

Received March 7, 2019, accepted March 24, 2019, date of publication April 3, 2019, date of current version April 16, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2909004

An Improved Authentication Scheme for Internet of Vehicles Based on Blockchain Technology

XIAOLIANG WANG¹, (Member, IEEE), PENGJIE ZENG¹, NICK PATTERSON²,
FRANK JIANG^{1,2}, AND ROBIN DOSS², (Senior Member, IEEE)

¹School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 411201, China

²School of Info Technology, Deakin University, Geelong, VIC 3220, Australia

Corresponding author: Frank Jiang (frank.jiang@deakin.edu.au)

This work was supported in part by the Cooperative Education Fund of China Ministry of Education under Grant 201702113002 and Grant 201801193119, in part by the Hunan Natural Science Foundation under Grant 2018JJ2138, in part by the Excellent Youth Project of Hunan Education Department under Grant 17B096, in part by the Scientific Research Fund of Hunan Provincial Education Department under Grant 14B058, in part by the H3C Fund of Hunan Internet of Things Federation under Grant 20180006, and in part by the Degree and Graduate Education Reform Project of Hunan Province under Grant JG2018B096.

ABSTRACT Thanks to the rapid development in mobile vehicles and wireless technologies, the Internet of Vehicles (IoV) has become an attractive application that can provide a large number of mobile services for drivers. Vehicles can be informed of the mobile position, direction, speed, and other real-time information of nearby vehicles to avoid traffic jams and accidents. However, the environments of IoV could be dangerous in the absence of security protections. Due to the openness and self-organization of IoV, there are enormous malicious attackers. To guarantee the safety of mobile services, we propose an effective decentralized authentication mechanism for IoV on the basis of the consensus algorithm of blockchain technology. The simulation under the veins framework is carried out to verify the feasibility of the scheme in reducing the selfish behavior and malicious attacks in IoV.

INDEX TERMS Blockchain, Internet of Vehicles, security and privacy, consensus algorithm.

I. INTRODUCTION

Internet of Vehicles (IoV) is a complex Ad-Hoc network that can increase the traffic efficiency. IoV has the same characteristics as conventional IoT (Internet of things) applications, but also has some particularities. It is applied in the open wireless network environment, and the network topology is constantly changing, which makes the processing and computing of mobile services in IoV more complex [1]. Meanwhile, it is easy to lead to security and privacy issues such as data tampering, identity counterfeiting and sensitive information disclosure, which may damage the property and the personal safety of drivers and passengers. For example, the Sybil attack is a prevalent attacking method based on counterfeiting identity. It fakes the vehicular identity to control vehicles through the counterfeit node, and sends false information to the server to falsify the traffic situation and affect the normal traffic resulting in traffic jam or traffic accidents. Block chain technology is suitable for decentralized application environments with

distributed consensus characteristics, especially in complex road traffic environments where vehicles do not trust each other. Under the protection of the blockchain technology, the data cannot be easily tampered with by attackers. Such an encryption feature can enable multiple service providers to jointly maintain the same account information of the user. A user only needs to maintain the account information on the ledger to complete the entire identity authentication on different servers, which can bring more efficiency. At the same time, unlike other Internet of Things, the energy consumption of IoV based on blockchain can be provided by the vehicle itself, thus avoiding the defect of large energy consumption of blockchain network. Therefore, based on this, this paper puts forward the following hypothesis: Can the identity authentication system of an Internet of Vehicles learn from the blockchain encryption technology to complete its decentralized management, privacy protection and solve the problem of intercepting malicious attacks? In the following sections, this paper will analyze, demonstrate and test the feasibility of block chain encryption technology applied to identity authentication of an Internet of Vehicles.

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

The paper is structured as follows. Section II presents literature review. In Section III, the blockchain knowledge about its infrastructure and authentication algorithm is introduced. The improved IoV authentication scheme based on blockchain technology is proposed in Section IV, and we present our experimental analysis in Section V. Section V concludes the paper.

II. LITERATURE REVIEW

In recent years, many researchers have proposed a large number of technical solutions for the performance of IoT [2]–[4]. Among them, IoV is one of the major focus of literature research because of its unique characteristics [5], [6]. Song *et al.* [7] propose that several vehicles whose average speed and moving direction are close and can be divided into one group based on navigation, and the interal-group communication will make the vehicle position as well as other vehicle positions undisclosed. However, due to the speed of the vehicle and the uncertainty of the environment, the communication between the geographically independent groups of vehicles is still facing a serious phenomenon of the difficult exchange of information and the repetition of the intermediate authentication process when the vehicle rejoins another group of vehicles (or the hive). Tedious authentication operation and delay can easily cause the vehicle to be more vulnerable to malicious attacks. For the lack of security of the above proposal, the RSP-based message authentication proposed by Yein *et al.* [8] can solve these problems through the use of public key identification and thus achieve privacy preservation, which is compatible with the scheme proposed by Li *et al.* [9]. Oulhaci *et al.* [10] and Kumar and Arora [11] have different solutions to enhance the privacy of the vehicle by the unicast communication in V2V (Vehicle to Vehicle) mode. However, they always have complex privacy protection protocols including traditional PKI (Public Key Infrastructure) distribution schemes. The communication overhead required in the entire complex transportation system will be enormous, and the time consumption required will not be met, especially with regards to the needs of actual use. Therefore, it is urgent to seek one or more message relay nodes in a group of vehicle organizations in order to alleviate the overall message transmission pressure. Bouali *et al.* [12] focus on electing a Miner-like node through consensus in the reputation system to greatly reduce the communication overhead of privacy protection, the authentication process, and more importantly, this method also consolidates the authentication encryption process. However, behind the prominent reduction of communication overhead and consolidation of the authentication encryption process, the more traditional PKI distribution scheme is still used. In addition, in the process of repeated elections, there is still the possibility that a malicious node becomes a Miner node. The problem of a malicious node becoming a Miner node can be solved by combining RSU (Roadside Unit) or establishing a security vector model proposed by Bayat *et al.* [13] and Zhou *et al.* [14]. The addition of RSU can be used to reduce the risk of malicious

nodes becoming important transit nodes. The vector model security algorithm is skillfully used in publishing messages to prevent malicious nodes from spreading false messages. Although, the security of identity authentication is emphasized, complex security algorithm rules may cause delays in the release of instant messages, which in turn may cause traffic congestion and even traffic accidents. In general, the various methods stated by the former still have problems in that the key distribution scheme is relatively old, the authentication encryption method makes the communication overhead and time overhead huge and unacceptable, the mature chain structure is lacking, and there is excessive communication overhead or time overhead [15]–[19]. Dorri *et al.* [20] proposed the concept of Lightweight Scalable Blockchain (LSB), which provides a decentralized privacy protection and blockchain-based security architecture for intelligent vehicle systems and establishes an intelligent ecosystem of OBM communities. This is a very good idea. However, the centralized key management can easily cause the list to be broken, resulting in a large number of key leaks. In addition, this way depends on the popularity of OBM. In the OBM scarce environment, even the mobile IP method is difficult to complete the basic communication. Sharma *et al.* [21] proposed a VN model of vehicle network block based on smart city blockchain. By setting up Miner nodes to manage and control the safety affairs and traffic management of vehicle network block, it provides a good solution for the application of blockchain in vehicle network. However, it relies heavily on sensor data, and lacks necessary intelligent contracts and improved PKI technology. It is a little rough in dealing with authentication security issues. At the same time, the authentication efficiency of the two schemes is relatively low. To solve these problems, the main contribution of this paper is to construct a new block-chain-based authentication scheme for vehicle network, including a new intelligent contract based on consensus mechanism and a public key-pair PKI scheme based on cryptographic accumulator. Ledger consensus technology can greatly reduce the time and space complexity of authentication through cryptographic accumulator algorithm, and give priority to the security of authentication process.

