Journal of Computer Science and Electrical Engineering
Print ISSN: 2663-1938
Online ISSN: 2663-1946
DOI: https://doi.org/10.61784/jcsee3082

DESIGN AND IMPLEMENTATION OF BLOCKCHAIN BASED PRIVACY PROTECTION CERTIFICATION FOR INTERNET OF VEHICLES

YuChen Gu[1*], HaoRan Liu[1], ZhanYi Peng[1], ZhiLei Zhao[1], YiHan Yao[2]
[1]*School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 102206, China.*
[2]*School of Digital Media and Design Art, Beijing University of Posts and Telecommunications, Beijing 102206, China.*
Corresponding Author:YuChen Gu, Email: 2022211565@bupt.cn

Abstract: The Internet of Vehicles aims to achieve zero traffic casualties, zero congestion and extreme communication, focusing on reliable interconnection mechanisms. With the development of intelligent transportation, information exchanges on automobile networks are frequent, and security certification with limited resources and low latency needs to be implemented to ensure the functions of the Internet of Vehicles. Therefore, this paper proposes a blockchain-based conditional privacy protection authentication method for the Internet of Vehicles. First, the dynamic revocation of illegal vehicles is realized through smart contracts, which improves the security and efficiency of the Internet of Vehicles; secondly, the proposed method is proved through theoretical deduction and logical demonstration under adaptive selection information attacks in the random oracle model. security; Finally, simulation tests on key algorithms of vehicle registration, login and authentication, and smart contract demonstrate the good feasibility, stability and efficiency of the proposed method. Experimental results show that the proposed method has significant advantages in authentication efficiency, especially suitable for resource-limited IoT, provides new ideas for communication security of IoT and can be widely used in the field of smart transportation.
Keywords: Internet of Vehicles; Conditional privacy; Authentication; Blockchain; Smart contract

1 INTRODUCTION

With the enhancement of vehicle sensing, communication, storage and computing capabilities, Vehicle Ad-hoc Networks (VANETs)[1] have become the core technology for realizing the next generation of intelligent transportation systems and future smart cities [2]. The core advantage of the Internet of Vehicles is its ability to provide key information in real time, thereby enhancing the intelligence and adaptability of the entire transportation system. However, the large amount of data exchanged and stored in VANETs [3] poses a serious threat to user privacy. Traditional Internet of Vehicles security mechanisms mostly rely on one or more central authorities to conduct identity verification, authorization and other security-related operations, causing their limitations to begin to emerge [1].
In addition, in domestic and foreign research, they are generally divided into the following three categories: public Key infrastructure (PKI)-based authentication schemes [4], identity-based signature (IBS)-based authentication schemes [5], and certificateless signature (CLS)-based authentication schemes [6]. When dealing with vehicle networking communication security issues, traceability and anonymous communication efficiency still need to be further improved. Therefore, ensuring the security of data transmission and protecting user privacy have become two important and urgent needs in VANETs [7].
As a mobile ad-hoc network that does not rely on external infrastructure, the vehicle-mounted ad hoc network consists of vehicles equipped with vehicle-mounted units (OBUs). Communication between vehicles (V2V) and vehicles and infrastructure (V2I) is realized through wireless communication technology. The network uses the Dedicated Short-Range Communication (DSRC) protocol [8], which allows vehicles to broadcast information and adjust driving routes, while roadside units are responsible for providing information and feeding back data, thereby improving road safety and traffic efficiency. It is a cutting-edge technology in intelligent transportation systems. However, in the open environment of the Internet of Vehicles, attackers can easily intercept and tamper with messages, which leads to privacy leaks and security risks. Therefore, vehicles need to be verified when transmitting information and take measures to protect privacy. The academic community has proposed the concept of "conditional privacy protection", which protects user privacy under normal circumstances, while allowing de-anonymity to trace identity under certain circumstances. This has become an important research direction in the design of the Internet of Vehicles. Blockchain technology combines technologies such as distributed data storage to achieve decentralization and data tamper-proof characteristics of the network. Through hierarchical architecture and consistency algorithms, blockchain technology solves trust issues and uses smart contracts to realize automated contract execution, providing an effective solution for digital transactions. Asymmetric encryption technology ensures secure communication through a key pair mechanism and ensures the immutability of transaction data. Elliptic Curve Cryptography (ECC)[9], as an efficient asymmetric encryption algorithm, provides a powerful authentication mechanism with its small key size.
Based on the development background and related technologies of the Internet of Vehicles introduced above, there are the following challenges in the current research on privacy protection certification of the Internet of Vehicles. On the

