Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2024.052233

ARTICLE

A Blockchain-Based Efficient Cross-Domain Authentication Scheme for Internet of Vehicles

Feng Zhao[1], Hongtao Ding[2], Chunhai Li[1,*], Zhaoyu Su[2], Guoling Liang[2] and Changsong Yang[3]

[1]Guangxi Engineering Research Center of Industrial Internet Security and Blockchain, Guilin University of Electronic Technology, Guilin, 541004, China

[2]School of Information and Communication, Guilin University of Electronic Technology, Guilin, 541004, China

[3]School of Computer Science and Information Security, Guilin University of Electronic Technology, Guilin, 541004, China

*Corresponding Author: Chunhai Li. Email: chunhaili@guet.edu.cn

Received: 27 March 2024 Accepted: 14 May 2024 Published: 18 July 2024

ABSTRACT

The Internet of Vehicles (IoV) is extensively deployed in outdoor and open environments to effectively address traffic efficiency and safety issues by connecting vehicles to the network. However, due to the open and variable nature of its network topology, vehicles frequently engage in cross-domain interactions. During such processes, directly uploading sensitive information to roadside units for interaction may expose it to malicious tampering or interception by attackers, thus compromising the security of the cross-domain authentication process. Additionally, IoV imposes high real-time requirements, and existing cross-domain authentication schemes for IoV often encounter efficiency issues. To mitigate these challenges, we propose CAIoV, a blockchain-based efficient cross-domain authentication scheme for IoV. This scheme comprehensively integrates technologies such as zero-knowledge proofs, smart contracts, and Merkle hash tree structures. It divides the cross-domain process into anonymous cross-domain authentication and safe cross-domain authentication phases to ensure efficiency while maintaining a balance between efficiency and security. Finally, we evaluate the performance of CAIoV. Experimental results demonstrate that our proposed scheme reduces computational overhead by approximately 20%, communication overhead by around 10%, and storage overhead by nearly 30%.

KEYWORDS

Blockchain; cross-domain authentication; internet of vehicle; zero-knowledge proof

1 Introduction

The IoV (Internet of Vehicles), a prominent application of IoT (Internet of Things) technology in the automotive industry [1–3], constitutes a high-speed mobile broadband wireless network supporting diverse services such as driving safety and information services. It stands as a vital component of ITS (Intelligent Transportation Systems). However, during participation in data sharing and information exchange within the Internet of Vehicles, vehicle users may expose sensitive information such as identity, location, and request details. Additionally, user data might fall victim to malicious tampering

during transmission by attackers [4–6], resulting in data becoming invalid due to the receiver's inability to verify it accurately [7,8]. While current research suggests that cross-domain authentication schemes can effectively address these issues, centralized cross-domain authentication schemes often encounter single point of failure issues.

Recently, emerging blockchain technology has been recognized as a pivotal component of distributed solutions [9], offering advantages such as decentralization, transparency, and security. In a blockchain-based cross-domain authentication system, authentication information is distributed across a blockchain network rather than centralized on a single server. Consequently, even if some nodes fail or are attacked, other nodes can continue to provide authentication services, addressing the issue of single point of failure [10]. However, current blockchain-based cross-domain authentication schemes [11–15] face challenges such as excessive cryptographic computations and high performance requirements for edge nodes, resulting in decreased authentication efficiency and difficulties in meeting the demands of IoV scenarios. On the contrary, zero-knowledge proofs enable a prover to demonstrate the truth of a statement to a verifier without divulging the specific details of the statement. Founded on mathematical principles and cryptographic techniques, zero-knowledge proofs furnish robust security guarantees, thwarting information leakage and forgery. They can ensure security while also striking a balance with efficiency, rendering them highly suitable for contemporary IoV cross-domain authentication scenarios. Therefore, to address the recurring cross-domain authentication requirements in IoV environments, we propose a blockchain-based efficient cross-domain authentication scheme for IoV, namely CAIoV. Our main contributions are summarized as follows:

- We propose a blockchain-based efficient cross-domain authentication scheme for Internet of Vehicles, referred to as CAIoV. Which categorizes cross-domain authentication into two types: Anonymous cross-domain authentication and safe cross-domain authentication. These two approaches are selected based on the varying access requirements of vehicle users, significantly enhancing both the security and efficiency of cross-domain authentication.
- To address the issue of user privacy leakage during the cross-domain process, we implement an anonymous cross-domain scheme using zero-knowledge proofs and smart contracts. Subsequently, we ensure safe cross-domain authentication by employing a Merkle hash tree structure and smart contracts. Which guarantees user privacy during the cross-domain process while ensuring the efficiency of cross-domain authentication.
- We evaluate the performance of the CAIoV scheme and experimental results demonstrate its advantages in security, efficiency, and reduced storage consumption.

The rest of this work is organized as follows. In Section 2, we review the related work. In Section 3, we present the schema framework and adversarial threat model. In Section 4, we describe our system in detail, in Sections 5 and 6, we perform security analysis and performance evaluation. Finally, the conclusion is presented in Section 7.

2 Related Work

2.1 The Centralized Cross-Domain Authentication Schemes

In the research of cross-domain identity authentication, traditional Public Key Infrastructure (PKI) is widely deployed in various safe communication fields. However, when applied to the Internet of Vehicles (IoV), it encounters numerous challenges. In IoV scenarios, privacy, authentication, latency, revocation, performance, and malicious credential detection have entirely different requirements. To meet these demands, Khan et al. [16] proposed Vehicle Public Key Infrastructure (VPKI) based on PKI

technology to facilitate key management and security services in IoV. In [17], Khan et al. conducted a comprehensive, specific, and thorough investigation of the latest advancements in VPKI and the flaws within VPKI. Traditional certificates are susceptible to being tracked or monitored by attackers due to their long-term unchanging nature. Wang et al. [18] proposed a spatio-temporal dynamic pseudonym mechanism which divides the entity's movement trajectory into multiple unrelated trajectory segments with different pseudonymous identities. This not only ensures data availability and real-time performance but also preserves the entity's trajectory privacy. Therefore, centralized cross-domain authentication schemes cannot be applied to current IoV scenarios due to the issue of single point of failure.

