}$$

where $\eta_j = z \cdot M_j$, $J = \{\rho(j) \in S | 1 \le j \le l\}$ represents the attribute used in the access structure (M, ρ), and l is the number of attributes in the access structure (M, ρ). *OBU* sends ciphertext $C = \left(U_1, U_2, U_3, V_j, W_j, Z\right)_{j\in[l]}$ to *RSU*. *RSU* records the ciphertext C in the block and uses the Ripple consensus to verify the validity of the data in the block. Once the verification is successful, the current block is connected to the blockchain.

D. RE-ENCRYPTION KEY GENERATION

TA randomly selects $\theta, \alpha' \in \{0,1\}^k$, calculates $s' = H_1(\theta, \alpha')$, selects vector $z' = (s', z_2', z_3', \ldots, z_n')$ from Z_p^* sharing the secret index s'. Let $\eta_j' = z \cdot M_j'$, where M_j' is the $j-th$ row vector of M' in the new access structure (M', ρ') (M' is a matrix of $l' \times n'$, ρ' is row mapping of M'). Randomly select $r_1', r_2', \ldots r_l' \in Z_p^*$ and calculate

$$\begin{cases} U_1' = (\theta||\alpha') \oplus H_2(e(g,g)^{bs'}),\ U_2' = g^{s'} \\ \left\{V_j' = g^{a\eta_j'} H_3(\rho'(j))^{-r_j'}\right\}_{j\in[l']} \\ \left\{W_j' = g^{r_j'}\right\}_{j\in[l']} \\ Z' = (H_5(U_1', U_2', (V_j', W_j')_{j=1}^{l'}, S, (M', \rho')))^{s'} \end{cases} \tag{4}$$

Output $RK_4 = \left(U_1', U_2', V_j', W_j', Z'\right)$. Randomly select β from Z_p^* and calculate

$$\begin{cases} RK_1 = A^{H_6(\theta)} \cdot g_1^\beta \\ RK_2 = g^\beta \\ RK_3 = B^{H_6(\theta)} \\ RK_4 \\ R_x = \left\{D_x^{H_6(\theta)}\right\}_{\forall x \in S} \end{cases} \tag{5}$$

TA sends the re-encryption key $RK = (RK_1, RK_2, RK_3, RK_4, R_x)$ to the SSC.

E. RE-ENCRYPTION

Suppose there are coefficient $\left\{\omega_j \in Z_p^*\right\}_{j\in J}$ such that $\sum_{j\in J} \omega_j M_j = (1, 0, \ldots, 0)$, then $\sum_{j\in J} \omega_j \eta_j = s$. After receiving the re-encryption key RK, SSC first verifies

whether the re-encryption key contains a valid attribute set S and the access structure (M', ρ'), namely to check whether the verification equation (6) is valid or not.

$$e(U_2', H_5(U_1', U_2', (V_1', W_1'), S, (M', \rho'))) = e(g, Z') \quad (6)$$

When equation (6) is true, the SSC verifies the validity of the ciphertext, that is., whether equation (7) holds.

$$\begin{cases} e(U_2, g_1) = e(g, U_3) \\ e(U_3, H_4(U_1, U_3, (V_1, W_1)^l, (M, \rho))) = e(g_1, Z) \\ e(\prod_{j\in J} V_j^{\omega_j}, g^a) = e(U_2, g) \cdot \prod_{j\in J} e(W_j^{-1}, H_3(\rho(j))^{\omega_j}) \end{cases} \quad (7)$$

If equation (7) is valid and then calculate

$$U_4 = \frac{e(U_2, RK_1)/e(U_3, RK_2)}{\prod_{j\in J} (e(V_j, RK_3) \cdot e(W_j, R_{\rho(j)}))^{\omega_j}} \quad (8)$$

Re-encryption key RK is used to encrypt the ciphertext C and re-encryption ciphertext is $C' = (U_1, U_2, U_3, U_4, RK_4, (V_j, W_j)_{j=1}^l, Z, S, (M, \rho))$.

F. INDEX AND SEARCH TOKEN GENERATION

The keyword set of plaintext m is $KW = \{kw_j\}_{j=1}^l$, and a bit string h_j is randomly selected for each keyword. The authentication code $y_j = e(g, g)^{bs} \cdot e(g, H_3(kw_j))^s$ of kw_j in the ciphertext C is calculated, and the index of ciphertext is $Index = (h_j, Y(y_j, h_j))$. Similarly, the authentication code $y_j' = e(g, g)^{bs'} \cdot e(g, H_3(kw_j))^{s'}$ in re-encrypted ciphertext C' is obtained, and the index of re-encrypted ciphertext is $Index' = \left(h_j, Y(y_j', h_j)\right)$.

According to the user's private key, the attribute set, the keyword kw' and the corresponding search key SK', we can calculate

$$\begin{cases} I = H_3(kw) \left(g^{ac} \cdot \varpi^b\right)^{1/d} \\ B' = B^{1/d} \\ \left\{D_x' = (D_x)^{1/d}\right\}_{x\in S} \end{cases} \quad (9)$$

So the search token of keyword kw is $tk = \left(I, B', D_x'\right)$, and $tk = \left(I, B', D_x'\right)$ is stored in the SSC, which is convenient to provide keyword search service for users.

G. VERIFICATION

In order to retrieve keyword, the user sends search token and the attribute set to SSC. The user can perform keyword search on the ciphertext or keyword search on the re-encrypted ciphertext.

Step 1: After receiving the user's search token tk and the attribute set S, the SSC verifies whether the attribute set S satisfies the access structure (M, ρ). If so, calculate

$$\begin{cases} Q_C = \prod_{j\in J} \left(e\left(V_j, B'\right) \cdot e(W_j, D_{\rho(j)}')\right)^{\omega_j} \\ O_{kw} = \dfrac{e(U_2, I)}{Q_C} \end{cases} \quad (10)$$

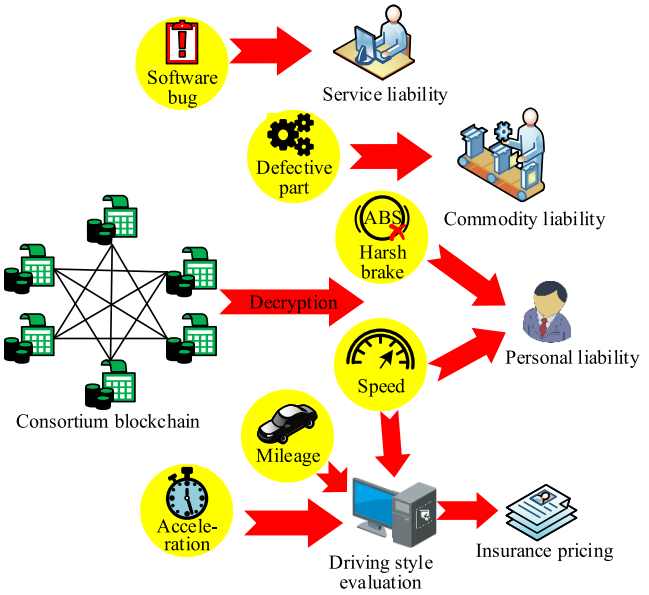

FIGURE 5. CPSC structure diagram.

