IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 28, 2019, accepted August 11, 2019, date of publication August 21, 2019, date of current version September 4, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2936575

A Traceable Blockchain-Based Access Authentication System With Privacy Preservation in VANETs

DONG ZHENG, CHUNMING JING, RUI GUO, SHIYAO GAO, AND LIANG WANG
School of Cyberspace Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China
National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, Xi'an 710121, China

Corresponding author: Chunming Jing (chunmingjing@126.com)

This work was supported in part by the Natural Science Foundation of China under Grant 61802303, Grant 61772418, and Grant 61602378, in part by the Key Research and Development Program of Shaanxi under Grant 2019KW-053, in part by the Innovation Ability Support Program in Shaanxi Province of China under Grant 2017KJXX-47, and in part by the Natural Science Basic Research Plan in Shaanxi Province of China under Grant 2019JQ-866, Grant 2018JZ6001, and Grant 2016JM6033.

ABSTRACT The vehicular ad-hoc networks (VANETs) is one of the most promising application in the communications of smart vehicles and the smart transportation systems. However, authentication and privacy of users are still two vital issues in VANETs. It is crucial to prevent internal vehicles from broadcasting the forged messages while preserving the privacy of vehicles against the tracking attack. Moreover, in the traditional mode, the transactional data storage provides no distributed and decentralized security, so that the third party initiates the dishonest behaviors possibly. In this paper, based on blockchain technique, we propose a traceable and decentralized the Internet of Vehicle system framework for communication among smart vehicles by employing of a secure access authentication scheme between vehicles and RoadSide Units (RSUs). On the one hand, this scheme allows that vehicles employ pseudonyms for Vehicle to Vehicle (V2V) and Vehicle to Infrastructure (V2I) communications anonymously in the non-fully trusted environment. On the other hand, the transparency of vehicles in authentication and announcement is preformed efficiently by the blockchain technology. In addition, the transaction information is tamper-resistant that provides the distributed and decentralized property for the different cloud servers. With the help of Certificate Authority (CA) and the RoadSide Units (RSUs), our proposal achieves the conditional privacy to trace the real identity of the malicious vehicle in the anonymous announcements as well. Finally, through the theoretical analysis and simulations, our scheme is able to construct a secure and decentralized system framework of VANETs with accountability and privacy preservation.

INDEX TERMS Blockchain-based, privacy-preserving, authentication, traceability, VANETs.

I. INTRODUCTION

With the rapid development of urbanization, the smart city has attracted extensive attention in both academia and industry. It is estimated that the number of vehicles all over the world will reach 2 billion within the next 10 to 20 years [1]. The emergence of Vehicular ad-hoc Networks (VANETs) brings great convenience and comfortable driving experience for people. Two types of communications, namely the vehicle-to-infrastructure (V2I) communication and the vehicle-to-vehicle (V2V) communication are established in VANETs to promote cooperation among vehicles and share valuable driving information via the dedicated short-range communication (DSRC) radio [2]. In addition, it achieves eco-friendly mode by decreasing the expenditure of many public resources and reducing the traffic accidents and congestions.

However, for the high mobility and volatility of vehicles in the VANETs, the whole system is vulnerable to various attacks. Moreover, the security, privacy and credibility in this network should be taken into consideration seriously. With the increasing privacy and authentication concerns of the vehicles [3]–[5], there are two primary topics that refer to establish an effective vehicular communication network. Firstly, all messages must be announced and forwarded anonymously in the VANETs since these messages

The associate editor coordinating the review of this article and approving it for publication was Longxiang Gao.

usually contain the sensitive information of users, such as geographical location, license plate numbers, and so on. However, forwarding messages anonymously cannot guarantee the authenticity of the messages. Specifically, it is difficult to prevent the distribution of forged messages from internal vehicles fairly. These false messages not only reduce transportation efficiency, but also disturb the behavior of driver to cause the accident [6]. Secondly, although the majority of researches in the VANETs focus on conditional privacy and authentication [7]–[10], these works are short of efficient authentication, sufficient scalability and enough distribution. In the traditional scheme, the registration, authentication and revocation of vehicles are concentrated in only one party [11], which is prone to be attacked, like self-tempering with data, leaking vehicular information and distributing the forged information in the network. In addition, the centralized cloud server in the VANETs may cause a single point of failure in data storage. Thus, it leaks the important private information including vehicle identity and communication content, etc.

It needs a reliable communication environment to provide the solution of these issues above. Blockchain is the underlying technology of the Bitcoin [12] that is a peer to peer e-cash system. This technique is a novel decentralized ledger-based method that each node manages a copy of database from system in blockchain-based networks [13]. The blockchain is beneficial for establishing a desirable data-sharing platform in the VANETs. All the activities of participants, identity authentications and broadcasted messages will be written into the immutable and unforgeable ledger with the properties of tamper-resistance and decentralization.

A. RELATED WORKS

The open access environment created by VANETs brings great challenges in privacy and security that is unfit to be implemented in the real world [14]. Zhang *et al.* [15] proposed an Identity-based Batch Verification (IBV) scheme for V2I and V2V communications in VANETs, which employed a temper-proof device to protect privacy, and every device stored the system's master key to generate pseudoidentities locally. However, storing the system's master key in each vehicle may expose the system to powerful attackers and unpredictable risks. Moreover, this scheme failed in taking the scalability issue and resultant communication overhead into consideration. With increasing privacy attention in VANETs, some issues of privacy, such as anonymity, reliability and traceability have become the spots to be studied. Calandriello *et al.* [16] proposed a hybrid method that strengthens the framework using pseudonyms with self-certification, which is not necessary to manage them without compromising on the robustness of the system. Tan *et al.* [17] proposed a certificateless authentication protocol between vehicles and roadside units to realize vehicle's identity authentication, and Vijayakumar *et al.* [18] designed a secure authentication and key management mechanism to enhance user's key security in VANETs. However, the implementation of these two mechanisms relies on a trusted third party in the centralized system and does not provide the distributed security. Wu *et al.* [19] utilized one-time authentication and group signatures to identify malicious users. However, it is inefficient to trace suspicious messages due to expensive bilinear pairing operations at the stage of tracing. Qin *et al.* [20] adopted secure RSUs management to achieve pseudonyms control. Unfortunately, it is unable to work efficiently in areas with RSUs that are assumed as light-hardware with a low-security level in traditional VANETs.

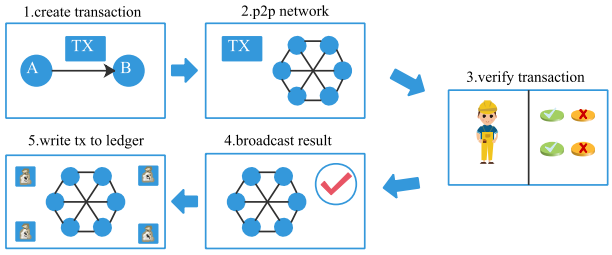

FIGURE 1. Transaction process of blockchain.

