Hindawi
Security and Communication Networks
Volume 2022, Article ID 8689651, 14 pages
https://doi.org/10.1155/2022/8689651

Review Article

A Summary of Security Techniques-Based Blockchain in IoV

Chen Chen[1] **and Shi Quan**[2]

[1]*School of Information Science and Technology, Nantong University, Nantong, China*
[2]*School of Transportation and Civil Engineering, Nantong University, Nantong, China*

Correspondence should be addressed to Shi Quan; sq@ntu.edu.cn

Received 28 October 2021; Revised 16 January 2022; Accepted 9 February 2022; Published 8 March 2022

Academic Editor: Haowen Tan

With the rapid development of the informatization and industrialization of the Internet of Vehicles (IoV), the number and application of connected vehicles are growing rapidly. The safety problem is related to the property and life of human beings, which has attracted extensive attention from academic and industrial circles. Based on the study of high-quality literature published in the past decade and other high-level research works, this paper first analyzes the forms of attack against the Internet of Vehicles from the two aspects of attack mode and target. Then, it summarizes the existing blockchain-based system framework of the Internet of Vehicles (BIoV) and then discusses the security solutions of blockchain-based vehicles from the aspects of authentication, privacy, trust management, access control, and so on, to support the distributed system architecture and solve the security challenges of the Internet of Vehicles. Finally, the technical difficulties and the direction of further research of BIoV are summarized.

1. Introduction

IoV has become the most promising and fastest-growing new network paradigm and has also brought many applications, such as emergency communication of traffic incidents, traffic congestion prediction, and new traffic service modes. So in IoV, the secure transmission of V2X [1] is crucial. Suppose a hacker invades a regular vehicle or interferes with vehicle communications through eavesdropping, jamming, or spoofing attacks. In that case, there is a potential for serious accidents that can damage the vehicle or endanger the lives of passengers. Therefore, the primary safety goal of the Internet of Vehicles is to disseminate critical event information (such as accident reports) in a timely, safe, and accurate manner to ensure safe driving [2]. Most models of IoV are on centralized patterns. But the main problem with centralized mechanisms is the single point of failure problem. Many researchers have proposed distributed model schemes, but due to the dynamic nature of IoV, it has other issues, such as distributed vital management, content distribution, message trust, and data privacy. We should need a security mechanism to ensure that entities in IoV cannot manipulate, alter, or delete critical event messages in VANET. If critical event messages generated by vehicle entities are in a distributed database, all information will be transparent and shared. The security technology-based blockchain can achieve this. Blockchain is a decentralized peer-to-peer network, and nodes do not need to trust each other. It includes data encryption, timestamps, distributed consensus, smart contracts, and other technologies. With the maturity of blockchain technology, it has been deeply integrated with various industries [3, 4], solving the technical bottlenecks unique to multiple industries. The integration of blockchain technology and IoV is also one of the current research hotspots.

Why can blockchain integrate with IoV? First, one of the main characteristics of blockchain is decentralization. We can use this feature to realize the rapid authentication of safety information on the Internet of Vehicles and achieve the purpose of traceability management of traffic accidents. By improving the traceability and transparency of related vehicle information, we provide the event-specific basis for decision-making. Second, because the blockchain is a decentralized, peer-to-peer trust-based network, the data in

the blockchain is reliable, accurate, consistent, timely, and widely accessible. It is resistant to malicious attacks and has no single point of failure [5]. In addition, blockchain can protect the security and privacy of vehicle nodes by using a hash function and encryption technology. All transactions and transactions in the blockchain are timestamped and authenticated using private keys, which can prevent malicious or forged messages; anonymized vehicle identities or data can protect user privacy. Therefore, blockchain has been applied to the Internet of Vehicles as a security mechanism, and related research has attracted increasing attention. For example, 30 companies, including BMW, Ford, Renault, General Motors and IBM, Bosch, and Blockchain, have joined MOBI's Mobility Open Blockchain initiative [6]. The mission of MOBI is to accelerate the application of blockchain. Ali et al. [7] are working on a project blockchain-based system, including designing and implementing a complete vehicle tracking lifecycle, from manufacturing, customs, registration, on the road, and violations to buying and selling.

This paper classifies attacks of IoV in terms of attack targets and methods. It then investigates security technology that combines IoV and blockchain, which are also the focus of this paper. Firstly, the network model system to BIoV is studied. Then, it discusses the security technology of BIoV, proposes the security analysis methods and evaluation parameters, and compares the currently popular methods. Finally, the future challenges and research directions of security technology are summarized.

2. Attack Categories

As early as 2005, Chavez et al. [8] suggested that hackers may attack cars, and identity authentication and encryption should keep cars safe. This section focuses on attack categories and security requirements of the IoV. Firstly, attacks of IoV can be classified into traditional security attacks and exclusive attacks, according to the target and mode. Conventional security attacks include physical control attacks, network layer attacks, identity attacks, forged information attacks, and application attacks. Exclusive attacks are common and seriously impact the IoV but do not exist or be uncommon and have little impact on the traditional network. The VeReMi [9] (an attack data set with tagged attributes), for example, launches five types of positional attacks by forging GPS positions.

2.1. Physical Control Attacks. IVI (In-Vehicle Infotainment) is an intelligent multimedia device integrated with the car center console, with radio, GPS navigation, entertainment, voice assistant, Bluetooth, WiFi, and other functions. Because of its ancillary functions and high integration, it has become an essential target for attackers. Through IVI, the attacker tries to open the system engineering mode and use ADB (Android Debug Bridge) or USB to connect. After the connection is successful, obtain the system login name and password by brute force. After the login succeeds, they try to raise the rights. If the operation succeeds, an attacker can access any file in the IVI system to steal private data or critical information. They start or stop the vehicle's regular service [10] by tampering with the system configuration to bypass vehicle safety restrictions. It is a severe threat to the safety of vehicle function and information.

2.2. Network Attacks. The IoV is built on top of the traditional network. For example, the network of IoV also has the functions of routing and forwarding, logical addressing, and congestion control. Therefore, IoV faces the same security problems as traditional networks, such as DOS (Denial of Service)/DDOS (Distributed Denial of Service) [11], Black-Hole Attacks, Replay Attacks, and Grey Hole Attacks. In addition, automobiles are also under wireless threats [12] by using cellular networks (4 G/5 G), WiFi, Bluetooth, and LTE-V2X.

In a cellular network, an attacker establishes a pseudobase station, hijacks and monitors t-box session and communication data through conventional methods such as DNS hijacking, and obtains sensitive data (such as user sensitive information and vehicle status information).

2.2.1. WiFi Communication. By cracking the WiFi authentication password, the attacker can connect to the In-Vehicle Networking and obtain the sensitive and private data of the vehicle without authorization. Hackers can also exploit known vulnerabilities in operating systems to launch infiltration attacks.

2.2.2. Bluetooth Communication. Attackers can hijack traffic between Bluetooth keys and vehicles and tamper with and replay malicious traffic. Not only does it result in vehicle theft, but also it threatens the functional safety of the vehicle. In general, cellular networks are the more secure of the three wireless technologies.

2.3. Identity Attacks. There are two main attack entities for identity attacks: vehicles and roadside unit (RSU). In IoV, malicious nodes are often disguised as RSU and attempt to trick users into obtaining their authentication information. The attackers then use their identity to access confidential information, even as an authentication against others. In addition, they can also impersonate the identity of other vehicles. For example, an attacker might mimic an emergency vehicle, which would give them a higher priority in the network and thus reduce congestion.

2.4. Fake Information Attacks. The spread of false information [13] also exists in IoV, and it will cause more severe harm. Like Sybil Attacks by Douceur [14], attackers can spread incorrect information about road congestion, effectively forcing other vehicles to divert. They can also lead to traffic jams or sending accident alerts. Because of its low computing cost, falsifying information becomes one of the common attacks. And the distributed feature of IoV will lead to more severe harm.

