IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received 13 May 2024, accepted 8 July 2024, date of publication 11 July 2024, date of current version 22 July 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3426668

RESEARCH ARTICLE

A Secure and Efficient Multi-Dimensional Perception Data Aggregation in Vehicular Ad Hoc Networks

RUICHENG YANG AND GUOFANG DONG, (Member, IEEE)
School of Electrical Information Technology, Yunnan Minzu University, Kunming, Yunnan 650500, China
Yunnan Key Laboratory of Unmanned Autonomous System, Kunming 650504, China

Corresponding author: Guofang Dong (yangruichengy@163.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61662089, and in part by Yunnan Minzu University Graduate Research Innovation Fund Project under Grant 2024SKY121.

ABSTRACT In vehicular ad hoc networks (VANETs), data aggregation is pivotal as it consolidates data from multiple vehicles for further analysis. Malicious users may launch attacks during the aggregation process to threaten the security and privacy of vehicles. Therefore, it is essential to ensure the security of vehicle data aggregation in vehicular networks. In order to deal with the security risks and challenges related to data aggregation in VANETs, this paper proposes a secure and efficient multi-dimensional perception data aggregation solution. The proposed solution integrates cloud computing with blockchain, presenting a blockchain-based data aggregation system for vehicular networks, enabling efficient and secure data collection and analysis tasks. This solution utilizes an enhanced Paillier cryptosystem to protect location privacy when aggregating sensor data. Additionally, it constructs multi-dimensional sensor data from different locations. A central control centre can fully recover and analyze the aggregated data results. The security analysis has demonstrated the security and effectiveness of the solution, while the performance evaluation has verified that the solution incurs low computational and communication overheads.

INDEX TERMS Data aggregation, privacy protection, blockchain, vehicular ad-hoc networks, security risks.

I. INTRODUCTION

The rapid development of wireless communication and Internet of Things (IoT) [1] technologies has propelled the evolution of traditional VANETs into the realm of Connected Vehicles (CV) [1]. In recent years, there has been significant interest and attention in the autonomous interaction between Roadside Units (RSUs) and vehicles within VANETs, eliminating the need for manual intervention [2]. Within the Connected Vehicles framework, each vehicle utilizes onboard devices to collect driving information and share it with other vehicles and RSUs, enhancing traffic efficiency and mitigating potential traffic incidents [3]. For instance, in the case of a traffic accident on a highway, nearby vehicles can promptly gather information and disseminate it, ensuring traffic safety.

The rapid advancement of in-vehicle technology has given rise to numerous automotive applications [4], and one notable development is the integration of cloud computing technology with VANETs, forming what is known as "vehicular cloud" [5]. As widely recognized, cloud computing ultimately provides users with a virtual resource pool, wherein multiple distributed servers are interconnected through the internet to offer various cloud services. Simultaneously, by accessing the cloud remotely, vehicle users can enjoy benefits such as unlimited storage space [6], robust computational capabilities, and internet entertainment services [7]. Utilizing VANETs allows vehicles on the road to establish connections with nearby vehicles and Roadside Units (RSUs) through their communication modules [8], [9], thereby facilitating the exchange of perception data.

The associate editor coordinating the review of this manuscript and approving it for publication was Cesar Vargas-Rosales.

In such a system, each vehicle is equipped with various sensors [10]. The numerous advantages mentioned above make establishing a ''vehicular cloud'' feasible [11]. This configuration enables vehicles to upload collected perception data to the terminal and access various services through VANETs [12]. Because multiple vehicles and RSUs can achieve seamless communication, the ''vehicular cloud'' introduces numerous potential applications, including but not limited to video surveillance, traffic management, real-time navigation, remote traffic management, and road monitoring [13]. However, as the number of applications increases, it also brings significant security issues.

Privacy is a crucial security concern in VANETs. Users inevitably attach sensitive information when uploading vehicle data, including personal details and travel trajectories [14], [15]. Unauthorized users may exploit this information for illegal activities, posing threats [16], [17]. A combination of anonymous communication and traceability is essential to address this issue. In the event of a crime or accident, trustworthy authorities should be able to identify the party responsible for the incident [18]. For instance, in cases where unauthorized individuals send false messages, leading to accidents, authorities need to trace the unauthorized sender and take necessary enforcement actions.

In recent years, security in VANETs has once again garnered widespread attention due to frequent incidents involving vehicle safety [19]. Although existing privacy-preserving schemes have secure encryption algorithms and can guarantee different functions separately, most encryption secret algorithms are related to bilinear pairing, which leads to overheads that cannot be reduced. Moreover, the existing schemes cannot ensure the computational overhead is within acceptable limits while collecting multidimensional data or cannot simultaneously satisfy the problems of location privacy and resisting collusion attacks, which reflects their limitations. Therefore, to address these problems, this paper proposes a new scheme which can make up for some of the limitations with the following contributions:

1) This paper proposes a data collection scheme to ensure the secure upload of perception data in VANETs. This scheme enables vehicles to collect multi-dimensional perception data in different locations, forming a composite database, thus achieving communication and computational resource savings. RSUs in the system perform composite data report statistics, safeguarding data privacy and calculating the amount of data uploaded in each segment. Additionally, the results of perception data aggregation can be searched and analyzed at the control centre.

2) A secure and efficient multi-dimensional perception data aggregation scheme has been designed by combining blockchain, the Chinese Remainder Theorem, and a modified Paillier cryptosystem. This scheme significantly improves over existing data aggregation approaches, eliminating the need for bilinear pairings. With high security and efficient utilization of local resources, it can assist in achieving secure and efficient data acquisition and analysis tasks in VANETs.

3) Through in-depth security analysis, the proposed scheme is validated for security aspects such as data integrity, location privacy, and resistance against collusion attacks. Performance evaluation demonstrates that the solution proposed in this paper can significantly reduce computational and communication costs compared to secure data aggregation protocols.