one hand, malicious attackers may take advantage of the openness of the Internet of Vehicles to tamper with data, forge identities or launch denial-of-service attacks, threatening driving safety and personal privacy. On the other hand, most of the currently widely used IoT security mechanisms are based on centralized architecture. They have inherent limitations when dealing with dynamically changing and widely distributed IoT environments, which are often accompanied by increased communication delays and potential security loopholes. Once the centralized certification center is attacked or failed, it may cause the entire IoT security system to be paralyzed.

2 WORK DESIGN AND IMPLEMENTATION PLAN

This paper proposes a conditional privacy protection certification framework and protocol for the Internet of Vehicles based on blockchain technology. The plan abandons the reliance on centralized and trusted third parties, introduces a mechanism that allows conditional tracking of illegal vehicles, and realizes decentralized dynamic revocation of illegal vehicles through smart contracts. The implementation and evaluation of the Ethereum test network proves that the solution is effective in terms of safety and performance, providing new ideas for safe communication in intelligent transportation systems, and also providing valuable reference for future safety research and practice of the Internet of Vehicles.

2.1 Implementation Method

The system model of this scheme consists of three parts, namely the upper layer (trusted institution), the lower layer (vehicles and roadside units), and the auxiliary layer (smart contract and blockchain). This section will provide a detailed introduction to the blockchain-based Conditional Privacy-preserving Aggregate Signature Schema for Vehicle Ad Hoc Networks (BCPAS) proposed in this work. BCPAS consists of seven parts: system initialization, smart contract deployment, vehicle registration, login and authentication, pseudonym identity update, vehicle revocation, and password update.

2.1.1 System initialization

In the initialization phase, the Trusted Authority (TA) generates release system parameters and uses the elliptic curve encryption algorithm to initialize the alliance chain.

Blockchain initialization: TA launches an alliance chain between predetermined network nodes based on the PBFT consensus mechanism to maintain the stable operation of the blockchain. During this process, TA certified all blockchain managers (pre-selected trusted RSUs) and granted them the right to participate in the consensus process. In addition, the alliance chain will maintain a vehicle pseudonym key table, aggregate V2I and V2V communication messages, and ensure that all transaction information is securely stored on the blockchain.

2.1.2 Smart contract deployment

TA compiles and deploys the input of smart contracts onto the alliance chain, and blockchain managers will verify these contracts and assign them a unique address, allowing authorized transactions to make calls. In BCPAS, smart contracts provide a secure and reliable Application Programming Interface (API) for vehicle pseudonym key table management services in alliance blockchain.

In the BCPAS scheme, the query authority is predefined for the vehicle pseudonym key table within the alliance blockchain, where only alliance blockchain nodes (including TA and some trusted alliance blockchain RSU nodes) are authorized to conduct queries. This configuration aims to provide conditional privacy protection for vehicles while enhancing the traceability and non-relevance of the Internet of Vehicles.

2.1.3 Vehicle registration

In order to obtain the certification factors required for communication, all vehicles and their owners need to register with the TA during the vehicle registration phase. This stage serves as the basis for this agreement to achieve conditional privacy protection. The entire process is carried out within a secure channel, and TA is offline during the entire process.

2.1.4 Login and authentication

When a vehicle needs to send a communication message to other nearby vehicles or RSUs for information exchange, the following steps need to be performed: First, the identity authentication process of the vehicle user is performed. The authentication is successful. OBU further selects a random number and then sets the signature for the message., and broadcasts the information to surrounding vehicles and RSUs. When a message is received, the recipient (i.e., adjacent vehicles or RSU) first verifies the freshness of the timestamp. If it has not expired, the recipient will further query the record with PIDi in the vehicle pseudonym key table maintained by the alliance chain, thereby obtaining the public key vpki of the associated vehicle. The recipient then verifies the validity of the signature σi.