III. BLOCKCHAIN TECHNOLOGY INTRODUCTION

A. THE INFRASTRUCTURE OF BLOCKCHAIN TECHNOLOGY

As an underlying paradigm of the Bitcoin system, blockchain technology combines Peer-to-Peer (P2P) technology, distributed ledger technology, asymmetric encryption technology, incentive theory and smart contract technology [22]–[24]. Blockchains are currently divided into the co-management chain, the contracted chain and the unique chain [24]. The common characteristics are openness, transparency, untouchability, traceability, time series and encryption [25]. The difference lies in the degree of decentralization, consensus mechanism and trust mechanism. As shown in Fig. 1, the blockchain system consists of data layer, network

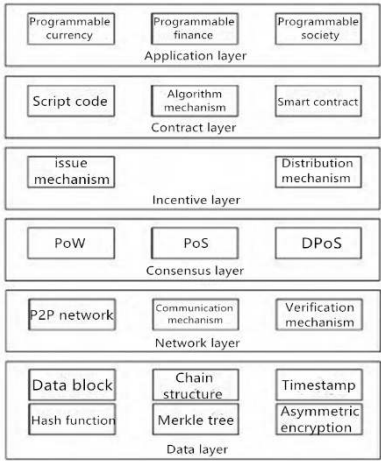


FIGURE 1. Infrastructure of blockchain technology.

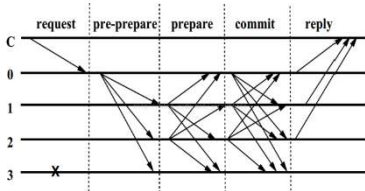


FIGURE 2. Byzantine problem solving process diagram.

layer, consensus layer, incentive layer, contract layer and application layer [26], [27].

B. BRIEF DESCRIPTION OF BLOCKCHAIN TECHNOLOGY AUTHENTICATION ALGORITHM

Blockchain technology involves many authentication algorithms, the more important are PBFT (Byzantine Fault Tolerance Algorithm) and Ripple consensus algorithm [28].

1) BYZANTINE FAULT TOLERANCE ALGORITHM

Based on the traditional Byzantine general problem, ensuring the correctness of the results depends mainly on three phases: the pre-prepare, the prepare and the commit. The process is shown in Fig. 2 below.

C is the sending request node, 0, 1, 2 and 3 are the nodes working as servers. Among them, 3 is the server of the downtime. The specific steps are as follows:

- 1. Request: requester C sends a request to any node, here is 0.
- 2. Pre-Prepare: after receiving the request from C, server 0 broadcasts and spreads it to server 1, 2, 3 respectively.
- 3. Prepare: after receiving the record and broadcasting again, 1-> 0, 2, 3, 2->0, 1 and 3, server 3 cannot broadcast because that it is the downtime server.
- 4. Commit: when server 0, 1, 2, 3 are in the Prepare phase, if more than a certain number of same identical requests are received, they enter Commit phase and the Commit request is broadcast.

5. Reply: when server 0, 1, 2, 3 in the Commit phase, if more than a certain number of same identical requests are received, feedbacks are given to C.

According to the above process, attaining consistency is possible in the case of $N \geq 3F + 1$, where N is the total number of nodes, and F is the total number of nodes in question.

When $N=4$ $F=0$:

	Data obtained	Final data
A	1 1 1 1	1
B	1 1 1 1	1
C	1 1 1 1	1
D	1 1 1 1	1

When $N= 4$ $F= 1$:

	Data obtained	Final data
A	1 1 1 0	1
B	1 1 0 1	1
C	1 0 1 1	1
D	0 1 1 1	1

When $N= 4$ $F= 2$:

	Data obtained	Final data
A	1 1 0 0	NA
B	1 0 0 1	NA
C	0 0 1 1	NA
D	0 1 1 0	NA

It can be seen that Byzantine Fault Tolerance can tolerate nearly 1/3 of the node errors.

2) RIPPLE CONSENSUS ALGORITHM

Ripple’s consensus is achieved between the verification nodes. Each verification node is pre-configured with a list of

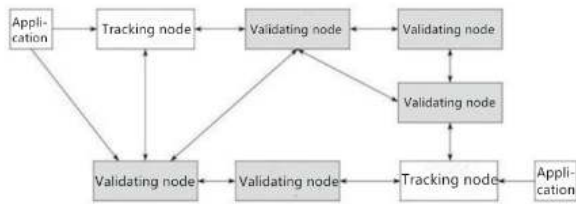


FIGURE 3. Node interaction diagram in the Ripple consensus process.

trusted nodes called UNL (Unique Node List). The nodes on the list can vote on a certain transaction as shown in Fig. 3. Every few seconds, the Ripple network will perform the following consensus process:

1. Each verification node will continuously receive the transactions sent from the network. After verifying with the local ledger data, the illegal transaction will be directly discarded and the legal transactions will be aggregated into a candidate set. The transaction candidate set also includes transactions that were previously unrecognized by the consensus process.

2. Each verification node sends its own transaction candidate set as a proposal to other verification nodes.

3. After the verification node receives the proposal from other nodes, if it is not from the node on the UNL, the proposal is discarded; if it is from the node on the UNL, the transaction in the proposal will be compared with the local transaction candidate set. If there is a similar transaction, the transaction will get a vote. In a certain period of time, when the transaction receives more than 50% of the votes, the transaction enters the next round. No more than 50% of the transactions will be left to the next consensus process to confirm.

4. The verification node sends the transaction that gets more than 50% of the votes as a proposal to other nodes and raises the threshold of the required number of votes to 60%. Then steps 3 and 4 are repeated until the threshold reaches 80%.

5. The verification node officially records the transaction confirmed by the 80% UNL nodes into the local ledger data, which is called Last Closed Ledger meaning the latest status of the ledger [29].

As shown in the algorithm flow of Fig. 4, in Ripple's consensus algorithm, the identity of the voting node is known to the user. Therefore, the efficiency of the algorithm is more efficient than the anonymous consensus algorithm such as the aforementioned PoW, and the confirmation time of the transaction is only a few seconds. However, this also determines that the consensus algorithm is only suitable for the Permissioned Chain, which is the scenario of the local blockchain. The Byzantine Fault Tolerance (BFT) capability of the Ripple Consensus Algorithm is $n(n-1)/2$. It can tolerate Byzantine errors happening in 20% of the nodes in the entire network without affecting the final correct consensus [29]. In fact, many authentication algorithms in certification agreement based on Swarm Intelligence are also a variant algorithms of Ripple's consensus algorithm.