II. RELATED WORK

Few location verification schemes can effectively protect the privacy of the verifier's location. This is because verifiers, when requesting location services, attempt to prove their presence in a specific location or area. Therefore, many scholars have proposed secure encryption protocols. Reference [20] introduces a secure protocol capable of preserving location privacy and, based on this, develops a more advanced encryption protocol utilizing location verification. This involves constructing a location-based key exchange where, if the verifier is within the declared area, they share a unified key with other verifiers. Homomorphic encryption algorithms, a popular research direction, have also been applied to security protocols. Reference [21] Introduce a Homomorphic and Circular Shift-based Encryption Protocol (CSEP). CSEP uses homomorphic encryption to encrypt user locations, while Location-Based Services (LBS) servers in vehicular networks use ciphertext to calculate distances. Reference [22] employs an ElGamal-based homomorphic encryption protocol, where clients use a semantically secure ElGamal encryption scheme to encrypt the coordinates of their locations. Furthermore, Reference [23] suggests a privacy protection approach for location information utilizing random encryption periods. When vehicles need to change certificates, a random encryption interval [23] is initiated, using a shared key to encrypt their information, creating an encrypted zone around the vehicles.

Cui et al. [24] proposed an efficient CLAS scheme for vehicular sensor networks with conditional privacy protection in a novel CLS scheme. They asserted that their plan was proven to be secure and could prevent existential forgery under an adaptive chosen message attack. However, Li et al. [25] demonstrated its insecurity, pointing out that this certificateless aggregate signature scheme [24] is susceptible to a malicious yet passive critical generation centre attack. Additionally, these schemes are related to the bilinear pairing method, hence incurring substantial computational costs.

Furthermore, Liu et al. [35] proposed a new TCEMD model that can disseminate emergency information with nearby vehicles and guarantees effectiveness against malicious attacks. Then, Cheng et al. [36] proposed a privacy-preserving scheme PPRM for MCS, which protects the user's location privacy and guarantees lightweight. Meanwhile, Cheng et al. [36] proposed the TFRU scheme to improve the accuracy and efficiency of reputation value updates and ensure security. Next, Liu et al. [37] proposed the PPRU scheme, which has a secure confidentiality feature and better achieves reputation updates while reducing computation and communication overheads, in addition to its security against Sybil attacks.

III. PRELIMINARIES

A. BLOCKCHAIN

Blockchain is connected in chronological order based on the creation time of blocks, and it is similar to a decentralized peer-to-peer (P2P) database [26], aiming to offer distributed solutions for a broad spectrum of applications in the IoT and VANETs. The main components of blockchain include transactions, consensus mechanisms, smart contracts, blocks, and P2P networks [27]. Specifically, the user functions as a distributed node in the blockchain system, collaborating to protect and maintain shared transaction records without needing any trusted supervisory authority [27]. All nodes participate in the activities of verifying, packaging, sharing, and saving new transactions within the blockchain system [33]. Therefore, mutually untrusted entities can establish trust in the network of this distributed environment. Additionally, blockchain possesses features such as tamper resistance, openness, decentralization, anonymity, and security [33].

1) TAMPER RESISTANCE

Information is encrypted using cryptographic techniques, and once it enters the blockchain, it becomes unchangeable.

2) OPENNESS

The foundation of blockchain technology is open source. Only the private information between the transacting parties is encrypted; furthermore, all data on the blockchain is open. Through public interfaces, any individual has the capability to access blockchain data and create associated applications, ensuring a high level of transparency in the entire system. While openness is often less emphasized, it is crucial and can even be considered one of the guarantees of the decentralization feature.

3) DECENTRALIZATION

The decentralized nature of blockchain is guaranteed by its distributed structure. Additionally, blockchain technology operates independently of any additional third-party governing bodies or reliance on specific hardware infrastructure, eliminating central control.

4) ANONYMITY

From a technical perspective, the identity information of various blockchain nodes does not necessarily have to be made public unless legal regulations require it. Information transmission can occur anonymously. To a certain extent, the anonymity feature of blockchain effectively protects user privacy.

5) SECURITY

Not under the control of any individual or entity, data written to the blockchain requires collective validation. Only with computational power exceeding 51% of the network can successful tampering occur. As long as control over 51% of all data nodes is impossible, arbitrary manipulation of network data is prevented. This inherent characteristic makes the blockchain relatively secure, avoiding subjective, human-induced data alterations.

B. MODIFIED PAILLIER CRYPTOSYSTEM

Due to the evolving needs of diverse environments, the Paillier cryptosystem has undergone improvements through scholarly research, and these changes have been utilized in diverse privacy protection schemes [29]. This paper is composed of three main components: key generation, encryption, and decryption.

1) KEY GENERATION

Given a security parameter κ, the key generation process begins by selecting two large secure primes $p = 2p' + 1$ and $q = 2q' + 1$ in the form of p and q, where $|p| = |q| = \kappa$, p' and q' are also prime. Next, compute the RSA modulus $N = p \cdot q$ and $\lambda = lcm\,(p-1, q-1)$. We consider $\mathbb{G} = QR_{N^2}$ to be a cyclic group of quadratic residues modulo N^2 with order $ord\,(\mathbb{G}) = \lambda\left(N^2\right)/2 = pp'qq' = N\lambda/2$, and the maximum order of elements in this group is $N\lambda/2$. Choose a random number $\mu \in \mathbb{Z}_{N^2}^{*}$ and a random value $x \in [1, ord\,(\mathbb{G})]$, then set $g = \mu^2 \bmod N^2$ and $h = g^x \bmod N^2$. $pk = (N, g, h = g^x)$ and x are the public key and private key, respectively.

2) ENCRYPTION

Given the data $m \in \mathbb{Z}_N$, choose a random number $r \in \mathbb{Z}_{N^2}$, and generate a ciphertext pair (C_1, C_2), where $C_1 = g^r \bmod N^2$ and $C_2 = h^r\,(1 + mN) \bmod N^2$.

3) DECRYPTION

Given the ciphertext pair (C_1, C_2), the data m can be decrypted to $m = \left[C_2/(C_1)^x - 1 \bmod N^2\right]/N$.