2.1.5 Pseudonym identity updates

In BCPAS, the validity of a vehicle pseudonym is set to a certain time period, ensuring privacy protection during the validity period of the pseudonym. In order to effectively prevent the disclosure of vehicle privacy, it is crucial to update the vehicle pseudonym in a timely manner before the vehicle pseudonym expires. In addition, this plan stipulates that the update operation of pseudonym identities must be performed in an offline environment. This measure aims to enhance pseudonym security and ensure that it will not be affected by online threats during the update process. Finally, RSU removes overdue information from the vehicle pseudonym key table of the alliance chain and updates VPKIT to enable future traceability of violating vehicles.

2.1.6 Vehicle cancellation

When building a security mechanism for the Internet of Vehicles based on blockchain technology, it is important to maintain accurate vehicle status information. When a vehicle leaves a specific area or waits to exit, the smart contract performs a revocation operation to update the vehicle status. In BCPAS, TA uses the blockchain consensus mechanism to call the vehicle revocation algorithm revokevPkID(PIDi) to perform the revocation operation. The revocation process includes deleting specific data from the vehicle pseudonym key table, broadcasting information on the revoked vehicle, adapting to the distributed characteristics of the Internet of Vehicles, and ensuring that other vehicles receive status updates in real time. In addition, in order to prevent attackers from maliciously modifying legal vehicle information, BCPAS adopts a mandatory access control mechanism to ensure that only TA has the authority to modify vehicle information in VPKIT.

2.1.7 Password updates

In the open network environment of the Internet of Vehicles, V2V and V2I communications need to protect user privacy and prevent the disclosure of user identity and location information. By updating the password, the correlation of each communication can be effectively isolated, making it difficult for an attacker to track the trajectory of a specific vehicle, thereby protecting user privacy. In addition, in case an attacker may try to obtain a password through various means (such as brute force cracking, social engineering, etc.), regular updates of the password can prevent unauthorized access and reduce the risk of being cracked. Even if the old password is cracked, the attacker cannot access the system, thus protecting the security of vehicle communications.

2.2 Technical Indicators

First, the performance of the smart contract implemented in this work is evaluated, and the three key functions of registration, public key query and vehicle cancellation are tested 200 times, and the average value is taken as the final test result.

Then analyze the performance overhead of key operations of non-smart contracts in BCPAS. This work analyzes the computing overhead of the vehicle in the scheme from three stages: pseudonym generation, message signature generation, and message signature verification. When the vehicle sends a single message for communication, the communication overhead of the vehicle-side broadcast message in the scheme is analyzed in detail.

3 SYSTEM TESTS AND RESULTS

This chapter introduces the construction and implementation of the Internet of Vehicles certification system based on alliance chain. The system consists of six core components: front-end interface, back-end services, Fabric SDK, smart contract, blockchain network and MySQL database. It aims to provide a safe and efficient identity authentication solution for the Internet of Vehicles. The front-end interface is built based on Vue3 and is responsible for visual display of system functions; the back-end service uses Go language gin+gorm framework to facilitate the implementation of vehicle and RSU authentication protocols, provides a data interface to the front-end and calls the Fabric SDK; the Fabric SDK is implemented in Go language and is responsible for calling the smart contract; the smart contract is deployed on the Alliance Chain Management Committee node, which carries contract execution and contains distributed ledger, which is used to store information required by TA in the authentication protocol; The MySQL database is used to store the information required by users and servers in the authentication protocol.

3.1 Test Protocol

In order to verify the feasibility and effectiveness of the proposed blockchain-based privacy protection certification scheme for the Internet of Vehicles, this chapter conducts a comprehensive test of the system. During the functional test, the established vehicle user information is input, the registration, login and certification stages of the Internet of Vehicles certification protocol are simulated, and the vehicle data is stored in the database. The test involves user interaction with the system to ensure that the system performs the registration and authentication processes as expected and verify its ability to store and manage user data. In terms of performance testing, traditional protocols lack comprehensive simulation analysis of the authentication process. This research builds a complete simulation environment to evaluate the performance of the solution. The work consists of a client (calling smart contracts), a backend service (implementing the authentication protocol between the vehicle and the RSU) and other parts (processing vehicle user registration), all implemented in GO language to ensure efficient and accurate simulation. The test results show that the proposed certification system meets expectations in terms of processing speed and response time, meets the real-time and efficiency requirements of the Internet of Vehicles, and its stability and reliability have been verified to ensure that actual deployment is feasible. Through testing, it has been proved that the program meets the requirements and has obvious performance advantages, providing an efficient and reliable solution for Internet of Vehicles security certification and privacy protection.