Step 2: Verify whether the keyword kw in tk is the same as that in $Index$, that is to verify whether equation (11) is true or not.

$$Y\left(h_j, O_{kw}\right) = Y\left(h_j, y_j\right) \quad (11)$$

Step 3: If the equation (11) is true, the SSC sends the retrieved ciphertext to the user, otherwise output $\perp$.

The process of searching re-encrypted ciphertext is similar. First, verify whether the attribute set S' satisfies the access structure $\left(M', \rho'\right)$. If it is satisfied, calculate $Q_{C'} = \prod_{j\in J} \left(e\left(V_j', B'\right) \cdot e(W_j', D_{\rho(j)}')\right)^{\omega_j'}$ and $O_{kw}' = \frac{e(U_2', I)}{Q_{C'}}$. Then verify whether the keyword kw in tk is the same as that in $Index'$. If that is the same, the retrieved re-encrypted ciphertext is sent to the user, otherwise output $\perp$.

H. CIPHERTEXT DECRYPTION

The user who obtains the ciphertext first verifies the validity of the ciphertext according to equation (7), outputs $\perp$ if the verification fails, otherwise calculates $R = \frac{e(U_2, A)}{Q_C^{d_j}}$ If $U_3 = g_1^{H_1(m,\alpha)}$, then calculate $m||\alpha = H_2(R) \oplus U_1$ to get plaintext, otherwise output $\perp$.

I. RE-ENCRYPTION CIPHERTEXT DECRYPTION

Let $J' = \{\rho'(j) \in S' | 1 \le j \le l'\}$, verify whether $e(U_2', H_5(U_1', U_2', (V_j', W_j')_{j=1}^{l'}, S', (M', \rho'))) = e(g, Z')$ is true, output $\perp$ if the equation is invalid, otherwise calculate $R' = \frac{e(U_2', A)}{Q_{C'}^{d_j}}$. If $U_3 = g_1^{H_1(m,\alpha)}$, $Z = H_4\left(U_1, U_3, (V_j, W_j)_{j=1}^l, (M, \rho)\right)^{H_1(m,\alpha)}$, then calculate $m||\alpha = H_2\left(U_4^{1/H_5(\theta)}\right) \oplus U_1$ to get plaintext, otherwise output $\perp$.

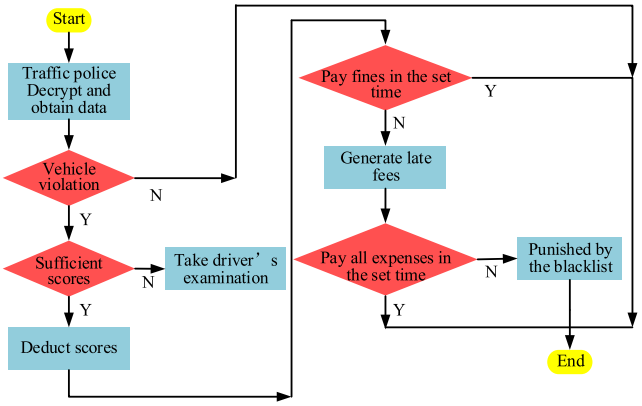

FIGURE 6. VPSC flow chart.

V. CUSTOMIZED SERVICES

A. INSURANCE CLAIM SETTLEMENT AND PRICING

CPSC structure as shown in Figure 5. There are three kinds of liability attributions for traffic accidents. Personal liability refers to the situation that the owner violates traffic rules, such as speeding, emergency braking, etc. Commodity liability refers to the condition in which the accident occurs due to the defective devices yielded by the manufacturer. Service liability refers to the scene where bugs in software provided by software providers cause accidents. The insurance company arbitrates according to the responding traffic data after the accident happens, and then automatically compensates the injured party based on the arbitration result. CPSC not only changes the long waiting period of existing insurance claims, but also avoids insurance fraud.

Insurance companies obtain the information of mileage, speed, and acceleration from traffic data. Data analysis technology is used to establish the driving style evaluation model, which analyzes vehicle owners' driving behaviors and habits. Then the insurance company provides the personalized insurance pricing aligned with their driving styles to users. Vehicle owners must pay exorbitant insurance if their mileage, speed and acceleration exceed the threshold, and vice versa, only pay the normal price of insurance. Compared with traditional car insurance pricing, personalized insurance pricing promotes car owners to correct bad driving habits, improves traffic safety and reduces insurance costs.

B. TRAFFIC VIOLATION PENALTY

Figure 6 shows the flow chart of VPSC. The traffic police decrypts the speed, location and lane change from the consortium blockchain. When the vehicle has the violations of speeding, retrograde, or illegal lane change, the traffic police deducts vehicle scores and fines. If the remaining scores are insufficient, the vehicle owner must take driver's theoretical test again. The vehicle owner has got to pay fines within the prescribed time, otherwise the late fee will arise. In case fines and late fees are not paid in the specified time, the vehicle owner is added to the blacklist. VPSC promotes car owners to restrain their driving behavior, and effectively curb the phenomenon of "buying and selling scores", that is, car owners with deficient scores buy scores from other car owners with sufficient scores to avoid the driver's theoretical examination.

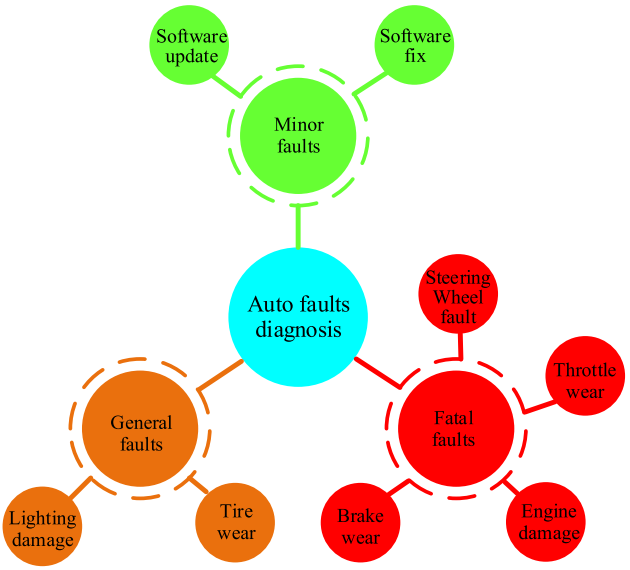

FIGURE 7. Automobile faults classification.