2.2 The Blockchain-Based Decentralized Cross-Domain Authentication Scheme

Blockchain technology is considered the most effective means of achieving decentralization [19]. Zheng et al. [20] designed a protocol scheme for internet of vehicles authentication and key agreement based on blockchain. However, due to its employment of a dual-chain structure, the maintenance cost becomes prohibitively high, thus limiting its applicability in IoV scenarios. Xu et al. [21] proposed a blockchain-based authentication and key negotiation protocol for multi-Trust Authority (TA) network models, reducing the computational load on TAs. Nonetheless, as Road Side Units (RSUs) serve as computational nodes, the requirements for edge device performance are excessively high, rendering it unsuitable for IoV deployment. In [22], Chen et al. proposed a privacy-preserving cross-domain authentication scheme compatible with both existing Public Key Infrastructure (PKI) and Certificate Transparency (CT) systems, utilizing a multi-level Merkle hash tree structure to efficiently handle large data volumes. However, in this scheme, efficiency significantly decreases as communication volume at edge nodes increases. Zhang et al. [23] presented a completely cross-domain authentication architecture with high security but excessive cryptographic computations, leading to impractical computational overheads for meeting the real-time demands of IoV. In [24], Zhang et al. introduced a cross-domain scheme based on master-slave chains with lower latency, yet its dual-chain usage imposes high requirements on edge device performance and maintenance costs, thereby restricting its widespread adoption in mobile scenarios. Huang et al. [25] proposed a cross-domain scheme employing blockchain, zero-knowledge proofs, homomorphic encryption, and random permutation technologies. However, it also demands high computational capabilities from edge devices and suffers from high latency, making it unsuitable for IoV applications. In [26], Li et al. proposed a cross-domain authentication and key negotiation system based on blockchain smart contracts, which offered lower computational and communication overheads due to the absence of complex encryption operations and certificate verification. However, its security remains unguaranteed. Jia et al. [27] introduced a cross-domain solution based on Inter-Blockchain Communication (IBC), effectively alleviating issues posed by traditional PKI systems but incurring excessive computational overhead during user cross-domain processes, thus rendering it impractical for IoV scenarios. In [28], Feng et al. proposed a cross-domain authentication scheme based on blockchain, employing threshold-shared multi-signatures to construct identity federations. While ensuring security, the complexity of the cross-domain authentication scheme leads to significant computational overheads.

In summary, there are already many schemes in the field of cross-domain authentication that utilize blockchain technology combined with digital signatures, cryptography, and other related technologies. However, few of these schemes can effectively balance efficiency and security to meet the needs of cross-domain scenarios in the Internet of Vehicles (IoV). Therefore, we developed an a blockchain-based efficient cross-domain authentication scheme for internet of vehicles to meet the

needs of modern IoV scenarios. Compared to other schemes outlined in our paper, our scheme is both more secure and efficient.

3 System Model

3.1 The Scheme Framework

The overall framework of the proposed scheme is shown in Fig. 1, which primarily consists of the following entity layers: Vehicle users, Road Side Units (RSUs), Trust Agencies (TAs), and IPFS storage nodes on the TA side. Aside from decentralized storage, all entities are required to register on the blockchain network. The descriptions of each layer are provided below.

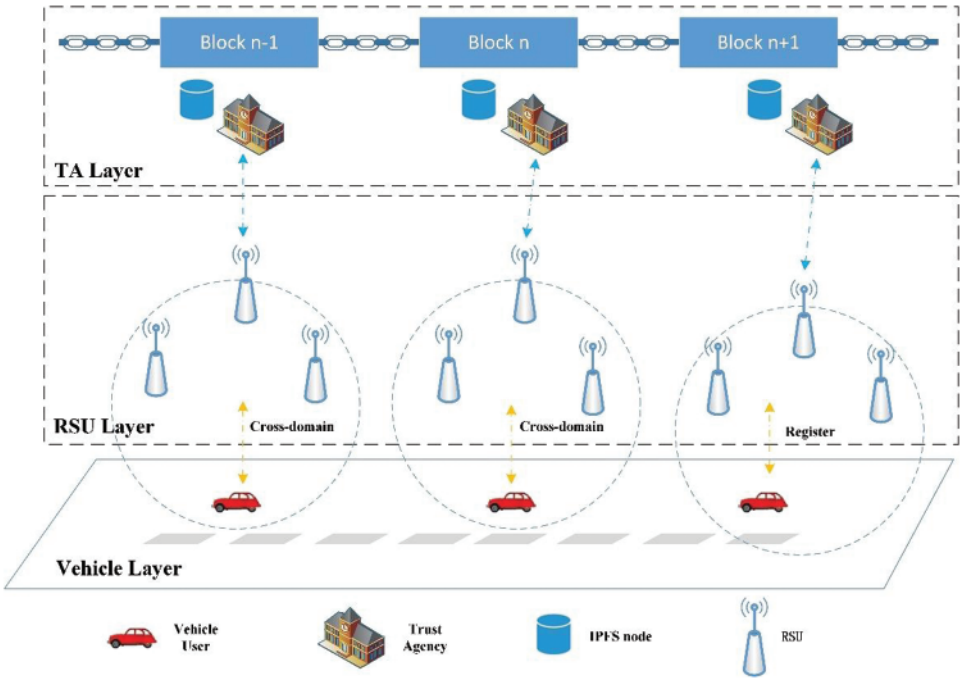

Figure 1: The overall framework of the scheme

At the Vehicle layer, vehicles equipped with multiple onboard sensors and On-Board Units (OBUs) collect various valuable information about other vehicles, roads, and the surrounding environment, such as road conditions and entertainment aspects. Therefore, vehicles serve as the source of data generation and provide partial information for users in other domains. This information is represented as $attr_i = \{attr_1, attr_2, \ldots, attr_i\}$. Additionally, their identities need to be verified by the Trust Agency.

At the Road Side Unit (RSU) layer, multiple servers equipped with communication, computation, and storage resources are distributed along the roads, forming a collection denoted as $RSU_i = \{RSU_1, RSU_2, \ldots, RSU_N\}$. However, due to the limited capabilities in various aspects, RSUs cannot independently complete tasks and require collaboration with the TA to fulfill relevant tasks. The servers surrounding the RSUs can utilize their own communication, computation, and storage capabilities to provide vehicles with high-quality Vehicle-to-Infrastructure (V2I) transmission and assist in the completion of cross-domain authentication between vehicles and the TA. This facilitates the subsequent provision of necessary services for authenticated vehicles.

At the Trust Agency (TA) layer, each entity serves as the administrator for its respective independent domain. Underneath, there are several Road Side Units (RSUs) with limited communication, computation, and storage resources. Moreover, the Trust Agency TA_i in different regions also acts as the nodes in the consortium blockchain, responsible for registering vehicles within their respective areas. Given the inefficiency of using blockchain to store and query vast amounts of data for cross-domain authentication, IPFS nodes are employed as substitutes for blockchain nodes. These IPFS nodes are tasked with providing vehicle users with distributed storage for encrypted data resource files (such as location information, driving speeds, etc.) and performing data queries during the authentication process, thereby significantly enhancing the efficiency of cross-domain operations.

At the storage layer, the CAIoV scheme employs blockchain technology and IPFS (Inter Planetary File System) for data storage and cross-domain identity verification. However, considering the relatively low efficiency of blockchain technology in storing and querying large amounts of data and the security risks posed by IPFS, this paper aims to balance efficiency and security by leveraging the advantages of both technologies. Specifically, IPFS is utilized as the storage layer for storing cross-domain data, while blockchain is used as a ledger to ensure consistency between on-chain and off-chain data. Which utilizes the efficiency of IPFS and the data consistency features of blockchain to ensure that the system is both efficient and secure in storing and verifying data.

3.2 Adversary Threat Model

In the proposed solution, a static adversarial model is established, which assumes that the majority of trust centers are honest. Malicious vehicle users and Road Side Units (RSUs) could be compromised by external attackers, denoted as $\mathcal{A}$, who can then attack and disrupt the system using the attack methods defined below.