Blockchain is a chain structure that combines data blocks in chronological order, and a distributed data ledger shared and maintained by all nodes in a decentralized system. Taking Bitcoin as an example, the transaction process in blockchain is shown in Figure1. With the characteristic of decentralization, open autonomy, anonymous traceability and non-tampering of information, it has shown a broad application prospect and attracted lots of attention from the academic and industrial fields. Many researchers in VANETs focus on improving efficiency, guaranteeing privacy and security via blockchain technology. Yuan and Wang [21] proposed a secured and decentralized blockchain-based autonomous intelligent transportation systems. Rowan *et al.* [22] proposed a novel blockchain-based public key infrastructure and an inter-vehicle session key establishment protocol to secure vehicle-to-vehicle communications. Chuang *et al.* [23] presented a privacy preservation authentication scheme (PPAS) for communication between vehicle and infrastructure in VANETs, which achieved the vehicle and the RSU to authenticate each other and satisfied most of the security requirements. However, this scheme provides no distributed system and is used to communicate with vehicles. Peng [24] proposed an on-board network anonymous authentication protocol. Although this protocol guarantees user's anonymity and efficient authentication, it cannot trace the malicious vehicle identity. Lu *et al.* [25] designed a blockchain-based anonymous reputation system for VANET, and Malik *et al.* [26] proposed blockchain-based anonymous authentication for vehicular networks. In spite of [25] and [26] are realized that preserve users' privacy in the authentication process, none of their schemes introduce method of vehicle announcement, and only are suitable in Bitcoin without compatibility. Lu *et al.* [27] proposed an alternative way to overcome the limitation of pre-storing lots of anonymous certificates while preserving conditional privacy. However, the vehicle should change the

anonymous certificates frequently to avert the linkability of communication data, so that it should frequently interact with RSUs which affected the efficiency of VANETs seriously. The decentralized framework proposed in this paper provides reducing CA dependency, authentication with minimal overheads, data storage scheme for vehicular announcement and preserves vehicle privacy.

B. OUR CONTRIBUTIONS

In this paper, we propose a secure and anonymous authentication scheme for communication of smart vehicles. In addition, we present a distributed storage mechanism based on blockchain to prevent distribution of forged messages while simultaneously preserving the identity privacy of vehicles. Detailly, we make the following contributions:

- We propose a novel blockchain-based the Internet of Vehicle system framework, which provides a decentralized and trusted communication environment for vehicles.
- Based on the proposed system framework, we design a secure access authentication scheme between vehicles and roadside units, which reduces the dependence of the Certificate Authority, provides the accountability audit of malicious vehicles, and realizes the privacy protection of vehicles.
- We also propose a distributed cloud storage scheme combined with blockchain, which is used to store vehicle announcement transactions, reducing the storage burden of blockchain, and protecting the privacy and integrity of transaction contents.
- Finally, we conduct security analysis of our schemes and time performance simulation at the different stage. Compared with other schemes, our scheme is practical and simple whiling ensuring security, and also has the characteristics of decentralization, conditional privacy, security authentication and trusted communication.

C. ORGANIZATION

The remainder of this paper is organized as follows: Section II describes the preliminaries, Section III introduces the framework of our proposal, Section IV details the process of the vehicle in the registration, authentication, announcement and forward transaction, Section V implements the results, which focus on theoretical analysis and simulation and Section VI concludes this paper.

II. PRELIMINARIES

A. BLOCKCHAIN

Blockchain is a decentralized distributed database system jointly maintained by all nodes in the blockchain network. It is composed of a series of data blocks generated based on the cryptography method, and each data block is a block in the blockchain. Blocks are linked together in an orderly fashion to form a data chain, according to the order in which they were created.

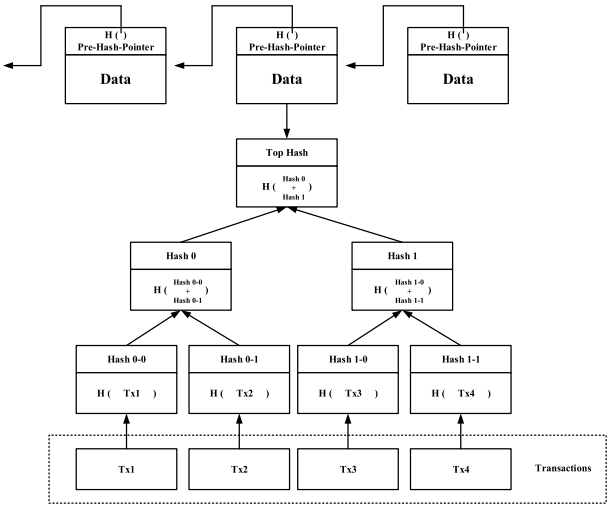

FIGURE 2. The structure of blockchain.

The link of the block is completed through the hash value of the block header data. The block chain uses this hash value as the unique identification of all blocks, and the unique block linked can be found in the block chain through the hash value of the parent block recorded in the block header. In this way, a chain from the latest block to the first block is created by the hash value sequence of each block linked to its parent block, thus forming a link-like data structure of all blocks, as shown in figure 2.

In paper, all roadside units are used as peer nodes to build a blockchain network, which is responsible for collective maintenance of blockchain data, and broadcast messages to vehicles along the road. The blockchain network mainly stores two kinds of data, one is vehicle identity information that contains the pseudonym, public key of vehicle and the mapping relationship between the pseudonym and the real identity. The other is the hash value of the legal vehicles announcement. The blockchain itself is not suitable for storing large amount of data, so we only store the index value of the announcements in the blockchain, so as to reduce the storage burden on the blockchain network and the difficulty of data consistency maintenance.

B. VANETs

VANETs is a special wire ad-hoc network, which provides communication service for V2V and V2I scenarios. As an important part of Intelligent transmission system (ITS), the main goal of VANETs is to provide comprehensive services for the running state of vehicle according to different functional requirement. VANETs includes three entities: CA, RSU, Vehicle(V). CA is charge of generator of system parameters and the registration of V. RSU is installed on both sides of the road, mainly responsible for vehicle authentication and communication services. The vehicle configured the On-Board Unit (OBU) can communicate with other entities wirelessly.