2.5. Application Attacks. Applications related to IoV can be classified by function into vehicle control, query, and services (which provide the procedures required by safe and unsafe applications). The most common examples are malware and spyware. A malicious node inserts malware into a legitimate, intelligent connected vehicle application. Users are installing malware at the same time they download and install the software. The purpose of malware is to collect vehicle terminal location information, authentication information, personal privacy [15] information, and other pieces of information. Due to the highly dynamic nature of the IoV, the onboard software system changes and updates frequently, so the vehicle must ensure the reliability of the source of the updates and information it receives. Otherwise, severe failure can occur in some cases.

2.6. Exclusive Attack. Most applications in IoV, such as traffic information, weather conditions, and navigation, rely on location information. Incorrect or misleading location information can lead to accidents, financial losses, and even life-threatening situations. The identity of a competent, connected vehicle is legal, but an attacker can launch an attack by forging the location, which is rare in a traditional network. Literature [16] describes detailed types of VeReMi: constant attacker, constant offset, random attack, random offset, and eventual stop.

Of course, the blockchain also has many security problems, such as a 51% attack. In [2], the paper proposes a regional blockchain. On the premise of ensuring the stability of the blockchain, by controlling the number of vehicles, malicious vehicles, and message transmission, several control parameters such as time and puzzle calculation time make the attack success rate reach 51%.

Unlike the traditional network's deep and hierarchical defense system, it urgently needs us to introduce new technologies and models to build a security system due to the particular requirements of decentralized and high mobility of computing, storage, and other resources.

3. The System Model of Blockchain-Based IoV (BIoV)

Most scenarios in IoV are real-time and mobile, generating and exchanging large amounts of data [17]. In particular, many of the classic technology centralized security technologies are unlikely to be suitable for scenarios. Therefore, blockchain can provide a large number of innovative solutions for most application scenarios. So, on the other hand, integrating blockchain into the Internet of Vehicles not only improves the security, privacy, and trust of the Internet of Vehicles but also enhances the performance and automation of the system. To sum up, to accommodate flexibility and handle large amounts of data, we should combine blockchain technology with the Internet of Vehicles. This section will focus on the system model of BIoV.

According to the communication entities in the IoV system, Hu et al. [18] divided IoV into three levels: vehicle-mounted communication nodes (VCNs), roadside communication nodes (RCNs), and blockchain cloud platform. VCNs are mobile nodes installed on the vehicle, responsible for communication with other vehicles. However, the calculation and storage capabilities of VCNs are relatively weak. RCNs are fixed nodes installed on a roadside base station, responsible for promptly sharing information with other nodes in the network, but have strong computing and storage capabilities. Therefore, RCNs are the consensus formation nodes of the Internet of Vehicles. The blockchain cloud platform will store all data on the Internet of Vehicles. Ma et al. introduced cloud computing in [19] and proposed security, privacy protection, and decentralized car networking architecture. The architecture uses blockchain and delegated PoS and consists of vehicles, sensors, actuators, RSU, and cloud computing nodes. RSU is the central blockchain storage node in this architecture. The cloud computing node is responsible for backing up and storing data such as the blockchain. The architecture contains two different subchains, namely, InterChain and IntraChain, which provide users with flexibility in access control. InterChain is responsible for sharing information between vehicles, roadside equipment, and other infrastructures. IntraChain maintains the communication between sensors, drivers, and personnel in the vehicle.

In [18, 19], roadside units (RSU/RCN) serve as nodes of the blockchain, but there is no mention of how to plan the deployment of roadside units. Therefore, such solutions require mathematical modeling of roadside units and the scale of roads and blockchains in natural environments. Therefore, Gao et al. [20]combined fog computing and SDN and proposed new system architecture. The fog computing platform comprises roadside units, vehicles, base stations, and other infrastructures. The SDN controller implements resource allocation, mobility management, and rule generation. SDN plane data consists of the vehicle, BS, and RSU, whose primary duty is to collect and forward the data to the quantization control plane. The control plane is composed of an SDN controller, RSU, and blockchain and determines the flow rules of the network. The nodes in the blockchain are composed of an authentication server, an access controller, a data management server, and a policy management server. Their functions are registration authentication, access control, data, and security policy management. This model gives a new solution. RSU no longer holds the nodes of the blockchain. However, the coordination and management between node servers is still a problem to be solved.

Lin et al. [21]combined blockchain, DRL (deep reinforcement learning), and spatial crowdsourcing technology and proposed a spatial crowdsourcing system (DB-SCS) based on deep reinforcement learning and blockchain. The DB-SCS system consists of three layers: the spatial crowdsourcing layer, the blockchain layer, and the DRL layer. In the spatial crowdsourcing layer, hierarchical task management and people management modules divide tasks and people into different security levels and manage them differently in task release and assignment. The blockchain layer uses the blockchain as a distributed server. Building a private blockchain based on Hyperledger Fabric [22, 23] by storing crowdsourcing tasks in the form of transactions on the

blockchain overcomes the single point of failure problem of traditional crowdsourcing. Using the subchain mechanism and decentralized server module, it is responsible for constructing different subblockchains for tasks of varying security levels, as a decentralized server to manage the functions and staff on the subblockchain. The fusion of DRL, deep learning and reinforcement learning, and the consensus algorithm of dynamic selection of blockchain realize spatial task allocation and blockchain performance improvement.

While the researchers are researching the BIoV model with the entity as the center, some researchers are also studying with the data. Gao et al. [20] and others divided BIoV from bottom to top: perception layer, communication layer, blockchain middle layer, computing layer, and application service layer. The framework integrates blockchain technology from the third layer. The communication layer realizes information interaction between vehicles through Bluetooth, VANET, and so on and uploads data to the blockchain middle layer through cellular networks, wide area networks, and other network services [24]. In the communication layer, authentication services based on blockchain ensure the reliability of communication objects. At the same time, hashing and other digital signature verification technologies safeguard the integrity of information. The middle layer of the blockchain provides essential blockchain application services. They deploy in the computing layer of the blockchain's all-node mining machine. It uses the public key address as a credential to encrypt and store information to ensure the confidentiality of data. The application layer uses smart contracts to force applications and underlying drivers to upgrade, avoiding intrusion caused by software and hardware vulnerabilities and ensuring that hackers cannot embed malicious code during updates. The network model proposed by Liu et al. [25] integrates blockchain technology into each layer, namely, data, network, artificial intelligence, application, and business. The network layer consists of the network coordination module and the P2P network sublayer of the blockchain. The AI layer, composed of the blockchain consensus sublayer and vehicle-oriented computational analysis services, includes the blockchain consensus protocol that runs on this layer. The smart contract sublayer of the blockchain runs in the application layer; the blockchain-dense sublayer rewards the first miner who provides a valid PoW using a digital token. Smart contracts are a set of predefined protocols that all peers operate in a blockchain-based system to meet specific service requirements. The business model of the Internet of Vehicles, data transaction business, and debt business constitute the business layer.

Jiang et al. [26] divided the blockchain data on the Internet of Vehicles into five categories: vehicle management blockchain data, automobile factory blockchain data, user privacy (audio and video) blockchain data, vehicle-insurance-purchase-blockchain data, and common things blockchain data. The blockchain nodes on the Internet of Vehicles are divided into five types of nodes: senior management nodes, vehicle monitoring nodes, privacy (audio and video) monitoring nodes, insurance nodes, and general transaction nodes.

We can compare the architectures studied in the above literature as shown in Table 1. With the further integration of blockchain and IoV, the performance requirements of blockchain will become higher and higher. A single chain may not meet the needs of multiservice scenarios in IoV, and a single chain will increase system load, resulting in more significant latency and computing costs.

To sum up, the architecture design of the BIoV system should follow the following principles:

(i) Availability and fault tolerance principle: when some nodes are offline, vehicles on the road communicate continuously

(ii) Easy deployment: using existing infrastructure saves money and time; communication with existing infrastructure achieves availability goals

(iii) Adaptability: the network framework can be applied to various scenarios of vehicle driving environment and can meet the growing requirements of vehicles, data, and safety

(iv) Security: it can guarantee the communication and data security of the Internet of Vehicles

4. Security Technology of BIoV

This section will focus on blockchain-based security technologies for the Internet of Vehicles. By keyword retrieval of Internet of Vehicles, blockchain, security technology, and so on, we searched relevant literature since 2010, manually screened the title and abstract of the paper, conducted corresponding screening according to the quality of the article, and sorted out and analyzed as many high-quality papers as possible. In Figure 1, the security technologies are classified based on the research of the papers we reviewed and concerning the existing Internet of Vehicles defense technologies.