Forgery Attack: Attacker $\mathcal{A}$ attempts to forge legitimate data, signatures, or other security identifiers to deceive trust centers or vehicle users. This type of attack is typically aims to bypass authentication, authorization, or data integrity protection and allow the attacker to perform unauthorized operations or manipulate data. Possible forgery attack methods in this scheme include digital signature forgery, message forgery, session forgery, and identity forgery.

Replay Attack: Attacker $\mathcal{A}$ intercepts captured valid communication and retransmits them to deceive trust centers or vehicle users. $\mathcal{A}$ typically captures packets in communication and resends these packets later to repeat the same operation or deceive. Common attack methods include i communications interception, repeating, and deception.

Denial-of-Service Attack (DoS attack): A common network security attack that aims to make target systems or network resources unavailable, thereby preventing legitimate users from accessing or using those resources. Attacker $\mathcal{A}$ achieves the goal of denial of service by consuming the target system's resources, exhausting bandwidth, or causing system crashes.

In order to combat these malicious attacks within the scheme, a security model is defined and then evidence is presented to show that these attacks can be prevented, thereby ensuring the security of vehicle users' information.

4 Description of Our Scheme

The efficient cross-domain authentication framework proposed in our paper consists of two parts: Identity initialization and cross-domain authentication. Specifically, the identity initialization part includes system initialization and vehicle user registration, while the cross-domain authentication part

consists of anonymous cross-domain authentication and safe cross-domain authentication. In Table 1, we summarize some of the abbreviations and symbols used in this work.

Table 1: The notations used in our proposed

Symbol	Notation
E	Elliptic curve
G	Cyclic group
q	The order of G
P	The generator of G
H()	One way hash function
TA_i	The trust agency of domain i
Sk_{D_i}	The trust agency private key of domain i
Pk_{D_i}	The trust agency public key of domain i
$attr_i$	The i-th identity attribute of the vehicle
ID_i	The ID of vehicle
PW_i	The password of vehicle
$\oplus$	XOR operation
$\|\|$	OR operation

4.1 Identity Initialization

4.1.1 System Initialization

Let P be a sufficiently large prime number, Z_P^* be a finite field and $E\left(Z_P^*\right)$ be an elliptic curve over the finite field Z_P^* is defined, where its generator (base point) is denoted as g and the order of g is a sufficiently large prime p. Then let $H_1,\ H_2,\ H_3$ be three hash functions where are satisfying $H_1\colon \{0,\ 1\}^* \rightarrow Z_P^*,\ H_2\colon \{0,\ 1\}^* \rightarrow Z_P^*,\ H_3\colon \{0,\ 1\}^* \rightarrow \{0,1\}^l$, where l represents the bit size of P. Suppose there are N trust agencies $\{TA_1, TA_2, \ldots, TA_N\}$ form a consortium chain, and each TA_i acts as a registration server for a IoV domain D_i, here the corresponding key pair is represented as $\left(Sk_{D_i},\ Pk_{D_i}\right)$, where $i \in [1,\ \mathrm{N}]$ and $Sk_{D_i} \in E(Z_P^*), Pk_{D_i} = Sk_{D_i} \cdot g$. This public-private key pair is used for the signature process during interactions between entities. Given the resource-limited nature of IoV scenarios, the signature algorithm used in this paper is based on the Elliptic Curve Digital Signature Algorithm (ECDSA), which exploits the discrete logarithm problem on elliptic curves to achieve digital signatures.

Finally, during the registration and authentication phases in this paper, when an entity sends a message, the sender uses the Hash-based Message Authentication Code (HMAC) algorithm to calculate the authentication tag for the message to be sent. This algorithm uses a pre-shared key to calculate the message's authentication identifier, which is predetermined by the trust center and shared with vehicle users. Then vehicle users and TAs use the same HMAC algorithm (specifically HMAC-SHA256) to process messages to ensure that they are not tampered with or forged during transmission. if a signature algorithm is not used when the message is subsequently sent, it will be encrypted and sent using this algorithm by default for the integrity and authenticity of the message. The following provides a detailed introduction to the algorithm:

The HMAC-SHA256 algorithm is a message authentication code algorithm based on the SHA-256 hash function and a key. Its process includes key preparation, message padding, internal hash algorithm processing, key processing, combination of internal hash result and key, and rehashing. Through this process, the generated HMAC-SHA256 authentication code is used to verify the integrity and authenticity of the message, where the confidentiality and selection of the key are crucial.

4.1.2 Registration

Before accessing relevant servers, vehicle users must go through an identity registration process if they have not already registered. The trust agency first checks the identity data of the registered vehicles. If the vehicle information cannot be found on the chain, the registration process will continue. The specific steps of the registration process are described below:

Step 1: First, the vehicle V_i in the domain D_i submit the unique identity information ID_i to the trust agency TA_i, and sets its password character information PW_i. Subsequently, the process of calculating the Merkle hash tree root value of the vehicle's identity attribute set $\{attr_1,\ attr_2,\ \ldots, attr_N\}$, where $attr_1$ represents the identity ID_i, while the other identity attributes could include, for example, the vehicle owner's name, biometric information, auxiliary collected information, etc. Each vehicle user calculates a Merkle tree root value H_{attr} for the identity attribute information using the hash function H_1 according to the Merkle hash tree structure. Then, the process includes hiding the character information of the vehicle user's registration password and the current timestamp T is recorded, followed by the calculation of $W_i = H_1(PW_i||T)$. Finally, the message $mesg = \{ID_i,\ W_i,\ H_{attr}\}$ is transmitted to the TA via an RSU.

Step 2: Upon receiving the message, TA_i verifies it with the HMAC-SHA256 algorithm. If the verification is successful, it selects a random number $X_i \in E(Z_P^*)$ and records the current timestamp T_i, then sets N_i to represent the number of user registrations, which is initially set to 0. Next H_{attr} is written to a smart contract for subsequent verification, with the contract address uniquely identified as $ipfsAddr_{V_i}$. This is followed by the hash function H_2 is applied to get $A_i = H_2(ID_i||X_i)$ and $E_i = A_i \oplus W_i$, then I_i is computed by $I_i = H_2\{N_i||T_i||A_i\}$, and the trust agency stores $\{I_i,\ ipfsAddr_{V_i}\}$ on the IPFS node, where I_i servers as zero-knowledge proof evidence. Finally, the message $cred_i = \{X_i,\ E_i,\ T_i\}$ is sent to V_i via an RSU.