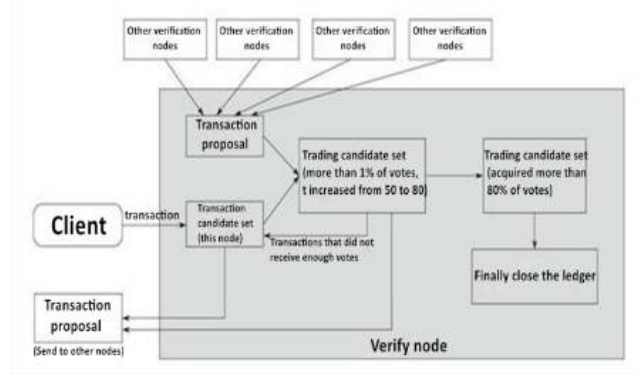


FIGURE 4. Ripple consensus algorithm flow.

IV. OUR SCHEME

A. SYSTEM ARCHITECTURE

The system architecture of this scheme is composed of three main bodies, among which an orderly block network is built: trusted cloud service providers, roadside units and vehicles. Vehicles need to submit their real identity data to the roadside unit for registration before transmitting information and receiving broadcasting. After checking the validity of the vehicle, the roadside unit encrypts the relevant information of the vehicle and transmits it to the cloud service provider. The cloud service provider determines whether to write the vehicle information into the trusted account book and distribute it to the rest of the roadside according to the consensus algorithm. In the unit, until the roadside unit feeds back the key symbolizing the unique identity of the vehicle to the vehicle, the whole registration process is completed. Vehicles are allowed to transmit data and share broadcasting with the same registered vehicle only after the above registration process has been completed. The system architecture diagram is shown in Fig. 5.

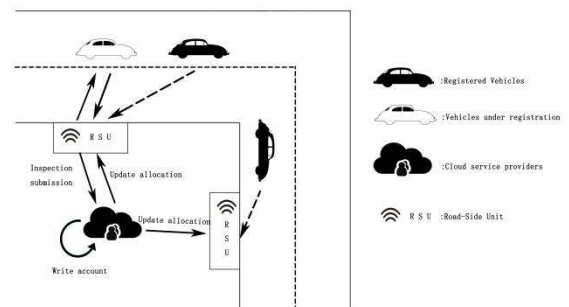


FIGURE 5. An Internet of Vehicles infrastructure based on blockchain technology.

B. IMPROVED AUTHENTICATION SCHEME BASED ON BLOCKCHAIN FRAMEWORK

1) SMART CONTRACT WITH NEW NODES

Because the IoV is in an environment full of mutual distrust, a standardized intelligent contract is needed to build trust.

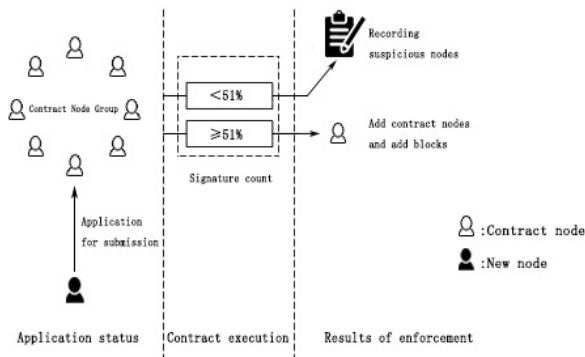


FIGURE 6. Smart contract design when a new node joins a group.

The concept of intelligent contract was first proposed by Nick Szabo in 1995. With the development of Ethereum, it now has a fairly well structured architecture with smart contract. So we design a new intelligent contract based on the Rayleigh consensus algorithm to distinguish the joining of new nodes and block the illegal joining of malicious nodes from the root. The new intelligent contract is shown in Fig. 6.

In the architecture of the system, to ensure that the system does not start to collapse from the root, the intelligent contract is implemented mainly for roadside units, cloud service providers and vehicle manufacturers. In this intelligent contract, the validated roadside units, cloud service providers and vehicle manufacturers form a contract node group according to the blocks. When a new node applies to join the contract node group, it first needs to submit an application to the contract node group. After receiving the application, each individual contract node will retrieve the credit record and credit rating of the current application node in the terminal database, and then choose whether to trust the node or not. If the contract node chooses to trust the node, it will submit its digital signature to the execution layer, otherwise the digital signature will not be granted. Then the digital signature is submitted to the execution layer, otherwise the digital signature is not granted. When the number of digital signatures collected is more than 51%, the new node is identified as a new contract node and added to the block. If the number of digital signatures is less than 51%, the application request is rejected, and the node information is recorded to the list of suspicious nodes and broadcast to other blocks. When the node re-applies, it will face more stringent audits to meet the strict restrictions on new nodes.

There are a lot of untrustworthy nodes in IoV. In the process of authentication for unknown nodes, the cost of authentication may be slightly increased. However, from the whole system architecture, the introduction of this intelligent contract can well maintain the security of the system, and thus solve the trust problem between the main bodies of the system.

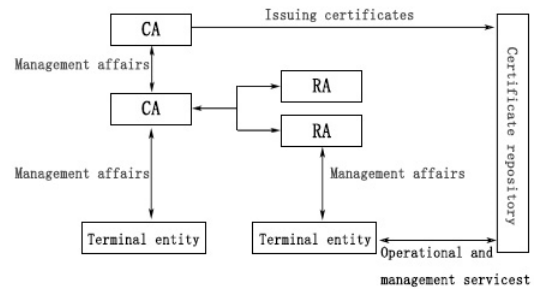


FIGURE 7. Centralized PKI schema diagram.

2) A NEW KEY DISTRIBUTION SCHEME BASED ON BLOCKCHAIN COMBINED WITH TRADITIONAL PKI AUTHENTICATION

At the level of trust, PKI security system is an unavoidable key issue. However, most of the distributed PKI technology is still in the research stage. There are some technical problems in architecture and system security, and it is not suitable to join the existing Vehicle Networking System Architecture. The mature centralized PKI technology also has some performance bottlenecks, so this paper will base on the centralized PKI technology and improve it into an efficient key distribution scheme based on cryptographic accumulator.

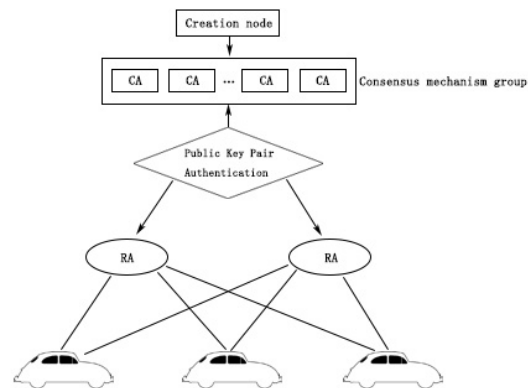


FIGURE 8. Improved key distribution scheme.