4.1. Identity Authentication. Anonymous authentication is a commonly used technology to protect vehicle identity and privacy in IoV [27]. Vijayakumar et al. [28] proposed a two-factor authentication and key management mechanism for secure data transmission in virtual networks, which provided a high level of security for the vehicle side of virtual networks. Azeez et al. [29] designed an efficient anonymous authentication mechanism with conditional privacy protection for virtual networks to reduce the storage overhead of vehicles and anonymous roadside certificates. Karati et al. [30] introduced a new identity-based signature encryption mechanism suitable for low-bandwidth communication. In [31], Zhang et al. proposed an effectively distributed aggregation-privacy-protection-authentication protocol. Islam et al. [32] proposed an effective password-based conditional privacy protection authentication and group key generation protocol. The above literature relies on a management center with a preestablished trust relationship with the vehicle.

Fromknecht and Velicanu [33] presented a decentralized PKI (Public Key Infrastructure) authentication system based on blockchain and Bitcoin. This paper builds CertCoin on

Table 1: Comparison of architecture of BIoV.

Classification of models	Literature	Key technologies used in the model	Strengths/weaknesses
Entity-centric model	[10]	Blockchain	RSU acts as a blockchain node, but the scale and deployment issues of nodes are not resolved
	[11]	Cloud computing and double-chain structure	
	[12]	SDN, fog computing, and blockchain	The problem of coordination between nodes has not been solved
	[13]	Blockchain, deep learning, and spatial crowdsourcing	The performance of the blockchain is improved, but the computing power and throughput performance requirements are increased
A model centered on the data life cycle	[2, 16]	The communication layer, the computing layer, and the application layer are integrated with the blockchain technology	Integrate data and blockchain to varying degrees, but the management and performance of the system bring great challenges
	[17]	Blockchain is incorporated into every layer of the model	
	[18]	Five types of data correspond to five subchains	

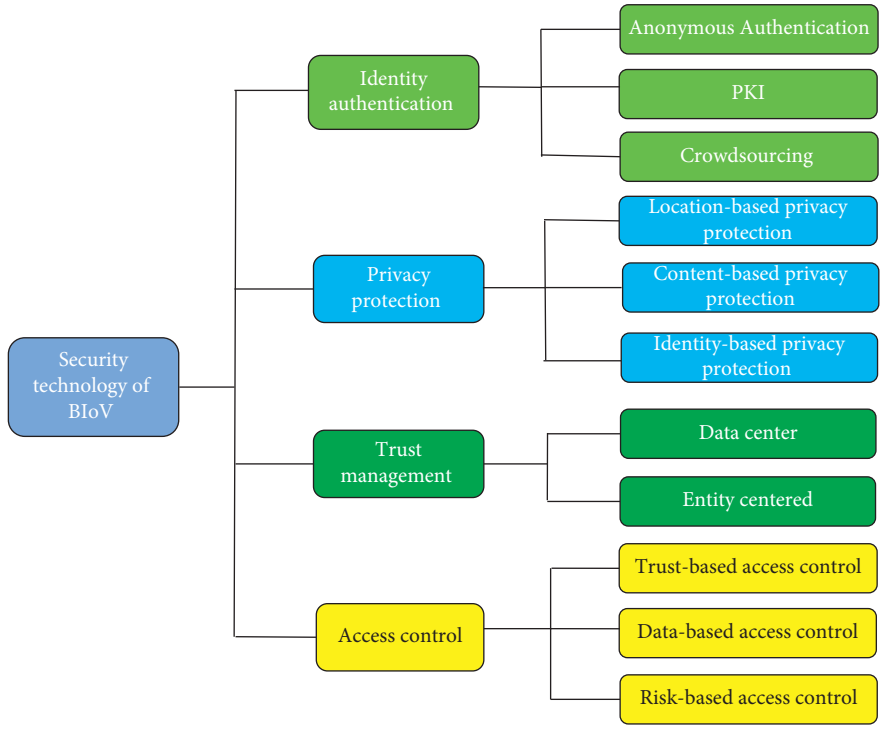

Figure 1: Security technology categories of BIoV.

top of Namecoin, whose core idea is to maintain a public ledger of a domain and its related public keys. It also supports domain name registration, domain name public key update, and authentication and provides revocation and restoration of the secret key. In addition, an accumulator is also used to reduce the storage of CertCoin.

Maria et al. [34] designed an anonymous authentication and switching authentication scheme. First, trusted authority (TA), RSU, vehicle, and blockchain network constitute the system. Then, system initialization, TA registration, anonymous authentication, and switching anonymous authentication comprise blockchain-based authentication. The Merkle Hash Tree (MHT) is the real-time authentication record. The blockchain server serves as an auxiliary for anonymous switching authentication. This scheme also can be used as vehicle illegal information tracking and traceability.

Yao et al. [35] firstly proposed a noninteractive anonymous cross-data center authentication mechanism. The instrument's flexibility is that the vehicle can decide when to revalidate and change the pseudonym and how often to verify and change. Blockchain-assisted Lightweight Anonymous Authentication (BLA) begins by registering the vehicle's OBU and service manager (SM). Then, SM can cooperate with RSU to complete the identity authentication. SM broadcasts the authentication results and writes the authentication results into the blockchain through the PBFT (Practical Byzantine Fault Tolerance) consensus algorithm. When the vehicle moves to the next RSU or new SM area, it does not need to authenticate again. This solution eliminates

the interaction between the vehicle and SM and reduces the communication overhead.

Noh et al. [36] discussed a distributed message authentication scheme based on blockchain. First, the RTA (root trusted authority) acts as the management system to issue the certificates of the vehicles entering the network. Vehicles need to verify the driver's biometric information before broadcasting messages. Other vehicles receive the broadcast message for authentication. After receiving the message within a certain period, the local TA generates a block according to the PoW consensus and verifies the block through the PBFT consensus. It guarantees anonymity and dispersion of broadcasting information. In particular, it enables vehicles to authenticate messages efficiently and distribute them.

Zheng et al. [37] proposed an access authentication system based on blockchain in a VANET environment. The system provides a trusted communication environment for intelligent vehicles and maintains anonymity without revealing the user's true identity. Secure access between vehicles and roadside units reduces reliance on authority centers and reduces the burden of vehicle identification. To prevent the spread of internal vehicle forged messages, this paper also designs a secure distributed transaction storage scheme based on blockchain, which can effectively protect the transaction information from attacks while tracking malicious vehicles.

To sum up, identity authentication is an essential part of the IoV. Vehicles should be registered and assigned keys by a unified authority before joining the network. To avoid a single point of failure, we need to implement blockchain through consensus or smart contracts, credit mechanisms between vehicles, or RSU. The role of blockchain is to store, update, and manage secret keys or certificates. In Table 2, we can compare the application of blockchain in the identity authentication scheme of the Internet of Vehicles mentioned above.

4.2. Privacy Protection. IoV uses V2X interconnectivity such as V2V (Vehicle-to-Vehicle), V2R (Vehicle-to-Road), V2I (Vehicle-to-Infrastructure), and V2P (Vehicle-to-Person) to create a social network with intelligent objects as participants. V2X has led to the existence of vehicle social networks (VSNs). According to literature [39], VSN is divided into three layers: social network, vehicular social networks, and vehicular networks. The data sharing message of the social network includes the personal information of the car owner and the motion status of the vehicle. For example, the leakage of location privacy will seriously affect the user's identity privacy. It is precise because vehicle safety is closely related to the owner's daily life and work; privacy leakage will affect his everyday life and even affect his life and property safety. Therefore, privacy protection on the Internet of Vehicles environment is urgently needed. Butt et al. [40] pointed out that the role of privacy management becomes crucial in SIoV as data is collected and stored at different layers of its architecture. The author analyzes the privacy issues and factors that need to be considered in privacy protection in the SIoV environment from different perspectives, such as personal privacy, behavior and action, communication, data, image, thought and feeling, location, and space association. In addition, the literature analyzes existing blockchain-based privacy protection methods. The difference is that we divide them into three types according to the objects of privacy protection: privacy protection technology based on location, content, and identity.