Step 3: Upon receiving $cred_i$, V_i verifies the integrity and authenticity of the message using the aforementioned algorithm. If successful, the obtained information is saved together as $CRED_i = \{ID_i,\ W_i,\ D_i,\ X_i,\ E_i,\ T_i\}$, which serves as the identity credential information for V_i. The pseudocode of the registration phase is shown below:

Pseudocode: Vehicle registration

Input: $ID_i,\ W_i,\ H_{attr}$
Output: true or false

```
1  Function Register(ID_i, W_i, H_attr)
2    if (verify(mesg) = True)
3      TA → ipfsAdd(H_attr)
4      IPFS ← I_i, ipfsAddr_{V_i}
5      TA → send{Enc(cred_i)}
6      V_i ← store(CRED_i)
7      return true;
```

(Continued)

Pseudocode (continued)

```
8     else return false;
9  end function
```

4.2 The Cross-Domain Authentication Scheme

The cross-domain authentication scenario is divided into anonymous cross-domain authentication and safe cross-domain authentication based on different efficiency and security requirements. The anonymous cross-domain authentication scheme is designed for efficient anonymous authentication, which is used when vehicles need to access publicly available information within the domain, such as nearby traffic conditions. On the other hand, the safe cross-domain authentication scheme is utilized when vehicles require access to tailored services that demand higher security levels. Specifically, In the former case, vehicles authenticate themselves anonymously using zero-knowledge proofs based on their identity credentials managed by the TA, enabling them to obtain basic road information services. In contrast, for the later, the authentication contract is deployed on the blockchain. By interacting with the blockchain, vehicle users achieve cross-domain authentication and thus access services with more higher security requirements. Below you will find detailed descriptions of both schemes. The overall scheme flowchart is shown in Fig. 2.

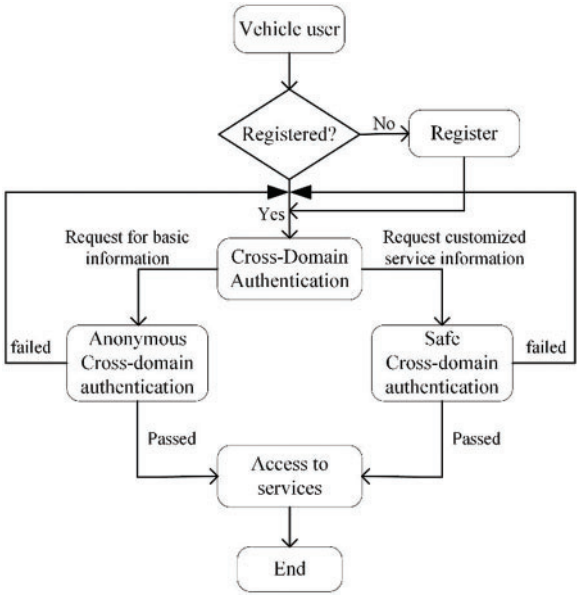

Figure 2: The overall scheme flowchart

4.2.1 Anonymous Cross-Domain Authentication Scheme

Anonymous cross-domain authentication primarily employs zero-knowledge proof technology. In the following, we provide a brief introduction to zero-knowledge proofs, zero-knowledge proof is a cryptographic technique that allows a prover to demonstrate the truth of a statement to a verifier without revealing any detailed information about the statement, except that it is indeed true. This type of proof ensures credibility while protecting privacy.

In this scheme, vehicle users achieve anonymous cross-domain identity verification by proving possession of a valid identity credential $CRED_i$ issued by the TA_i. If the verification is successful, the vehicle user can access the services provided by servers near the RSU to obtain the traffic situation information.

Specifically, in the anonymous authentication process, let us consider a scenario where a vehicle user V_i requires anonymous authentication at the trust agency TA_j. When V_i initiates a cross-domain access request, TA_j must check V_i' identity. The process of the specific scheme is described as follows:

Step 1: Vehicle anonymous proof generation

To first address the potential issue of repeated anonymous proofs, this paper proposes that the trust agency TA_i periodically publishes a nonce value R to IPFS to prevent this problem. Then V_i obtains the public verification key $PV_F = \{N_i,\ T_i\}$ from IPFS and calculates $A_i = E_i \oplus W_i$. Subsequently, V_i compute the zero-knowledge proof evidence π_z according to formula (1) below. Finally, $\{\pi_z,\ D_i\}$ is transmitted to TA_j via an RSU.

$$\pi_z = H_3\{N_i||T_i||A_i||D_i||D_j||R\} \tag{1}$$

Step 2: Anonymous verification process

Upon receiving the message π_z from the vehicle V_i, the TA_j first retrieves the zero-knowledge proof evidence I_i and the currently published nonce value R from IPFS. These parameters are then used to calculate $\pi_z^{'}$ according to formula (2) below:

$$\pi_z^{'} = H_3\{I_i||D_j||D_i||R\} \tag{2}$$

Then the TA_j determines whether $\pi_z = \pi_z^{'}$ holds. If this is the case, the verification is successful and V_i completes the authentication. Otherwise, the verification will fail. During the whole process, the vehicle user only needs to provide the zero-knowledge proof and the vehicular networking domain information, without revealing any other information, thus ensuring anonymity. The following is the pseudocode of the anonymous verification process:

Pseudocode: Anonymous cross domain authentication

Input: $PV_F,\ D_i,\ R$
Output: true or false

```
Function Anonymous(PV_F, D_i, R)
    V_i → compute(A_i, π_z)
    V_i → send({π_z, D_i})
    TA_j → compute{π_z'}
    if(π_z ≠ π_z') return false;
    else return true;
end function
```

4.2.2 Safe Cross-Domain Authentication Scheme

For applications or services with higher security requirements, stricter vehicle users authentication is required in cross-domain scenarios. Otherwise, there could be security risks. This imposes higher demands on the confidentiality and security of identity authentication.

In particular, unlike anonymous cross-domain authentication, verification of other registered attributes is required for the vehicle's identity attribute set $\{attr_1,\ attr_2, \ldots, attr_N\}$. In addition, since

the vehicle user's identity attribute set is autonomously controlled by the user, ensuring the credibility of the user identity information requires the consistency between on-chain and off-chain identity information on the blockchain to complete safe authentication. Considering the transparency of the blockchain and excluding directly. uploading identity information to the chain, we defined a three-layer Merkle hash tree. This structure is used to store the hash values of the vehicle user's identity attributes, to ensure the consistency of blockchain information and meet the security requirements of this scheme. Specifically, each vehicle user identity attribute serves as a leaf node in the Merkle tree, and ultimately a Merkle hash tree root is calculated. This ensures that attackers cannot access the vehicle user's identity information and thus ensures the security of their identity attributes. When a vehicle user V_i requesting access to services that require higher security authentication, the specific authentication process is as follows:

Step 1: $V_i \rightarrow TA_j$: $\{request\}$

The cross-domain vehicle user requests access to services provided by nearby RSUs by sending a $\{request\}$ message.

Step 2: $TA_j \rightarrow V_i$: $Enc_{Sk_{D_j}}\{request(attr_1)\}$

Upon receiving the request message from V_i, TA_j verifies the message using the HMAC-SHA256 algorithm. To enhance security, the trust center sends information about the vehicle's identity attribute $request(attr_1)$ which encrypted with the private key Sk_{D_j} and signs the message before transmitting it to the vehicle user through the RSU.