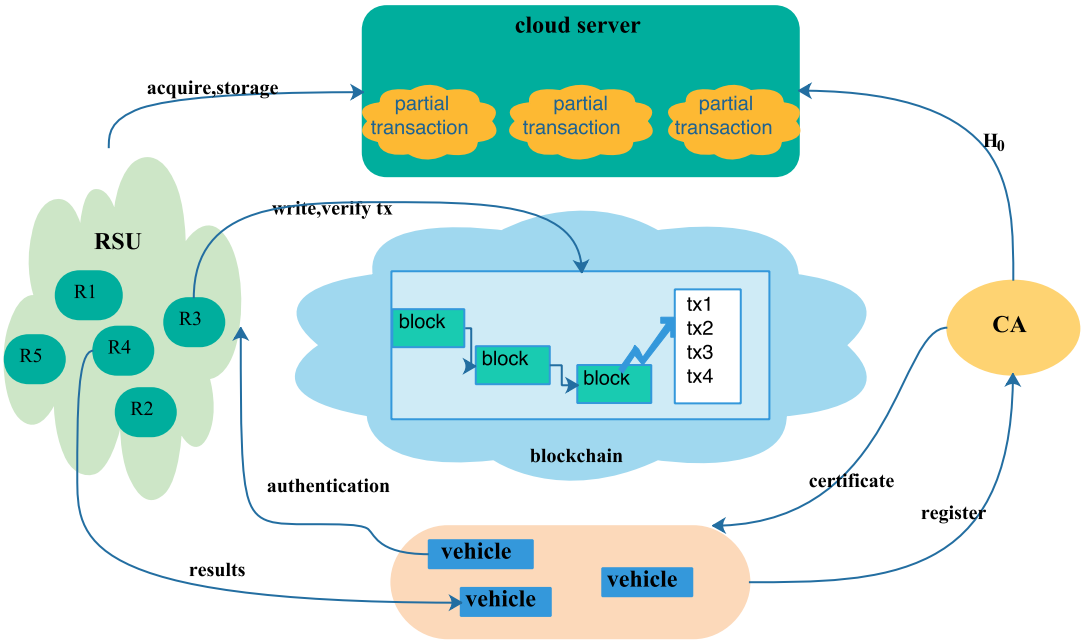

FIGURE 3. The framework of blockchain-based Internet of Vehicles system.

C. ASSUMPTIONS

In this paper, we employ the following assumptions to design the framework of the proposal:

- The CA has enough storage space to maintain the dataset containing the relationship between the vehicle' pseudonym and its real identity.
- The RSUs has stronger computing power than general-purpose computers to authenticate vehicles and confirm the consistence of transactions.
- Only it is beyond the adversaries' capability to compromise more than 50% participates in blockchain network.
- The cloud servers are unfamiliar to each other and have sufficient storage capacity as well.

In these four assumptions, Assumption 1) is the basic requirement for conditional anonymity of vehicles, and only CA has authority to trace malicious vehicles for evidence collection in case of disputes. Assumption 2) ensures RSU to be a node that deals with data authentication and transmission, which maintains operation of blockchain network, and eliminates the limitations on computing power. Assumption 3) is the prerequisite to ensure that the blockchain itself is secure, and Assumption 4) guarantees that the cloud servers have capacity to manage data in V2V and V2I communication.

III. THE FRAMEWORK OF PROPOSED SYSTEM

We propose a blockchain-based authentication system with preserving-privacy in VANETs, where vehicles use pseudonyms issued by CA to communicate with other entities. This system establishes a trust communication environment against internal forged messages while preserving the identity privacy of vehicles simultaneously. Meanwhile, with the participation of blockchain technique, the decentralized framework is trustful and secure, and reduces the dependence on CA in the traditional schemes. The overview of the framework is shown in Figure 3, and the detail of each component is also described.

A. CERTIFICATE AUTHORITY(CA)

CA is responsible to issue the certificate for registered vehicles and calculates two special hash functions, which are used to prepare to authenticate vehicles and trace malicious vehicles under the supervision of RSUs.

B. ROADSIDE UNIT(RSU)

All the broadcasted messages and transactions are verified by RSUs, and then be recorded in the blockchain. As the peer nodes of the blockchain network, RSUs are also responsible for authentication of vehicle identity that stored in each vehicle through V2I communication. Additionally, in order to guarantee CA trustable, RSUs maintain the relationship between vehicle' pseudonym and real identity in blockchain.

C. CLOUD SERVER

There are two main functions of the cloud server. The first is that manages the vehicle pseudonyms issued by CA for the convenience of identity verification, while the other is that stores the details of the transactions announced by vehicles that contains traffic information in a decentralized way.

D. VEHICLE

The privacy-preserving authentication scheme is running based on the blockchain. According to the unique hash recorded in the blockchain, vehicles can monitor RSUs by checking the transactions content stored in cloud server.

TABLE 1. Notations.

Notions	Definition
V	Set of vehicles
R	Set of Road Side Units
S	Set of cloud servers
$\rightarrow$	Unicast commutation
VID_i	The real identity of i-th vehicle
PID_i	The pseudonym of i-th vehicle
$verf$	Verify the existence of vehicle pseudonyms
cal	Calculate the corresponding hash function
$*$	An entity operates on challenge of integers
ver	Verify the authenticity of the signature
com	Compare the equality of two hash functions
pak	Pack up a transaction
$storage$	Store the contents of transaction or message
$E_X()$	Encrypt with X
$D_X()$	Decrypt with X

Moreover, vehicles are able to report malicious participants to RSUs for evidence collection, and then the malicious vehicles will be punished under the cooperation of the CA and RSUs.

E. TRANSACTION

The transaction in this paper includes the transaction of vehicle identity and transaction of traffic announcement. The hash value of the latter is stored in blockchain, and the specific information of traffic condition is stored in the distributed cloud servers. Every transaction contains the timestamp and the signature of initiator, while there is no information linkable to the real identity in the transaction for privacy preservation.

F. CERTIFICATE

When register in system with real identity, the vehicles obtain certificate issued by CA that includes pseudonyms, a pair of public-private keys and two hash values. However, in this certificate, there is no real identity so that the vehicle's privacy is preserved.

IV. OUR STRUCTURE OF SYSTEM FRAMEWORK

In this section, we detail structure about our proposal, it contains the five stages: system initialization, vehicle registration, vehicle authentication, vehicle announcement, and forwarding of message. The notions used in this paper are listed in TABLE 1.

A. SYSTEM INITIALIZATION

We propose a blockchain-based privacy protection mechanism for communications of smart vehicles. The mechanism is composed of four participants, including the Certificate Authority (CA), Vehicles $V = \{V_1, V_2, \ldots, V_i, \ldots, V_n\}$, Roadside Units $R = \{R_1, R_2, \ldots, R_i, \ldots, R_m\}$ and Cloud Server $S = \{S_1, S_2, .., S_i, \ldots, S_q\}$. The blockchain network among all RSU is located on the highway, which stores the certificates of vehicles and hash value of communication

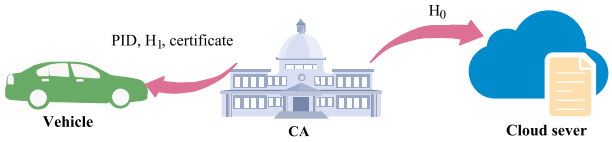

FIGURE 4. Distribution of registration data.

