2021 IEEE 19th International Conference on Embedded and Ubiquitous Computing (EUC) | 978-1-6654-0036-7/21/$31.00 ©2021 IEEE | DOI: 10.1109/EUC53437.2021.00017

A Blockchain-based Fast Authentication and Collaborative Video Data Forwarding Scheme for Vehicular Networks

Weihui Qiu
School of Computer Science
China University of Geosciences
Wuhan, P.R. China
qiu@cug.edu.cn

Xin Yang
Wuhan Institute of Marine Electric Propulsion
CSSC, P.R. China, 430064
396271305@qq.com

Ming Wei
School of Computer Science
China University of Geosciences
Wuhan, P.R. China
mingwei@cug.edu.cn

Wei Ren*
School of Computer Science, China University of Geosciences
Wuhan, P.R. China
Key Laboratory of Network Assessment Technology, CAS
(Institute of Information Engineering,
Chinese Academy of Sciences, Beijing, P.R. China 100093)
Guizhou Provincial Key Laboratory of Public Big Data,
Guizhou University, Guiyang 550025, P.R. China
weirencs@cug.edu.cn

Tianqing Zhu
School of Computer Science
China University of Geosciences
Wuhan, P.R. China
tianqing.zhu@ieee.org

***Abstract*—Internet of Things (IoT) current present two trends with respect to ubiquity and mobility. The number of devices increases remarkably and most forthcoming devices are mobile, e.g., Internet of Vehicles (IoV). In large scale mobile IoT, the management of device identification, fast authentication, and certification of public keys experiences upcoming difficulties. Centralized security architecture may not be suitable and in contrast cross-domain security architecture will tackle the ubiquity and mobility better. We note that blockchain is a new decentralized architecture equipped with basic cryptographic settings, which provides new tools such as token and guarantees many security properties such as block integrity. In this paper we design a blockchain-based fast authentication video data forwarding scheme for IoV. Compared with existing protocols, it has the advantages of decentralization, high authentication efficiency, strong trust, and resistance to common attacks. We evaluate our scheme with real experiments over Hyperledger Fabric and the authentication delay is manageable (e.g, 4 seconds in IoV).**

***Index Terms*—Blockchain, authentication, Internet of Vehicles, Internet of Things.**

I. Introduction

Trend of large scale mobile Internet of Things (IoT) introduces many new applications in our daily life, e.g., Internet of Vehicles (IoV). Compared with traditional IoT, IoV characters by stronger computation capability, more battery life, and mobile devices in a large area. Those features of IoV enable and foster more applications that cannot be conducted in traditional IoT.

For example, vehicles may request certain services on the road while driving, e.g., road traffic, traffic control information, and nearby accidence. A prerequisite step is to authenticate those vehicles for further service provision. As the speed is fast, such a authentication procedure should be timely with low delay. However, current centralized authentication solutions need handshakes between vehicles and servers, which may introduce unacceptable delay. Also, vehicles may be driven to different management domains, which further increases the delay due to the interaction between domains. The reason is that one domain may not be able to manage a large number of vehicles.

Moreover, IoV enlarges sensing abilities from simple text message to multimedia vision. Vehicles are equipped with video monitors to capture and record real-time surroundings. These vision data can be shared as evidence for some critical applications such as determining accident responsibility. Certainly, the authentication of vehicles should be guaranteed for the trustworthiness of presented sensing data.

Currently, security risks in large-scale IoT terminal devices have been intensively studied [1], such as terminal forgery, node control and data tampering. Existing schemes for authentication and management of IoT devices usually rely on a centralized architecture. Devices have to communicate with central servers so that delay increases with the growth of node number. Moreover, once a central server is tampered, all vehicles will be influenced and the data security cannot be guaranteed.

In this paper, we propose a blockchain-based fast

978-1-6654-0036-7/21/$31.00 ©2021 IEEE
DOI 10.1109/EUC53437.2021.00017

Authorized licensed use limited to: China University of Geosciences Wuhan Campus. Downloaded on September 08,2023 at 08:02:48 UTC from IEEE Xplore. Restrictions apply.

authentication and collaborative video data forwarding scheme for IoV, without concerning about the tamper of central servers. In our scheme, blockchain is employed for providing public key hash, identity management, data integrity. We also add extra edge servers and to further tackle the authentication delay. The contribution of the paper is as follows:

1) We propose a blockchain based cross-domain and fast authentication identity management scheme for large scale IoV. With the combination of blockchain and cryptography, identity authentication can be anonymous, and identity management can be cross-domain.
2) We add extra edge servers between the central server and IoV in our scheme, which delegate part of the functions of the central server in the traditional architecture. Therefore, the pressure of the central server is reduced, and the time delay for authentication is decreased.

The rest of the paper is organized as follows: Section II reviews related works. Section III describes the content of our scheme, followed by experiment evaluation and detailed analysis in section IV. Section V summarizes the paper.