Step 3: $V_i \rightarrow TA_j$: $msg\{attr_1,\ H'_{attr}\}$

After receiving messages and signatures from the Trust Center, vehicle users verify the signatures using the public key Pk_{D_j}. If verification is successful, it computes a Merkle hash tree root value H'_{attr} using all identity attributes. Subsequently, the message $msg\{attr_1,\ H'_{attr}\}$ is transmitted to the Trust Center via RSU.

Step 4: TA_j: $H_{attr} = H'_{attr}$ *is true or false*

After receiving the message msg, TA_j verifies the message using the above algorithm. If the verification is successful, it is based on $attr_1$ to find the unique address of the smart contract generated during registration $ipfsAddr_{V_i}$. Subsequently, it retrieves the Merkle hash tree root value H_{attr} from the smart contract. Then it compares the H'_{attr} from the message with H_{attr}. If they are equal, the verification is successful; otherwise, it fails.

The following is the main pseudocode of safe cross-domain authentication:

Pseudocode: Safe cross domain authentication

Input: $attr_1,\ H'_{attr},\ ipfsAddr_{V_i}$
Output: true or false
Input: $attr_1,\ H'_{attr},\ ipfsAddr_{V_i}$
Output: true or false
1 **Function** Safe($attr_1,\ H'_{attr},\ ipfsAddr_{V_i}$)
2 $TA_j \rightarrow$ request($attr_1$)
3 $V_i \rightarrow$ send($\{attr_1,\ H'_{attr}\}$)
4 TA $\rightarrow$ find($ipfsAddr_{V_i}$)
5 TA $\rightarrow$ getByIPFSAddr(H_{attr})

(Continued)

Pseudocode (continued)

```
6     if(H_attr ≠ H'_attr) return false;
7     else return true;
8  end function
```

5 Security Analysis

We assume that the attacker $\mathcal{A}$ has the following capabilities:

- $\mathcal{A}$ can attack nodes on IPFS or the blockchain but cannot control more than 51% of the nodes in the entire network.
- $\mathcal{A}$ can monitor, tamper with, and forge data streams from vehicle users.

We also assume two basic premises:

(1) It is assumed that the one-way hash function used is secure, meeting its design goals such as irreversibility, collision resistance.
(2) Zero-knowledge proofs allow the prover to prove the truth of a statement to the verifier without revealing any other information about the statement.

Next, we will demonstrate how this cross-domain authentication scheme can resist the adversary's attack methods, namely forgery attacks, replay attacks, and denial of service attacks.

If attacker $\mathcal{A}$ attempts a forgery attack, in the case of anonymous cross-domain authentication, $\mathcal{A}$ needs to complete the authentication process by calculating the public verification key PV_F, A_i and π_z. However, due to the characteristics of the hash function according to assumption (1), it is impossible to forge W_i and compute A_i. Furthermore, according to assumption (2), zero-knowledge proofs allow the prover to prove the truth of a statement without revealing any other information about the statement. Therefore, $\mathcal{A}$ cannot forge π_z. Consequently, attacker $\mathcal{A}$ cannot complete cross-domain authentication by forging identities.

When attacker $\mathcal{A}$ uses a replay attack, in anonymous cross-domain authentication, since the TA periodically sends a nonce value R to IPFS nodes, and both the vehicle user and the TA use the same HMAC algorithm (HMAC-SHA256) to process messages, according to assumption (1), the possibility of cracking this algorithm is negligible. This ensures the integrity and authenticity of messages, thus mitigating against replay attacks. In the case of safe cross-domain authentication, if attacker $\mathcal{A}$ attempts to intercept crucial information from vehicles, they would need to forge the message $request(attr_1)$. However, since the TA uses the Elliptic Curve Digital Signature Algorithm (ECDSA) to process this message, it is impossible for $\mathcal{A}$ to forge the signature due to the properties of this algorithm. Therefore, safe cross-domain authentication is also resistant to replay attacks. In summary, both anonymous and safe cross-domain authentication can mitigate replay attacks.

Finally, as far as denial-of-service attacks (DDoS) are concerned, the cross-domain authentication scheme proposed in this paper leverages blockchain technology. The blockchain network consists of numerous widely distributed nodes. Therefore, attackers find it difficult to attack all nodes simultaneously, especially considering that their locations and topologies are usually unknown. This distributed nature reduces the likelihood of an attacker successfully launching a DDoS attack. Additionally, the consensus mechanism in blockchain requires nodes in the network to validate and verify transactions before consensus is reached. This means that attackers would need to control more than 51% of nodes to successfully manipulate or prevent transaction confirmations, further reducing the risk of DDoS

attacks. In summary, the distributed architecture used in this paper effectively mitigates the risk of DDoS attacks.

6 Performance Evaluation

In this section, we utilized Ethereum to implement the smart contract portion of the solution and tested the time overhead required for deploying the smart contract. Subsequently, we conducted further experiments on a desktop computer running the 64-bit Windows 10 operating system with an Intel(R) Core (TM) i5-10400F CPU @ 2.90 GHz. We employed OpenSSL and the C++ Chrono library to compare and analyze the computational, communication, and storage overheads of the proposed solution outlined in this paper. The software packages utilized include VS. Code, the Geth client, the Remix compiler, among others.

Next, we introduce the parameters used in the experiment. We adopt the SHA-256 hash algorithm and utilizes the elliptic curve secp256k1. The construction of zero-knowledge proof in this paper is as follows:

(1) $(PE_F,\ PV_F) \leftarrow \textbf{\textit{KeyGen}}(Fun,\ 1^{\lambda})$. This algorithm generates zero-knowledge proof keys based on the predefined function *Fun* and security parameter λ. The keys include a public evaluation key PE_F and a public verification key PV_F.

(2) $(z,\ \pi_z) \leftarrow \textbf{\textit{Solve}}(PE_F,\ x,\ y)$. The prover calculates the proof using the public evaluation key PE_F, the public reference input x provided by the verifier, and the private input y. The output is $z \leftarrow Fun(x,\ y)$ and the correctness proof π_z.

(3) $\{0,\ 1\} \leftarrow \textbf{\textit{Verify}}(PV_F,\ x,\ z,\ \pi_z)$. The verifier checks the result z and its proof π_z using the public verification key PV_F and the public reference input x. The verification algorithm outputs 1 (true) only if $Fun(x,\ y) = z$, otherwise 0 (false).

6.1 Computational Overhead

In this section, we provided the details on implementing smart contracts developed using Solidity syntax. The smart contract code was written, compiled, debugged, and deployed using the online Remix IDE. In this study, three smart contracts were used: One for registration, one for anonymous cross-domain authentication, and one for safe cross-domain authentication. Deploying smart contracts requires a certain time cost, and in our Ethereum test environment, a single a smart contract invocation typically took 6 to 7 ms. Therefore, we used an average value of 6.5 ms for subsequent smart contract computational cost calculations in this paper.

Next, we analyzed the computational cost during the registration phase of the proposed scheme. In this phase, the basic operations include hash functions, XOR operations, concatenation, ECC multiplication, and comparisons. However, XOR operations, concatenation, and comparisons can be considered negligible compared to other operations. For the one-way hash function $H(\cdot)$ and ECC multiplication operations, the average latency was measured using OpenSSL and the C++ Chrono library (C++11 standard library). After several measurements, it was found that the average latency for the hash function was 1.563 ms, while for the ECC multiplication it was 3.108 ms.