C. MAINTENANCE SERVICE

Automobile faults can be divided into minor faults, general faults and fatal faults, as shown in Figure 7. In case of a fault, *OBU* immediately transmits a fault report to the maintenance service provider, which includes fault types, fault components, location, fault time, *OBU's ID*, and the vehicle owner's contact number. The maintenance service provider leverages the MSSC to make maintenance strategies based on failure reports. For instance, software updating only needs remote control. Nevertheless, the maintenance service provider sends a general repair notice to the owner under the circumstances of uneven tire wear and lighting damage. Furthermore, when the vehicle has steering wheel malfunction, engine power loss or other fatal failures, the maintenance service provider sends the warning message to the owner and makes an appointment for on-site repairs.

VI. SECURITY ANALYSIS AND PERFORMANCE EVALUATION

In this section, we describe the security analysis and performance evaluation of our proposed DSCSCB. The experimental results show that our scheme has better performance.

A. SECURITY ANALYSIS

1) CORRECTNESS FOR DATA

a: CORRECTNESS FOR CIPHERTEXT

Simplify Q_C to get

$$Q_C = \prod_{j\in J}\left(e\left(V_j, B'\right)\cdot e(W_j, D'_{\rho(j)})\right)^{\omega_j}$$
$$= \prod_{j\in J}\left(e(g^{a\eta_j}H_3(\rho(j))^{-r_j}, g^{c/d_j})\cdot e\left(g^{r_j}, H_3\left(\rho(j)\right)^{c/d_j}\right)\right)^{\omega_j}$$

$$= \prod_{j\in J}\left(e\left(H_3(\rho(j))^{-r_j}, g^{c/d_j}\right)\cdot e\left(g^{a\eta_j}, g^{c/d_j}\right)\right.$$
$$\left.\cdot e\left(g^{r_j}, H_3(\rho(j))^{c/d_j}\right)\right)^{\omega_j}$$
$$= \prod_{j\in J} e(g,g)^{ac\eta_j\omega_j/d_j}$$
$$= e(g,g)^{acs/d_j} \tag{12}$$

R is simplified as

$$R = \frac{e(U_2, A)}{Q_C^{d_j}} = \frac{e\left(g^s, g^b g^{ac}\right)}{e(g,g)^{acs}} = e(g,g)^{bs} \tag{13}$$

Then $H_2(R) \oplus U_1 = H_2\left(e(g,g)^{bs}\right) \oplus (m||\alpha) \oplus H_2(e(g,g)^{bs}) = m||\alpha$, so the ciphertext decryption is correct.

b: CORRECTNESS FOR RE-ENCRYPTED CIPHERTEXT

$R' = e(g,g)^{bs'}$ can be obtained from correctness for ciphertext and U_4 is simplified as (14), as shown at bottom of the next page,

Then

$$H_2\left(U_4^{\frac{1}{H_6(\theta)}}\right) \oplus U_1$$
$$= H_2\left(e(g,g)^{bs}\right) \oplus (m||\alpha) \oplus H_2(e(g,g)^{bs}) = m||\alpha,$$

so the decryption process of re-encrypted ciphertext is correct.

2) THE SECURITY OF DATA

a: THE SECURITY OF CIPHERTEXT

The validity of the ciphertext is verified by equations $e(U_2, g_1) = e(g, U_3)$ and $e(U_3, H_4(U_1, U_3, (V_1, W_1)^l, (M,\rho))) = e(g_1, Z)$, where $Z = (H_4(U_1, U_3, (V_j, W_j)_{j=1}^l, (M,\rho)))^s$ can be regarded as a signature. We use unidirectionality and collision resistant hash functions to prevent U_1, U_3, $(V_j, W_j)_{j=1}^l$ and the access structure (M,ρ) from being tampered with. Besides, the integrity of U_2 is bound by U_3. If any of U_1, U_2, U_3, and $(V_j, W_j)_{j=1}^l$ in the ciphertext is forged or tampered with, the Eq. (7) will not hold. Therefore, the security of ciphertext is guaranteed.

b: THE SECURITY OF RE-ENCRYPTED CIPHERTEXT

The validity of the attribute set S and the access structure (M', ρ') are verified by the equation $e(U_2', H_5(U_1', U_2', (V_1', W_1'), S, (M', \rho'))) = e(g, Z')$ before re-encrypting the ciphertext. The equation $e(\prod_{j\in J} V_j^{\omega_j}, g^a) = e(U_2, g) \cdot \prod_{j\in J} e(W_j^{-1}, H_3(\rho(j))^{\omega_j})$ guarantees the security of $(V_j, W_j)_{j=1}^l$. The security of U_1, U_3, $(V_j, W_j)_{j=1}^l$ and the access structure (M,ρ) is guaranteed by the signature Z. Furthermore, the validity of U_2 is verified by the equation $e(U_2, g_1) = e(g, U_3)$. Clearly, RK_4 is the part of the re-encryption key and its security is guaranteed by the trusted authority. Hence the re-encrypted ciphertext $C' = (U_1, U_2, U_3, U_4, RK_4, (V_j, W_j)_{j=1}^l, Z, S, (M,\rho))$ is secure and effective.

c: THE SECURITY OF KEYWORDS

The authentication code $y_j = e(g,g)^{bs} \cdot e(g, H_3(kw_j))^s$ is the result of encrypting the keyword kw_j. It is almost impossible to deduce the keyword from the authentication code. Even though $e(g,g)^b$ is obtained, $s = H_1(m,\alpha)$ cannot been known. Thus no information of the keyword can be obtained. Similarly, the keyword of the re-encrypted ciphertext are also secure. Users must send a search token to the smart contract before performing keyword search. In addition, each keyword corresponds to different d_j, which further improves the concealment and security of the keyword.

3) COLLUSION RESISTANT

The attribute set S and the access structure (M', ρ') are verified by U_2'. Besides, RK_1, RK_3, and R_x are closely related to RK_4 through θ. However, RK_1 is closely related to RK_2 through β. As long as any of RK_1, RK_2, RK_3, and R_x is tampered with, the re-encrypted ciphertext is invalid. If the attribute set, the access structure, and RK_4 are tampered with, the equation $e(U_2', H_5(U_1', U_2', (V_1', W_1'), S, (M', \rho'))) = e(g, Z')$ will not hold. Therefore our algorithm successfully resists collusion attacks.