II. Related Works

Authentication and key agreements on IoT devices have been intensively studied. However, most of the authentication schemes are based on Public Key Infrastructure (PKI). These schemes use a lot of computing and communication resources, so the efficiency of identity authentication has not been very high, such as the protocol proposed by Raya and Hubaux [2]. Mallissery et al. [3] reduced communication overhead and combined short-term certificates and Merkle signature schemes. However, once such schemes encounterd high-density devices, the authentication efficiency was still vulnerable to the central node's calculation and communication bottlenecks. In order to solve the traditional PKI usability and security defects, Jiang et al. [4] first proposed a privacy-protected thin-client authentication scheme (PTAS), which used the idea of private information retrieval (PIR) to make the thin-client behave like a full node users operate normally while protecting their privacy. The program had high security and comprehensive functions. Smart card is also a very important tool in cryptography, so Ying and Nayak [5] designed an effective authentication scheme based on smart card. This scheme reduced computing and communication overhead and resisted offline password guessing attacks. However, this scheme was vulnerable to replay attacks and session attacks.

Privacy protection has always been a very important topic. How to ensure the user's information security during the authentication process is a focus of many people's researches. Li et al. [6] proposed an effective revocable message authentication scheme to solve the security and privacy issues of the vehicle network. The core of the scheme is an online/offline certificateless signature with valid revocation rights. In order to deal with revocation, the key generation center will periodically update the time keys of unrevoked users, and use blockchain technology to store revocation lists to enhance the transparency of user revocation. Zero knowledge proof (ZKP) was proposed by S. Goldwasser, S. Micali and C. Rackoff in the early 1980s. It refers to the ability of the prover to convince the verifier that a certain assertion is correct without providing any useful information to the verifier. A large number of facts prove that ZKP algorithms are very useful in cryptography. If ZKP algorithms can be used for verification, many problems can be solved efficiently. Based on the above characteristics, ZKP algorithms can be applied to privacy protection issues in the authentication process. Yang et al. [7] used smart contracts and ZKP algorithms to improve the existing claim identity model in blockchain to realize unlinkable identities and avoid the exposure of attribute ownership. This scheme realized effective attribute privacy protection and had a wide range of applications. Prada [8] paper described how to use the key from physical fingerprint of devices to authenticate the device in the ZKP. This method didn't require expensive security elements, and even enabled a lightweight device to prove its identity and sign messages.

In terms of identity authentication, many researchers have their own methods. Esposito et al. [9] proposed a novel solution for the distributed management of identity and authorization. It used blockchain technology to master the global view of security policies and integrates it into the FIWARE platform. Hammi et al. [10] proposed an original decentralized system, trust bubble, to ensure robust identification and authentication of devices. Relying on the security advantages provided by blockchain and used to create a secure virtual area (bubble), things in the area can recognize and trust each other. In addition, it also protects the integrity and availability of data. Bagga et al. [11] has designed a new type of blockchain-supported batch authentication scheme to accelerate the speed of authentication. The scheme has higher security and functional characteristics, and has strong robustness against various attacks. The author also experimented with storage, communication, and calculation costs, showing that this scheme is feasible.

There are also many research contents in the IoV that this article focuses on, many of which are combined with Road Side Unit (RSU) to design solutions. Yang et al. [12] proposed a decentralized trust management system for vehicle networks based on blockchain technology. In this system, vehicles can verify information received from neighboring vehicles through inference models. Based on the verification result, the vehicle will generate a rating for each message source vehicle. The rating uploaded from the vehicle. RSU calculates the trust value offset of related vehicles and packs these data into a "block".

Authorized licensed use limited to: China University of Geosciences Wuhan Campus. Downloaded on September 08,2023 at 08:02:48 UTC from IEEE Xplore. Restrictions apply.

Then, each RSU will try to add their "blocks" to the trusted blockchain maintained by all RSUs. The system is effective and feasible in collecting, calculating and storing the trust value of the vehicle network. Xu et al. [13] designed a blockchain-based authentication and key agreement for the multi-trusted organization network model, and put Trusted Authority's (TA) computing load on the RSU to improve the authentication efficiency. In addition, through blockchain technology, multiple TAs are used to manage ledgers that store vehicle-related information, so that vehicles can easily achieve cross-regional authentication.

After the identity authentication is successful, there are many functions that can be applied, such as data sharing. Chi et al. [14] comprehensively considerd the security and efficiency of data sharing. A secure data sharing framework based on identity authentication and hyperledger architecture is designed to ensure the security of data sharing. Selecting the scope of data sharing based on the community test results evaluated by the sharing degree can effectively narrow the scope of querying shared data and improve the efficiency of data sharing. Tian et al. [15] combined blockchain technology and loT technology, They proposed a blockchain system framework for loT identity authentication which realized identity authentication among devices, cloud servers, IoT base stations, and devices.To prepare for the arrival of the "Industry 4.0" era, Lin et al. [16] proposed a blockchain-based secure mutual authentication system BSeln to implement fine-grained access control strategies. The system can provide privacy and security guarantees such as anonymous authentication, auditability, confidentiality, and had good security and scalability.