As shown in Fig. 8, the PKI technology based on password accumulator will have a more reliable authentication process. Vehicle manufacturers and government administrators will act as Genesis Nodes in the regional network block, providing the unique identity ID of each outgoing vehicle to the cloud service provider as a third-party trusted authentication authority (CA), and when the vehicle initiates a registration request to the roadside unit (RA). When the roadside unit (RA) receives the identity ID and public key information of the vehicle, after verifying the validity of the vehicle information, it attaches its public key to the vehicle information and submits it to the cloud service provider (CA). At this time, the consensus mechanism group composed of multiple CAs starts to operate. The cloud service providers mainly use the

Rayleigh consensus mechanism and query the existence of vehicle identity ID to determine whether the vehicle identity is authentic or not. After verifying the vehicle information, the CA which undertakes the registration information writes the vehicle information into its own account book, and then issues the digital certificate of admission to the network to the vehicle with the help of the roadside unit (RA), and sends the vehicle information and digital signature to other CA nodes through the network. The other CA nodes only need to verify the authenticity of the digital certificate and trust the CA identity of issuing the digital certificate, then they can send the vehicle information and digital signature to other CA nodes. Vehicle information is written into your own account book.

C. NODE JOINING PROCESS BASED ON BLOCKCHAIN AND PUBLIC KEY PAIR TECHNOLOGY

In this section and the following sections, in order to improve the readability of the algorithm, we use CA to refer to cloud service providers and RA to refer to roadside units. In the process of information interaction between CA and RA, the public key pair authentication method based on crypto accumulator is used to improve the authentication efficiency. The following shows the process of vehicle node joining blockchain network:

Suppose the registered vehicle is A, its ID is denoted as ID_A , and its public key information is PK_A .

a) $A \rightarrow RA$: $S_{DC}(ID_A || PK_A)$, where S is the sending operation, vehicle A sends its own factory ID and public key information to RA;

b) $RA \rightarrow CA$: $E_{A1}(ID_A || PK_A || \omega_{RA})$, where E is an encryption function. After receiving vehicle information, RA initially verifies the validity of vehicle identity, attaches its own public key to the information and sends it to CA after encryption.

c) $CA \rightarrow RA \rightarrow A$: $Ver_{A1}(ID_A || PK_A || \omega_{RA}) \rightarrow S_{DC}(A1(ID_A || PK_A || \omega_{RA} || PK_{CA}))$, CA receives the information encrypted by RA, decrypts it with private key, and uses Ver verification algorithm of password accumulator to determine whether the result is 1. If the content is true and the corresponding factory ID of the vehicle can be queried, the public key is issued to RA, and the digital certificate of network entry license is granted to the vehicle.

While CA agrees to issue digital certificates to vehicles, CA will write registration information into its books and transmit it to other CAs through the network. Other CAs will verify relevant data items under the trust mechanism. If the data information is trustworthy, the registration information of vehicle A will be written into the book. Otherwise, the registration information of vehicle A will be discarded and a distrust report will be fed back to the CA that undertakes the registration information. To achieve the establishment of a safe and reliable vehicle blockchain network, well suppress the intrusion of malicious vehicles, from the root to ensure the security of the system.

Table 1 shows the data format of authentication information between CAs:

TABLE 1. The data items for blockchain authentication.

Information item	Details
Blockchain version number	Current version information
Accept date	Time of acceptance of certification
Authenticator Identification	Authenticator unique ID
Certificate content	Describe authentication records
Validity of the certificate	Certification is valid within the time limit
RA Device Identification Code	Verify the identity of the key sender

D. IMPROVEMENT OF AUTOMOBILE (NODE) IDENTITY AUTHENTICATION PROCESS BASED ON BLOCKCHAIN AND PUBLIC KEY PAIR TECHNOLOGY

There are a large number of unfamiliar vehicle nodes in IoV. In the authentication process of unfamiliar vehicle nodes, it is necessary to ensure the legality of vehicle nodes and their trustworthiness to other vehicles. To check whether the vehicle has access qualification, two authentication processes are needed. One is to verify the legitimacy of the vehicle's identity to the roadside unit, the other is to verify the roadside unit and cloud system. Verification process of service supplier is as follows. When a vehicle (assumed to be A) verifies its identity to a roadside unit:

a) $A \rightarrow RA$: $E_{PK_{RA}}(PK_A || ID_A || RN || Time)$, vehicle A sends its own public key PK_A and identity ID_A to the roadside unit. For the sake of information security, random number RN and application timestamp $Time$ are added, and public key PK_{RA} encryption information is promulgated by roadside unit.

b) $RA \rightarrow A$: $E_{PK_{RA}}(M || RN)$, the roadside unit decrypts through the public key, verifies the random number generated by the corresponding time stamp, verifies the legitimate identity of the vehicle through the vehicle information distributed

by the cloud service provider, and returns the admissibility information and the random number RN by using the public key PK_{RA} encryption if the identity is legitimate; if the identity is illegal, records the vehicle ID and broadcasts the rest of the roadside in the block. Unit.

The verification process between roadside units and cloud service providers is as follows:

c) $RA \rightarrow CA: E_{PK_{CA}}(PK_A || ID_A || RN || Time || SK_{RA})$, the roadside unit attaches the information submitted by vehicle A in the previous process to its own key SK_{RA} , and then encrypts it with the public key PK_{CA} of the cloud service provider, and sends it to the cloud service provider;

d) $CA \rightarrow RA: E_{PK_{CA}}[SK_{CA} || ID_A || SK_{RA} || E_{PK_{CA}}(PK_A || ID_A || RN || Time || SK_{RA})]$. After receiving the information submitted by the roadside unit, cloud service providers look up the information corresponding to the vehicle ID and the roadside unit key in the corresponding blockchain, and determine that it is correct, generate the session key SK_{CA} (periodically modified and updated) and send it to the roadside unit, and add the authentication record to the corresponding block account. In this section, the remaining blocks are broadcast, otherwise the request is rejected.

e) $RA \rightarrow A: D_{PRK}(SK_{CA} || ID_A) \rightarrow E_{SK_{RA}}(DC)$. Roadside units use private key PRK to decrypt session key SK_{CA} and vehicle ID information, and then encrypt and authenticate digital certificate DC through their own key to send to vehicle A. The whole authentication process is completed.

Finally, the framework of the system is extended to include the following decentralized mechanisms to complement its functionality, so as not to distort or even collapse the network.

The first mechanism is to save the DNS service that points to the source. For example, a blockchain provides services in the field of Bitcoin. The user sends the appropriately encoded transaction on the blockchain to create or modify the record on the service. The blockchain needs to filter nodes periodically, so that the blockchains can successfully complete the search for valid and corresponding data sequences (certificates), and use them to modify its node database accordingly.