4) THE SECURITY OF CONSORTIUM BLOCKCHAIN

The trusted authority only generates the private key and the search key for users who have the identity tag i in the local list. That is to say, only users who satisfy the access structure can perform keyword search, proxy re-encryption and secure data sharing in the entire consortium blockchain network. Search requests that do not satisfy the access structure will be ignored, which will not only ensure the security of the blockchain network, but also reduce the communication overhead and computational overhead to a certain extent. Users with different attribute sets have different identity tags. This identity tag is only used to distinguish the user's identity and does not reveal the user's identity privacy.

The *OBU* needs to pay the credit value as a collateral when it requests customized services, which avoids false requests and replay attacks. After the service sector provides customized services, the smart contract automatically deducts the credit value as the service fee and then returns the remaining credit value to the *OBU*. When the service sector needs relevant data to analyze and predict the customer's habits, so as to provide better services for customers, the service sector will reward the credit value to the *OBU* providing the data, which promotes secure data sharing.

Our scheme uses Ripple consensus to verify the data. Assuming there are f verification nodes in the network and the probability that the verification nodes become malicious nodes is $1/2$. Data cannot be tampered with unless there are at least $\frac{f-1}{5}$ malicious nodes in the network. Thereby the probability of successfully tampering with the block is

TABLE 2. Performance comparison between our scheme and other schemes.

Performance	Ref. [41]	Ref. [42]	Ref. [43]	DSCSCB
Confidentiality	✓	✓	✓	✓
Anti-collusion	✓	✓	×	✓
Data fine grain management	×	×	×	✓
Multidimensional service	×	×	✓	✓
Tamper-proofing	✓	✓	✓	✓
Decentration	×	✓	✓	✓

$1/2^{(f-1)/5}$. For instance, if there are 201 verification nodes in the network, the probability of successfully tampering with the block is $1/2^{40} \approx 9.095 \times 10^{-13}$. Therefore the data in the block is almost impossible to be tampered with.

B. PERFORMANCE EVALUTION

The *OBU* encrypts the data and the access structure to generate the ciphertext and sends it to the *RSU*. The *RSU* records the ciphertext into the block, and the verification node verifies the data in the block. After the verification succeeds, the block is connected to the blockchain. The search service smart contract will send the ciphertext to the service sector that satisfies the access structure. The service sector receives the corresponding ciphertext for decryption, and provides customized services to the *OBU*. For example, the insurance company designs appropriate insurance pricing and automatic claim settlement services for the *OBU*. The traffic police automatically deducts credit value and fines for the *OBU* that violates traffic rules, so as to regulate the driving behavior of the vehicle owner. The vehicle maintenance provides maintenance services for the fault vehicle. In the process of providing services, if the service sector needs to cooperate with other companies in the same field, keyword search can be carried out. The company that satisfies search keywords and the access structure will receive re-encrypted ciphertext. Then the company decrypts the re-encrypted ciphertext to obtain the corresponding plaintext, providing high quality and efficient services for the *OBU*.

Table 2 evaluates the performance of the existing schemes and our proposed DSCSCB. We propose an attribute-based proxy re-encryption algorithm that supports keyword search to realize secure data sharing and proxy re-encryption, which is beneficial to data fine-grained management and access control, protects data confidentiality and security, and can resist collusion attacks. Service sectors use the acquired data to provide multi-dimensional and customized services for the *OBU*. We use the consortium blockchain technology to break the centralized structure in the traditional intelligent transportation. The chain structure and the Ripple consensus effectively prevent data from being tampered with. Table 2 shows that our scheme has better performance than other schemes and is more suitable for secure data sharing and customized services for intelligent transportation.

C. COMPUTATIONAL OVERHEAD

The computational overhead mainly includes encryption, re-encryption, decryption and re-encrypted ciphertext decryption (re-decryption). Table 3 shows the comparison results of our scheme with references [44], [45] and [46], where T_B is the bilinear operation, T_E is the exponential operation on the multiplicative cyclic group. Compared with the above two operations, the multiplication operation's computation cost is very small and can be ignored. $|l|$ represents the number of attributes in the access structure and $|J|$ represents the number of attributes satisfying the access structure. The experiment runs on the Intel i5 processor with 8G memory and 3.0GHz frequency. The above two operations consume 1.57ms and 0.311ms respectively.

Figure 8 shows a comparison of computational overhead. Figure 8(a) shows that the computational overhead increases linearly with the number of attributes in the data encryption process. We use the hash function to sign the ciphertext. However, in references [44], [45] and [46], there is only data encryption and no signature process. Our scheme not only protects the integrity and non-repudiation of data, but also takes less time.

$$
\begin{aligned}
U_4 &= \frac{e(U_2, RK_1)/e(U_3, RK_2)}{\prod_{j\in J}\left(e(V_j, RK_3)\cdot e(W_j, R_{\rho(j)})\right)^{\omega_j}} \\
&= \frac{e\left(g^s, \left(g^b g^{ac}\right)^{H_6(\theta)}\cdot g_1^{\beta}\right)\Big/ e\left(g_1^s, g^{\beta}\right)}{\prod_{j\in J}\left(e\left(g^{a\eta_j}H_3(\rho(j))^{-r_j}, (g^c)^{H_6(\theta)}\right)\cdot e\left(g^{r_j}, H_3\left(\rho\left(j\right)\right)^{cH_6(\theta)}\right)\right)^{\omega_j}} \\
&= \frac{e\left(g^s, g^{bH_6(\theta)}\right)\cdot e\left(g^s, g^{acH_6(\theta)}\right)}{\prod_{j\in J}\left(e\left(g^{a\eta_j}, g^{cH_6(\theta)}\right)\cdot e\left(H_3(\rho(j))^{-r_j}, g^{cH_6(\theta)}\right)\cdot e\left(g^{r_j}, H_3\left(\rho\left(j\right)\right)^{cH_6(\theta)}\right)\right)^{\omega_j}} \\
&= \frac{e\left(g^s, g^{bH_6(\theta)}\right)\cdot e\left(g^s, g^{acH_6(\theta)}\right)}{e\left(g, g\right)^{acsH_6(\theta)}} \\
&= e\left(g, g\right)^{bsH_6(\theta)}
\end{aligned}
\tag{14}
$$

TABLE 3. Comparison of the computational overhead.