III. Proposed Scheme

In this section, we first introduce system model, followed protocol design and dataflow. Then we use a use case to explain our protocol.

A. *System Model*

In this paper, we proposed a blockchain-based fast authentication and collaborative video data forwarding scheme for IoV. The architectural model of the scheme is shown in Fig. 1. The proposed model consists of blockchain network, central server, edge servers and vehicles. The details of these entities are as follows:

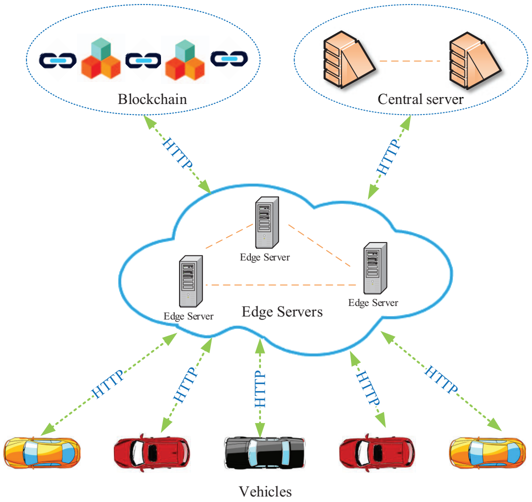

Fig. 1. Architectural model of fast authentication and collaborative video data forwarding scheme

1) Blockchain: The blockchain network acts as a trusted decentralized distributed database which stores server information, vehicle information and accident information. Compared with the traditional PKI system, the user information stored in the blockchain network is always safe unless a 51% attack occurs. Besides, since all IoV information is stored in the same blockchain network, the cross-domain authentication problem of IoV devices can be solved through the secondary forwarding of edge servers.
2) Central server: The central server works as a server for storing large-scale data. It stores information describing accidents such as videos. In this way, it solves the problem that the blockchain cannot store large-scale data.
3) Edge servers: Edge servers are distributed in cities. By delegating part of functions to the edge servers, e.g., identity authentication, data forwarding and decrypt the encrypted video, it reduces the pressure on the central server and decreases the time delay for authentication.
4) Vehicles: Vehicles denote those cars driving on the road. As long as the smart driving recorder is installed and registered, vehicles can be connected to the system and use it or other vehicles need the assistance of this vehicle when an accident occurs.

B. *Protocol Design*

The protocol model is shown in Fig. 2. There are four parts: Part 1: vehicles, Part 2: edge servers, Part 3: central server, and Part 4: blockchain server. The protocol is divided into three phases: initialization phase (green), identity authentication phase (orange) and data forwarding phase (blue). The entire program process is divided into 13 steps.

1) Initialization phase: This phase can be regarded as initialization. The side of vehicles are completed when the driving recorder APP is installed. And the side of edge servers are completed during deployment. There are two steps in this phase.

Step 1.1: The vehicle uploads hash value of its public key and VID to blockchain.

Authorized licensed use limited to: China University of Geosciences Wuhan Campus. Downloaded on September 08,2023 at 08:02:48 UTC from IEEE Xplore. Restrictions apply.

TABLE I
SYMBOLS USED IN THE PROTOCOL.

Symbol	Accuracy
VID	The unique symbol of vehicle
SID	The unique symbol of edge server
PK_V	The public key of vehicle
PK_S	The public key of edge server
Hash(PK_V)	The hash value of vehicle's public key
Hash(PK_S)	The hash value of edge server's public key
Discovery	Send discovery broadcast
Time	System Timestamp
SM4Key	A symmetric key
S	The result of vehicle's private key to signature Time and VID
S'	The result of edge server's private key to signature Time and VID
E_{PKv}	The result of encrypting PK_S and SM4Key with the public key of the vehicle
E_{SM4Key}	The result of encrypting Video Data with SM4Key
Video Data	Video captured by the driving recorder
Text Data	Text information collected by vehicle sensors
Token	A kind of certificate to find nearby vehicles

Step 1.2: The edge server uploads hash value of its public key and SID to blockchain.

2) Identity authentication phase: This phase is mainly designed to confirm mutual identity information. There are six steps in this phase.

Step 2.1: After a traffic accident occurs, the vehicle broadcasts a discovery message on the network. The message includes S and PK_V. S includes information about Time and VID signed by vehicle's private key. Multiple edge servers will receive this broadcast message.