3.2 Performance Test

The performance testing part aims to evaluate the performance of the proposed blockchain-based IoT certification system in terms of processing power and response speed. This section details the performance testing of smart contracts and the performance overhead analysis of other key operations.

3.3.1 Smart contract performance testing

Performance testing of smart contracts focuses on the execution time of the contract algorithm, which is a key indicator to measure system efficiency. The experiment uses the open-source Fabric test-network scripts released by the Hyperledger community (https://github.com/hyperledger/fabric-samples) and the LevelDB block-storage configuration that ships with the default docker-compose template. A JavaScript client built with fabric-gateway v1.4.0 was run on an Ubuntu 22.04 LTS virtual machine (8 vCPU, 16 GB RAM) to repeatedly invoke the smart-contract APIs. All functions —including initialization, data insertion, update, query and deletion—were executed 100 times each, and the round-trip latency was measured at the client side via the built-in performance.timer() utility. The raw latency logs were then averaged to obtain the time-cost data presented in Table 1. The test results show that the execution time of the smart contract is within the acceptable range, which proves the efficiency of the system at the smart contract level..

Table 1 function Execution Time

Operation	Average execution time (μs)
vehicle registration	502
Public key query	445
Vehicle cancellation	587

Concretely speaking, this scheme tests registration, public key query and vehicle revocation 200 times respectively for a given data set, and takes the mean value as the final result. The results show that the time cost of vehicle registration, public key query and vehicle revocation are 502μs, 445μs and 587μs respectively. Therefore, even if these operations are frequently invoked, the time cost is still acceptable, which proves the reliability and efficiency of the smart contract in this scheme.

3.3.2 Calculation overhead analysis

Computing overhead analysis focuses on evaluating computing efficiency in the IoT certification solution. This paper analyzes the computational costs of key operations such as pseudonym generation, message signature generation, and message signature verification. By conducting simulation experiments on laptops with certain configurations, the execution times of different encryption operations were collected and multiple tests were conducted to ensure the accuracy of the results.

In this paper, a notebook computer configured as shown in Table 2 is used to simulate the execution time of different encryption operations, and tested 200 rounds through the MIRACLC/C++ encryption library, and the average value is used as the final simulation result. See Table 3 for details.

Table 2 Simulation Machine Configuration

configuration	specific parameters
memory	16GB
memory frequency	4800MHz
operating system	Windows 11
graphics card	NVIDIA GeForce RTX 3060
CPU	12th Gen Intel(R) Core(TM) i7-12700H

Table 3 Encryption Operation Execution Time

encryption operation	Average execution time (ms)
Tpa	0.0012
Tsm	0.1738
Tim	0.0245
Th	0.0003

Note:Tpa is the time taken to perform a point-add operation, Tsm is the time taken to perform a scalar multiplication operation, Tim is the time taken to perform a whole multiplication operation, Th is the time taken to perform a hash operation.

The total calculation overhead of the three stages of Scheme 1, Scheme 2, Scheme 3 and this scheme is 1.0467ms, 1.0458ms, 1.5669ms, and 0.8723ms respectively.

In order to intuitively compare the differences in computing costs between the proposed scheme in this work and the other three schemes in the certification process, Figure 1 and Figure 2 show the computing costs of the vehicle at different stages of the certification process and the entire stage respectively.