Scheme	encryption	Re-encryption	decryption	Re- decryption
Ref. [44]	$(3\|l\|+4)T_E+2T_B$	$(\|J\|+3)T_E+5(\|J\|+1)T_B$	$(\|J\|+3)T_E+3T_B$	$(\|J\|+6)T_E+5T_B$
Ref. [45]	$(3\|l\|+2)T_E+T_B$	$(3\|J\|+10)T_E+(5\|J\|+2)T_B$	$\|J\|T_E+7T_B$	$(\|J\|+2)T_E+9T_B$
Ref. [46]	$(3\|l\|+6)T_E+2T_B$	$(11\|J\|+17)T_E+(2\|J\|+7)T_B$	$T_E+(2\|J\|+6)T_B$	$2T_E+(2\|J\|+7)T_B$
Our scheme	$(3\|l\|+4)T_E$	$(4\|J\|+4)T_B$	$(\|J\|+1)T_E+T_B$	$(\|J\|+2)T_E+3T_B$

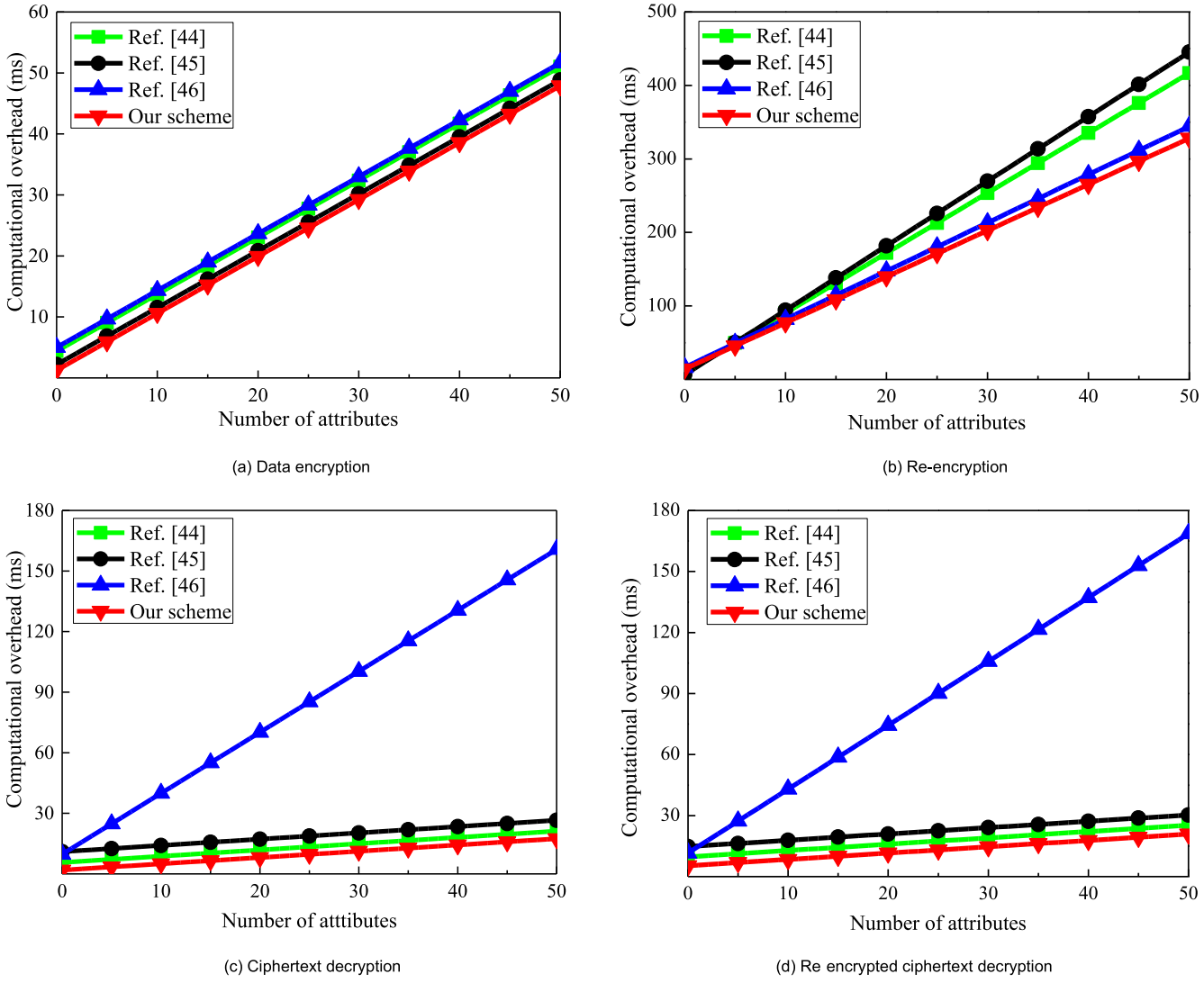

FIGURE 8. Computational overhead comparison diagram.

Figure 8(b) shows that the computational overhead of re-encryption, which increases linearly with the number of attributes. Before performing re-encryption, we first verify whether the re-encryption key contains a valid attribute set and the access structure, and then verify the validity of the ciphertext. If any verification process fails, we discard the data and terminate re-encryption. Our scheme has certain advantages over other schemes. Ref. [44] defines a parameter with complex calculation, which costs too much. In the process of re-encryption in Ref. [45], the proxy needs to frequently verify the user's token, resulting in a large computational overhead.

Figure 8(c) shows that as the number of attributes increases, the computational cost of our scheme in the