Step 2.2: After receiving the message, the edge server calculates the hash value of PK_V according to VID and PK_V transmitted by the vehicle. Then the edge server go to blockchain to check whether the hash value PK_V corresponding to VID is consistent with the one on blockchain.

Step 2.3: If the hash value PK_V corresponding to VID and the one on blockchain are the same, blockchain replies Yes. Once the edge server determines that the PK_V is correct, the signature will be verified using PK_V. If the signature is also correct, the vehicle is considered as verified.

Step 2.4: After passing the verification, the edge server replies with encrypted PK_S and S' to the vehicle, S' includes information about Time and SID signed by server's private key.

Step 2.5: The vehicle selects the edge server with the shortest response time from **Step 2.1** to **Step 2.4**. After the vehicle is selected, it decrypts the PK_S and calculates the hash value. Then blockchain checks whether the hash value PK_S corresponding to the SID is consistent with the one on the blockchain.

Step 2.6: If the hash value PK_S corresponding to the SID and the one on the blockchain are the same, the blockchain responds Yes. Once the vehicle determines that the PK_S is correct, the signature will be verified using PK_S. If the signature is also correct, the edge server is considered as verified.

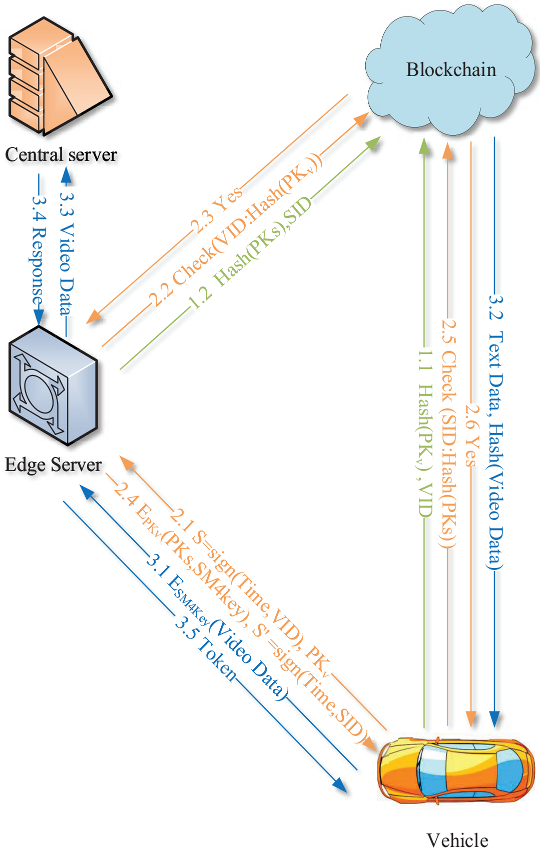
Central server
Blockchain
2.3 Yes
2.2 Check(VID:Hash(PK$_v$))
1.2 Hash(PKs),SID
3.3 Video Data
3.4 Response
Edge Server
1.1 Hash(PK$_v$) , VID
2.5 Check (SID:Hash(PKs))
2.6 Yes
3.2 Text Data, Hash(Video Data)
2.1 S=sign(Time, VID), PK$_v$
2.4 E$_{PKv}$(PKs,SM4key), S' =sign(Time,SID)
3.1 E$_{SM4Key}$(Video Data)
3.5 Token
Vehicle

Fig. 2. Protocol model of fast authentication and collaborative video data forwarding scheme.

3) Data forwarding phase: This phase describes the uploading processes of vehicle data, in which the data are uploaded to the blockchain and server respectively. There are five steps in this phase.

Step 3.1: After the verification is passed, the vehicle sends the encrypted video to the edge server.

Step 3.2: Text data and the hash value of video data are send to blockchain.

Step 3.3: The edge server decrypts and forwards video data to the central server.

Step 3.4: The central server replies with a response message to the edge server, indicating that it has been stored successfully.

Step 3.5: After the forwarding is completed, the edge server generates and returns the $Token$ to the vehicle. And then vehicle find nearby vehicles upload more videos to help determine liability.

C. Data Flow

Here, we use sequence diagrams to show the data flow in the protocol. The sequence diagram describes the

Authorized licensed use limited to: China University of Geosciences Wuhan Campus. Downloaded on September 08,2023 at 08:02:48 UTC from IEEE Xplore. Restrictions apply.