Qian et al. [41] proposed a privacy-aware content caching architecture based on blockchain. In this architecture, blockchain technology completes and records transactions. After a consensus mechanism finishes, transactions are written into blocks, thus solving the problem of privacy data disclosure in content caching.

Lin et al. [21] proposed a spatial crowdsourcing system (DB-SCS) based on deep reinforcement learning (DRL) and blockchain. The authors integrate deep reinforcement learning (DRL) and blockchain into the spatial crowdsourcing process of SDN-IOV applications. In DB-SCS, to protect the privacy of tasks in task assignment and publishing, two methods are proposed: hierarchical task classification and management strategy based on multiblockchain and task assignment scheme based on DRL.

Xu et al. [42] proposed a remote authentication model based on a privacy protection blockchain called RASM (remote authentication security model) for intelligent vehicles in the V2X network. This security model aims to enhance privacy security while ensuring decentralization, traceability, and nonrepudiation. RASM consists of two main steps. The first step is identity authentication; vehicles share their trusted identity to the blockchain network as evidence. In the second step, the vehicle will calculate and estimate the criteria used to decide. Finally, the authors tested the scheme in a real network environment, and the success rate of 97.09% proved that the system could effectively improve the privacy security of V2X vehicles.

A conditional Privacy Protection Statement Protocol (BTCPS), which contains three entities, vehicle, trusted institution, and RSU, was proposed by Liu et al. [43]. The protocol has two parts: the anonymous aggregation vehicle announcement protocol and privacy protection. The second step is the TM model based on blockchain. The trust value mechanism of direct and indirect trust realizes message synchronization and prevents abnormal vehicles from spreading false messages.

Luo et al. [44] introduced blockchain to realize location privacy protection of vehicles based on location services in IoV. This solution solves the distributed K-anonymous privacy protection technology that cannot detect malicious vehicles and sensitive location privacy leakage. In addition, the scheme considers the reliability of the vehicles and realizes the coordination between the vehicles. The scheme also includes a data structure to make trusted records of vehicles publicly available, which can detect malicious vehicles.

Different from K-anonymous privacy protection technology, Feng et al. [45] proposed a trusted stealth area construction scheme based on trust, called TACA, to protect vehicle location privacy, which is similar to the idea of stealth

Table 2: Comparison of identity authentication.

Literature	Registration authority	Functions of RA	Functions of blockchain	Method
[30]	Namecoin	Public key signature information	Publish, update, and validate	Merkle tree
[34]	The offline registration	Random number and public key	Validate	RSU collaboration
[35]	AD	SM area management	Alliance chain validation	Consensus algorithm
[36]	RTA	Public-private key for the vehicle and system key K	Validate	PoW and PBFT
[38]	CA	A certificate and two special hash functions	RSU	Pseudonyms and hashes

area [44]. In addition, with the assistance of edge computing and blockchain, the RSU can quickly evaluate the trust value by using the trust data gathered from the blockchain. The scheme proposes that multiple anonymous persons in the adjacent vehicle area are selected to construct the stealthy region in a cross-region manner. This scheme can effectively protect the location privacy of the vehicle and avoid the leakage of RV's (request vehicle) request content and LSP's (Location-Based Service Provider) service results during transmission.

Akhter et al. [46] proposed a multilevel privacy protection authentication protocol based on blockchain, which includes two certification centers. The Global Certification Center (GAC) is responsible for storing all vehicle information. The Local Certification Center (LAC) maintains a block to realize fast switching between clusters within the vehicle. In addition, the paper also puts forward that a tree can represent the blockchain-based authentication system. At the top level, the GAC stores all vehicle information (public and private keys, etc.). All vehicles must be registered with the LAC before a road permit. The LAC is responsible for physically verifying each vehicle and generating a public-private key pair. All LACs maintain a blockchain called an LABC by storing only information about locally registered vehicles, storing only public keys and vehicle types in the second layer of the tree structure. All CHs in the same state are members of LABC (as the third level of the tree), thus obtaining a list of all locally registered vehicles. Whenever a new vehicle approaches and requests to join the cluster, the CH can verify the vehicle's authenticity. Communication between the blockchain and its members is encrypted using the RSA-1024 digital signature algorithm. The author implements the authentication protocol in virtual machines and tests the computer, storage, and propagation costs in the authentication process.

To sum up, we compare the above literature on privacy protection, as shown in Table 3. Privacy protection mainly focuses on two aspects: privacy protection of the Internet of Vehicles social network and privacy protection of vehicle location. Privacy protection focuses on two parts: the privacy protection of a social network of Internet of Vehicles and the privacy protection of the vehicle location. The privacy protection of social networks mainly focuses on protecting vehicle identity information, transaction content, and so on. Location privacy protection especially involves vehicle tracking and location and service provision. However, for location privacy protection, conditional privacy protection in the case of information sharing needs to be established to ensure the regular use of Internet of Vehicles location services and other applications.

4.3. Trust Management. Most existing trust management methods focus on collecting various pieces of evidence and analyzing the historical behavior of nodes to evaluate their trustworthiness of nodes. Unlike the object-oriented foundation, trust models can also be divided into three types [38, 47]: message-centric, entity-centric, and hybrid or composite models. Likewise, deployment strategies for trust management can be classified into centralized and decentralized types. Trust in the Internet of Vehicles is based on the trust value gained by the vehicle's past behavior (reputation) and neighbors' opinions on the messages broadcast by the warning vehicle in the event to realize the vehicle's importance. Trust management can facilitate peer incentives that perform well and achieve good trust scores. The system also punishes dishonest or misbehaving peers. When misbehavior exceeds a certain threshold, trust scores are low, and trust is revoked. Therefore, trust management has profound significance for the security of the Internet of Vehicles and is also the basis for identity authentication and access control.

Yang et al. [48] designed a trust model based on the data center category and used blockchain to conduct decentralized trust management for vehicle networks. They used a Bayes reasoning model to assess the credibility of messages received from neighbors. The vehicle periodically uploads the rating for each original vehicle generated to an adjacent RSU. The RSU calculates the offset of the confidence value, formed into blocks, which finally add to the blockchain that the RSU plans to hold. Through this strategy, the RSU maintains a dependable and consistent blockchain.

Lu et al. [15] adopted a blockchain-based anonymous reputation system (BARS) to implement suggestions to build trust and protect privacy. BARS systems include certificates to protect vehicle privacy, certificate management, certification bodies (CAS), law enforcement agencies (LEA), and vehicles and RSUs. There are three blockchain structures in BARS: MesBC (blockchain for messages) for continuous proof of the reputational evaluation, CerBC (blockchain for certificates) for all certificates issued, and RevSC (blockchain for revoked public keys) for revoked public keys. BARS uses extensive blockchain technology to achieve transparency, conditional anonymity, and robustness. The reputation valuation algorithm objectively reflects the message's credibility.

Table 3: Comparison of privacy protection.

Literature	Object	Method	Superiority
[41]	Content	Cognitive engine	Flexible short response time
[42]	Content	Software-defined networking, deep reinforcement, and learning spatial crowdsourcing	High throughput and low overhead
[43]	Identity	Remote authentication model	Trace
[44]	Identity	Conditional privacy statement protocol	Trust management method preventing forged messages
[45]	Location	Trust management method based on Dirichlet distribution	Detection of malicious vehicles
[46]	Location	Construction of trusted stealth region based on trust mechanism	Limited computing time and communication costs
[38]	Identity	Cluster-based MAC authentication protocol (ACB-MAC)	High throughput and lower latency

Javaid et al. [49] proposed a data sharing and trust management system for the BIoV. This document initially uses the Physical Nonclone Function (PUF) function to generate and assign a unique vehicle identifier. Then, two smart contracts are designed: one for the interaction between RSU and smart vehicle, and the other for the storage and retrieval of data from the blockchain, to establish distributed trust management and realize safety data sharing while protecting privacy. In [50], the author introduces the PoW dynamic mechanism to expand the traffic flow generated by vehicles and designs the data structure of the vehicle's blockchain in detail. The diagram attributes to each vehicle user a blockchain account with a 20-byte address similar to Bitcoin and Ethereum. The operation of the address size protocol is divided into two phases: the configuration phase for vehicle registration and the data transfer phase for communication between vehicles. Smart contracts with PUF, certificates, and dPoW consensus algorithms constitute the blockchain's IoV confidence management system.