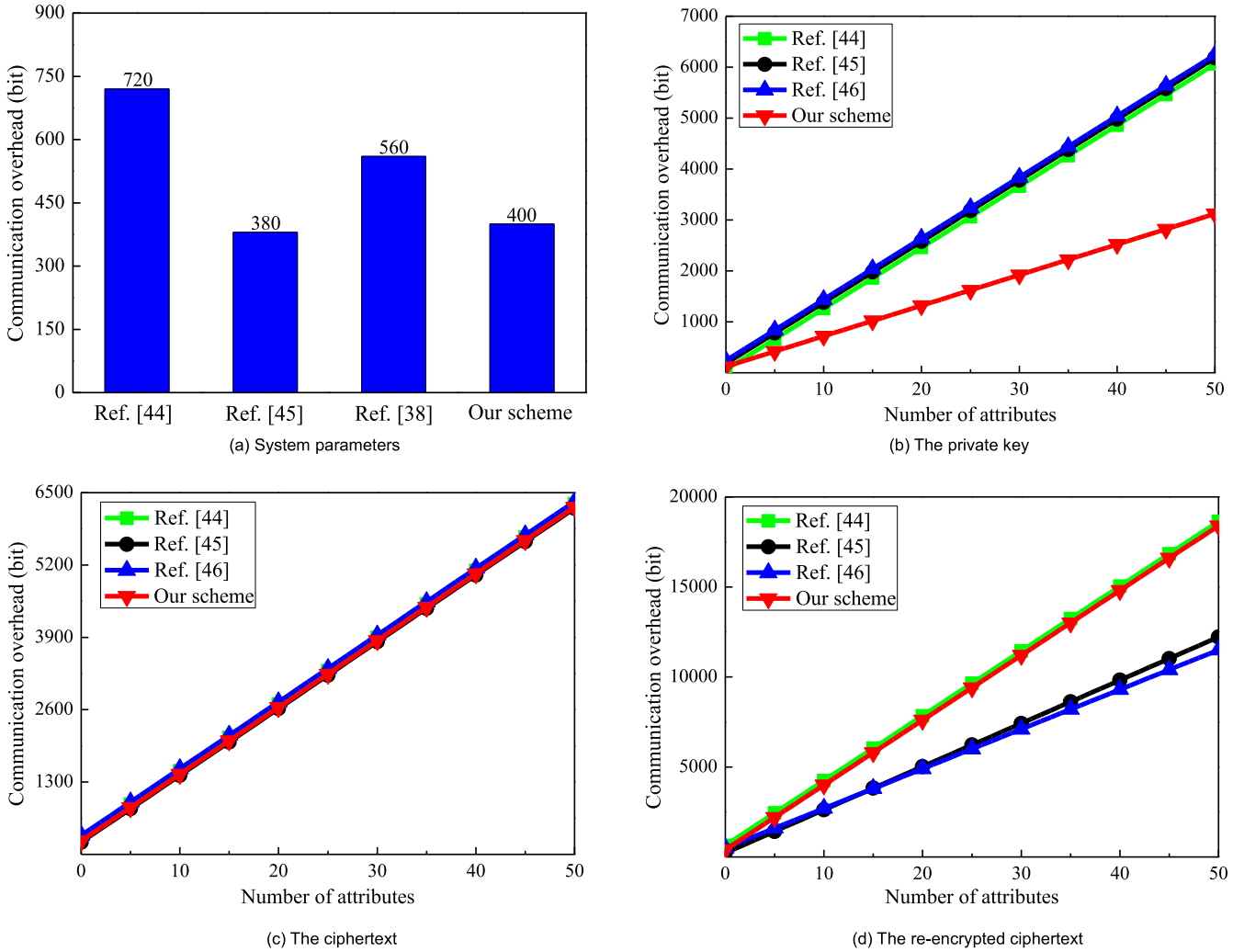

FIGURE 9. Communication overhead comparison diagram.

TABLE 4. Comparison of the communication overheads.

Scheme	System parameters	The private key	Ciphertext	Re- encrypted ciphertext
Ref. [44]	$10\|G_1\|+3\|G_2\|$	$(2\|S\|+1)\|G_1\|$	$(2\|I\|+5)\|G_1\|$	$(6\|J\|+10)\|G_1\|+\|G_2\|$
Ref. [45]	$5\|G_1\|+\|G_2\|$	$(2\|S\|+3)\|G_1\|$	$(2\|I\|+3)\|G_1\|+\|G_2\|$	$(4\|J\|+3)\|G_1\|+\|G_2\|$
Ref. [46]	$8\|G_1\|+2\|G_2\|$	$(2\|S\|+4)\|G_1\|$	$(2\|I\|+5)\|G_1\|+\|G_2\|$	$(2\|J\|+7)\|G_1\|+(\|J\|+2)\|G_2\|$
Our scheme	$6\|G_1\|+\|G_2\|$	$(\|S\|+2)\|G_1\|$	$(2\|I\|+4)\|G_1\|$	$6(\|J\|+1)\|G_1\|+\|G_2\|$

decryption process is the least. The search service smart contract simultaneously performs keyword matching and ciphertext partial decryption in the verification stage, which greatly reduces the computational overhead of decryption by the service sector. Our scheme only needs 17.431ms for ciphertext decryption with 50 attributes. Compared with the other three schemes, the computational overhead is reduced by 47.08% on average. In Ref. [46], the bilinear operation with large computational cost is frequently used in the decryption process, so the calculation overhead of the ciphertext decryption is the largest.

Figure 8(d) shows that the computational cost of re-decryption is linearly related to the number of attributes. As the number of attributes increases, our scheme advantages are more obvious. This scheme verifies whether the attribute set and access structure have been tampered with by the equation $e(U_2', H_5(U_1', U_2', (V_j', W_j')_{j=1}^{l'}, S', (M', \rho'))) = e(g, Z')$ before decrypting the re-encrypted ciphertext. Once the re-encrypted ciphertext is tampered with, the search service smart contract discard it, which reduces the network burden and computational overhead. Our scheme only needs 20.882ms to decrypt the ciphertext with 50 attributes.

Compared with the other three schemes, the computational overhead is reduced by 45.35% on average.

D. COMMUNICATION OVERHEAD

Suppose that $|G_1|$ and $|G_2|$ represent the bit length of G_1 and G_2 respectively, which are 60bit and 40bit. The length of Z_p^* is very small and can be ignored. $|S|$ represents the number of user attributes, $|l|$ represents the number of attributes in the access structure, and $|J|$ represents the number of attributes satisfying the access structure. The communication overhead in the process of secure data sharing and customized services provided by the service sector mainly includes system parameters, the private key, the ciphertext and the re-encrypted ciphertext. Table 4 shows the comparison results of communication cost between our scheme and references [44], [45] and [46].

In the process of system parameters generation, $g, g^a, g_1, H_3, H_4, H_5 \in G_1$ and $e(g,g)^b \in G_2$. So the communication overhead of system parameters is $6|G_1| + |G_2| = 6 \times 60 + 40 = 400bit$. During private key generation, $A, B \in G_1$ and $D_x \in G_1$ $(x \in S)$. So the communication overhead of the private key is $(|S|+2)|G_1| = 60(|S|+2)$. In the ciphertext, $U_1, U_2, U_3, Z \in G_1$ and $V_j, W_j \in G_1$ $(j \in l)$, so the communication cost of the ciphertext is $(2|l|+4)|G_1| = 60(2|l|+4)$. The calculation process for the communication overhead of re-encrypted ciphertext is similar, which will not be described again here.

Figure 9 shows the comparison of communication overhead between this paper and other three schemes. Figure 9 (a) and (b) show that the communication overhead of system parameters and the private key in our scheme has obvious advantages over the other three schemes. Figure 9 (c) shows the communication overhead of ciphertext. In our scheme, ciphertext contains the signatures, so the communication overhead is slightly larger than that of Ref. [45], but it has certain advantages compared with Ref. [44] and Ref. [46]. The communication overhead of the re-encrypted ciphertext is shown in Figure 9 (d). Compared with references [45] and [46], our scheme has more communication overhead. The re-encrypted ciphertext contains the parameter RK_4 with large communication overhead. This parameter can prevent the user's attribute set and the access structure from being tampered with, and solve the unverifiability of the re-encrypted ciphertext in Ref. [45]. In addition, U_1, U_3, $\left(V_j, W_j\right)_{j=1}^{l}$ and (M, ρ) are signed by Z, so their validity can be guaranteed. However, Ref. [46] cannot guarantee the validity of the components in the re-encrypted ciphertext. Therefore, the communication overhead of the re-encrypted ciphertext in this paper is greater than that in Ref. [45] and Ref. [46].