C. CHINESE REMAINDER THEOREM

The Chinese Remainder Theorem (CRT) can solve any pair of relatively prime modular congruences [28]. Utilizing this theorem, a set of congruences can be employed to construct multi-dimensional data into composite data. The detailed description is as follows:

CRT: Assuming $q_1, q_2, \ldots, q_l$ is a relatively prime number, and let $d_1, d_2, \ldots, d_l$ be an integer. Then, when $1 \le k \le l$, the congruence system $s \equiv d_k \bmod q_k$ has a unique solution modulo $Q = q_1 \times q_2 \times \cdots \times q_l$, which is:

$$s \equiv d_1 Q_1 y_1 + d_2 Q_2 y_2 + \cdots + d_l Q_l y_l \bmod Q \qquad (1)$$

where, $Q_k = Q/q_k$ and $y_k \equiv 1/Q_k \bmod q_k$, $1 \le k \le l$.

IV. SYSTEM MODEL AND DESIGN GOALS

This section introduces the system model in the proposed scheme. Subsequently, the design objectives that the scheme must achieve are presented.

A. SYSTEM MODEL

In the system model we have constructed, the entire system consists of three entities: vehicle users, Roadside Units (RSUs), and the Control Center(CC), as illustrated in Figure 1. Specifically, we divide the map into multiple segments, and vehicles within different segments are responsible for collecting various traffic data in their vicinity. After completing the collection task, vehicles encrypt the data using the modified Paillier cryptosystem and upload it to the RSU within their segment. Simultaneously, a blockchain is generated within the segment to ensure the authenticity of the data. After RSUs collect data uploaded by various vehicles, they aggregate the data and upload it to the CC (usually every 5 minutes), generating a blockchain within the segment to ensure data authenticity. Finally, the CC performs decryption and analysis of the collected data. The specific definitions of these entities in the system will be detailed below.

1) VEHICLE USERS

Vehicle users are responsible for collecting various real-time traffic data in their vicinity and encrypting and signing this traffic data. Next, they send these encrypted data to RSUs for further processing, simultaneously generating a blockchain.

2) ROADSIDE UNITS

RSUs can provide rapid local responses. They receive data uploaded by vehicle users, perform signature verification, aggregate the received messages and generate a signature to ensure data integrity and validity if the verification is successful. Then, they send the aggregated data to the CC, simultaneously generating a blockchain.

3) CONTROL CENTER

The CC is primarily responsible for generating and managing all parameters of entities in the system, as well as decrypting and analyzing the data. Upon receiving aggregated data from RSUs, it performs signature verification. If the verification is successful, the CC proceeds with the decryption and analysis of the data.

B. DESIGN GOALS

The scheme aims to establish a secure vehicle data aggregation system. Considering batch operations, this scheme is based on the modified Paillier cryptosystem, the Chinese Remainder Theorem, and blockchain. Therefore, this scheme is suitable for real-world vehicle data aggregation. The design objectives are outlined as follows:

The scheme features data signature verification, data confidentiality, and integrity checks. To protect the security of information and prevent malicious attacks on the model, the proposed solution in this paper introduces a mechanism for validating the effectiveness of signatures. During the signature verification phase, this solution provides secure protection for the data uploaded by vehicles; in other words, The original vehicle data can only be decrypted and accessed by the CC. After the recovery of vehicle data, the solution can provide a method for the system to detect the integrity of stored data.

The scheme features batch verification and anonymity. The batch verification is supported by this scheme, meaning that the data signatures from RSU and CC can be verified simultaneously for their validity. During the verification process, the identity of the vehicle user should be hidden from the regular message recipients, protecting the sender's privacy information.

The scheme needs to have low computational cost and communication overhead. The proposed solution aims to achieve high computational and communication efficiency, considering the application scenario's low processing latency, minimal communication costs, and short transmission intervals.

V. PROGRAM DETAILS

This subsection provides a detailed explanation of the task flow and specific data collection and upload details.

A. SYSTEM INITIALIZATION

1) Given a security parameter κ, the CC selects two large secure primes p and q, where $|p| = |q| = \kappa_1$. Subsequently, for the modified Paillier cryptosystem used, it generates its public key $pk = (N, g, h)$ and private key $sk = x$, where $N = p \cdot q$ and $h = g^x \bmod N^2$ is a suitable element. For a region with n segments, the CC selects n equidistant prime numbers $(j_1, j_2, \ldots, j_n)$, where $|j_1| = |j_2| = \ldots = |j_n| = \kappa$ and satisfies the condition $n \cdot \kappa < |N|$. For a segment $k$with coordinates (u_k, v_k), the CC assigns a prime number j_k to it. Then, the CC computes:

$$\begin{cases} Q = \prod_{k=1}^{n} j_k \\ Q_k = \dfrac{Q}{j_k},\ y_k \equiv \dfrac{1}{Q_k} \bmod j_k \\ \Delta_k = Q_k \cdot y_k \end{cases} \tag{2}$$

2) In addition, the CC selects a constant w, where $|w| = \kappa - 2$. Subsequently, it chooses two secure hash functions $H_0 : \{0, 1\}^* \rightarrow \mathbb{Z}_N$ and $H_1 : \{0, 1\}^* \rightarrow \{0, 1\}^{\kappa-2}$, ensuring $|H(\cdot) + w| < \kappa$. To ensure the effectiveness and correctness of data transfer, the CC randomly selects a value $r_{ij} \in \mathbb{Z}_N^*$ to compute the public key $x_{ij} = r_{ij} \cdot N$ and private key $y_{ij} = \left(r_{ij} \cdot N\right)^{-1}$ for U_i; similarly, RSUs do the same, randomly selecting a value $r_j \in \mathbb{Z}_N^*$ to compute the public key $x_j = r_j \cdot N$ and private key $y_j = \left(r_j \cdot N\right)^{-1}$, and the keys are securely transmitted to U_i and RSUs through a secure channel.

3) Finally, the CC publishes the parameter $params = \left\{pk, H_0, H_1, x_{ij}, x_j, j_k : k = 1, 2, \ldots, n\right\}$.