In the vehicle user registration phase, after calculating the cost of the hash function H(·) and ECC multiplication used in this scheme, the computational cost of the vehicle user registration phase is $T_{Reg} = 12.468$ ms. Then we analyzed the latency during the cross-domain authentication phase. From the cross-domain steps, we can infer that the computational cost for anonymous cross-domain

authentication is approximately $T_{anonymous} \approx 9.342$ ms, and for safe cross-domain authentication, is approximately $T_{safe} \approx 24.9$ ms.

Due to the utilization of smart contract technology in this study, the time overhead of smart contracts is taken into account. Considering the inherent latency of communicating on the same public chain test network, in the anonymous cross-domain authentication phase, a smart contract is invoked once to retrieve relevant data; While in the safe cross-domain authentication phase, the trust center invokes smart contract once to obtain the Merkel hash root value. Consequently, the total computational costs for each phase are shown in Table 2 below.

Table 2: The total computational costs for each phase

	T_{Reg}/ms	T_{Auth}/ms
[29]	17.139	59.178
[30]	14.031	32.679
[31]	10.941	79.533
[32]	*NULL*	48.291
CAIoV-I	12.468	15.842
CAIoV-II	12.468	31.4

Finally, we compare the computational overhead between the CAIoV scheme and other authentication schemes mentioned in [29–32]. Here, T_{Reg} denotes the total time overhead of the registration phase, and T_{Auth} represents the total time for the vehicle authentication process. The comparative results are illustrated in Fig. 3, which provides a detailed comparison of the computational overhead of each part of our proposed scheme with other schemes. It can be observed that in the proposed scheme, both the anonymous cross-domain authentication and safe cross-domain authentication phases exhibit significantly lower computational overhead compared to other schemes. Furthermore, in the anonymous authentication process, due to the use of zero knowledge proof technology, the number of message interactions during the authentication process is relatively low, and the relevant cryptographic calculations are also relatively few, resulting in the lowest computational cost in this stage; For safe cross domain authentication, due to the need for more message interaction and more encryption and decryption operations, it requires more computational overhead. But compared to other schemes, the additional computational overhead is also acceptable. This indicates that the CAIoV scheme has relatively small computational overhead, making it suitable for IoV where computational resources are limited.

6.2 Communication Overhead

For the communication overhead, the settings in this paper are as follows: The timestamp is 16 bits; For message signatures, the paper uses ECDSA signatures on the secp256k1 curve, resulting in a signature length of 512 bits; For the message verification code sent during the transmission of the entity message, the paper employs the HMAC algorithm, with an authentication tag size of 256 bits; for the hash functions H_1, H_2 and H_3 used in this paper, This article uses the SHA-256 algorithm, resulting in a fixed bit string length of 256 bits. The communication effort is compared through specific calculations.

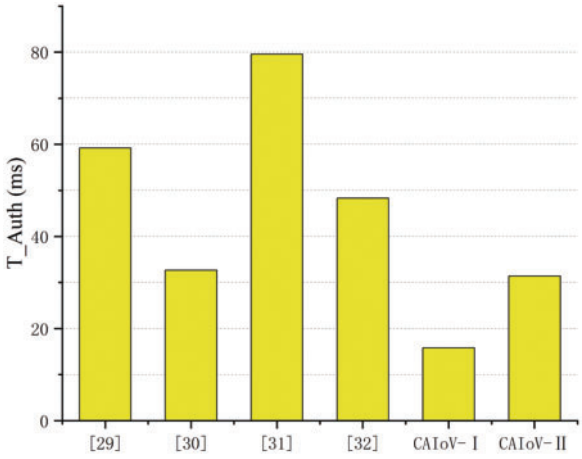

Figure 3: The comparison of computational costs

First, let's analyze the registration phase. The vehicle user needs to send a message, record a timestamp and perform two hash operations; while the trust center needs to send a message, record a timestamp and also perform two hashing operations. Therefore, the total communication overhead in the registration phase is 1568 bits. For anonymous cross-domain authentication, the vehicle user needs to send a message and perform a hash operation, while the trust center needs to send a message and perform a hash operation. Thus, the communication overhead for the anonymous cross-domain authentication level is 1024 bits. Finally, with safe cross-domain authentication, the message size is larger because the authentication methods required are more complex. Specifically, the vehicle user needs to send two messages and perform a hash operation, while the trust center needs to send a message, sign the message and perform two hash operations. The total communication effort is 2048 bits.

In Table 3, this paper compares the communication overhead between the proposed scheme and various related authentication schemes. It primarily compares the communication overhead during the registration phase, denoted as C_{Reg}, and during the authentication stage, denoted as C_{Auth}. C_{Reg} represents the total communication overhead during the registration process based on the previously mentioned fixed communication amounts, while C_{Auth} represents the entire communication overhead during the authentication process.

Table 3: The comparison of communication costs

	[29]	[30]	[31]	[32]	CAIoV-I	CAIoV-II
$C_{Reg}/bits$	1688	2160	1328	*NULL*	1568	1568
$C_{Auth}/bits$	3392	2176	2320	1920	1024	2048

The comparison of communication costs during the authentication phase is shown in Fig. 4. It can be seen that the communication overhead of the anonymous cross-domain authentication scheme proposed by our scheme is much lower compared to other schemes. In addition, the communication overhead of the safe cross-domain authentication scheme is also lower compared to the schemes [29–31], but slightly higher compared to [32]. Considering that the latter scheme [32] requires significantly more computational effort, the communication overhead of this article's scheme remains

comparatively low. In addition, the security level of this scheme is much higher than that of the scheme [31]. Therefore, the proposed scheme is efficient and secure despite a slight increase in communication overhead.

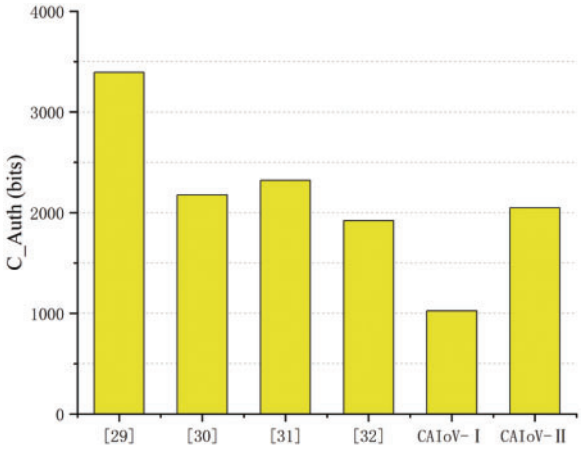

Figure 4: The comparison of communication costs

6.3 Storage Overhead

For storage overhead, we initially tested the storage performance of our proposed solution as the number of Merkle tree leaf nodes increases. As shown in Fig. 5, it can be observed that the time taken to store data on IPFS slightly increases with the increase in the number of Merkle tree leaf nodes. However, the time remains quite small, the storage performance of our solution exhibits minimal fluctuations even with increasing data volume. To obtain a more specific assessment of the storage performance of our solution, we analyzed the sizes of data stored at various stages for vehicle users in the proposed solution.