The second is secure communication and file exchange. As mentioned above, messages in the blockchain are read by each network participant, including vehicles, Road-Side Unit, and cloud service providers. Whenever a dedicated communication channel is required, protocols such as FBST [30] or Whisper [31] should be used. The ledger or certificate sharing requirements in the system can be addressed through a content-addressable P2P file system, such as IPF [32].

V. EXPERIMENT ANALYSIS

A. EXPERIMENTAL ENVIRONMENT

Veins is an open source framework for running vehicular network simulations. It is based on two well-established simulators: OMNeT++, an event-based network simulator, and SUMO, a road traffic simulator. It extends these to offer a comprehensive suite of models for IVC simulation. It relies on a comprehensive detailed model of the IEEE 802.11p and IEEE 1609.4 DSRC/WAVE network layers, including

multi-channel operation, QoS channel access, noise and interference effects. Simulations at the city block level can be simulated in real time on a single work station and can be deployed on a compute cluster and simulated in a MRIP distributed parallel manner. Table 2 illustrates our experimental settings.

TABLE 2. Experimental settings.

Device	Device parameters
CPU	Intel (R) Core (TM) i7-7500U at 2.90GHz
RAM	4GB
Operating system	Ubuntu (R) 16.04 (virtual machine)

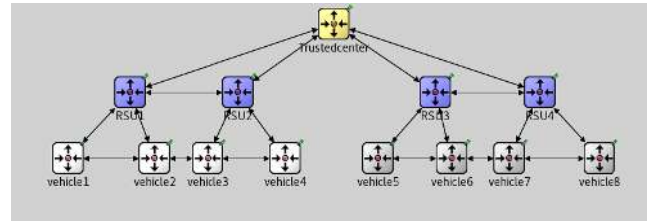


FIGURE 9. Diagram of experiment setting.

B. SIMULATION SCENARIO

In this experiment, a total of thirteen nodes are established as shown in Fig. 9, in which the Trusted center node is a cloud service provider (also a key distribution center), RSU1 and RSU2 are roadside unit nodes, providing services for vehicles to join the account book, and Vehicle 1-8 are common vehicles in the Internet of Vehicles. The transmission information between them is TicTocMsg15 (hidden in the figure). The purpose of this design is to eliminate the influence of malicious vehicles. By simulating the connection of vehicle information between two sections into blocks, and then through a large number of data injection and long-term simulation experiments, we can get the average encryption time cost of using blockchain technology in Internet of Vehicles, as well as the communication cost in the encryption process.

C. SIMULATION ANALYSIS

1) TRANSCIEVER PACKETS AT DIFFERENT NODES

As the experimental simulation is a regional simulation, and the information needs to be exchanged largely in amount and persistently in time during the running of the specific vehicle, this experiment will finalize the cut-off time point of the data at 6,757s, which is sufficient to show a certain trend change. In this experiment, the horizontal coordinate represents the simulation time in seconds (s), while vertical coordinate represents the approximation of the number of

packets sent and received in the time interval divided by the total simulation time (ms) in units /ms. The advantage of this processing is that the overall trend of the amount of information sent and received can be obtained more clearly. In order to observe the readability and accuracy, the simulation time of this experiment is not uniform, and the controllable range is adjusted. The maximum data for sending and receiving packets can be obtained from the parameter “upper” below the chart.

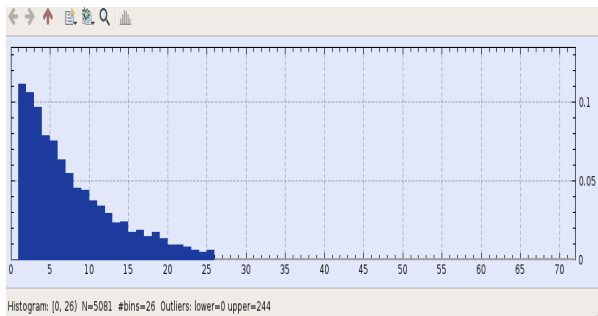


FIGURE 10. Transceiver packets graph at Trusted center.

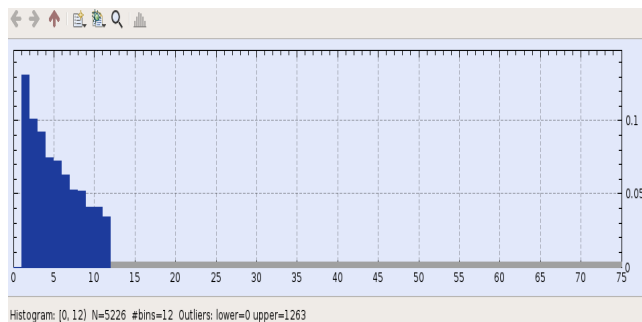


FIGURE 11. Transceiver packets graph at the vehicle (vehicle2).

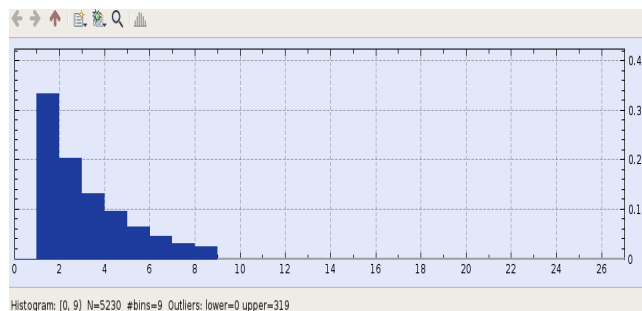


FIGURE 12. Transceiver packets graph at the RSU (RSU1).

Through the comparison between Fig. 10, Fig. 11 and Fig. 12, the difference between the three types of nodes in sending and receiving packets and the delay time is clearly seen. We find that the vehicle (vehicle 2) of the “bottom layer” has the largest packets sent and received during the simulation time. The number can even reach 1,263. The second node with large packets is the RSU (RSU 1) of the

“middle layer”, and the minimum number of packets sent and received is Trusted center (the trusted center). In addition, at the beginning of the experiment, the number of packets sent and received by vehicles (Vehicle 2) and RSU (RSU 1) decreased slightly. And with the passage of simulation time, the number of packets sent and received tends to be stable. Similar to the stability of Trusted center cylinder curve, at the beginning of simulation, the process of sending and receiving data packets by vehicle 2 and RSU (RSU 1) will also undergo a slight decrease in the number of data packets (it can be seen that the descent range of longitudinal coordinates is 0.03–0.14), and then tend to be stable. This is actually the phenomenon of public key packaging in the process of data packet interaction in the blockchain. Correspondingly, because of the existence of key decryption, this phenomenon will not have any impact on the core data of vehicle registration and authentication and the digital certificates issued by cloud service providers, which guarantees the privacy and security of vehicle networking.

In our simulation, the time consumption includes the time when the vehicle submits the registration application to the key distribution center, the time needed by the encryption calculation of the key distribution center, the response time when the key distribution center submits the user’s application to the RSU and requests to verify the authentication, and the time when the key distribution center returns the key to the vehicle after the authentication is completed.