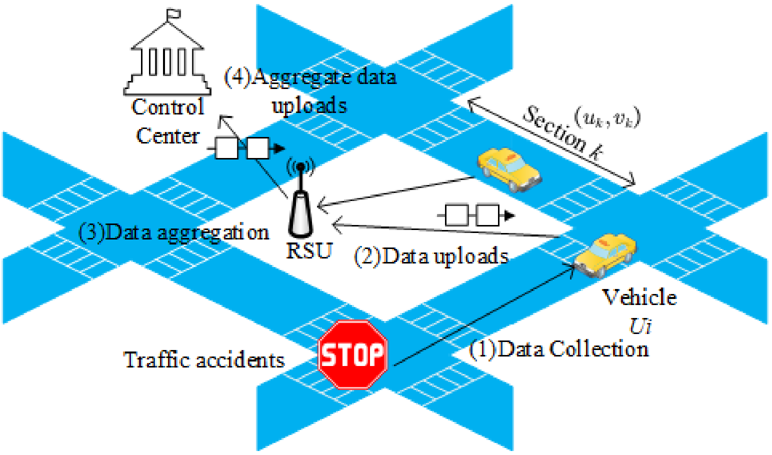

FIGURE 1. System mode.

B. THE PROCESS OF COLLECTING SENSOR DATA

This section is operated by the user entity U_i and mainly accomplishes the collection of data as detailed below:

1) For vehicle U_i, we define $w_{i,k}$ as the data collected by sensors in segment k, where $|w_{i,1}| = |w_{i,2}| = \cdots = |w_{i,n}|$ and $w_{i,k} < w$, $k = 1, 2, \ldots, n$. Additionally, $f_{i,k}$ represents whether sensor data is collected in segment k, expressed as follows:

a) If data is successfully collected in segment k, i.e., $w_{i,k} > 0$, then $f_{i,k} = 1$.

b) If data is not successfully collected in segment k, i.e., $w_{i,k} = 0$, then $f_{i,k} = 0$.

To achieve near real-time data upload, each vehicle U_i collects data for the corresponding road segment in an area within a time interval t, such as collecting data every 15 minutes. The vehicle then generates an encrypted data report following these steps:

2) U_i transforms the data $(w_{i,1}, w_{i,2}, \ldots, w_{i,n})$ and $(f_{i,1}, f_{i,2}, \ldots, f_{i,n})$ into two composite values $A_{i,w}$ and $A_{i,f}$, where $A_{i,w} = \sum_{k=1}^{n} w_{i,k} \cdot \Delta_k$ and $A_{i,f} = \sum_{k=1}^{n} f_{i,k} \cdot \Delta_k$.

3) U_i chooses two random numbers $(d_{i,w}, d_{i,f}) \in \mathbb{Z}_{N^2}$ and generates the following ciphertext:

$$\begin{cases} C_{i,1} = g^{d_{i,w}} \bmod N^2, & C_{i,2} = h^{d_{i,w}} \left(1 + A_{i,w}N\right) \bmod N^2 \\ C_{i,3} = g^{d_{i,f}} \bmod N^2, & C_{i,4} = h^{d_{i,f}} \left(1 + A_{i,f}N\right) \bmod N^2 \end{cases} \tag{3}$$

where $(C_{i,1}, C_{i,2})$ and $(C_{i,3}, C_{i,4})$ are ciphertext pairs for $A_{i,w}$ and $A_{i,f}$ respectively.

4) To ensure the correctness of the data, U_i also calculates the signature of the ciphertext:

$$u_{ij} = H_0 \left(C_{i,1} \| C_{i,2} \| C_{i,3} \| C_{i,4}\right) \tag{4}$$

$$\sigma_{ij} = H \left(u_{ij} \| T\right)^{y_{ij}} \tag{5}$$

where T is the timestamp.

5) Finally, U_i sends the encrypted report $\text{Report}_D = PD_{ij} \| C_{i,1} \| C_{i,2} \| C_{i,3} \| C_{i,4} \| \sigma_{ij} \| T$ to RSUs, where $PD_{ij} = H(U_i)$.

C. GENERATION OF USER LAYER BLOCKCHAIN

This part is generated in the user phase, and mainly completes the work of generating the blockchain at the user level and placing the collected data into the blocks with the following details:

1) Vehicle U_i records the transaction $\text{Report}_D = PD_{ij} \| C_{i,1} \| C_{i,2} \| C_{i,3} \| C_{i,4} \| \sigma_{ij} \| T$ in a block and disseminated across segment $k$for the purpose of checking information authenticity. The block retains three additional components: the Merkle root, as well as the preceding and current hash values. The Merkle root's value is acquired through hashing the pseudonym PD_{ij} and ciphertext $C_{a,1} = C_{i,1} \| C_{i,2} \| C_{i,3} \| C_{i,4}$ within the Merkle tree, as depicted in Figure 2. The formula for calculating the current block's hash value is as follows:

$$H_b = SHA256 \times \left(index + H_{pb} + PD_{ij} + T + C_{a,1} + \sum_{ij} \text{transaction}_{ij} \right) \tag{6}$$

The calculation process suggests that once a block is appended to the chain, the contents of the block are difficult to tamper with because the calculation of the block's current hash value involves the block's previous hash value.

2) After a new block is created, it will be broadcast within its associated partition. Regular nodes within that partition validate the transactions recorded in the new block; each node only validates information relevant to itself to meet the real-time upload requirements in the vehicular network. If the validation result matches the original data, the node successfully verifies the information and broadcasts the result to other nodes within the partition. Once correctness confirmation messages are received from $3n/5 + 1$ or more other nodes, the new block is considered to be effective and has been incorporated into the user layer blockchain. The number of nodes controlled by malicious nodes should be less