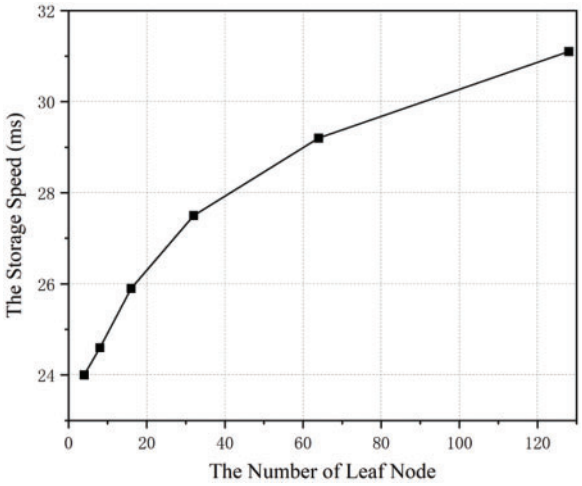

Figure 5: The IPFS storage speed

In exploring the storage costs for vehicle users in our scheme, we define the storage overhead costs as follows: the SHA-256 hash digest is 32 bytes, the timestamp length is 2 bytes, the vehicle identity

and address information are 8 bytes, and the random number and domain information are defined as 4 bytes.

In the registration phase of the proposed scheme, vehicle user ultimately needs to store the credential $CRED_i = \{ID_i,\ W_i,\ D_i,\ X_i,\ E_i,\ T_i\}$. Specifically, ID_i occupies 8 bytes, W_i and E_i occupy 32 bytes respectively, T_i occupies 2 bytes, D_i and X_i each occupy 4 bytes. Therefore, the total storage cost S_{Reg} for the registration phase is 82 bytes.

In the anonymous cross-domain authentication phase, the vehicle user needs to store the zero-knowledge proof evidence $\pi_z = H_2\{N_i||T_i||A_i \oplus Nym_i\}$, which totals 32 bytes. In the safe cross-domain authentication phase, the vehicle user needs to store Pk_{D_i}, $ipfsAddr_{V_i}$ and the hash digest of identity attributes. Specifically, Pk_{D_i} and $ipfsAddr_{V_i}$ occupy 8 bytes each, while the hash digest occupies 32 bytes, totaling 48 bytes.

In Fig. 6, we compared the storage cost of our proposed scheme with other schemes in the registration and authentication phases. It is observed that our proposed system incurs lower storage cost in the registration phase compared to other systems. In addition, the anonymous cross-domain authentication scheme only requires identity credentials to be stored, resulting in minimal memory consumption. Likewise, the memory resources consumed by the safe cross-domain authentication scheme are less compared to other schemes. In addition, our scheme has advantages in terms of computing and communication costs, and vehicle nodes do not require excessive storage space. Therefore, the CAIoV scheme proposed in this paper is extremely efficient.

Figure 6: The comparison of storage costs

7 Conclusion

To tackle the challenges of cross-domain authentication in the current IoV, we propose a blockchain-based efficient cross-domain authentication scheme for IoV (CAIoV). Built upon traditional cross-domain authentication schemes, it is tailored to the requirements of cross-domain scenarios in IoV. It incorporates technologies such as zero-knowledge proofs, Merkle trees, and smart contracts. The scheme is divided into anonymous cross-domain and safe cross-domain to meet the demands of low-latency and high-quality connections in IoV environments. Finally, we conduct

comparative analyses of the scheme's performance in terms of computational costs, communication overheads, and data storage expenses. The results demonstrate that the CAIoV scheme is highly efficient, secure, and incurs low storage costs, making it well-suited for deployment in contemporary cross-domain scenarios within IoV.

Acknowledgement: We express our gratitude to the participants who generously dedicated their time and effort to contribute to our study. We also extend our appreciation to the funding agency for providing the necessary resources for conducting this research. Finally, we acknowledge the anonymous reviewers whose insightful comments and suggestions significantly enhanced the quality of this manuscript.

Funding Statement: This work is supported by the National Natural Science Foundation of China (62362013) and the Guangxi Natural Science Foundation (2023GXNSFAA026294).

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Hongtao Ding, Feng Zhao, Chunhai Li, Guoling Liang, Zhaoyu Su, Changsong Yang; data collection: Hongtao Ding; analysis and interpretation of result: Hongtao Ding; draft manuscript preparation: Hongtao Ding, Chunhai Li, Changsong Yang. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: Data will be available upon request.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] M. A. Ferrag *et al.*, "Blockchain technologies for the internet of things: Research issues and challenges," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 2188–2204, Apr. 2019. doi: 10.1109/JIOT.2018.2882794.

[2] P. Zhu, J. Hu, X. Li, and Q. Zhu, "Using blockchain technology to enhance the traceability of original achievements," *IEEE Trans. Eng. Manage.*, vol. 70, no. 5, pp. 1693–1707, May 2023. doi: 10.1109/TEM.2021.3066090.

[3] S. M. Hussain, K. M. Yosof, and S. A. Hussain, "Interoperability issues in internet of vehicles—A survey," presented at the 2018 Proc. 3rd Int. Conf. Contemp. Comput. Informat. (IC3I), Gurgaon, India, Oct. 10–12, 2018.

[4] C. Chen, B. Xiang, Y. Liu, and K. Wang, "A secure authentication protocol for internet of vehicles," *IEEE Access*, vol. 7, pp. 12047–12057, Jan. 2019. doi: 10.1109/ACCESS.2019.2891105.

[5] C. Hu, C. Zhang, D. Lei, T. Wu, X. Liu and L. Zhu, "Achieving privacy-preserving and verifiable support vector machine training in the cloud," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 3476–3491, Jun. 2023. doi: 10.1109/TIFS.2023.3283104.

[6] C. Zhang, X. Luo, J. Liang, X. Liu, L. Zhu and S. Guo, "POTA: Privacy-preserving online multi-task assignment with path planning," *IEEE Trans. Mob. Comput.*, vol. 23, no. 5, pp. 5999–6011, May 2024. doi: 10.1109/TMC.2023.3315324.

[7] Z. Wang *et al.*, "FRNet: An MCS framework for efficient and secure data sensing and privacy protection in IoVs," *IEEE Internet Things J.*, vol. 10, no. 18, pp. 16343–16357, Sep. 2023. doi: 10.1109/JIOT.2023.3267782.

[8] C. Li *et al.*, "Anonymous and traceable authentication for securing data sharing in parking edge computing," *Peer-to-Peer Networking Appl.*, vol. 14, no. 4, pp. 2099–2114, May 2021. doi: 10.1007/s12083-021-01104-7.

[9] C. Zhang, M. Zhao, J. Liang, Q. Fan, L. Zhu and S. Guo, "NANO: Cryptographic enforcement of readability and editability governance in blockchain databases," *IEEE Trans. Dependable Secur. Comput.*, pp. 1–14, Nov. 2023. doi: 10.1109/TDSC.2023.3330171.