TABLE 2. Registration of the vehicle Vi.

1. $V_i \longrightarrow CA: < VID_i, OtherDetails >$
2. $CA \xrightarrow{verf} VID_i: < Verify(VID_i) >$
3. $CA \xrightarrow{cal} HASH: < H_0(PID_i||P_{ki}), H_1(VID_i||cert) >$
4. $CA \longrightarrow S_i: < H_0 >$
5. $CA \longrightarrow V_i: < PID_i||cert||ECC(P_{ki}, S_{ki})||H_1 >$

information among vehicles. In the initialization, different participants prepare to be occupied with numerous domain parameters required for later security operations. We assume that CA builds the system for Elliptic curve cryptography (ECC) based PKI and five secure hash functions are H_0,H_1,H_2,H_3,H_4. These parameters with publicly hashing functions are stored in the vehicles publicly during the registration. In our system, it assumes that the CA to generate a public-private key pair in ECC scheme for each registered vehicle. In addition, RSUs are supplied with the vehicle's public key issued by CA for signature verification in the Ledger.

The blockchain network among RSUs provides a venue for vehicle's identity authentication and transaction verification among vehicles (e.g. traffic accident notice.), which they verify each other while storing and retrieving transactions.

B. REGISTRATION OF THE VEHICLE

In this phase, the CA as a trusted third party generates a series of system parameters according to the unique ID provided by the registered vehicle in Figure 4. In order to preserve the identity privacy of vehicle information and communication, the CA issues a pseudonym to the registered vehicle for the communication, which has a unique mapping relationship with the real ID of the vehicle and is stored in the database of the CA. Specially, the CA also outputs the hash values to the registration vehicles and the cloud servers respectively so as to facilitate authentication of vehicles and reduce the communication burden on CA. The integrated registration procedure, as shown in TABLE 2, involves the following interactive steps:

step 1 Vehicle: obtains real ID from the Motor Vehicle's Division (MVD), and establishes a secure channel between the CA and itself, then sends its real ID and other details to the CA;

step 2 CA: verifies firstly the existence of real identity about registered vehicle, if so, secondly generates the certificate that includes pseudonym PID_i, a pair of ECC Public-Private keys namely $P_{ki}$and S_{ki} according to real identity of vehicle;

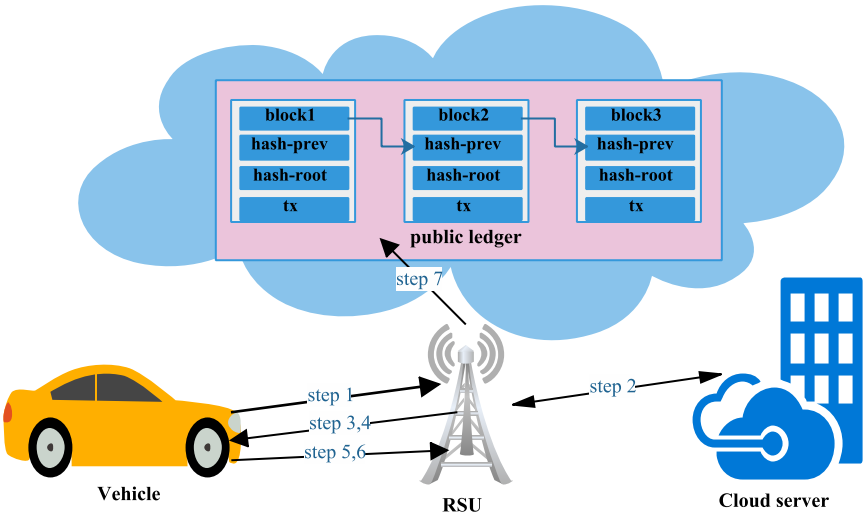

FIGURE 5. Identity authentication of vehicle.

step 3 Hash: the CA calculates two hash functions, which are $H_0 = (PID_i||P_{ki})$ and $H_1 = (VID_i||cert)$ in order to authentication of vehicle identity and storage of vehicle information in future;

step 4 Cloud Server: stores hash value H_0 sent by the CA;

step 5 Registered Vehicle: gets a Pseudo ID, certificate, H_1 and a pair of Public-Private keys from the CA, and stores these in the On-Board Unit (OBU).

Compared with the traditional model, the CA in our scheme designs two hash functions. H_0 obtains vehicle pseudonym and public key P_{ki}, which is stored in cloud sever. H_1 that represents the mapping relationship of vehicle real identity with pseudonym is stored in OBU, and only the registration authority and the registered vehicle know the real identity of the vehicle. Moreover, the mapping of actual identity with the assigned PID_i is also stored in a hash map in CA's database. This ensures easy lookup in case of traceability and accountability of malicious vehicles. Further, in order to reduce the dependence on CA and prevent malicious activity of CA, H_1 will also be recorded on blockchain at the stage of vehicle authentication, so that both CA and vehicles cannot be repudiated.

C. IDENTITY AUTHENTICATION AND REVOCATION

In the proposal, the RSUs as peer nodes build the blockchain network. As the vehicle is active on the road, it authenticates with RSU in Figure 5.

When the vehicle comes in the range of first RSU on the road, it sends an authentication request with its own PID to the RSU. In addition to calculating the corresponding result of the request, the RSU obtains the trueness of the result by querying on the cloud server. Finally, RSU records the authentication result on the blockchain. During authentication, the vehicle communicates with the RSU by using its own pseudonym, and neither the RSU nor the cloud server learns

TABLE 3. Identity authentication.

1. $V_i \longrightarrow R_i : < PID_i, P_{ki} >$
2. $R_i \xrightarrow{cal} HASH : < H_0(PID_i\|\|P_{ki}) >$
Query H_0 from cloud sever, return **True** to R_i if H_0 exist.
3. $R_i \longrightarrow V_i : < E_{P_{ki}}(\text{challenge integer } N_{R_i}) >$
4. $CA{*}Challenge : < D_{S_{ki}}(\text{challenge integer } N_{R_i}) >$
Then, storing N_{R_i} in OBU.
5. $V_i \longrightarrow R_i : < Sig_{S_{ki}}(H_1)\|\|H_2(N_{R_i}\|\|M_{V_i}\|\|M_{V_i}) >$
6. $R_i \longrightarrow Signature : < Ver_{P_{ki}}(sig_{S_{ki}}(H_1)) >$ $< Cal(H_2) >$
If the verification is **correct**, proceed to the seventh step.
7. $R_i \longrightarrow Blockchain : < Tx_1(sig_{S_{ki}}(H_1)\|\|PID_i\|\|P_{ki}) >$
Broadcast it into blockchain network.