E. CONSORTIUM BLOCKCHAIN DELAY

The Ripple consensus used in this paper can generate a new block in only 3-6 seconds and do not need any confirmation time, so it only takes 3-6 seconds to generate a valid block. However, the Delegated Proof of Stake (DPoS) consensus generates a new block every 2 seconds, requiring 12 seconds of confirmation time. The Proof of Work (PoW) consensus generates a block every 10 minutes, requiring 60 minutes of confirmation time. Compared with DPoS and PoW, the Ripple consensus generates blocks and confirms data faster, so the delay is less.

VII. CONCLUSION

This paper proposed a novel scheme of secure data sharing and customized services for intelligent transportation based on the consortium blockchain, which not only conquers the disadvantage of the centralized data management in traditional intelligent transportation, but also ensures the confidentiality and security in the data interaction process, and thus effectively resists collusion attacks. The proposed attribute-based proxy re-encryption algorithm has the function of keyword searching by dividing the key into the attribute key and the search key, which not only supports keyword retrieval and proxy re-encryption, but also realizes secure data sharing, and then prevents the privacy data leakage of the *OBU*. After that, service sectors can use the smart contract to provide convenient and customized services, such as insurance pricing, vehicle maintenance, etc. Security analysis and performance evaluation show that our scheme has obvious advantages in the aspects of security, computational overhead, communication overhead and delay. Therefore, our scheme is suitable for secure data sharing and customized services in intelligent transportation.

In future research, we aim to propose an algorithm with better performance and less computational cost and communication overhead.

REFERENCES

[1] L. Zhu, F. R. Yu, Y. Wang, B. Ning, and T. Tang, "Big data analytics in intelligent transportation systems: A survey," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 1, pp. 383–398, Jan. 2019.

[2] K. C. Dey, A. Mishra, and M. Chowdhury, "Potential of intelligent transportation systems in mitigating adverse weather impacts on road mobility: A review," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 3, pp. 1107–1119, Jun. 2015.

[3] E. Talavera, A. Diaz Alvarez, and J. E. Naranjo, "A review of security aspects in vehicular ad-hoc networks," *IEEE Access*, vol. 7, pp. 41981–41988, 2019.

[4] B. Aslam, S. Park, C. C. Zou, and D. Turgut, "Secure traffic data propagation in vehicular ad hoc networks," *Int. J. Ad Hoc Ubiquitous Comput.*, vol. 6, no. 1, p. 24–39, 2010.

[5] X. Feng and L. Wang, "S2PD: A selective sharing scheme for privacy data in vehicular social networks," *IEEE Access*, vol. 6, pp. 55139–55148, 2018.

[6] P. Liu, B. Liu, Y. Sun, B. Zhao, and I. You, "Mitigating DoS attacks against pseudonymous authentication through puzzle-based co-authentication in 5G-VANET," *IEEE Access*, vol. 6, pp. 20795–20806, 2018.

[7] N. K. Prema, "Efficient secure aggregation in VANETs using fully homomorphic encryption (FHE)," *Mobile Netw. Appl.*, vol. 24, no. 2, pp. 434–442, Apr. 2019.

[8] J. Li, Y. Wang, Y. Zhang, and J. Han, "Full verifiability for outsourced decryption in attribute based encryption," *IEEE Trans. Services Comput.*, early access, May 31, 2017, doi: 10.1109/TSC.2017.2710190.

[9] J. Li, N. Chen, and Y. Zhang, "Extended file hierarchy access control scheme with attribute based encryption in cloud computing," *IEEE Trans. Emerg. Topics Comput.*, early access, Mar. 12, 2019, doi: 10.1109/TETC.2019.2904637.