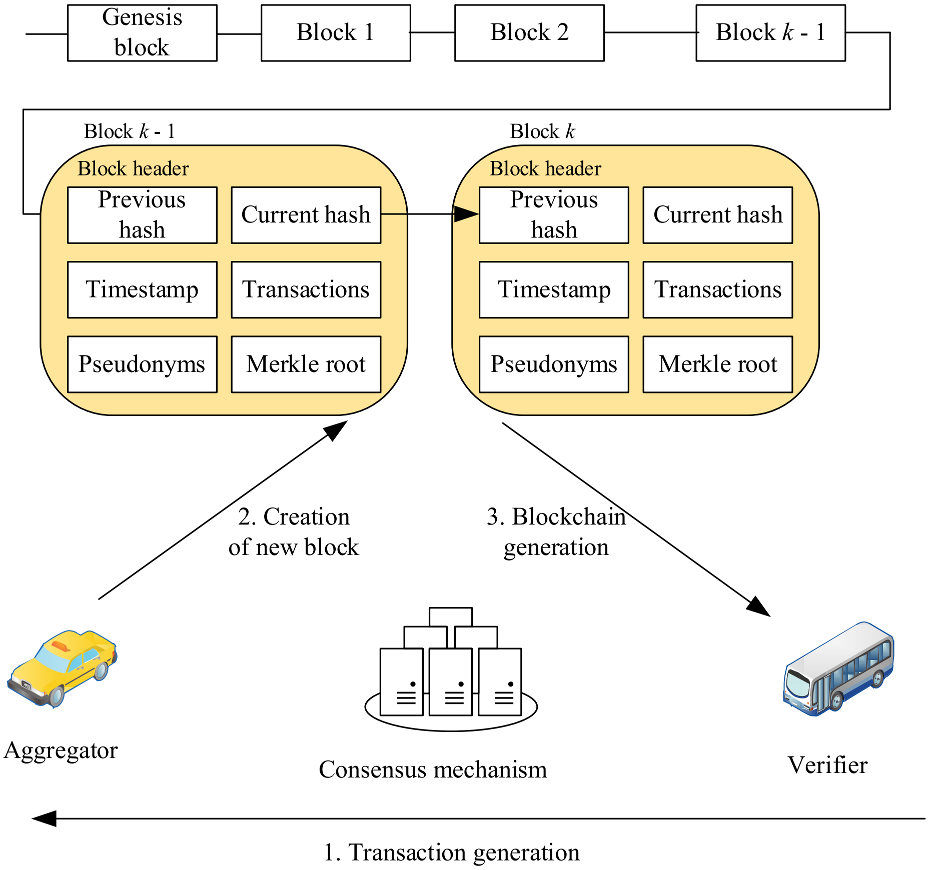

FIGURE 2. Generation of blockchain.

than $2/5$ of the total number of nodes in this system. This is for security reasons because we require the new block must be verified by $3n/5+1$ or more nodes before it can be added to the blockchain. This threshold setting ensures the security of the system. In other words, an attacker can only successfully tamper with information in a block if they control more than $3/5$ of the network nodes.

D. DATA AGGREGATION

This part is operated by the RSU entity, mainly to complete the data aggregation work, the details are as follows:

1) After RSU receive Report$_D$, RSU first verify its correctness by checking if the equation $\sigma_{ij}^{x_{ij}} = H\left(H_0\left(C_{i,1}\left\|C_{i,2}\right\|C_{i,3}\left\|C_{i,4}\right)\|T\right)$ holds true. If it holds, RSU perform the following steps to aggregate data reports from m vehicles, as shown in equation 7, where the number of vehicles uploading data m satisfies $\lceil\log_2 m\rceil + |w_{i,k}| < |w|, k = 1, 2, \ldots, n$.

where $(C_{w,1}, C_{w,2})$ and $(C_{f,3}, C_{f,4})$ are ciphertext pairs for the data aggregation of $\sum_{i=1}^{m} A_{i,w}$, and $\sum_{i=1}^{m} A_{i,f}$.

2) Then, RSU calculate the signature of the aggregated ciphertext pairs:

$$u_j = H_0\left(C_{w,1}\left\|C_{w,2}\right\|C_{f,3}\left\|C_{f,4}\right.\right) \tag{7}$$

$$\sigma_j = H\left(u_j\|T\right)^{y_j} \tag{8}$$

3) RSU generate the data aggregation message Aggregation$_D = C_{w,1}\left\|C_{w,2}\right\|C_{f,3}\left\|C_{f,4}\right\|\sigma_j\|T$, sending it to CC. Eq. (9), as shown at the bottom of the next page.

E. GENERATION OF RSUs LAYER BLOCKCHAIN

This part is generated in the RSU stage, and it mainly completes the work of generating the blockchain in the RSU layer and placing the aggregated data into the block with the following details:

1) RSUs record the transaction Aggregation$_D$ $=$ $C_{w,1}\left\|C_{w,2}\right\|C_{f,3}\left\|C_{f,4}\right\|\sigma_j\|T$ in a block and disseminated across other RSU for the purpose of checking information authenticity. Similar to the method of creating blocks in the user layer, this block includes transactions, the Merkle root, and the preceding and current hash values. The formula for calculating the current block's hash value is as follows:

$$H_b = SHA256 \times \left(index + H_{pb} + PD_j + T + C_{a,2} + \sum_j \text{transaction}_j\right) \tag{10}$$

where $C_{a,2} = C_{w,1}\left\|C_{w,2}\right\|C_{f,3}\left\|C_{f,4}\right.$.

2) After a new block is created in the RSUs layer, it will be broadcast to other RSUs and incorporated into the RSUs

layer blockchain by a consensus mechanism. It shares the exact consensus mechanism as the user layer. First, regular nodes in the RSUs layer validate the transactions recorded in this new block, with each node only validating data relevant to itself. If the validation result matches the original data, the validation is passed, and the result is broadcast to other nodes in the RSUs layer. Once correctness confirmation messages are received from $3n/5+1$ or more other RSUs, the block is considered valid and added to the RSUs blockchain.