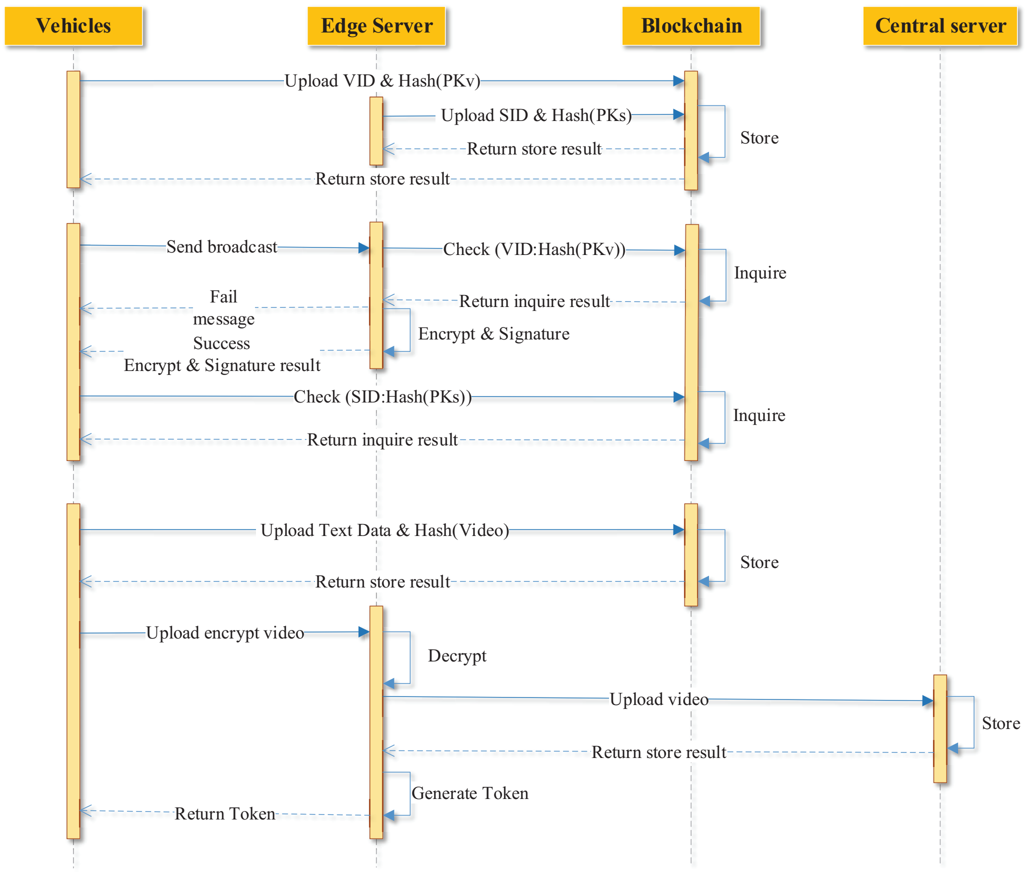

Fig. 3. Sequence diagram of fast authentication and collaborative video data forwarding scheme.

interaction between classes in the system, and these interactions are modeled as message exchanges. The sequence diagram describes the messages of the classes and the exchanges between classes to complete the desired behavior. Each message in the sequence diagram represents an operation of the class or a trigger event that causes the state machine to change. Through the sequence diagram, you can clearly understand the operating process and required conditions of the system. The sequence diagram is shown in Fig. 3.

The sequence diagram is also divided into three parts. In the first part, the vehicle and edge servers upload their respective identity information. Blockchain stores it and returns a message if the storage is successful. The identity information will be used in the subsequent authentication phase. The second part is to send a broadcast to find the edge server after a vehicle accident occurs. The broadcast contains the result of the signature and the vehicle public key. After the edge server receives the message, the blockchain verifies whether the vehicle is registered and sends inquire results to the edge server. If it is registered, the edge server will perform signature and encryption operations and reply the result to the vehicle, otherwise it will directly reject the vehicle's authentication. After receiving the returned information, the vehicle will also go to the blockchain to verify the identity of the edge server. The blockchain returns the inquire result. If the server's identity verification is passed, the next step of data forwarding will be performed, otherwise the verification will be ended. In the third part, the vehicle uploads the text information and the hash value of the video to the blockchain, and the large-scale video information will be encrypted and uploaded to the edge server, the edge server will decrypt and store it to the central server. After all the steps are completed, the central server returns to the stored results. The edge server generates and return $Token$ to vehicle, with this $Token$, the vehicle can look for nearby vehicles and upload more videos to help determine the liability. The whole process ends.

D. Use Case

In this subsection, we will further elaborate on the scheme in combination with actual application scenarios. Imagine a scenario where a vehicle is driving on a road and a traffic accident occurs for some reason. At this time, the smart driving recorder installed on the vehicle will discover that an accident has occurred based on the abnormal information of the sensor, and it will automat-

Authorized licensed use limited to: China University of Geosciences Wuhan Campus. Downloaded on September 08,2023 at 08:02:48 UTC from IEEE Xplore. Restrictions apply.

ically collect and store 30 seconds of sensor information and driving video contents before and after the vehicle. After that, the driving recorder will send a discovery broadcast to the edge server cluster to find the edge server with the fastest response. The edge server will go to the blockchain to confirm whether the vehicle is qualified and return with information. The driving recorder will select the edge server with the fastest response and verify the identity of the edge server. After re-verification, the text information and video hash value will be uploaded to the blockchain. The video will be encrypted and uploaded to the edge server, and then be uploaded to the central server after decrypte. Finally, the edge server returns a token to the vehicle, and the vehicle uses this token to find more nearby vehicle videos and upload these videos. After completing these series of automatic operations, the insurance company of the vehicle retrieves accident information for liability determination from the system and transfer funds.