Singh et al. [51] studied that smart contracts deployed through the CA/TA and that the USR was working in a distributed way to maintain a consistent vehicle confidential database and improve reliability, availability, and consistency. This paper introduces the concept of sharing blockchain, which uses an authoritative consensus mechanism, which can reduce the propagation delay of transactions and improve the throughput and efficiency of the whole system. In addition, the authors also introduce incentive strategies to help the vehicles participating in event detection obtain various services and pay incentives through the detection and accurate reporting of the actual event. The authors implemented the scheme in the private Ethereum blockchain and proved the feasibility of the framework by testing average throughput and runtime performance.

Han et al. [52] defined malicious behaviors and malicious RSUs of vehicles, then proposed a vehicle trust evaluation algorithm based on the hidden Markov Model (HMM), built Hyperledger Fabric, designed three smart contracts, and realized the functions of adding, updating, and querying data transactions. Finally, to solve the problem of malicious vehicles sending false information, the author builds a trust management model of a truck network based on blockchain, which improves the accuracy of malicious behavior detection.

In conclusion, in terms of trust management, blockchain technology has been fully integrated with IoV. The introduction of consensus mechanism, smart contract, incentive strategy, and the comparison of their technology applications shows in Table 4. At the same time, it also reflects the advantages of blockchain, a public distributed ledger, in terms of trust management, which can fully solve the problem of node trust in the Internet of Vehicles. However, we cannot ignore the cost of communication, computing, and storage. Therefore, we need to look at trust management solutions and do lightweight optimizations.

4.4. Access Control. With expanding scale in IoV, the amount of generated data is increasing exponentially. Secure systems must effectively control access to this information to protect the network from specific attacks (data analysis, tracking, etc.).

Sharma and Chakraborty [53] propose a system for vehicle data management that incorporates secure identity authentication, privacy protection, and access control. This system consists of a vehicle, a model, a chain, a registry, and a service provider. The vehicle can request information from the service provider, who adds the access request details, along with the permission status, to the blockchain as transactions.

Considering the need for both attribute-based data access control and location-based data access control, Jiang et al. [54] developed a location-based data access control scheme (LB-DAC) for vehicle networking. Data owners, data users, cloud storage servers, attribute permissions, location permissions, fog computing nodes, and blockchain systems are the seven entities defined within the LB-DAC scheme. Data owners can encrypt data and upload it to the cloud server under specific access control policies. Decryption can only occur if the vehicle's attributes and location meet specific requirements. As a result, the addition of fog nodes enables the positioning function. When the vehicle arrives at the designated area, the vehicle receives a location key. Additionally, it provides computing resources for decrypting vehicles. As a tamper-proof bulletin board, the blockchain is responsible for publishing public parameters of property permissions and location permits.

Mendiboure et al. [55] introduced SDN to improve the scalability of blockchain networks and shorten the

Table 4: Comparison of trust management schemes.

Scheme	Smart contract	Consensus algorithm	Incentive mechanism	Others
[48]	N	Y	N	Bayes reasoning model
[15]	N	Y	N	Reputation evaluation algorithm
[49, 50]	Y	Y	N	PUF
[51]	Y	Y	Y	Sharing blochchain
[52]	Y	Y	Y	HMM

authentication/access control/undo process. The authors defined three types of nodes in this paper: local nodes, which only involve the local blockchain subnet, used to authenticate/control the access of devices (vehicles, SDN controllers, and roadside devices) located in the geographical area; internal nodes, nodes involving two or more local blockchain subnets, enabling transitional verification/control of access across different geographic regions; global node: a node that contains both the global blockchain network and the local blockchain subnet. It retrieves information about each local blockchain subnetwork and updates the global status of the network. When the SDN controller attempts to connect to the vehicle, the blockchain node checks whether the current geographical area of the vehicle belongs to the area authorized by the controller; if not, the contact deny.

Liu et al. [56] introduced the edge-chain system and designed a dynamic access control model based on risk prediction, RPBAC, to secure access control of Internet of Vehicles devices. The blockchain network consists of vehicle nodes and roadside cells (RSUs), where the edge chain is on the RSU, and the vehicle node serves as the lightweight node. The RSU, as a full node and an edge node (edge service), provides access control services for the vehicle node. Blockchain is responsible for safe storage, the smart contract is responsible for automatic execution of the control strategy, and the intelligent control module is responsible for a wise decision. The intelligent management control module establishes the RPBAC model by introducing GAN. The RPBAC model obtains the behavior data of the requesting vehicle from the blockchain and receives the numerical matrix from the historical behavior through data preprocessing. As the input of GAN, the numerical matrix predicts the requested vehicle's risk level. The risk prediction model is built on TensorFlow 1.12.0 and coded by Python. The expected risk level, combined with the security requirements of the resource owner's vehicle, is used to assess the access rights of the requesting vehicle and generate the corresponding access control policies.

In addition, attribute-based encryption (ABE) is an encryption technique that can simultaneously achieve data confidentiality and access control, especially those ABE schemes with revocation functions. However, most of the existing revocable ABE schemes require nodes to update the private keys of all nonrevoked nodes during the update and withdrawal process. Therefore, the key update work may become a system bottleneck. Wang et al. [57] proposed a dynamic fine-grained access control scheme based on ABE. According to the vehicle's attributes, the message sender can determine which vehicles receive the message and revoke the decryption authorization for some vehicles without updating all unrevoked keys, reducing computational delay and communication overhead.

In summary, research on blockchain-based IoV access control technology is still at an early stage. In combination with identity authentication and privacy protection technology, there are more access control methods. But there are few methods for application access control. In the later stage, the application access control table can be designed according to the size of the blockchain to realize the access control of the application.

4.5. Other Solutions. To speed up distributed key management in heterogeneous networks and improve efficiency, Lai et al. [58] adopted blockchain technology. The framework consists of two schemes, namely, a new blockchain-assisted key management scheme and a dynamic transaction collection scheme. In the key management scheme, the authors eliminate the central manager and introduce multiple security managers to play an essential role in the authentication and verification of the key transmission process. The processed records are stored on the blockchain and shared between the SMs. On the other hand, the dynamic transaction acquisition scheme enables the system to reduce the key transmission time of the blockchain network during the vehicle switching process, and the acquisition cycle can change dynamically according to different traffic levels.

On behalf of ensuring the security and traceability of data sharing in-vehicle networks, Kang et al. [59] proposed a reputation-based blockchain scheme. Two smart contracts, DSSC (a data storage smart contract) and ISSC (information sharing smart contract), are deployed on the blockchain. DSSC realizes secure data storage, and ISSC realizes the efficient data sharing function. The paper also cites subjective logic to construct the interactive individual reputation evaluation. The authors propose a three-component local view TWSL (three-weight subjective logic), which is different from traditional subjective logic (TSL). They also consider interaction frequency, event timelines, track similarity, and combine local opinions with recommendations to achieve accurate reputation management and high-quality data sharing. Chen et al. [60] built a data sharing system composed of a two-layer blockchain based on a new content-centered vehicle Internet data sharing model-Vehicle Naming Data Network (VNDN), which has emerged in recent years. At the bottom, we divide vehicles into groups of blockchains based on their mobility trend similarity or PBO (a private blockchain for OBUs). At the top level, a preselected RSU executes the consensus process. Assume that

all vehicles inclined to participate in the information sharing system are legitimate entities registered with a trusted institution. The authors also model the balance between demand and supply as a matching game. To encourage nodes to provide forward services, the authors propose a reputation management mechanism that combines negative and forward transaction records to improve the security of information interaction in VNDN.