to acquire the vehicle's real identity. As is shown in TABLE 3, the authentication process is divided into seven steps:

step 1 The vehicle launches an authentication request by sending a message that obtains pseudonym PID_i and public key P_{ki} to nearby RSU.

step 2 After receiving the request, RSU calculates the hash value according to H_0 algorithm and deserves corresponding result. For verifying the legality of the vehicle, the RSU queries the trueness of the result with the assistance of the cloud server. If the query result is consistent with the calculation result, the cloud server returns TURE to the RSU, which represents the vehicle is legal. Otherwise, authentication is failed.

step 3 After determining the authenticity of the vehicle identity, the RUS initiates the random integer negotiation process, which sends a random integer N_{R_i} encrypted by the vehicle's public key P_{ki} to the vehicle.

step 4 The vehicle receives the ciphertext and decrypts it with its private key S_{ki}, then stores the integer N_{R_i} in OBU for announcement event in future.

step 5 In order to determine if the vehicle received the integer from the RSU and the integrity of the random number, the vehicle has to select another random number M_{V_i} and calculate a hash function H_2 obtained two integers mentioned before. Additionally, in order to prevent the CA from malicious activity, the vehicle needs to signature on H_1 that is the mapping of real identity and certificate and stores it in the blockchain network. Finally, the vehicle sends $Sig_{S_{ki}}(H_1)||H_2(N_{R_i}||M_{V_i})||M_{V_i}$ to RSU.

step 6 The RSU makes use of the public key P_{ki} of the vehicle to verify the hash value H_1 with the vehicle's signature and calculates the corresponding hash value according to the received random integer M_{V_i} and the known negotiation random integer N_{R_i}. If the calculated result is the same as the received hash value H_2, it indicates that the negotiation of the random number is successful.

step 7 The RSU as a peer node of blockchain network, packs up a transaction $Tx_1(sig_{S_{ki}}(H_1)||PID_i||P_{ki})$ and stores it in the blockchain network where all RSUs are able to get transaction Tx_1.

As a result, the RSUs have public key and certificate of the authenticated vehicle without having to authenticate it repeatedly. For the cloud server, it is responsible for storing the specific information of the transaction in the blockchain. Additionally, the cloud server also stores some parameter information (such as H_0) issued by the CA for the vehicle after being registered. It is worth noting that the information is not stored centrally on a certain server, but it is divided into multiple parts and stored randomly in different servers. When the OBU or RSU needs to query or verify the transaction information, the corresponding transaction content can be obtained from multiple servers according to the unique hash value of the transaction. The content of transactions is obtained through multiple servers, which can resist privacy disclosure, guarantee transaction integrity, exclude collusion attacks, and enhance the authentication and trust level of cloud storage.

D. ANNOUNCEMENT OF VEHICLE

When the vehicle is driving on the road, it may encounter sudden traffic conditions in front, such as traffic accidents, congestion and complicated road conditions. Under normal circumstances, this article regards these traffic conditions as the event D, which represents the textual description, photo or videos of the traffic conditions token by vehicles. The specific information about the traffic conditions is not discussed here. The scenario of vehicular announcement is indicated in Figure 6.

The vehicle uses its own pseudonym for various activities to protect identity privacy. There is a traffic occurring,

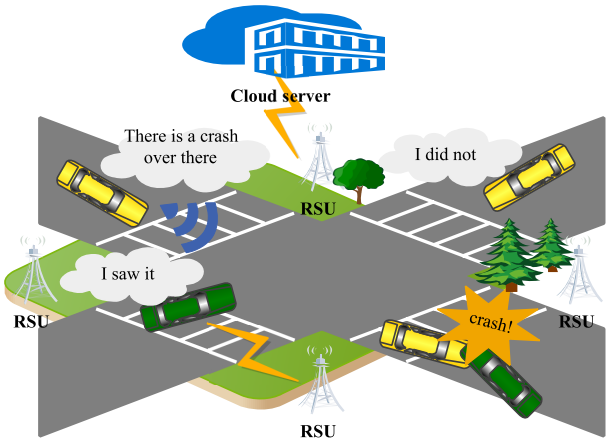

FIGURE 6. Announcement of vehicle.

TABLE 4. Announcement and storage of thing.

1. $V_i \longrightarrow R_i: < H_3(N_{R_i}\|\|D\|\|PID_i)\|\|D\|\|PID_i >$
2. $R_i \xrightarrow{cal} H_3': <$Calculate $H_3'(D\|\|N_{R_i}\|\|PID_i) >$
3. $R_i \xrightarrow{com} H_3: <$Compare $H_3' = H_3 >$, if true, pack up Tx_2.
4. $R_i \xrightarrow{pack} Tx_2: < Tx_2(H_3\|\|D\|\|PID_i\|\|timestamp) >$
5. $R_i \xrightarrow{storage} S_{1\to q}: < part_1 < Tx_2 >, ..., part_t < Tx_2 >>$
6. $R_i \longrightarrow Blockchain: <$calculate $H_4(Tx_2) >$, store H_4 in blockchain and broadcast the transaction.

the vehicle authenticated is able to inform the RSUs of the traffic conditions. The announcement phase is shown in TABLE 4:

step 1 The vehicle utilizes the random number N_{R_i} negotiated with the RSU to ensure the integrity of the event D. It delivers the message which contains the traffic conditions, vehicle identity and hash value $H_3(N_{R_i}||D||PID_i)$ to the RSUs.

step 2 The RUS directly verifies the integrity of event D and does not verify the identity of the sender, because only the authenticated vehicle can declare the traffic conditions.

step 3 If the result is correct, the RSU packs up a new transaction.

step 4 The RSU packages the traffic event to form a new transaction whose content is $Tx_2(H_3||D||PID_i||$ $timestamp)$.

step 5 The details of the transaction Tx_2 are divided into multiple parts ($t <= q$), which are stored in different cloud servers.

step 6 After hashing the Tx_2 about event D, the RSU stores $H_4(Tx_2)$ in blockchain and broadcasts this transaction to all peer nodes.