[10] B. Cao *et al.*, "When internet of things meets blockchain: Challenges in distributed consensus," *IEEE Netw.*, vol. 33, no. 6, pp. 133–139, Nov. 2019. doi: 10.1109/MNET.2019.1900002.

[11] W. Yuan, X. Li, M. Li, and L. Zheng, "Dynamic cross-domain authentication scheme using group signature in IoT," *Appl. Sci.*, vol. 13, no. 10, pp. 5847, Apr. 2023. doi: 10.3390/app13105847.

[12] 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 Things J.*, vol. 4, no. 6, pp. 1832–1843, Dec. 2017. doi: 10.1109/JIOT.2017.2740569.

[13] C. Zhang, M. Zhao, W. Zhang, Q. Fan, J. Ni and L. Zhu, "Privacy-preserving identity-based data rights governance for blockchain-empowered human-centric metaverse communications," *IEEE J. Sel. Areas Commun.*, vol. 42, no. 4, pp. 963–977, Apr. 2024. doi: 10.1109/JSAC.2023.3345392.

[14] F. Song, J. Liang, C. Zhang, Z. Fu, Z. Qin and S. Guo, "Achieving efficient and privacy-preserving location-based task recommendation in spatial crowdsourcing," *IEEE Trans. Dependable Secur. Comput.*, vol. 20, no. 5, pp. 4245–4257, Dec. 2023. doi: 10.1109/TDSC.2023.3342239.

[15] C. Zhang, W. Wang, W. Zhang, J. Nie, J. Liang and L. Zhu, "Achieving distributed and privacy-preserving cross-chain transactions in account-model blockchain systems," presented at the 2023 IEEE Int. Conf. Metaverse Comput. Netw. Appl., Kyoto, Japan, Jun. 26–28, 2023. doi: 10.1109/MetaCom57706.2023.00060.

[16] T. Khan *et al.*, "Certificate revocation in vehicular ad hoc networks techniques and protocols: A survey," *Sci. China Inf. Sci.*, vol. 60, no. 100301, pp. 380, Sep. 2017. doi: 10.1007/s11432-017-9203-x.

[17] S. Khan *et al.*, "Survey on issues and recent advances in vehicular public-key infrastructure (VPKI)," *IEEE Commun. Surv. Tutorials*, vol. 24, no. 3, pp. 1574–1601, May 2022. doi: 10.1109/COMST.2022.3178081.

[18] W. Wang *et al.*, "A triple real-time trajectory privacy protection mechanism based on edge computing and blockchain in mobile crowdsourcing," *IEEE Trans. Mob. Comput.*, vol. 22, no. 10, pp. 5625–5642, Jun. 2022. doi: 10.1109/TMC.2022.3187047.

[19] S. M. Karim, A. Habbal, S. A. Chaudhry, and A. Irshad, "BSDCE-IoV: Blockchain-based secure data collection and exchange scheme for IoV in 5G environment," *IEEE Access*, vol. 11, pp. 36158–36175, Apr. 2023. doi: 10.1109/ACCESS.2023.3265959.

[20] J. Zheng, X. Wang, Q. Yang, W. Xiao, Y. Sun and W. Liang, "A blockchain-based lightweight authentication and key agreement scheme for internet of vehicles," *Connect. Sci.*, vol. 34, no. 1, pp. 1430–1453, May 2022. doi: 10.1080/09540091.2022.2032602.

[21] Z. Xu, W. Liang, K. Li, J. Xu, and H. Jin, "A blockchain-based roadside unit-assisted authentication and key agreement protocol for internet of vehicles," *J. Parallel Distrib. Comput.*, vol. 149, pp. 29–39, Mar. 2021. doi: 10.1016/j.jpdc.2020.11.003.

[22] J. Chen, Z. Zhan, and F. Liu, "XAuth: Efficient privacy-preserving cross-domain authentication," *IEEE Trans. Dependable Secur. Comput.*, vol. 19, no. 5, pp. 301–331, Jun. 2022. doi: 10.1109/TDSC.2021.3092375.

[23] H. Zhang, X. Chen, X. Lan, H. Jin, and Q. Cao, "BTCAS: A blockchain-based thoroughly cross-domain authentication scheme," *J. Inf. Secur. Appl.*, vol. 55, no. 102538, pp. 1567–4223, Dec., 2020. doi: 10.1016/j.jisa.2020.102538.

[24] J. Zhang *et al.*, "A blockchain-based cross domain authentication scheme in edge computing environment," presented at the 2023 IEEE 13th Int. Conf. Electron. Inf. Emerg. Commun., Beijing, China, Jul. 14–16, 2023. doi: 10.1109/ICEIEC58029.2023.10201164.

[25] C. Huang, L. Xue, D. Liu, X. Shen, W. Zhuang and R. Sun, "Blockchain-assisted transparent cross-domain authorization and authentication for smart city," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17194–17209, Feb. 2022. doi: 10.1109/JIOT.2022.3154632.

[26] G. Li, Y. Wang, B. Zhang, and S. Lu, "Smart contract-based cross-domain authentication and key agreement system for heterogeneous wireless networks," *Mobile Inf. Syst.*, vol. 2020, pp. 2964562, Sep. 2020. doi: 10.1155/2020/2964562.

[27] X. Jia *et al.*, "IRBA: An identity-based cross-domain authentication scheme for the internet of things," *Electronics*, vol. 9, no. 4, pp. 634, Apr. 2020. doi: 10.3390/electronics9040634.

[28] C. Feng, B. Liu, Z. Guo, K. Yu, Z. Qin and K. Choo, "Blockchain-based cross-domain authentication for intelligent 5G-enabled internet of drones," *IEEE Internet Things J.*, vol. 9, no. 8, pp. 6224–6238, Apr. 2022. doi: 10.1109/JIOT.2021.3113321.

[29] X. Xie, B. Wu, and B. Hou, "BEPHAP: A blockchain-based efficient privacy-preserving handover authentication protocol with key agreement for internet of vehicles," *J. Syst. Archit.*, vol. 138, no. 102869, May 2023. doi: 10.1016/j.sysarc.2023.102869.

[30] M. Eddine, M. Ferrag, O. Friha, and L. Maglaras, "EASBF: An efficient authentication scheme over blockchain for fog computing-enabled internet of vehicles," *J. Inf. Secur. Appl.*, vol. 59, no. 102802, Jun. 2021. doi: 10.1016/j.jisa.2021.102802.

[31] H. Vasudev, D. Das, and A. Vasilakos, "Secure message propagation protocols for IoVs communication components," *Comput. Electr. Eng.*, vol. 82, no. 106555, Mar. 2020. doi: 10.1016/j.compeleceng.2020.106555.

[32] M. N. Aman, U. Javaid, and B. Sikdar, "A privacy-preserving and scalable authentication protocol for the internet of vehicles," *IEEE Internet Things J.*, vol. 8, no. 2, pp. 1123–1139, Jan. 2021. doi: 10.1109/JIOT.2020.3010893.