Akhter et al. [61] proposed a blockchain-based secure cluster MAC protocol (SCB-MAC) based on the traditional IEEE802.11 standard, which defined the formation of the cluster, handshake mode, and transmission of specific and nonsecure messages in detail. Assume that all vehicles are equipped with the hardware and software resources needed to send and receive information, such as OBUs, sensors, a global positioning system (GPS). They can connect to high-speed Internet. A Certification Authority (CA) physically verifies all vehicles. The CA assigns a public and private key pair to each car. The CA is considered secure enough to protect the privacy of the vehicle. Select a cluster leader (CH) and others as cluster members (CM) in a centralized vehicle system. CH will handle all NSMT between CMs as an access point. Each cluster has a blockchain to store secure messages. All CMs (including CH) are complete nodes, and anyone can initiate a transaction in a specified blockchain to notify of an emergency. The vehicle will sign the message with its private key to confirm its identity and ensure nonrepudiation. The blockchain server will check the authentication, generate a block from the transmission, and broadcast it to all members.

This section examines security solutions beyond identity authentication, privacy protection, trust management, and access control. These solutions only explore security issues at a specific point on the Internet of Vehicles, such as reputation-based data sharing, without considering privacy protection while considering data sharing. Therefore, we suggest that we take full advantage of the technical characteristics of IoV and blockchain and solve the security problems of the Internet of Vehicles through the IoV architecture and technology innovation of the integrated block.

5. Security Analysis Methods and Performance Parameters in BIoV

5.1. Security Analysis Methods. Based on thoroughly investigating blockchain-based IoV security technology in the last section, we analyzed that each protocol and scheme's simulation environment and analysis methods differed. This section focuses on security analysis methods and performance parameters in BIoV.

5.1.1. Informal Safety Analysis. Informal security analysis refers to the theory or process analysis of the following security elements according to the characteristics of security protocols proposed in this paper. Table 5 shows the comparison of relating schemes.

Bidirectional authentication: in the designed certification process, certification entities are for mutual certification.

Key management: in the scheme designed in this paper, after mutual authentication and key protocol are completed, the secret key is generated, stored, and revoked, and this forms the life cycle management of the private key

Privacy protection: in schemes, protocols, and other processes, it is necessary to consider preventing the disclosure of information such as original identity and how to share sensitive information (such as anonymity and location)

Resist attacks: according to the design of the agreement and scheme, it is necessary to consider resisting the man-in-the-middle attack, DOS attack, and other kinds of attacks proposed in Section 2

5.1.2. Formal Safety Analysis Methods. The formal security analysis method is proved by mathematical theorem. First, establish the theorem. Secondly, the popular security verification tool ProVerif [66] verifies the security of the proposed authentication protocol. ProVerif is an automatic formal verification cryptographic protocol tool based on the Dolev-Yao model developed by Bruno Blanchet. It is implemented in the Prolog language. It can describe a variety of cryptographic primitives, including shared key and public key cryptography (encryption and digital signature), hash functions, and Diffie-Hellman key exchange protocols. It can specify rewrite rules and equations for input languages, such as applying PI calculus or the Horn word. The authentication protocol used for authentication is divided into three parts [67]: (1) declaring encryption primitives, (2) defining processes on the primary process and a single entity as child processes, and (3) instantiation child processes using the immediate process. When using the ProVerif tool to verify the cryptographic protocol, this tool will give a corresponding attack sequence if the protocol has vulnerabilities. ProVerif can prove the following attributes: confidentiality (the adversary does not have access to the secret), authentication and its more general counterpart, high secrecy (the adversary does not see the difference when the secret value changes), and only equivalence between processes with different terms. Table 6 lists a comparison of formal safety analysis methods in the literature.

5.2. Performance Evaluation Characteristic Parameters and Comparison. We summarize the blockchain types and performance evaluation parameters involved in the literature, as shown in Table 7. We can see that, by evaluating the methods proposed in the literature in a blockchain, in addition to the regular communication overhead and computational overhead, the researchers also assess the storage overhead.

(1) Communication overhead: this parameter is the maximum packet size required for protocol

Table 5: Comparison of informal safety analysis methods.

Security characteristics	[62]	[63]	[64]	[65]
Bidirectional authentication	Y	Y	Y	N
Key management	Y	Y	N	Y
Privacy protection	PFS/PBS	Y	N	N
Resist attacks	Man-in-the-middle attack	Man-in-the-middle attack	DOS attack, physical attack, and man-in-the-middle attack	Resist cyberattacks

Table 6: Comparison of formal safety analysis methods.

Literature	[25]	[35]	[53]	[55]	[58]
Mathematical theorem proof	Y	Y	N	Y	N
ProVerif	N	N	Y	Y	Y

Table 7: Blockchain simulation and parameters.

Literature	Simulation tools	Blockchain	Parameters for performance evaluation
[21]		Hyperledger Fabric 1.2	Storage overhead and computational overhead
[35]	Cygwin	NO	Computational overhead and communication overhead
[51]		Ethereum blockchain	Computational overhead and communication overhead
[61]	Truffle framework	Ethereum blockchain	Storage overhead delay

transport. Literature [48] points out that there are two kinds of data, namely, secure and nonsecure messages, transmitted through a wireless channel in the vehicular network. Safety messages are triggered by specific road-related events and broadcast by the vehicle; the packet size of the message is set to 800 bytes. Unsafe data generated by a car are accumulated in a certain period, packaged into a packet, and uploaded to a nearby RSU. The size of the nonsecure message packet is usually more significant than the size of the secure message. In literature [50], the size of the blockchain data packet is 512 bytes, and the size of the application data packet is 64 bytes.

(2) Computational complexity: the computational complexity is related to the algorithm used by the protocol or scheme. We can define the algorithm complexity involving signature, verification, encryption, and decryption in the process as O (Sig), O (Sig), O (Enc), and O (Enc) functions. We can compare literature [44] and literature [45], as shown in Table 8.

From the above comparison, we can see the location privacy protection scheme combined edge computing and RSU adopted in the literature [45] can quickly evaluate the trust value by using the trust data gathered from the blockchain. We want to protect vehicle location privacy while reducing computing time and communication costs. Of course, literature [44] strengthens the reliability of vehicles by analyzing various requirements of requesting and cooperating vehicles.

(3) Decentralization: quantitative decentralization refers to the degree of decentralization of the system, and it can also judge the influence of system modification on the degree of decentralization. We can design and optimize algorithms and frameworks to maximize decentralization. In [50], the Gini coefficient $g_{(\lambda)}$ is used to measure the dispersion of the proposed protocol by considering the geographical location distribution of miners' nodes. The Gini coefficient is in [0, 1], where 0 represents complete dispersion and 1 represents total concentration. Therefore, the more dispersed or uniform the geographic distribution of miner nodes is, the closer the coefficient is to 0. In this paper, $\lambda(x)$ is used to express the geographical distribution density of RSU, and the Gini coefficient $g_{(\lambda)}$ can be expressed as

$$g_{(\lambda)} = \frac{\int_a \int_a |\lambda(x) - \lambda(y)| \mathrm{d}y \mathrm{d}x}{\int_a \int_a \lambda(x) \mathrm{d}y \mathrm{d}x} = \frac{\int_a \int_a |\lambda(x) - \lambda(y)| \mathrm{d}y \mathrm{d}x}{2M}, \tag{1}$$

where a is the area of the two-dimensional coordinate (x, y) of the geographical location of RSU and the distribution density of $\lambda(x)$ in this area.

(4) Delay: the time required for the successful transmission of a message [46]. Then, the average delay $E[D]$ can be expressed as

$$E[D] = E\left[T_{\text{interval}}\right] - \frac{P_{\text{fdrop}}}{1 - P_{\text{fdrop}}} * E\left[T_{\text{drop}}\right]. \tag{2}$$

Among them $E[T_{\text{interval}}]$ represents the average time interval between two successful packets received, $P_{f\,\text{drop}}$ shows the packet loss probability, and $E[T_{\text{drop}}]$ expresses the average packet loss time.

Communication delay is an important indicator to judge whether the technical security solution of the Internet of Vehicles is efficient. The most common simulation indicators: the same method evaluates the change of the communication delay with the number of nodes to determine the

Table 8: Comparison of computational complexity.