In this scheme, the introduction of random number realizes the temper-proof mechanism of the traffic event D, which ensures the integrity of the traffic event D. Meanwhile,

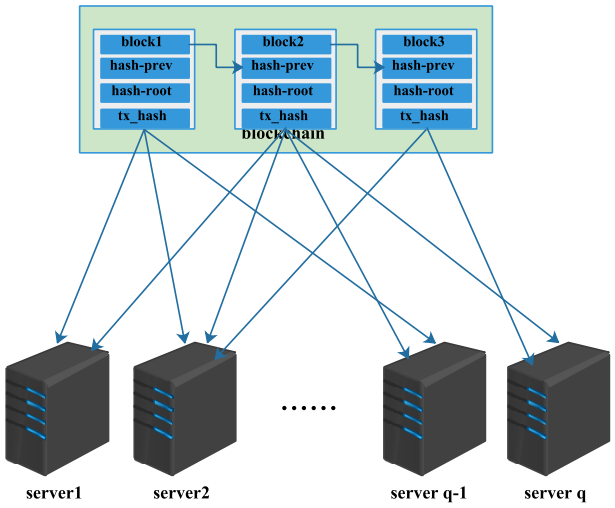

FIGURE 7. Storage of transaction.

vehicle's pseudonym protects its own privacy and provides an opportunity for the RSU to search for the corresponding random number. Obviously, it can be known that the transaction has added the timestamp of the traffic event D on the basis of the verified message, indicating the occurrence time of the traffic event D.

All the transactions about traffic event D are hashed in the chronological Merkle tree (CMT) and only the root hash is included in the blockchain. It is worth noting that the details of the transaction are divided into multiple parts stored in different cloud servers in a distributed way in Figure 7. It is accessible to all nodes via a homologous transaction hash that is stored in blockchain. The corresponding hash value will also be changed if the transaction content is modified by partial cloud servers. In this case, the entity cannot gain the transaction information on the cloud servers according to the hash in the blockchain. The distributed storage mechanism of transaction details can resist the joint attack between cloud severs, and it protects the privacy of the vehicle and integrity of traffic information in the transaction.

E. FORWARD OF ANNOUNCEMENT

First vehicle that announces the traffic event D to RSUs in blockchain is responsible for trueness of the event, and other vehicles active on the road are able to verify this when they obtain the content of transaction about the traffic condition from cloud severs according to the unique hash value stored in the blockchain. The others receive the notification issued by the RSU that the transaction hash related to the traffic information, they can send a request to the cloud servers to query the transaction details via the hash. Therefore, vehicles along the road can efficiently learn the road condition information to help them take timely measures. Moreover, after the authenticity of the transaction about event D is confirmed, the vehicle can choose whether to forward the transaction or not. If so, the vehicle needs to append its own pseudonym and signature on the transaction to spread it.

However, if there is a problem with the validity of the transaction, such as the traffic condition is secure but the transaction says there is a traffic accident, etc., other vehicles can report the vehicle announcing the transaction. Then, the RSU requests real identity of the malicious vehicle from CA according to the hash H_1 in registration. Finally, with the help of CA, RSU broadcasts malicious vehicle into blockchain.

V. SECURITY AND PERFORMANCE ANALYSIS

A. SECURITY ANALYSIS

1) PRIVACY-PRESERVING

Vehicle A uses its own pseudonym PID_i issued by CA for V2V and V2I communications without any information about its real identity. For trade-off between security and privacy, pairs of identities and pseudonyms are stored with high-security level in CA. It means that only CA knows the real identity of any issued pseudonym for each vehicle so that only CA has the authority to track the malicious vehicle when it performs misbehaviors or broadcasts forged messages. Moreover, the mapping of real identity and pseudonym is also recorded on blockchain at the stage of authentication, and RSUs cannot learn the mapping specific information, which improves confidence level of CA effectively. In order to preserve the privacy of vehicles, no information linkable to the real identity is included in the transaction.

2) TRANSACTION TAMPERING RESISTANCE

In proposed mechanism, the transactions recorded on Blockchain have already got the agreements from all RSUs and blockchain maintains interactive consistency of RSUs. A hash-chain is used to guarantee the order and information of blocks. These hash values are unique for each block. Modifying any content of any block will cause a change to the hash values of the other blocks. Depending on the properties of hash function, if an adversary or the malicious RSU begins a perfect tampering, she/he not only needs to modify the content of the block but also modify and recalculate the hash values of all blocks after the modified block. Therefore, if there are hundreds of blocks regardless of workload while the consensus adopted in the blockchain composed of all RSUs is proof of work. As long as the malicious node does not exceed the half of all RSUs, the transaction information cannot be modified, and the longer the block chain is, the better security will be.

3) PREVENTION OF REPLAY ATTACK

Each transaction has a unique identifier txid. Therefore, transactions with the same identifier will be rejected by the consensus RSUs. In addition, the transaction with an incorrect negotiated random number is rejected in the phases of verification, and thus replay attacks are prevented.

4) DISTRIBUTED STORAGE OF DATA

The content of each transaction is divided into multiple parts stored in the different cloud servers in a distributed way,

TABLE 5. Feature comparion.

Schemes	Privacy	Decentralization	MultiStorage	Accountability	Compatibility
[23]	Yes	No	-	No	-
[24]	Yes	No	-	No	-
[25]	Yes	Yes	No	Yes	No
[26]	Yes	Yes	No	-	No
[27]	Yes	No	-	Yes	-
Ours	Yes	Yes	Yes	Yes	Yes

and the unique hash of the transaction is recorded on blockchain, it becomes accessible to all nodes via a homologous transaction hash that stored in blockchain. Therefore, each server has different parts of the transaction, and users can easily get the transaction information from the cloud servers according to its hash value. Compared with the traditional cloud storage, the proposed storage scheme does not have the centralized server and the right of each cloud server is equal. For each server, only a small part of the content of each transaction is known, which protects the privacy of the transaction. If adversary initiates an attack on the cloud servers, he/she has to attack each server that stores the corresponding transaction. Moreover, the distribution of the servers is random, while the cost consumed by the adversary is far greater than the value of the transaction, so that it enables to resist the joint attack between the servers.

5) TRACEABILITY

Vehicle A uses its private key to generate a signature for each broadcasted message, while RSU can use vehicle A's public key to verify the signature. Meanwhile, the other vehicles that forward the message contained the traffic condition must append its own pseudonym and signature on the message before spread it. When the malicious vehicle with forged message is found, the system will trace the malicious users and get the real identity of the malicious vehicle with assistance of the CA and RSUs. As a trusted institution, it is impossible for CA to tamper with the relevance of the malicious vehicle' real identity and pseudonym, because the mapping of vehicle' pseudonym and real identity is recorded on the blockchain. Simultaneously, a report is sent to the cloud servers to clear the identity information of the malicious vehicle while pursuing the responsibility of the malicious vehicles.

B. PERFORMANCE ANALYSIS

In this section, there are some significant features to be discussed, which affects the flexibility and practicability of this scheme in VANETs. Additionally, we evaluate the performance of the parts of proposal.