F. DATA RECOVERY AND ANALYSIS

This part is operated by the CC entity, which mainly completes the data recovery and analysis work as detailed below:

1) After CC receives Aggregation$_D$, CC checks if $\sigma_j^{x_j} = H\left(H_0\left(C_{w,1}\left\|C_{w,2}\right\|C_{f,3}\left\|C_{f,4}\right)\|T\right)$ holds true to verify its correctness. If it holds, CC decrypts the received ciphertext pairs $\left(C_{w,1}, C_{w,2}\right)$ and $\left(C_{f,3}, C_{f,4}\right)$ using the key x:

$$\begin{cases} \sum_{i=1}^{m} A_{i,w} = \dfrac{C_{w,2}/\left(C_{w,1}\right)^x - 1 \bmod N^2}{N} \\ \sum_{i=1}^{m} A_{i,f} = \dfrac{C_{f,4}/\left(C_{f,3}\right)^x - 1 \bmod N^2}{N} \end{cases} \tag{11}$$

2) Finally, CC can compute the average $\bar{w}_k$ of the vehicle data collected in segment k. According to the Chinese Remainder Theorem:

$$\bar{w}_k = \frac{\sum_{i=1}^{m} A_{i,w} \bmod j_k}{\sum_{i=1}^{m} A_{i,f} \bmod j_k} = \frac{\sum_{i=1}^{m} w_{i,k} \bmod j_k}{\sum_{i=1}^{m} f_{i,k} \bmod j_k} \tag{12}$$

VI. SECURITY ANALYSIS

1) This proposed perception data aggregation scheme maintains location privacy during the sensor data collection phase. In this phase, as the location is represented on the segment, safeguarding the vehicle's location privacy during the data upload is achieved. Using the Chinese Remainder Theorem, the perception data of U_i can be restored to $\left(A_{i,w}, A_{i,f}\right)$, and needs to be protected. $A_{i,w}$ and $A_{i,f}$ are encrypted with the public key $pk = (N, g, h)$ to generate ciphertext pairs $\left(C_{i,1}, C_{i,2}\right)$ and $\left(C_{i,3}, C_{i,4}\right)$, in this scheme. Since we utilize the improved Paillier cryptosystem and prove the semantic security of this cryptosystem against adaptive chosen ciphertext attacks [34], the information contained in $\left(C_{i,1}, C_{i,2}\right)$ and $\left(C_{i,3}, C_{i,4}\right)$ are also semantically secure. In the event of collusion between invaded RSUs and malicious vehicles, since the colluding entities cannot obtain the secret key $sk = x$, they cannot acquire individual data reports $A_{i,w}$ and $A_{i,f}$ without the private key. This ensures the protection of location privacy for vehicles contributing data. After m data reports received, due to the homomorphic additivity property of the improved Paillier cryptosystem, RSU can aggregate encrypted data reports, resulting in $\left(C_{w,1} = \prod_{i=1}^{m} C_{i,1} \bmod N^2, C_{w,2} = \prod_{i=1}^{m} C_{i,2} \bmod N^2\right)$ and $\left(C_{f,3} = \prod_{i=1}^{m} C_{i,3} \bmod N^2, C_{f,4} = \prod_{i=1}^{m} C_{i,4} \bmod N^2\right)$, without knowing the content of the data aggregation result. Given the ciphertext pairs $\left(C_{w,1}, C_{w,2}\right)$ and $\left(C_{f,3}, C_{f,4}\right)$, the control center can use the private key $sk = x$ to recover the contents of $\sum_{i=1}^{m} A_{i,w}$, and $\sum_{i=1}^{m} A_{i,f}$.

2) The proposed perception data aggregation scheme can achieve the security goal of tamper resistance. To ensure data integrity, signature verification is performed after each data upload, as follows:

Each vehicle U_i generates a signature σ_{ij} for the encrypted report $\left(C_{i,1}, C_{i,2}\right)$ and $\left(C_{i,3}, C_{i,4}\right)$ using a timestamp T.

$$\sigma_{ij} = H\left(H_0\left(C_{i,1}\left\|C_{i,2}\right\|C_{i,3}\left\|C_{i,4}\right)\|T\right)^{y_{ij}} \tag{13}$$

After receiving the aggregated encrypted reports Report$_D$ $= PD_{ij}\left\|C_{i,1}\right\|C_{i,2}\left\|C_{i,3}\right\|C_{i,4}\left\|\sigma_{ij}\right\|T$ from the U_i, the RSUs verifies the signatures by checking if $\sigma_{ij}^{x_{ij}} = H\left(H_0\left(C_{i,1}\left\|C_{i,2}\right\|C_{i,3}\left\|C_{i,4}\right)\|T\right)$ holds. as follows:

$$\begin{aligned} \sigma_{ij}^{x_{ij}} &= H\left(u_{ij}\|T\right)^{x_{ij}\cdot y_{ij}} \\ &= H\left(H_0\left(C_{i,1}\left\|C_{i,2}\right\|C_{i,3}\left\|C_{i,4}\right)\|T\right)^{x_{ij}\cdot y_{ij}} \\ &= H\left(H_0\left(C_{i,1}\left\|C_{i,2}\right\|C_{i,3}\left\|C_{i,4}\right)\|T\right)^{r_{ij}\cdot N\cdot\left(r_{ij}\cdot N\right)^{-1}} \\ &= H\left(H_0\left(C_{i,1}\left\|C_{i,2}\right\|C_{i,3}\left\|C_{i,4}\right)\|T\right) \end{aligned} \tag{14}$$

If the verification is successful, it ensures the integrity of the data, as any tampering attempt would result in a signature mismatch.

This signature-based verification process adds a layer of security to the system, protecting against data tampering.

3) The proposed perception data aggregation scheme can achieve the security goal of protecting data correctness. A signature accompanies each data transmission stream between RSUs and vehicles to ensure the correctness of data

$$\begin{cases} C_{w,1} = \prod_{i=1}^{m} C_{i,1} \bmod N^2 = \prod_{i=1}^{m} g^{d_{i,w}} \bmod N^2 \\ C_{w,2} = \prod_{i=1}^{m} C_{i,2} \bmod N^2 = \left(\prod_{i=1}^{m} h^{d_{i,w}}\right)\left(1 + \sum_{i=1}^{m} A_{i,w}\cdot N\right) \bmod N^2 \\ C_{f,3} = \prod_{i=1}^{m} C_{i,3} \bmod N^2 = \prod_{i=1}^{m} g^{d_{i,f}} \bmod N^2 \\ C_{f,4} = \prod_{i=1}^{m} C_{i,4} \bmod N^2 = \left(\prod_{i=1}^{m} h^{d_{i,f}}\right)\left(1 + \sum_{i=1}^{m} A_{i,f}\cdot N\right) \bmod N^2 \end{cases} \tag{9}$$

TABLE 1. Execution time of cryptographic operation.

cryptographic operation	Average implementation time(ms)
T_p	11. 1042
T_m	0. 0024
T_h	0. 0004
T_{pm}	1. 4202
T_{pa}	0. 0172
T_e	1. 6248

transmission, and the verification of the signature ensures the accuracy of data transmission. Therefore, this scheme can accomplish the security objective of protecting data correctness.