Process of [45]	Computational complexity	Process of [44]	Computational complexity
Position verification	O (1)	Verification	O (sig)
Cross-regional trust stealth zone construction	O (1)	Request cooperative signature	O (sig)
Restore key and verify integrity	O (Enc)	Returns response	O (sig) + O (Enc)

scalability of the scheme; the comparison of the communication delay between different ways reflects the efficiency of the method.

6. Summarization and Prospect

Through the above discussion on various aspects of blockchain-based IoV technology, security and privacy issues in IoV applications have focused on people's attention. We can enhance decentralized privacy protection, traceability, and other types of security by integrating blockchain technology. The research achievements in identity authentication, privacy protection, trust management, access control, and so on have been made. However, the following problems remain unresolved. However, the following issues remain unresolved: (1) development of a blockchain-based IoV security framework, which is different from the traditional IoV network architecture. We can use existing infrastructure to build IoV systems at maximum cost savings; (2) studying new blockchain models. The model addresses current challenges such as growing nodes, ledger, and data, reducing complexity and latency, and increasing scalability; (3) strengthening the control layer. This layer mainly uses intrusion detection and attack mitigation control. These methods require numerical and theoretical analysis and can keep the network running in the face of errors, emergency demand outages, or physical attacks; (4) studying lightweight blockchain. The important limitations of smart contracts and consensus mechanisms are computing power, communication, and energy consumption; moreover, with the increasing number of vehicles, there is a lot of data transmission and storage consumption. Therefore, we should design a lightweight blockchain-based IoV framework or lightweight authentication and privacy protection protocols; (5) combination with existing new technologies. Blockchain can be combined with edge computing to enhance data analytics and improve the security of nodes on the Internet of Vehicles. Blockchain can also be combined with deep learning to build risk prediction models and improve access control security for Internet of Vehicles systems. Blockchain can also be combined with SDN and AI technologies to improve the transparency of the control plane. Therefore, the significance of the research work carried out in this paper is to summarize, classify, and discuss the existing blockchain-based Internet of Vehicles security technology, grasp its development direction, summarize verification and effective evaluation methods, and provide direction and method guidance for the following research work.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was supported by the following projects: (1) the Graduate Research Innovation Project of Jiangsu Province, China (Grant no. KYCX21_3087); (2) the National Natural Science Foundation of China (Grant no. 61771265); (3) the Key Science and Technology Foundation of Nantong (Grant no. MS22021034).

References

[1] R. Shrestha, S. Y. Nam, R. Bajracharya, and S. Kim, "Evolution of V2X communication and integration of blockchain for security enhancements," *Electronics*, vol. 9, no. 9, p. 1338, 2020.

[2] R. Shrestha and S. Y. Nam, "Regional blockchain for vehicular networks to prevent 51% attacks," *IEEE Access*, vol. 7, pp. 95033–95045, 2019.

[3] S. Xie, Z. Zheng, W. Chen, J. Wu, H.-N. Dai, and M. Imran, "Blockchain for cloud exchange: a survey," *Computers & Electrical Engineering*, vol. 81, Article ID 106526, 2020.

[4] P. Fraga-Lamas and T. M. Fernandez-Carames, "A review on blockchain technologies for an advanced and cyber-resilient automotive industry," *IEEE Access*, vol. 7, pp. 17578–17598, 2019.

[5] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, "A new type of blockchain for secure message exchange in VANET," *Digital communications and networks*, vol. 6, no. 2, pp. 177–186, 2020.

[6] T. Ali Syed, A. Alzahrani, S. Jan, M. S. Siddiqui, A. Nadeem, and T. Alghamdi, "A comparative analysis of blockchain architecture and its applications: problems and recommendations," *IEEE Access*, vol. 7, pp. 176838–176869, 2019.

[7] T. Ali, A. Nadeem, M. Shoaib, M. Nauman, and A. Alzahrani, "Blockchain-based-vehicle-life-cycle-tracking-system," 2019, https://www.researchgate.net/project/Blockchain-Based-Vehicle-Life-Cycle-Tracking-Syste.

[8] M. L. Chavez, C. H. Rosete, and F. R. Henriguez, "Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study," in *Proceedings of the 15th International Conference on electronics (2005), communications and Computers*, August 2010, Article ID 166e70.

[9] P. Sharma and H. Liu, "A machine-learning-based data-centric misbehavior detection model for internet of vehicles," *IEEE Internet of Things Journal*, vol. 8, no. 6, pp. 4991–4999, 2021.

[10] S. Bono, M. Green, A. Stubblefield, A. Juels, A. D. Rubbin, and M. Szydlo, "Security analysis of a cryptographically-enabled RFID device," *USENIX Security Symposium*, vol. 31, 2005.

[11] Sumra, I. Ahmed, H. BinHasbullah, J. L. A. Manan, and I. Ahmad, "Classification of attacks in vehicular ad hoc network (vanet)," *International Information Institute (Tokyo)*, vol. 5, p. 2995, 2013.

[12] S. Checkoway, D. McCoy, and B. Kantor, "Comprehensive experimental analyses of automotive attack surfaces," *20th USENIX Security Symposium*, USENIX Security, vol. 11, 2011.

[13] R. Shrestha and S. Y. Nam, "Trustworthy event-information dissemination in vehicular ad hoc networks," *Mobile Information Systems*, vol. 2017, Article ID 9050787, 2017.

[14] J. R. Douceur, "The sybil attack," *Peer-to-Peer Systems*, Springer, Berlin, Heidelberg, pp. 251–260, 2002.

[15] Z. Lu, W. Liu, Q. Wang, G. Qu, and Z. Liu, "A privacy-preserving trust model based on blockchain for VANETs," *IEEE Access*, vol. 6, pp. 45655–45664, 2018.

[16] S. So, P. Sharma, and J. Petit, "Integrating plausibility checks and machine learning for misbehavior detection in VANET," in *Proceedings of the 2018 17th IEEE International Conference on Machine Learning and Applications (ICMLA)*, pp. 564–571, ICMLA, Orlando, FL, USA, December 2018.

[17] S. Chen, X. Zhu, H. Zhang, C. Zhao, G. Yang, and K. Wang, "Efficient privacy preserving data collection and computation offloading for fog-assisted IoT," *IEEE Transactions on Sustainable Computing*, vol. 5, no. 4, pp. 526–540, 2020.

[18] W. Hu, Y. Hu, W. Yao, and H. Li, "A blockchain-based byzantine consensus algorithm for information authentication of the internet of vehicles," *IEEE Access*, vol. 7, pp. 139703–139711, 2019.

[19] X. Ma, C. Ge, and Z. Liu, "Blockchain-enabled privacy-preserving Internet of vehicles: decentralized and reputation-based network architecture," in *Proceedings of the International Conference on Network and System Security*, December 2019.

[20] J. Gao, K. O. B. Obour Agyekum, E. B. Sifah et al., "A blockchain-SDN-enabled internet of vehicles environment for fog computing and 5G networks," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4278–4291, 2020.

[21] H. Lin, S. Garg, J. Hu, G. Kaddoum, M. Peng, and M. S. Hossain, "Blockchain and deep reinforcement learning empowered spatial crowdsourcing in software-defined internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3755–3764, 2021.

[22] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for internet of things: a survey," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8094, 2019.

[23] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4298–4311, 2020.

[24] F. Dai, H. Chen, Z. Qiang, Z. Liang, B. Huang, and L. Wang, "Automatic Analysis of Complex Interactions in Microservice Systems," *Complexity*, vol. 2021, Article ID 2128793, 2020.

[25] K. Liu, W. Chen, Z. Zheng, Z. Li, and W. Liang, "A novel debt-credit mechanism for blockchain-based data-trading in internet of vehicles," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 9098–9111, 2019.

[26] T. Jiang, H. Fang, and H. Wang, "Blockchain-based internet of vehicles: distributed network architecture and performance analysis," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4640–4649, 2019.

[27] Z. Lu, G. Qu, and Z. Liu, "A survey on recent advances in vehicular network security, trust, and privacy," *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 2, pp. 760–776, 2019.

[28] P. Vijayakumar, M. Azees, A. Kannan, and L. Jegatha Deborah, "Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 1015–1028, 2016.