It makes a comparison on the supported features between our work and other related schemes [23]–[27] in terms of privacy, decentralization, multi-storage, accountability, compatibility. We use the symbol "-" to represent that the corresponding property is not considered. As shown in TABLE 5, [23] and [24] realized the privacy protection of vehicles in the authentication process, but did not provide distributed security, nor could it realize the accountability of malicious vehicles. References [25] and [26] proposed a blockchain-based vehicle anonymous authentication mechanism, but none of them introduced the distributed storage method of vehicle announcement, and it was only suitable for the bitcoin without compatibility. Reference [27] achieved the conditional privacy protection for vehicle authentication, but there is no feature of the distributed storage, and the efficiency of the Internet of vehicles will be seriously affected due to the frequent interaction between vehicles and roadside units. It can be concluded that only our scheme satisfies all of the properties above.

Algorithm 1 Forward of Announcement

```
procedure: Acquire(event D)
  def i = degree of report
  def flag = true
  content ⟵ hash of transaction about D
  while report_num < i do
    if content = right then
      write PID & signature on transaction of event D,
      forward Announcement
    else
      RSU ⟵ report announcer
      flag = false
    end if
    if flag = false then
      report_num++
    end if
  end while
  CA ⟵ revocation request
  broadcast malicious vehicle into blockchain
end procedure
```

We discuss the required communication rounds for the successful authentication in RSU side, where totally n vehicles get involved. In our design, for each vehicle, only 3 rounds are required for message sending and receiving. Hence, with the additional 1 broadcast, the total communication rounds for each RSU is $3n + 1$ in our design. Accordingly, the comparison result on communication cost is given in TABLE 6, indicating that our scheme requires less communication.

We implement the scheme in Golang environment using a laptop 2.3GHz Intel Core i5 and 8GB 2133MHz LPDDR3.

TABLE 6. Comparion of communication cost.

Scheme	[17]	[18]	Ours
Communication Rounds	$4n$	$4n+1$	$3n+1$

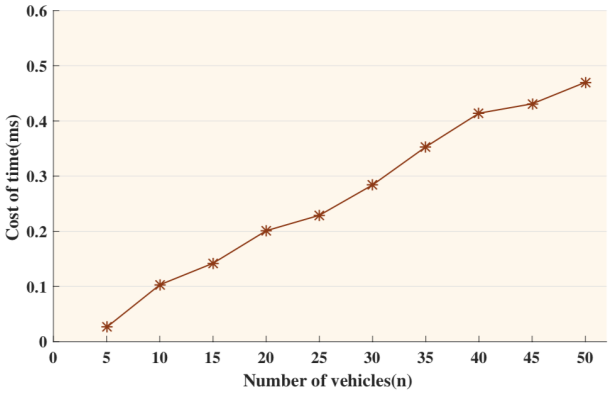

FIGURE 8. Registration of vehicle.

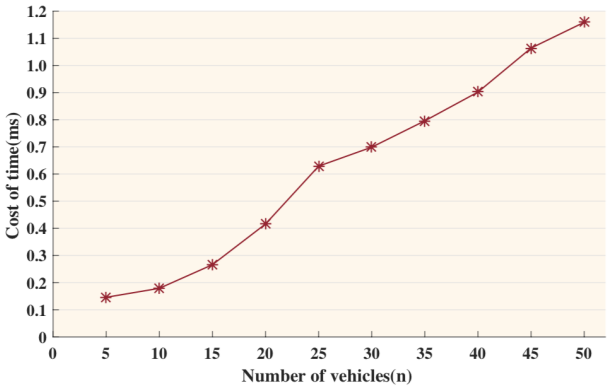

FIGURE 9. Announcement of vehicle.

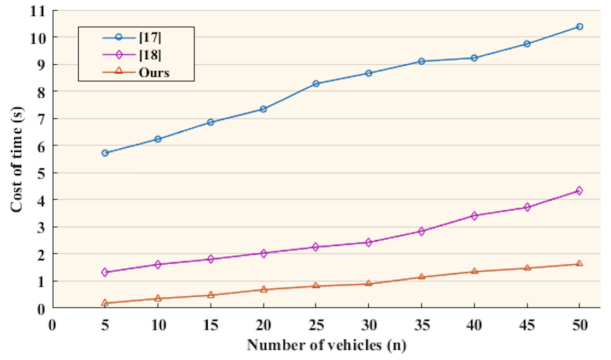

FIGURE 10. Authentication of vehicle.

Each vehicle is equipped with a computer to receive or send data with RSUs or CA through V2I communication for the anonymous authentications. We measure the time cost for each part of the proposal to present performance of this scheme. All results are shown in Figure 8, 9, 10.

In our scheme, we use the elliptic Curves recommended by NIST [28] in our signature phase. Then we simulate the registration, authentication and announcement of vehicles respectively to analyze efficiency of system we proposed. The number of vehicles range from 1-50 and the average values over an interval of every 5 vehicles is gathered. As shown in Figure 8, when a vehicle registered with CA, there are mainly two hash functions to be calculated, the average registration time for a vehicle is about 0.01ms. Moreover, there are mainly three hash operations during the vehicle declaration period, and approximate announcement time cost per vehicle is 0.023ms in Figure 9. However, it is worth noting that the different forms of event D affects the efficiency of the vehicle announcement. Hence, we carry out simulation of event D in accordance with 256 bits data.

Figure 10. shows the authentication efficiency between vehicles and RSUs. In the reference [18], its scheme requires five encryption operations, four decryption operations, one signature and verification operation using the asymmetric algorithm. The scheme in the reference [17] requires two encryption operations and two decryption operations using the symmetric algorithm, whose certificateless-based authentication scheme mainly uses $2n+1$ bilinear pairing operations and n exponential operations, where the pairing exponential calculation leads to higher computation cost. In our scheme, there is no pairing operation, mainly involves only one ECC encryption-decryption operation and one signature operation with verification. The results of simulation demonstrated that our proposal is a more efficient authentication protocol in VANETs.

VI. CONCLUSION

In this paper, we propose a blockchain-based access authentication system in VANET environment. The system not only provides a trust communication environment for smart vehicles, but also preserves anonymity without revealing the real identity of users. Moreover, our proposal reduces the dependence on the authority center and burden of vehicle identity authentication in terms of efficiency. In order to prevent the distribution of forged messages from internal vehicles, we also design a secure and distributed blockchain-based transaction storage scheme, which can efficiently protect transaction information from adversary attacks while tracing the malicious vehicles. Finally, we analyze the security and validity of the proposed system and evaluate the performance of this access authentication system.

REFERENCES

[1] D. Jia, K. Lu, J. Wang, X. Zhang, and X. Shen, "A survey on platoon-based vehicular cyber-physical systems," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 1, pp. 263–284, 1st Quart., 2016.

[2] Y. Li, "An overview of the DSRC/WAVE technology," in *Proc. Int. Conf. Heterogeneous Netw. Qual., Rel., Secur. Robustness*. Berlin, Germany: Springer, 2010, pp. 544–558.