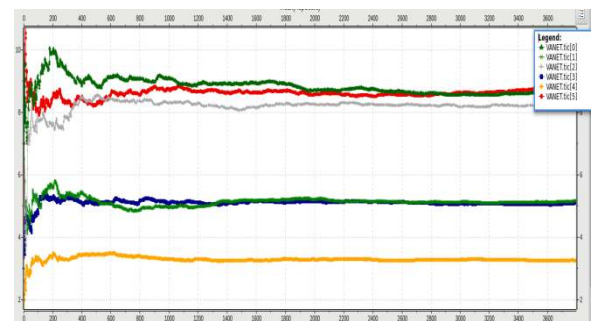


FIGURE 13. The average operating time consumption of each node (single mean operation).

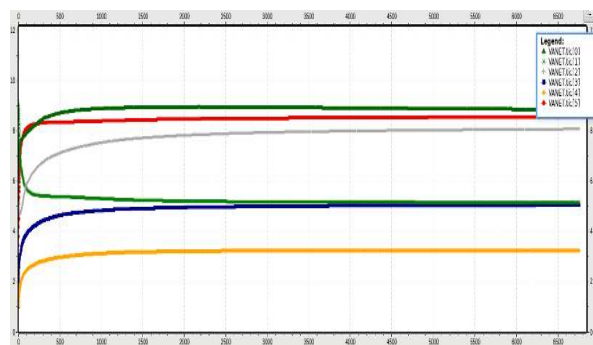


FIGURE 14. The average operating time of each node (three mean operations).

The Veins simulation platform provides a Mean (averaging) operation. As shown in Fig. 13 and Fig. 14,

by continuously conducting the Mean operation, we can clearly know the average time cost of transceiver operation of the node. It can be seen from Fig.13 and Fig.14 that most of the time-consuming happens in the encryption calculation process of the key distribution center, and the average time spent in the encryption calculation is about 9ms (+100ms). The process of verifying security in the RSU is very fast, and the average time is only 3~5ms (+100ms). This is due to the excellent underlying consensus algorithm of the blockchain, which responds to requests in a timely manner in the areas where vehicles are connected to each other. It should be noted that the horizontal ordinate of the experimental chart is in seconds (s), and the vertical ordinate is in milliseconds (ms).

The above results can be translated into the following value tables, which indicate the time consumed by the three main node classes in the whole authentication process.

TABLE 3. Time overhead value table.

Node class	Average time overhead
Cloud service providers (Trustedcenter)	8.4 ms
Road measuring unit (RSU2)	3.2 ms
Vehicle (vehicle3)	4.9 ms

From the above experiments, it can be verified that the Internet of Vehicles based on blockchain techniques can fully adapt to the heavy traffic system with the time overhead for the authentication process, and can operate efficiently while preventing malicious attacks.

2) THE COMMUNICATION OVERHEAD OF TRANSCIVER PACKETS

Given the fact the message transmission rate of the system is very fast, as well as the frequent message exchanging and destruction process, the statistical results of communication overhead are demonstrated by a linear line graph. That is, we accelerate the simulation time (the data cut-off point is 6757s) to obtain the line overlapping dense section which can define the communication cost, instead of directly calculating the communication cost by the weight formula. This ensures more accurate reflection of communication overhead. It can be clearly seen from Fig. 15 that the memory required for the vehicle to submit the registration request to the key distribution center (successful or not) is about 17 KB, but the peak value may exceed 70 KB. From Fig. 16, It can be clearly seen that the memory reserved by the key distribution center in the

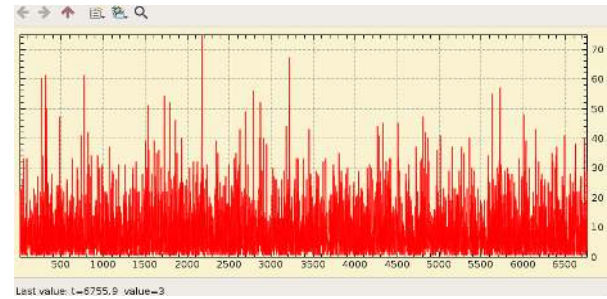


FIGURE 15. Communication overhead chart for vehicle registration and feedback.

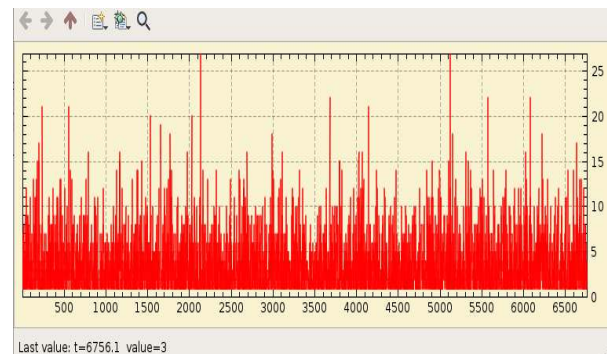


FIGURE 16. Communication overhead chart for RSU verification authentication process.

process of submitting an authentication application to RSU needs only about 8 KB, but its peak value may reach more than 25 KB. There, in practical applications, more memory needs to be reserved to prevent packet loss or message overflow loss.

The above experimental maps are integrated into a table of values as follows (the values in the table are all estimates with an error interval of (+2):

TABLE 4. Communication overheads.

Specific authentication steps	Communication overhead
Application for registration of vehicles	17KB
Roadside Unit Verification Report	8KB
Terminal feedback	25KB

From the above experiments, we can see that the communication overhead has a certain volatility in frequent message

generation and destruction. However, because the average cost is small, the communication infrastructure provided to vehicle nodes will be improved with the development of communication technology, so the communication costs required are within reasonable bounds, which verifies the feasibility and stability of this scheme in a large-scale traffic network.

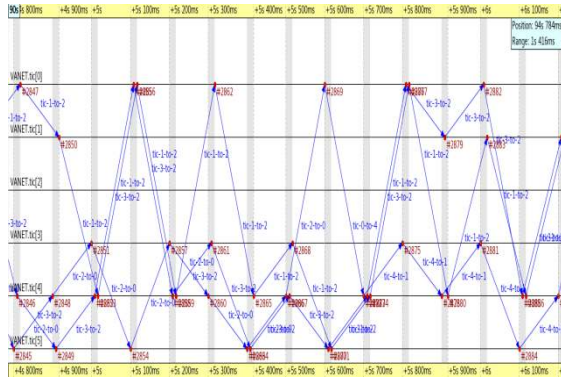


FIGURE 17. Partial authentication message transmission process.

In addition, in order to intuitively understand the whole experiment, we use a broken line analysis diagram to show the whole process of authentication as shown in Fig. 17. It is worth mentioning that in order to make the broken line at a relatively gentle slope, this experiment sets the transmission delay of messages between nodes into 100 ms. Because of the long simulation time, the stable time interval of exchange messages is selected in Fig. 17. As shown in Fig. 17, the message is sent from Node 0, 4 and 5, and the blue arrow is the direction of message transmission. The source and direction of the message are indicated beside the arrow. The upper and lower rulers are displayed in real time, and a delay of 100 ms is set so that the broken line can be better observed. In addition, #28 is the operation number, which is helpful to observe the sequence of each step.