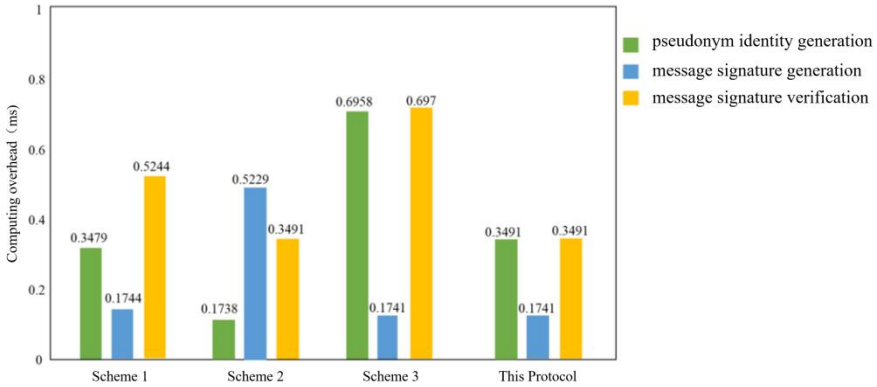

Figure 1 Computing Overhead at Different Stages of the Authentication Process

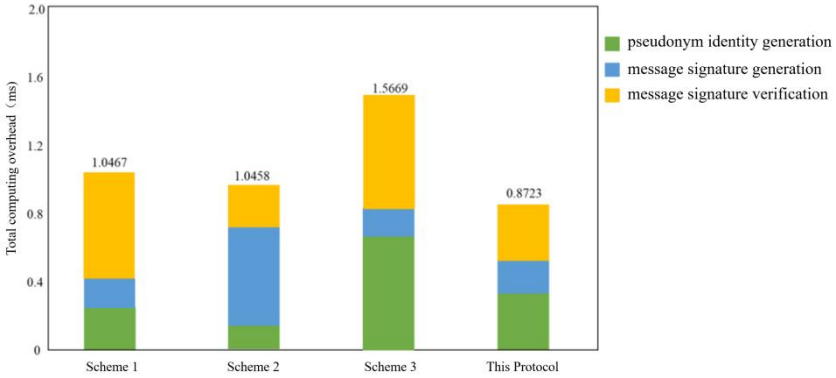

Figure 2 Total Computing Overhead of the Authentication Process

It can be seen from Figure 2 that this scheme is the lowest among all schemes for the total computing overhead in the authentication phase. Especially compared with previous works[10-12], this scheme reduces the total computing overhead by about 45%.

3.3.3 Communication overhead analysis

The communication overhead analysis takes into account the message size that the vehicle needs to send during the communication process. Parameters such as cyclic group size, infinite field size and timestamp size are defined, and the communication overhead of vehicle broadcast messages in each scheme is analyzed. The results show that the proposed scheme has advantages in terms of communication overhead, especially when sending vehicle messages in batches.

This scheme only considers the situation where the vehicle sends a single message for communication. The size of the parameters involved in the communication process is predefined as follows: the size of the cyclic group G is 40 bytes, the size of the infinite field z is 20 bytes, and the size of the timestamp is 4 bytes. The following is a detailed analysis of the communication overhead of vehicle-side broadcast messages in each scheme, as shown in Figure 3.

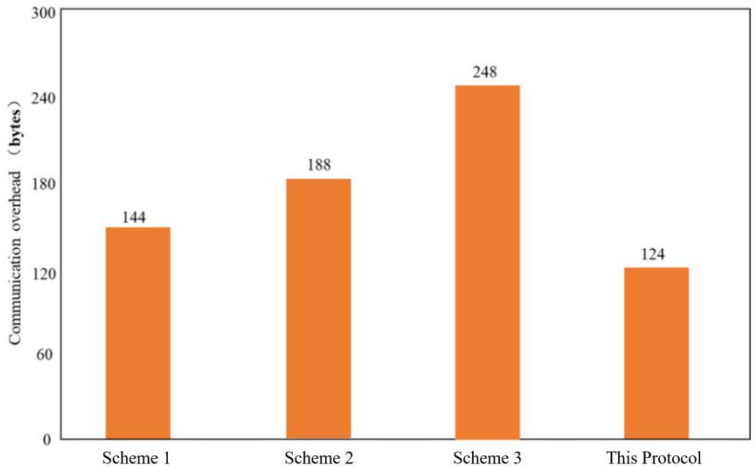

Figure 3 Comparison of Communication Overhead

It can be seen from Figure 3 that the communication overhead of this scheme is the lowest among all the comparison schemes. By well integrating the alliance chain with cryptographic primitives such as elliptic curves, even if there are security loopholes in the trusted party, BCPAS can still utilize acceptable communication overhead to achieve

conditional privacy protection. Compared with the schemes in documents that also adopt ECC technology and other documents, BCPAS reduces the communication overhead by 35% and 50% respectively. In particular, when the traditional authentication scheme requires the transmission of multiple messages and signatures to complete batch message broadcasting for vehicles, BCPAS only needs to transmit multiple messages and one signature at a time, thereby greatly reducing the occupation of channel resources and message transmission costs.