[3] T. Zhang and Q. Zhu, "Distributed privacy-preserving collaborative intrusion detection systems for VANETs," *IEEE Trans. Signal Inf. Process. Netw.*, vol. 4, no. 1, pp. 148–161, Mar. 2018.
[4] F. Dötzer, "Privacy issues in vehicular ad hoc networks," in *Proc. Int. Workshop Privacy Enhancing Technol.* Berlin, Germany: Springer, 2005, pp. 197–209.
[5] B. Parno and A. Perrig, "Challenges in securing vehicular networks," in *Proc. Workshop Hot Topics Netw. (HotNets-IV)*, 2005, pp. 1–6.
[6] Y.-C. Wei and Y.-M. Chen, "Efficient self-organized trust management in location privacy enhanced VANETs," in *Proc. Int. Workshop Inf. Secur. Appl.* Berlin, Germany: Springer, 2012, pp. 328–344.
[7] J. Ren and L. Harn, "An efficient threshold anonymous authentication scheme for privacy-preserving communications," *IEEE Trans. Wireless Commun.*, vol. 12, no. 3, pp. 1018–1025, Mar. 2013.
[8] C. Sun, J. Liu, X. Xu, and J. Ma, "A privacy-preserving mutual authentication resisting DoS attacks in VANETs," *IEEE Access*, vol. 5, pp. 24012–24022, 2017.
[9] D. He, S. Chan, and M. Guizani, "An accountable, privacy-preserving, and efficient authentication framework for wireless access networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1605–1614, Mar. 2016.
[10] U. Rajput, F. Abbas, H. Eun, and H. Oh, "A hybrid approach for efficient privacy-preserving authentication in VANET," *IEEE Access*, vol. 5, pp. 12014–12030, 2017.
[11] R. G. Engoulou, M. Bellaïche, S. Pierre, and A. Quintero, "VANET security surveys," *Comput. Commun.*, vol. 44, pp. 1–13, May 2014.
[12] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: http://www.bitcoin.org/bitcoin.pdf
[13] Y.-M. Li, Y. Tan, and Y.-P. Zhou, "Analysis of scale effects in peer-to-peer networks," *IEEE/ACM Trans. Netw.*, vol. 16, no. 3, pp. 590–602, Jun. 2008.
[14] L. Zhu, C. Chen, X. Wang, and A. O. Lim, "SMSS: Symmetric-masquerade security scheme for VANETs," in *Proc. 10th Int. Symp. Auton. Decentralized Syst.*, Mar. 2011, pp. 617–622.
[15] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. IEEE INFOCOM-27th Conf. Comput. Commun.*, Apr. 2008, pp. 246–250.
[16] G. Calandriello, P. Papadimitratos, J.-P. Hubaux, and A. Lioy, "Efficient and robust pseudonymous authentication in VANET," in *Proc. 4th ACM Int. Workshop Veh. Ad Hoc Netw.*, 2007, pp. 19–28.
[17] H. Tan, D. Choi, P. Kim, S. Pan, and I. Chung, "Secure certificateless authentication and road message dissemination protocol in VANETs," *Wireless Commun. Mobile Comput.*, vol. 2018, May 2018, Art. no. 7978027.
[18] P. Vijayakumar, M. Azees, A. Kannan, and L. J. Deborah, "Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 4, pp. 1015–1028, Apr. 2016.
[19] Q. Wu, J. Domingo-Ferrer, and Ú. Gonzalez-Nicolas, "Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications," *IEEE Trans. Veh. Technol.*, vol. 59, no. 2, pp. 559–573, Feb. 2010.
[20] B. Qin, Q. Wu, J. Domingo-Ferrer, and W. Susilo, "Robust distributed privacy-preserving secure aggregation in vehicular communication," *Control Cybern.*, vol. 42, no. 2, pp. 277–296, 2012.
[21] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in *Proc. IEEE 19th Int. Conf. Intell. Transp. Syst. (ITSC)*, Nov. 2016, pp. 2663–2668.
[22] S. Rowan, M. Clear, M. Gerla, M. Huggard, and C. M. Goldrick, "Securing vehicle to vehicle communications using blockchain through visible light and acoustic side-channels," 2017, *arXiv:1704.02553*. [Online]. Available: https://arxiv.org/abs/1704.02553
[23] M.-C. Chuang and J.-F. Lee, "PPAS: A privacy preservation authentication scheme for vehicle-to-infrastructure communication networks," in *Proc. Int. Conf. Consum. Electron., Commun. Netw. (CECNet)*, Apr. 2011, pp. 1509–1512.
[24] X. Peng, "A novel authentication protocol for vehicle network," in *Proc. 3rd Int. Conf. Syst. Inform. (ICSAI)*, Nov. 2016, pp. 664–668.
[25] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for VANETs," *IEEE Access*, vol. 6, pp. 45655–45664, 2018.
[26] N. Malik, P. Nanda, A. Arora, X. He, and D. Puthal, "Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 674–679.
[27] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, "ECPP: Efficient conditional privacy preservation protocol for secure vehicular communications," in *Proc. IEEE INFOCOM-27th Conf. Comput. Commun.*, Apr. 2008, pp. 1229–1237.
[28] D. Johnson, A. Menezes, and S. Vanstone, "The elliptic curve digital signature algorithm (ECDSA)," *Int. J. Inf. Secur.*, vol. 1, no. 1, pp. 36–63, Aug. 2001.

DONG ZHENG received the Ph.D. degree from Xidian University, in 1999. He joined the School of Information Security Engineering, Shanghai Jiao Tong University. He is currently a Professor with the Xi'an University of Posts and Telecommunications, China. His research interests include information theory, cryptography, and information security. He is also a Senior Member of the Chinese Association for Cryptologic Research and a member of the Chinese Communication Society.

CHUNMING JING received the bachelor's degree from the Xi'an University of Posts and Telecommunications, in 2017. He is currently pursuing the master's degree with the National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications. His research interests include blockchain technology, vehicular ad hoc networks, and security and privacy in the Internet of Things.

RUI GUO received the Ph.D. degree from the State Key Laboratory of Networking and Switch Technology, Beijing University of Posts and Telecommunications, China, in 2014. He is currently a Lecturer with the National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications. His current research interests include attribute-based cryptograph, cloud computing, and blockchain technology.

SHIYAO GAO received the B.S. degree from the Xi'an University of Posts and Telecommunications, China, in 2017, where she is currently pursuing the M.S. degree and doing the research at the National Engineering Laboratory for Wireless Security. Her research interests include blockchain technology and information security.

LIANG WANG received the B.S. degree from the Institute of Information Technology, GUET, in 2016. He is currently pursuing the M.S. degree with the National Engineering Laboratory for Wireless Security, Xi'an University of Posts and Telecommunications, China. His research interests include anonymous authentication, vehicular ad hoc networks, and blockchain.