VII. PERFORMANCE ANALYSIS

A. COMPUTATIONAL OVERHEAD

1) SYSTEM PARAMETER SETTING

This paper conducted experiments using a laptop configured with Intel Core i7-5500U CPU@2.40GHz, 12GB RAM. The experiments were performed in a virtual machine running on the Ubuntu 20.04 operating system. The cryptographic operations were implemented in C language, utilizing the GNU Multiple Precision Arithmetic Library (GMP) and the PBC library. The execution times for relevant cryptographic operations were tested and the results are presented in Table 1. First, we define symbols that can be used to calculate computational overhead.

Let T_p denote the computational overhead of bilinear pairing operation, T_m represent the computational overhead of point multiplication operation, T_h represent the computational overhead of hash operation, T_{pm} represent the multiplication operation based on bilinear pairing, T_e represent the exponentiation operation, T_{pa} represent the point-and-add operations based on bilinear pairing. The computational cost of XOR and concatenation operations is negligible in the overhead domain. It should be noted that the computational overhead is compared from the perspectives of the vehicle user, roadside unit, and receiving end. We analyze the overall system's computational cost using scheme of this paper and compare it with three other schemes proposed by Shen et al.' scheme [30], Rasheed et al.' scheme [31], and Mei et al.' scheme [32].

Meanwhile, after having the base operation computing time, we set the number of entities for the simulation of the simulation, and in order to be closer to the actual situation, we set the number of user entities between 100 and 1000, and the corresponding number of RSUs between 5 and 50. In order to facilitate comparison, the number of users is uniformly used as a variable.

2) COMPUTATIONAL OVERHEAD OF PROGRAMMES

The computational costs for each scheme are shown in Table 2. For the data aggregation scheme proposed in this paper, to generate the encrypted data report $C_{i,1} \| C_{i,2} \| C_{i,3} \| C_{i,4}$, U_i needs to perform 4 exponentiation operations and 4 multiplication operations in $\mathbb{Z}_{N^2}$. RSU performs 2 hash operations and 1 exponentiation operation. Meanwhile, the control center performs 2 exponentiation operations and 4 multiplication operations in $\mathbb{Z}_{N^2}$ for the decryption process. In Shen et al. [30], at the vehicle user end, 4 hash operations, 1 exponentiation operation, 1 multiplication operation, 1 bilinear pairing operation, and 1 addition operation are performed in $\mathbb{Z}_{N^2}$. At the RSU, 3 hash operations, 2 exponentiation operations, 3 multiplication operations, 2 bilinear pairing operations, and 2 addition operations are performed in $\mathbb{Z}_{N^2}$. For Rasheed et al. [31], at the vehicle user end, 4 multiplications based on bilinear pairing operations are performed in Z_{N^2}. Meanwhile, RSU performs 3 bilinear pairing operations and 1 multiplication based on bilinear pairing operation in $\mathbb{Z}_{N^2}$.Mei et al. [32] perform 2 multiplications based on bilinear pairing operations and 4 multiplications in $\mathbb{Z}_{N^2}$ at the vehicle user end. Meanwhile, RSU performs 4 bilinear pairing operations and 2 multiplications based on bilinear pairing operations in $\mathbb{Z}_{N^2}$.

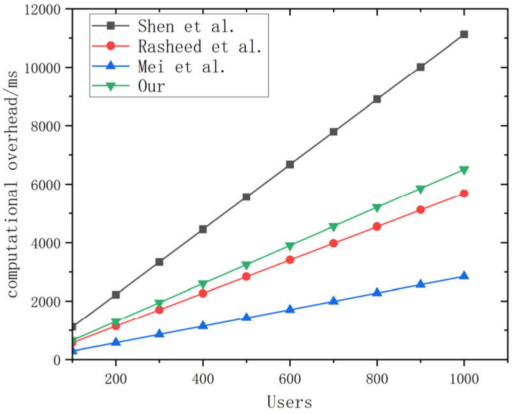

FIGURE 3. Comparison of Computing cost at the sender.

We conducted simulations for the proposed scheme and compared it with Shen et al. [30], Rasheed et al. [31], and Mei et al. [32]. We compared the total computational costs of the entire system, including the sender, receiver, and overall computation. Due to the nature of aggregation, the variable affecting the total cost is the number of vehicle users participating in the RSU domain. For ease of comparison and realism, we assumed the number of vehicle users increased from 100 to 1000.

The simulation results for the comparison with Shen et al.'s scheme [30], Rasheed et al.'s scheme [31], and Mei et al.'s scheme [32] at the sender are shown in Figure 3. Clearly, when the number of users is 100, the computational cost of our scheme is slightly higher compared to Rasheed et al.'s scheme [31], and Mei et al.'s scheme [32]; as the number of vehicle users increases, the computational cost grows linearly, and our scheme's cost is lower than Shen et al.'s scheme [30].

TABLE 2. Comparison of computational cost.