In this use case, we can see that all these operations are done automatically by the system. Since the vehicle has been registered in the blockchain as early as when the smart driving recorder was installed, no additional steps are required, and the process of identity authentication and data forwarding can be completed within seconds with only simple information. The accident owner does not need to spend extra time to complete the accident liability delineation and insurance claims. It can not only reduce the accident processing time, but also put an end to improper transactions.

IV. Experiments and Analysis

In this section, we introduce the specific implementation method of the scheme, analyze the time delay of the experimental results, and make a supplementary explanation from the perspective of security analysis and advantages.

A. System Implementation

1) Blockchain: We choose Hyperledger Fabric as our blockchain platform. Hyperledger Fabric is one of the largest projects in the blockchain industry which consists of a set of open source tools and multiple subprojects. The project is global collaborative sponsored by the Linux Foundation, which includes leaders of different fields. Their goal is to build a strong, business-driven blockchain framework. Hyperledger Fabric is a blockchain framework designed to help companies build a private or consortium-permitted blockchain network in which multiple organizations can share authorities of controlling nodes in the network [17].

2) Smart driving recorder: There is no mature driving recorder development platform, so we choose the commonly used Raspberry Pi additional camera as the intelligent driving recorder development platform. It uses Android as the operating system and can greatly facilitate the development process.

3) Server: The edge servers and central server are developed in Java and PHP language. The mature Spring-Boot is used as the framework to quickly build a server platform. And the developed jar package is deployed on the linux server. By converting the ports on the server into URL addresses, they can be accessed and used by the smart driving recorders.

4) Others: The data transmits among the driving recorder, edge servers, the central server and the blockchain through the HTTP protocol. Therefore, it is very convenient to access the API interface through URL.

B. Experiment Results

Our scheme will be used in practical applications. Therefore, in the early stage, in order to verify the effectiveness and feasibility of the proposed system, we conducted a preliminary implementation and performance evaluation of the scheme.

In the data forwarding stage, we limit the size of the uploaded video to 60 MB. Limiting the size of the video can prevent malicious uploads and ensure the normal storage of the server. This value is based on time and clarity, and the actual test also meets this value. We divide the entire scheme into five stages to test the time delay. In the first stage, local keys are generated, including asymmetric keys and symmetric keys, denoted by T1. In the second stage, the vehicle sends a broadcast to find the edge server before it receives a reply message, which is represented by T2. In the third stage, the vehicle receives the message to the blockchain to verify the identity of the edge server, denoted by T3. In the fourth stage, the vehicle encrypts the video locally, denoted by T4. In the fifth stage, the encrypted video is uploaded until the reply message is received, which is indicated by T5. The entire process takes time T=T1+T2+T3+T4+T5. Since the size of the video in the entire process has a great impact on time, let's take 30 MB as an example. In order to eliminate the influence of accidental circumstances, we conduct 10 experiments on each stage and calculate the average time. The time sum of the identity authentication phase is 4.008 seconds while the time sum of the data forwarding phase is 25.650 seconds. The average time is 29.658 seconds. The detailed results are shown in Table II.

The content of the table shows that the biggest impact of the entire process is the process of uploading encrypted videos to the edge server in the last step, which accounts for up to 76.8%. Because large-scale of data needs to be sent in this part, the time depends on the network bandwidth and upload speed.

We also evaluated the time impact of the video size on the entire process, and selected five different video sizes of 5MB, 15MB, 30MB, 45MB, and 60MB for experiments. The experimental results are shown in Fig. 4 and Fig. 5.

It can be seen from Fig. 4 and Fig. 5 that:

Authorized licensed use limited to: China University of Geosciences Wuhan Campus. Downloaded on September 08,2023 at 08:02:48 UTC from IEEE Xplore. Restrictions apply.