[29] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 9, pp. 2467–2476, 2017.

[30] A. Karati, S. H. Islam, G. P. Biswas, M. Z. A. Bhuiyan, P. Vijayakumar, and M. Karuppiah, "Provably secure identity-based signcryption scheme for crowdsourced industrial internet of things environments," *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2904–2914, 2018.

[31] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and C. Hu, "Distributed aggregate privacy-preserving authentication in VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 3, pp. 516–526, 2017.

[32] S. H. Islam, M. S. Obaidat, P. Vijayakumar, E. Abdulhay, F. Li, and M. K. C. Reddy, "A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs," *Future Generation Computer Systems*, vol. 84, pp. 216–227, 2018.

[33] C. Fromknecht and D. Velicanu, "CertCoin: A NameCoin Based Decentralized Authentication System" 6.857 Class Project," 2014, https://courses.csail.mit.edu/6.857/2014/files/19-fromknecht-velicann-yakoubov-certcoin.pdf.

[34] A. Maria, V. Pandi, J. D. Lazarus, M. Karuppiah, and M. S. Christo, "BBAAS: blockchain-based anonymous authentication scheme for providing secure communication in VANETs," *Security and Communication Networks*, vol. 2021, Article ID 6679882, 11 pages, 2021.

[35] Y. Yao, X. Chang, J. Misic, V. B. Misic, and L. Li, "BLA: blockchain-assisted lightweight Anonymous authentication for distributed vehicular fog services," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 3775–3784, 2019.

[36] J. Noh, S. Jeon, and S. Cho, "Distributed blockchain-based message authentication scheme for connected vehicles," *Electronics*, vol. 9, no. 1, p. 74, 2020.

[37] D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, "A traceable blockchain-based access authentication system with privacy preservation in VANETs," *IEEE Access*, vol. 7, pp. 117716–117726, 2019.

[38] J. Zhang, "Trust management for VANETs," *International Journal of Distributed Systems and Technologies*, vol. 3, no. 1, pp. 48–62, 2012.

[39] S. Kim and R. Shrestha, "Internet of vehicles, vehicular social networks, and cybersecurity," *Automotive Cyber Security*, Springer, Singapore, pp. 149–181, 2020.

[40] T. A. Butt, R. Iqbal, K. Salah, M. Aloqaily, and Y. Jararweh, "Privacy management in social internet of vehicles: review, challenges and blockchain based solutions," *IEEE Access*, vol. 7, pp. 79694–79713, 2019.

[41] Y. Qian, Y. Jiang, L. Hu, M. S. Hossain, M. Alrashoud, and M. Al-Hammadi, "Blockchain-based privacy-aware content caching in cognitive internet of vehicles," *IEEE Network*, vol. 34, no. 2, pp. 46–51, 2020.

[42] C. Xu, H. Liu, P. Li, and P. Wang, "A remote attestation security model based on privacy-preserving blockchain for V2X," *IEEE Access*, vol. 6, pp. 67809–67818, 2018.

[43] X. Liu, H. Huang, F. Xiao, and Z. Ma, "A blockchain-based trust management with conditional privacy-preserving announcement scheme for VANETs," *IEEE Internet of Things Journal*, vol. 7, no. 5, pp. 4101–4112, 2020.

[44] B. Luo, X. Li, J. Weng, J. Guo, and J. Ma, "Blockchain enabled trust-based location privacy protection scheme in VANET," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 2, pp. 2034–2048, 2020.

[45] J. Feng, Y. Wang, J. Wang, and F. Ren, "Blockchain-based data management and edge-assisted trusted cloaking area construction for location privacy protection in vehicular

networks," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2087–2101, 2021.

[46] A. F. M. S. Akhter and M. Ahmed, A. A. Shah, A. F. M. S. Shah, A. Anwar, and A. Zengin, A secured privacy-preserving multi-level blockchain framework for cluster based VANET," *Sustainability*, vol. 13, no. 1, p. 400, 2021.

[47] S. A. Soleymani, A. H. Abdullah, W. H. Hassan et al., "Trust management in vehicular ad hoc network: a systematic review," *EURASIP Journal on Wireless Communications and Networking*, vol. 2015, no. 1, p. 146, 2015.

[48] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 1495–1505, 2019.

[49] U. Javaid, M. N. Aman, and B. Sikdar, "DrivMan: driving trust management and data sharing in VANETs with blockchain and smart contracts," in *Proceedings of the 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring)*, pp. 1–5, Kuala Lumpur, Malaysia, May 2019.

[50] U. Javaid, M. N. Aman, and B. Sikdar, "A scalable protocol for driving trust management in internet of vehicles with blockchain," *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11815–11829, 2020.

[51] P. K. Singh, R. Singh, S. K. Nandi, K. Z. Ghafoor, D. B. Rawat, and S. Nandi, "Blockchain-based adaptive trust management in internet of vehicles using smart contract," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 6, pp. 3616–3630, 2021.

[52] L. Han, D. Han, and D. Li, "Behavior analysis and blockchain based trust management in vanets," vol. 151, pp. 61–69, 2021.

[53] R. Sharma and S. Chakraborty, "BlockAPP: using blockchain for authentication and privacy preservation in IoV," in *Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps)*, pp. 1–6, Abu Dhabi, UAE, December 2018.

[54] M. Jiang, H. Wang, W. Zhang, H. Qin, and Xi Sun, "Location-based data access control scheme for internet of vehicles," *Computers & Electrical Engineering*, vol. 86, Article ID 106716, 2020.

[55] L. Mendiboure, M. A. Chalouf, and F. Krief, "A scalable blockchain-based approach for authentication and access control in software defined vehicular networks," in *Proceedings of the 2020 29th International Conference on Computer Communications and Networks (ICCCN)*, pp. 1–11, Honolulu, HI, USA, September 2020.

[56] Y. Liu, M. Xiao, S. Chen, F. Bai, J. Pan, and D. Zhang, "An intelligent edge-chain-enabled access control mechanism for IoV," *IEEE Internet of Things Journal*, vol. 8, no. 15, pp. 12231–12241, 2021.

[57] T. Wang, L. Kang, and J. Duan, "Dynamic fine-grained access control scheme for vehicular ad hoc networks," *Computer Networks*, vol. 188, Article ID 107872, 2021.

[58] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1832–1843, 2017.

[59] J. Kang, R. Yu, X. Huang et al., "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4660–4670, 2019.

[60] C. Chen, C. Wang, T. Qiu, N. Lv, and Q. Pei, "A secure content sharing scheme based on blockchain in vehicular named data networks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 5, pp. 3278–3289, 2020.

[61] A. F. M. S. Akhter, A. F. M. S. Shah, M. Ahmed, N. Moustafa, U. Çavuşoğlu, and A. Zengin, "A secured message transmission protocol for vehicular ad hoc networks," *Computers, Materials & Continua*, vol. 68, no. 1, pp. 229–246, 2021.

[62] R. Ma, J. Cao, D. Feng et al., "A secure authentication scheme for remote diagnosis and maintenance in internet of vehicles," *2020 IEEE Wireless Communications and Networking Conference (WCNC)*, pp. 1–7, Seoul, Korea (South), May 2020.

[63] T. Alladi, S. Chakravarty, V. Chamola, and M. Guizani, "A lightweight Authentication and attestation scheme for in-transit vehicles in IoV scenario," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 14188–14197, 2020.

[64] M. N. Aman, U. Javaid, and B. Sikdar, "A privacy-preserving and scalable authentication protocol for the internet of vehicles," *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 1123–1139, 2021.

[65] M. Wazid, P. Bagga, A. K. Das et al., "AKM-IoV: authenticated key management protocol in fog computing-based internet of vehicles deployment," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8804–8817, 2019.

[66] B. Blanchet and V. Cheval, "ProVerif: Cryptographic protocol verifier in the formal model," 2020, https://prosecco.gforge.inria.fr/personal/bblanche/proverif/.

[67] B. Blanchet and V. Cheval, "ProVerif 2.00: automatic cryptographic protocol verifier, user manual and tutorial," pp. 05–16, 2018, https://bblanche.gitlabpages.inria.fr/proverif/manual.pdf.