3) COMPARISON OF EXPERIMENTAL RESULTS

In order to highlight the advancement of this scheme in blockchain authentication efficiency, we try to do a comparative experiment to make a comparison with Dorri *et al.*'s scheme [20] mentioned in literature review in terms of authentication efficiency.

As shown in Fig. 18, the X-axis represents the length of the blockchain in the state of vehicle networking. Considering the enormity of vehicle networking, the length order of magnitude is set as 10^4 . The Y-axis represents the time cost of vehicle authentication under the corresponding blockchain length, in milliseconds (ms). Our scheme represents the cryptographic public key pair authentication method used in our scheme, while Dorri *et al.*'s [20] scheme represents the vehicle authentication efficiency scheme based on Lightweight Scalable Blockchain (LSB) proposed by Dorri *et al.* [20].

It can be clearly seen that when the length of block chain is less than 1.7×10^4 , the time cost is better than our scheme, but

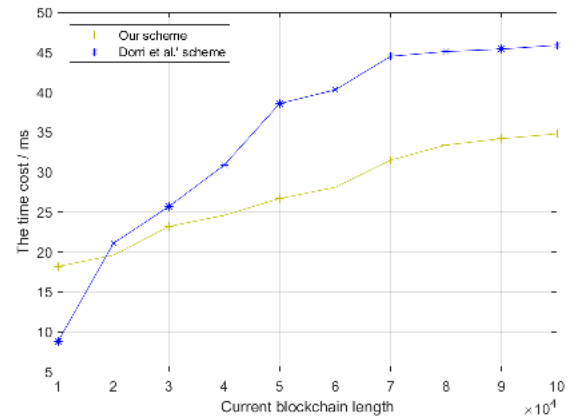


FIGURE 18. Comparing experimental curves of certification efficiency.

after that, due to the continuous expansion of vehicle network, the pressure on OBM will increase dramatically, which also leads to the time cost of Dorri *et al.*'s [20] scheme increasing rapidly with the increase of the length of block chain in the initial stage. Dorri *et al.*'s [20] schemes tend to be stable after the length of block chains reaches 7×10^4 orders of magnitude, and the total cost of authentication can be completed in about 45 ms. Our schemes can maintain a controllable and stable growth in time cost, and can also maintain a stable time cost of 34 ms after the length of block chains reaches 7×10^4 orders of magnitude to ensure the efficiency of authentication. After many experiments, we find that our scheme can improve the authentication efficiency by 29.5% on average compared with Dorri's scheme, and the peak efficiency can increase by 37.4% compared with Dorri *et al.*'s [20] scheme, which is a considerable improvement in efficiency.

4) SIMULATION SUMMARY

This experiment verifies the feasibility and reliability of the scheme by simulating the average time cost and communication cost of establishing the system for vehicle authentication in a traffic block. According to the simulation result of the above experiment, the system has the ability to withstand large-scale data exchange, authentication, encryption operations, in addition to achieving the purpose of excluding malicious attacks through the bottom consensus algorithm. However, there is still large packet loss in the vehicle registration and key distribution process which provides scope for further improvement.

VI. CONCLUSION

The new emerging blockchain technology can solve the problem of identity authentication and identity counterfeiting of multi-nodes systems in Internet of Vehicles. For example, blockchain technology combined with the PKI authentication mechanism can solve the identity authentication problem between the vehicles, the servers and the RSUs in Internet of Vehicles, and is also able to solve the problem of user account management, including the multiple logins of the

same account or user. In addition, the encryption feature of the blockchain itself can be used to encrypt the identity information of the vehicle node and prevent the leakage of user information. In this paper, the blockchain-based technology is developed further to Internet of Vehicles. The blockchain framework is adopted to design a new key distribution mechanism, the blockchain ledger technology is used to design a new node joining mechanism, and the blockchain consensus technology is further developed to design a new vehicle identity authentication mechanism. It is shown from experiments the improved authentication scheme can effectively improve the quality of authentication, so as to effectively resist malicious attacks against Internet of Vehicles.