TABLE II
EXPERIMENT RESULTS OF TIME DELAY

Stage	1	2	3	4	5	6	7	8	9	10	Avg
T1	1.52	1.58	1.51	1.53	1.55	1.55	1.53	1.48	1.58	1.59	1.54
T2	1.38	1.41	1.53	1.45	1.36	1.36	1.26	1.46	1.24	1.27	1.37
T3	1.20	1.11	1.08	1.03	1.04	1.09	1.14	1.06	1.09	1.10	1.09
T4	2.78	3.10	2.78	2.83	2.81	3.01	3.02	2.94	2.78	2.75	2.88
T5	23.06	22.92	22.57	23.02	22.82	22.71	22.57	22.67	22.65	22.73	22.77

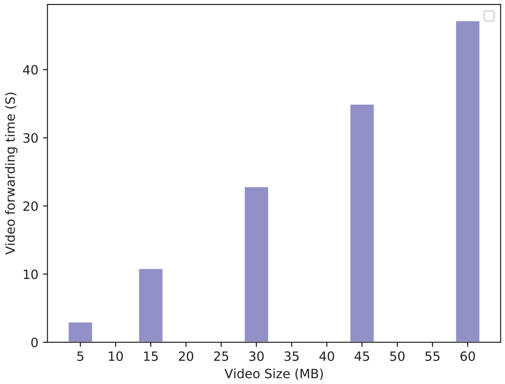

Fig. 4. The forwarding time of different size video

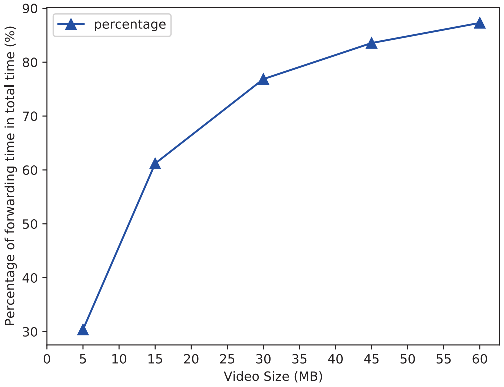

Fig. 5. The impact of video data size on scheme time

1) With the increase of the video size, the time consumption of the whole scheme gradually increases, while the time consumption of the certification stage does not change.
2) The size of videos has a great impact on the time of the whole scheme. Reducing the size of videos can greatly shorten the time consumption of the scheme. How to compress the size of the video without affecting the video quality will be an important research field in the future.

The data forwarding phase is originally proposed in our scheme. We formulated four indicators. Decentralization and anonymity ensure the security of user identity information. Cross-domain allows vehicles to authenticate identities out of geographical restrictions. Multi-level authentication improves the system performance. Table III shows the comparison of our proposed scheme with previous researches.

TABLE III
OUR PROPOSED SCHEME COMPARED WITH PREVIOUS RESEARCHES.

Research	Decentralization	Anonymity	Cross-domain	Multi-level
[6]	No	No	Yes	Yes
[11]	Yes	No	Yes	Yes
[13]	Yes	No	Yes	Yes
[14]	Yes	No	Yes	No
[15]	No	No	Yes	Yes
Ours	Yes	Yes	Yes	Yes

C. Security Analysis

We analyze the common attack methods that the scheme can withstand, The first is the replay attack, the intruder intercepts the message sent by A to B from the network, which makes host B mistakenly believe that the intruder is host A. Then host B sends a message which should be sent to A to the intruder who pretends to be A. This attack is usually solved by adding time stamps and random numbers. This scheme adds a time stamp mechanism, so it can be resisted. In addition, due to the one-way nature of the hash function, we upload the hash value of the key instead of the key, which further reduces the risk of key leakage. Followed by man-in-the-middle attack, common attack methods such as DNS spoofing and session hijacking. Check the hosts file of the machine to prevent attackers from joining malicious sites and switched network should be used instead of a shared network, which can reduce the probability of eavesdropping. The third is attack counterfeit attack, under the premise that the installed blockchain client is trusted, we believe that there will be no trusted server or client to fake the server or client, this is meaningless. The last one is tracking attack: Because the location of the car is constantly moving, and only after a traffic accident, the driving recorder will communicate with the edge server. As long as the false alarm rate of accidents is controllable, the driving recorder client will not frequently report falsely, resulting in frequent communication with edge servers. Therefore, tracking attacks can also be prevented. In other aspects, as the symmetric key for encrypting images is generated on the edge server, the security of the edge server must be ensured. Once the edge server is compromised, the entire session will be controlled.

Authorized licensed use limited to: China University of Geosciences Wuhan Campus. Downloaded on September 08,2023 at 08:02:48 UTC from IEEE Xplore. Restrictions apply.

D. Advantages of Two Layer Forwarding

A layer of edge server is added in our scheme, the edge server layer acts as a bridge between the blockchain and the vehicle. Which not only reduces the time of identity authentication, but also reduces the pressure on the central server by placing video decryption and forwarding on the edge server. We encrypt the video data before transmitting it, which ensures that the user data is not stolen. Although it increases the computational overhead, it is very worthwhile. Store big data such as videos on the central server instead of the blockchain, which can alleviate the pressure on the blockchain.Since blockchain is non-tamperable, we use it to store data, which ensures the authenticity of the data.