[10] J. Li, X. Lin, Y. Zhang, and J. Han, "KSF-OABE: Outsourced attribute-based encryption with keyword search function for cloud storage," *IEEE Trans. Services Comput.*, vol. 10, no. 5, pp. 715–725, Sep./Oct. 2017.
[11] J. Li, W. Yao, Y. Zhang, H. Qian, and J. Han, "Flexible and fine-grained attribute-based data storage in cloud computing," *IEEE Trans. Services Comput.*, vol. 10, no. 5, pp. 785–796, Sep. 2017.
[12] J. Li, W. Yao, J. Han, Y. Zhang, and J. Shen, "User collusion avoidance CP-ABE with efficient attribute revocation for cloud storage," *IEEE Syst. J.*, vol. 12, no. 2, pp. 1767–1777, Jun. 2018.
[13] C. P. Ge, W. Susilo, J. D. Wang, Z. Q. Huang, L. M. Fang, and Y. J. Ren, "A Key-Policy Attribute-Based Proxy Re-Encryption Without Random Oracles," *The Comput. J.*, vol. 59, no. 7, pp. 970–982, Jul. 2016.
[14] C. Ge, W. Susilo, L. Fang, J. Wang, and Y. Shi, "A CCA-secure key-policy attribute-based proxy re-encryption in the adaptive corruption model for dropbox data sharing system," *Des., Codes Cryptogr.*, vol. 86, no. 11, pp. 2587–2603, Nov. 2018.
[15] G. Chunpeng, Z. Liu, J. Xia, and F. Liming, "Revocable identity-based broadcast proxy re-encryption for data sharing in clouds," *IEEE Trans. Dependable Secure Comput.*, early access, Feb. 14, 2019, doi: 10.1109/TDSC.2019.2899300.
[16] X. Yang, X. Yi, I. Khalil, Y. Zeng, X. Huang, S. Nepal, X. Yang, and H. Cui, "A lightweight authentication scheme for vehicular ad hoc networks based on MSR," *Veh. Commun.*, vol. 15, pp. 16–27, Jan. 2019.
[17] Y. Wang, Y. Ding, Q. Wu, Y. Wei, B. Qin, and H. Wang, "Privacy-preserving cloud-based road condition monitoring with source authentication in VANETs," *IEEE Trans. Inf. Forensics Security*, vol. 14, no. 7, pp. 1779–1790, Jul. 2019.
[18] J. Ni, K. Zhang, Y. Yu, X. Lin, and X. Shen, "Privacy-preserving smart parking navigation supporting efficient driving guidance retrieval," *IEEE Trans. Veh. Technol.*, vol. 67, no. 7, pp. 6504–6517, Jul. 2018.
[19] G. Kumar, R. Saha, M. K. Rai, and T.-H. Kim, "Multidimensional security provision for secure communication in vehicular ad hoc networks using hierarchical structure and End-to-End authentication," *IEEE Access*, vol. 6, pp. 46558–46567, 2018.
[20] S. Kanchan, G. Singh, and N. S. Chaudhari, "SAPSC: SignRecrypting authentication protocol using shareable clouds in VANET groups," *IET Intell. Transp. Syst.*, vol. 13, no. 9, pp. 1447–1460, Sep. 2019.
[21] J. Cui, D. Wu, J. Zhang, Y. Xu, and H. Zhong, "An efficient authentication scheme based on semi-trusted authority in VANETs," *IEEE Trans. Veh. Technol.*, vol. 68, no. 3, pp. 2972–2986, Mar. 2019.
[22] X. Han, Y. Yuan, and F. Y. Wang, "Security problems on blockchain: The state of the art and future trends," *Acta Autom. Sinica*, vol. 45, no. 1, pp. 206–225, Jan. 2019.
[23] J. Kang, R. Yu, X. Huang, M. Wu, S. Maharjan, S. Xie, and Y. Zhang, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4660–4670, Jun. 2019.
[24] A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A distributed solution to automotive security and privacy," *IEEE Commun. Mag.*, vol. 55, no. 12, pp. 119–125, Dec. 2017.
[25] Y.-T. Yang, L.-D. Chou, C.-W. Tseng, F.-H. Tseng, and C.-C. Liu, "Blockchain-based traffic event validation and trust verification for VANETs," *IEEE Access*, vol. 7, pp. 30868–30877, 2019.
[26] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, "Block4Forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles," *IEEE Commun. Mag.*, vol. 56, no. 10, pp. 50–57, Oct. 2018.
[27] L. Cheng, J. Liu, G. Xu, Z. Zhang, H. Wang, H.-N. Dai, Y. Wu, and W. Wang, "SCTSC: A semicentralized traffic signal control mode with attribute-based blockchain in IoVs," *IEEE Trans. Comput. Social Syst.*, vol. 6, no. 6, pp. 1373–1385, Dec. 2019.
[28] Z. Jin, R. Wu, X. Chen, and G. Li, "Charging guiding strategy for electric taxis based on consortium blockchain," *IEEE Access*, vol. 7, pp. 144144–144153, 2019.
[29] S. Nakamoto. (2018). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available:https://bitcoin.org/bitcoin.pdf.
[30] J. Xu, K. Xue, S. Li, H. Tian, J. Hong, P. Hong, and N. Yu, "Healthchain: A blockchain-based privacy preserving scheme for large-scale health data," *IEEE Internet Things J.*, vol. 6, no. 5, pp. 8770–8781, Oct. 2019.
[31] T. Zhang, H. Pota, C.-C. Chu, and R. Gadh, "Real-time renewable energy incentive system for electric vehicles using prioritization and cryptocurrency," *Appl. Energy*, vol. 226, pp. 582–594, Sep. 2018.
[32] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet Things J.*, vol. 4, no. 6, pp. 1832–1843, Dec. 2017.
[33] L. Zhang, M. Luo, J. Li, M. H. Au, K.-K. R. Choo, T. Chen, and S. Tian, "Blockchain based secure data sharing system for Internet of vehicles: A position paper," *Veh. Commun.*, vol. 16, pp. 85–93, Apr. 2019.
[34] X. Zhang and D. Wang, "Adaptive traffic signal control mechanism for intelligent transportation based on a consortium blockchain," *IEEE Access*, vol. 7, pp. 97281–97295, 2019.
[35] C. Tartary, S. Zhou, D. Lin, H. Wang, and J. Pieprzyk, "Analysis of bilinear pairing-based accumulator for identity escrowing," *IET Inf. Secur.*, vol. 2, no. 4, p. 99–107, Dec. 2008.
[36] H.-M. Hu and Z.-F. Zhou, "General multi-party protocol for computing inverses over a shared secret modulus," *Chin. J. Comput.*, vol. 33, no. 6, pp. 1040–1049, Jul. 2010.
[37] M. Blaze, G. Bleumer, and M. Strauss, "Divertible protocols and atomic proxy cryptography," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Spinger, 1998, pp. 127–144.
[38] L. Zhenhua, Z. Peilin, and D. Shuhong, "Attribute-based proxy re-encryption scheme with keyword search," *J. Electron. Inf. Technol.*, vol. 40, no. 3, pp. 683–689, Mar. 2018.
[39] X. Yin, X. Ma, and K. S. Trivedi, "An interacting stochastic models approach for the performance evaluation of DSRC vehicular safety communication," *IEEE Trans. Comput.*, vol. 62, no. 5, pp. 873–885, May 2013.
[40] N. Szabo. (1994). *Smart Contracts*. [Online]. Available: http://szabo.best.vwh.net/smart.contracts.html
[41] Q. Kong, R. Lu, M. Ma, and H. Bao, "A privacy-preserving sensory data sharing scheme in Internet of vehicles," *Future Gener. Comput. Syst.*, vol. 92, pp. 644–655, Mar. 2019.
[42] M. Li, L. Zhu, and X. Lin, "Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4573–4584, Jun. 2019.
[43] P. K. Sharma, N. Kumar, and J. H. Park, "Blockchain-based distributed framework for automotive industry in a smart city," *IEEE Trans. Ind. Informat.*, vol. 15, no. 7, pp. 4197–4205, Jul. 2019.
[44] K. Liang and W. Susilo, "Searchable attribute-based mechanism with efficient data sharing for secure cloud storage," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 9, pp. 1981–1992, Sep. 2015.
[45] D. Tiwari and G. R. Gangadharan, "SecCloudSharing: Secure data sharing in public cloud using ciphertext-policy attribute-based proxy re-encryption with revocation," *Int. J. Commun. Syst.*, vol. 31, no. 5, p. e3494, Mar. 2018.
[46] C. S. Feng, W. P. Luo, Z. G. Qin, D. Yuan, and L. P. Zou, "Attribute-based proxy re-encryption scheme with multiple features," *J. Commun.*, vol. 40, no. 6, pp. 177–189, Jun. 2019.

DI WANG received the B.S. degree in electronic and information engineering from the Jiangxi University of Science and Technology, Jiangxi, China, where she is currently pursuing the M.S. degree in communication and information system. Her current research interests include blockchain technology and information security.

XIAOHONG ZHANG received the B.S. degree in physics from Jiangxi Normal University, Jiangxi, China, in 1984, the M.S. degree in optical information processing from the Chinese Academy of Sciences, Changchun, China, in 1990, the Ph.D. degree in control theory and information safety from the University of Science and Technology Beijing (USTB), in 2002, and the Ph.D. degree from the Beijing University of Posts and Telecommunications (BUPT), in 2006. She was a Visiting Scholar with the University of California at Berkeley, Berkeley, CA, USA, from 2014 to 2015. She is currently a Full Professor with the Department of College of Information Engineering, Jiangxi University of Science and Technology, Ganzhou, China. Her main research interests include blockchain technology, information security, nonlinear dynamics, and wireless sensor networks.