REFERENCES

- [1] T. Qiu, X. Liu, K. Li, Q. Hu, A. K. Sangaiah, and N. Chen, "Community-aware data propagation with small world feature for Internet of vehicles," *IEEE Commun. Mag.*, vol. 56, no. 1, pp. 86–91, Jan. 2018.
- [2] B. Wang, X. Gu, and S. Yan, "STCS: A practical solar radiation based temperature correction scheme in meteorological WSN," *Int. J. Sensor Netw.*, vol. 28, no. 1, pp. 22–33, 2018.
- [3] S. Zhang, X. Li, Z. Tan, T. Peng, and G. Wang, "A caching and spatial K-anonymity driven privacy enhancement scheme in continuous location-based services," *Future Gener. Comput. Syst.*, vol. 94, pp. 40–50, May 2019.
- [4] T. Qiu, R. Qiao, and D. Wu, "EABS: An event-aware backpressure scheduling scheme for emergency Internet of Things," *IEEE Trans. Mobile Comput.*, vol. 17, no. 1, pp. 72–84, Jan. 2018.
- [5] Y. Lai, L. Zhang, F. Yang, L. Zheng, T. Wang, and K.-C. Li, "CASQ: Adaptive and cloud-assisted query processing in vehicular sensor networks," *Future Gener. Comput. Syst.*, vol. 94, pp. 237–249, May 2019.
- [6] T. Qiu, X. Wang, C. Chen, M. Atiquzzaman, and L. Liu, "TMED: A spider-web-like transmission mechanism for emergency data in vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 67, no. 9, pp. 8682–8694, Sep. 2018.
- [7] J.-H. Song, V. W. S. Wong, and V. C. M. Leung, "Wireless location privacy protection in vehicular ad-hoc networks," *Mobile Netw. Appl.*, vol. 15, no. 1, pp. 160–171, 2010.
- [8] A. D. Yein, Y.-H. Huang, C.-H. Lin, W.-S. Hsieh, C.-N. Lee, and Z.-T. Luo, "Using a random secret pre-distribution scheme to implement message authentication in VANETs," *Appl. Sci.*, vol. 5, no. 4, pp. 973–988, 2015.
- [9] L. Li, Y. Mao, Y. Li, and Y. Yuan, "Privacy addressing-based anonymous communication for vehicular ad hoc networks," *Wireless Pers. Commun.*, vol. 71, no. 3, pp. 2349–2359, 2013.
- [10] T. Oulhaci, M. Omar, F. Harzine, and I. Harfi, "Secure and distributed certification system architecture for safety message authentication in VANET," *Telecommun. Syst.*, vol. 64, no. 4, pp. 679–694, 2017.
- [11] K. Kumar and S. K. Arora, "Review of vehicular ad hoc network security," *Int. J. Grid Distrib. Comput.*, vol. 9, pp. 17–34, 2016.
- [12] T. Bouali, S.-M. Senouci, and H. Sedjelmaci, "A distributed detection and prevention scheme from malicious nodes in vehicular networks," *Int. J. Commun. Syst.*, vol. 29, no. 10, pp. 1683–1704, 2016.
- [13] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, "A secure authentication scheme for VANETs with batch verification," *Wireless Netw.*, vol. 21, no. 5, pp. 1733–1743, 2015.
- [14] A. Zhou, J. Li, Q. Sun, C. Fan, T. Lei, and F. Yang, "A security authentication method based on trust evaluation in VANETs," *EURASIP J. Wireless Commun. Netw.*, vol. 15, pp. 1–8, Mar. 2015.
- [15] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
- [16] Y. Zhang and J. Wen, "The IoT electric business model: Using blockchain technology for the Internet of Things," *Peer-to-Peer Netw. Appl.*, vol. 10, no. 4, pp. 983–994, 2017.
- [17] K. Zhao and Y. Xing, "Summary of research on blockchain technology in Internet of Things security," *Inf. Netw. Secur.*, vol. 5, pp. 1–6, 2017.
- [18] J. He and G. C. Gong, "Research on blockchain technology in the field of IoT security," *Telecommun. Eng. Technol. Standardization*, vol. 30, no. 5, pp. 12–16, 2017.
- [19] B. Lee and J.-H. Lee, "Blockchain-based secure firmware update for embedded devices in an Internet of Things environment," *J. Supercomput.*, vol. 73, no. 3, pp. 1152–1167, 2017.
- [20] 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.
- [21] P. K. Sharma, S.-Y. Moon, and J.-H. Park, "Block-VN: A distributed blockchain based vehicular network architecture in smart city," *J. Inf. Process. Syst.*, vol. 13, no. 1, pp. 184–195, 2017.
- [22] Y. Yuan and F. Y. Wang, "Current status and prospects of blockchain technology development," *J. Automat.*, vol. 42, no. 4, pp. 481–494, 2016.
- [23] Y. Zhu, G. Gan, and D. Deng, "Security research in key technologies of blockchain," *Inf. Secur. Res.*, vol. 2, no. 12, pp. 1090–1097, 2016.
- [24] P. Marc, "Blockchain technology: Principles and applications," in *Research Handbook on Digital Transformations*. 2015.
- [25] S. Underwood, "Blockchain beyond Bitcoin," *Commun. ACM*, vol. 59, no. 11, pp. 15–17, 2016.
- [26] Y. Zhang, "Research on the impact of blockchain technology on the development of China's financial industry," *Int. Finance*, vol. 5, pp. 41–45, 2016.
- [27] A. Wright and P. De Filippi, "Decentralized blockchain technology and the rise of lex cryptographia," *Tech. Rep.*, 2015.
- [28] M. D. Piero, "What is the blockchain?" *Comput. Sci. Eng.*, vol. 19, no. 5, pp. 92–95, 2017.
- [29] X. G. Wang, "Overview of blockchain technology consensus algorithm," *Inf. Comput.*, vol. 9, pp. 72–74, 2017.
- [30] X. Wang, S. Li, S. Zhao, and Z. Xia, "A VANET privacy protection scheme based on fair blind signature and secret sharing algorithm," *Automatika*, vol. 58, no. 3, pp. 287–294, 2017.
- [31] S. Ghaffarzadegan, H. Bo il, and J. H. L. Hansen, "Generative modeling of pseudo-whisper for robust whispered speech recognition," *IEEE/ACM Trans. Audio, Speech, Language Process.*, vol. 24, no. 10, pp. 1705–1720, Oct. 2016.
- [32] Z. Feng, N. Jing, and L. He, "IPF: In-place X-filling algorithm for the reliability of modern FPGAs," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 22, no. 10, pp. 2226–2229, Oct. 2014.



XIAOLIANG WANG received the B.E. degree in computer engineering from Xiangtan University, China, the master's degree in computer science from Xiangtan University and the Institute of Computing Technology, Chinese Academy of Sciences, China, and the Ph.D. degree from Hunan University, China. He was with Xiangtan University. He was a Postdoctoral Researcher with The University of Alabama, USA. He is currently an Associate Professor of information technology

and the Director of the Department of Internet of Things Engineering, Hunan University of Science and Technology, China. He leads a team of researchers and students in the areas of information security and the Internet of Things, such as VANET security and anonymous authentication in ad hoc networks. He has published more than 30 highly reputed SCI/EI indexed journals/conferences articles. His research has been funded by the Natural Science Foundation Committee and the Ministry of Education, China. He was with the Nanjing Government of China.



PENGJIE ZENG is currently pursuing the bachelor's degree with the Hunan University of Science and Technology. He currently holds a technology development position with the Raspberry Pi-Based Intelligent Agricultural Traceability System Project Team. His research field is the application of block chain in the Internet of Things, cyberspace security, privacy protection, and large data processing and analysis. He received the Second Prize in the National College Students

Innovative Electronic Design Competition and the Third Prize in the School-Level Financial Management Data Analysis Competition.



NICK PATTERSON received the Ph.D. degree from Deakin University, in 2013. He has great capacity to learn and grasp new ideas quickly, the flexibility to work well on his own initiative, and a friendly attitude to excel in cross-functional team environments. He is a self-starter with personal drive and commitment to provide exceptional service to stakeholders. He thrives in investigating and researching technological problems and vulnerabilities that may lead to fraud or cyber-crime and design solutions for protection. Finally, he has shown dedication and loyalty in the past as well as being effective in stressful situations and meeting deadlines. His research interests include IT security, forensics, hacking countermeasures, biotechnology, criminology, and agile project management. He was a recipient of the Alfred Deakin Thesis Medal, in 2014, for research that was focused on Improving the World.



FRANK JIANG received the master's degree in computer science from The University of New South Wales (UNSW), Australia, and the Ph.D. degree from the University of Technology Sydney. He has 3.5 years of Postdoctoral research experience with UNSW. He has published over 100 highly reputed SCI/EI indexed journals/conferences articles. His main research interests include data-driven cyber security, predictive analytics, biologically inspired learning mechanism, and its application in the complex information security systems.



ROBIN DOSS (SM'16) received the B.E. degree in electronics and communication engineering from the University of Madras, India, and the master's and Ph.D. degrees from the Royal Melbourne Institute of Technology (RMIT), Australia. He was a part of the Technical Services Group, Ericsson, Australia, and a Research Engineer with RMIT University. He is currently a Professor of information technology and the Deputy Head of the School of Information Technology, Deakin University, Australia. He leads a team of researchers and Ph.D. students in the broad areas of communication systems and cybersecurity with a focus on emerging domains, such as the Internet of Things (IoT), pervasive computing, applied machine learning, and ambient intelligence. His research has been funded by the National Security Science and Technology Branch of the Office of National Security in collaboration with the Defence Signals Directorate, the Australian Research Council, and industry partners. He is the Founding Chair of the Future Network Systems and Security Conference series and an Associate Editor of the *Cyber-Physical Systems Journal*.

• • •