V. Conclusion

In this paper, we design a blockchain-based fast authentication video data forwarding scheme for IoV. Different from the traditional centralized authentication scheme, the edge servers in this scheme assist the mutual authentication between the blockchain and the IoV devices. In this way, it solves the problem of low authentication efficiency caused by the computing and communication bottleneck of the centralized server. In addition, blockchain network in the agreement solves the problem of cross-domain authentication of highly mobile IoV devices (such as vehicles and drones) and improves the efficiency of authentication. The analysis shows that our scheme is secure. The experiments results show that the time of authentication phase is only 4 seconds, and the time of video data forwarding phase is 25.65 seconds (taking a 30MB video as an example). The total time is less than 30 seconds which is tolerable in practical. The limitation of this research is that it is not well applied in actual scenarios. It uses network to transmit information instead of using near field communication and 5G technology. Besides, the deployment of edge servers on the roadside for experiments has not been carried out. In the future work, we will focus on the use of IoT devices in actual application scenarios, and improve the communication methods between IoT devices to make them better used in real life.

Acknowledgement

The research was financially supported by National Natural Science Foundation of China (No. 61972366), the Provincial Key Research and Development Program of Hubei (No. 2020BAB105), the Foundation of Key Laboratory of Network Assessment Technology, Chinese Academy of Sciences (No. KFKT2019-003), Major Scientific and Technological Special Project of Guizhou Province (No. 20183001), and the Foundation of Guizhou Provincial Key Laboratory of Public Big Data (No. 2018BDKFJJ009, No. 2019BDKFJJ003, No. 2019BDKFJJ011).

References

[1] Nord, Jeretta Horn, Alex Koohang, and Joanna Paliszkiewicz. ”The Internet of Things: Review and theoretical framework.” Expert Systems with Applications 133 (2019): 97-108.

[2] Raya, Maxim, and Jean-Pierre Hubaux. ”Securing vehicular ad hoc networks.” Journal of computer security 15.1 (2007): 39-68.

[3] S. Mallissery, M.M. Pai, A. Smitha, R.M. Pai, J. Mouzna, Improvizmg the public key infrastructure to build trust architecture for VANET by using short-time certificate management and Merkle signature scheme, in: 2014 Asia-Pacific Conference on Computer Aided System Engineering (APCASE),IEEE, 2014, pp. 146–151.

[4] Jiang, Wenbo, et al. ”PTAS: Privacy-preserving thin-client authentication scheme in blockchain-based PKI.” Future Generation Computer Systems 96 (2019): 185-195.

[5] B. Ying, A. Nayak, Anonymous and lightweight authentication for secure vehicular networks, IEEE Trans. Veh. Technol. 66 (12) (2017) 26–10636.

[6] Li, Kang, et al. ”Efficient message authentication with revocation transparency using blockchain for vehicular networks.” Computers & Electrical Engineering 86 (2020): 106721.

[7] Yang, Xiaohui, and Wenjie Li. ”A zero-knowledge-proof-based digital identity management scheme in blockchain.” Computers & Security 99 (2020): 102050.

[8] Prada-Delgado, Miguel Ángel, et al. ”PUF-derived IoT identities in a zero-knowledge protocol for blockchain.” Internet of Things 9 (2020): 100057.

[9] Esposito, Christian, Massimo Ficco, and Brij Bhooshan Gupta. ”Blockchain-based authentication and authorization for smart city applications.” Information Processing & Management 58.2 (2021): 102468.

[10] Hammi, Mohamed Tahar, et al. ”Bubbles of Trust: A decentralized blockchain-based authentication system for IoT.” Computers & Security 78 (2018): 126-142.

[11] Bagga, Palak, et al. ”Blockchain-based batch authentication protocol for Internet of Vehicles.” Journal of Systems Architecture (2020): 101877.

[12] Yang, Zhe, et al. ”Blockchain-based decentralized trust management in vehicular networks.” IEEE Internet of Things Journal 6.2 (2018): 1495-1505.

[13] Xu, Zisang, et al. ”A blockchain-based roadside unit-assisted authentication and key agreement protocol for internet of vehicles.” Journal of Parallel and Distributed Computing 149 (2021): 29-39.

[14] Chi, Jiancheng, et al. ”A secure and efficient data sharing scheme based on blockchain in industrial internet of things.” Journal of Network and Computer Applications 167 (2020): 102710.

[15] Tian, Zongqing, et al. ”Feasibility of Identity Authentication for IoT Based on Blockchain.” Procedia Computer Science 174 (2020): 328-332.

[16] Lin, Chao, et al. ”BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0.” Journal of Network and Computer Applications 116 (2018): 42-52.

[17] Androulaki, Elli, et al. ”Hyperledger fabric: a distributed operating system for permissioned blockchains.” Proceedings of the thirteenth EuroSys conference. 2018.

Authorized licensed use limited to: China University of Geosciences Wuhan Campus. Downloaded on September 08,2023 at 08:02:48 UTC from IEEE Xplore. Restrictions apply.