4 CONCLUSION

In view of the shortcomings of existing Internet of Vehicles authentication mechanisms in centralized dependence, key escrow, efficiency and privacy considerations, this paper proposes a conditional privacy protection authentication scheme with alliance chains and smart contracts as the core: lightweight signatures are implemented through elliptic curve cryptography, and distributed identity registration, dynamic revocation and pseudonym updates are completed with the help of the alliance chain's PBFT consensus and smart contracts, eliminating the single point of failure and key escrow risks in traditional PKI/IBS/CLS architecture. Experimental results show that the average time spent on vehicle registration, public key query and revocation operations of this scheme is less than 600 μs, and the overall computing and communication overhead are reduced by about 45% and 35%-50% respectively compared with similar studies, meeting the needs of low-latency and resource-limited scenarios for the network of vehicles. Therefore, this work provides a new decentralized certification paradigm for the Internet of Vehicles with efficient, scalable and traceable support conditions, which can directly serve the safe communication of smart transportation systems.

Faced with the development of the Internet of Vehicles and the enhanced capabilities of attackers, future research can focus on two aspects: First, develop practical Internet of Vehicles certification solutions to reduce implementation costs, enhance decentralized attributes, improve security and privacy protection, and use blockchain decentralization. Features ensure data security, transparent recording and automatic execution of smart contracts, improving efficiency and data protection; The second is to explore lightweight authentication solutions to reduce computing, communication and storage pressures and improve system performance and operability after application of quantum cryptographic algorithms.

COMPETING INTERESTS

The authors have no relevant financial or non-financial interests to disclose.

REFERENCES

[1] Jabbar R, Dhib E, Said A B, et al. Blockchain technology for intelligent transportation systems: A systematic literature review. IEEE Access, 2022, 10: 20995 -21031.

[2] He D, Zeadally S, Xu B, et al. An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks. IEEE Transactions on Information Forensics and Security, 2015, 10(12): 2681-2691.

[3] Azam F, Yadav S K, Priyadarshi N, et al. A comprehensive review of authentication schemes in vehicular ad-hoc network. IEEE access, 2021, 9: 31309-31321.

[4] Chen H, Zhang C, Chen H. DAG blockchain-based PKI authentication fast response scheme. Journal of Computer Engineering and Networks, 2025, 12(45): 134-141.

[5] Li C, Zhang X, Wang Y, et al. Identity-based chameleon hashes in the standard model for mobile devices. IEEE Transactions on Information Forensics and Security, 2025, 20(16): 145-153.

[6] Li C, Zhou H, Liu Q, et al. Efficient multi-KGC certificateless signature scheme for cross-device authentication in internet of medical things. Telecommunication Systems, 2025, 88(2): 201-212.

[7] Liu Xuejiao, Yin Yidan, Chen Wei, et al. A blockchain-based secure sharing solution for Internet of Vehicles . Zhejiang University Journal (Engineering Edition), 2021, 55(5): 957-965.

[8] Hu Lin. Performance analysis and resource allocation of vehicle active safety communication based on DSRC . University of Electronic Science and Technology, 2020.

[9] Dong Jiankuo, Liu Zhe, Lu Sheng, et al. Research progress on efficient software implementation technology for elliptic curve cryptography . Journal of Computer Science, 2023, 46(05):909-928.

[10] Chiang W K, Wang W Y. An efficient certificateless signcryption for mutual and batch authentication in vehicular ad-hoc networks. Peer-to-Peer Networking and Applications, 2025, 18(4): 321-330.

[11] Ali I, Chen Y, Ullah N, et al. An efficient and provably secure ECC-based conditional privacy-preserving authentication for vehicle-to-vehicle communication in VANETs. IEEE Transactions on Vehicular Technology, 2021, 70(2): 1278-1291.

[12] Sutrala A K, Bagga P, Das A K, et al. On the design of conditional privacy preserving batch verification-based authentication scheme for internet of vehicles deployment. IEEE Transactions on Vehicular Technology, 2020, 69(5): 5535-5548.