Scheme	Sender	Receiver	Total
[30]	$4T_h+T_e+T_m+T_p+T_{pa}$	$3T_h+2T_e+3T_m+2T_p+2T_{pa}$	$7T_h+3T_e+4T_m+3T_p+3T_{pa}$
[31]	$4T_{pm}$	$3T_p+T_{pm}$	$3T_p+5T_{pm}$
[32]	$2T_{pm}+4T_m$	$4T_p+2T_{pm}$	$4T_p+4T_{pm}+4T_m$
Ours	$4T_e+4T_m$	$2T_h+3T_e+4T_m$	$2T_h+7T_e+8T_m$

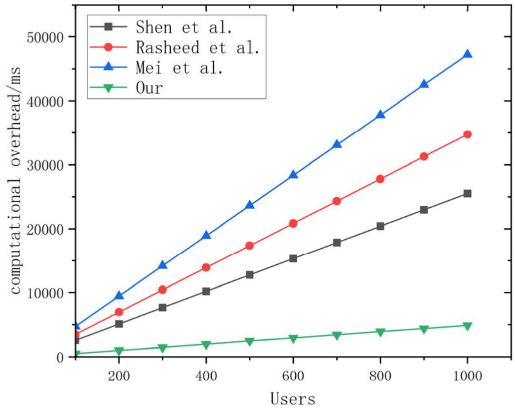

FIGURE 4. Comparison of Computing cost at the receiver.

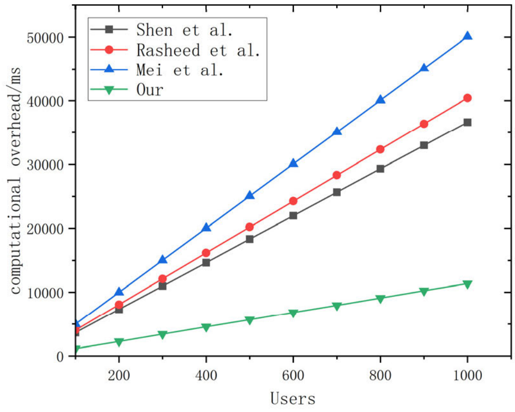

FIGURE 5. Total computing cost comparison.

TABLE 3. Comparison of communication cost.

Scheme	Communications overhead
[30]	$3\lvert\mathbf{Z}_q^*\rvert+6\lvert\mathrm{G}\rvert$
[31]	$(nb+1)\lvert\mathrm{G}_A\rvert$
[32]	$6\lvert\mathrm{G}\rvert+4\lvert H\rvert$
Ours	$4\lvert\mathbf{Z}_{N^2}\rvert+2\lvert H\rvert$

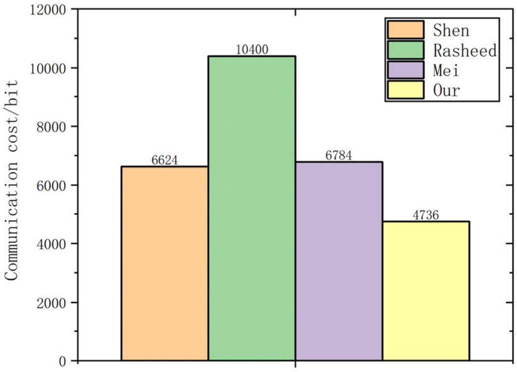

FIGURE 6. Communication cost comparison.

The simulation results for the comparison with Shen et al.'s scheme [30], Rasheed et al.'s scheme [31], and Mei et al.'s scheme [32] at the receiver are shown in Figure 4. From Figure 4, it can be observed that the computational cost of Mei et al.'s scheme [32] is quite substantial. While the schemes of Shen et al.'s scheme [30], and Rasheed et al.'s scheme [31] have relatively low computational costs, our proposed scheme is still more efficient than both of them.

The comparison of the total computational cost of the proposed scheme with other schemes is illustrated in Figure 5. It is noteworthy that the change trend in the simulation results is consistent between Figure 3 and Figure 4. In other words, as the number of vehicle users increases, the computational cost of both our scheme and the other schemes is on the rise. However, the computational costs of these three schemes have consistently been higher than those of our proposed scheme. Overall, compared to the proposed scheme, Shen et al.' scheme [30], Rasheed et al.' scheme [31], and Mei et al.' scheme [32] exhibit higher computational costs at both the sender and the receiver. Moreover, the total computational cost of the proposed scheme is also lower than the other schemes. Therefore, this paper's proposed scheme is more efficient than previous schemes.

B. COMMUNICATIONS OVERHEAD

Communication Overhead Parameter Setting: The comparison of communication overhead between the proposed scheme and previous schemes is presented in Table 3. The lengths of $\left|\mathbb{Z}_{N^2}\right|$, $\left|\mathbb{Z}_q^*\right|$, $|H|$, $|\mathbb{G}_A|$, and $|\mathbb{G}|$ are 1024 bits, 160 bits, 160 bits, 160 bits, and 1024 bits, respectively.

Please note that in Table 3, *nb* represents the bit length of plaintext. For the sake of comparison, we take *nb* as 64, as specifically shown in Figure 6. Through the comparison

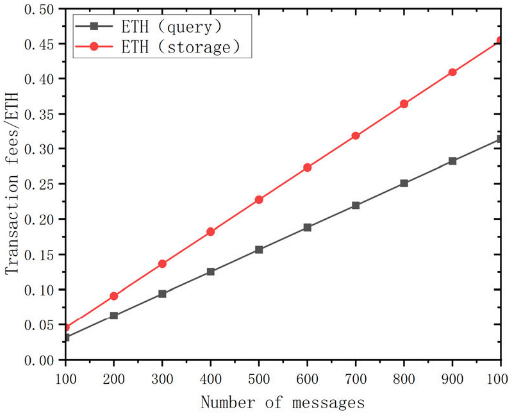

FIGURE 7. **Blockchain performance evaluation.**

in Figure 6, the communication costs for the aforementioned schemes are denoted as $3\left|\mathbb{Z}_q^*\right| + 6\left|\mathbb{G}\right|$, $(nb+1)\left|\mathbb{G}_A\right|$, and $6\left|\mathbb{G}\right| + 4\left|H\right|$. The communication cost for our scheme is denoted as $4\left|\mathbb{Z}_{N^2}\right| + 2\left|H\right|$. Furthermore, if the plaintext is large, the communication cost of Rasheed et al.' scheme [31] can be quite high. Although our scheme has larger $\left|\mathbb{Z}_{N^2}\right|$ overhead compared to Shen et al.' scheme [30], Shen et al.'s scheme has higher communication overhead. Compared to Mei et al.' scheme [32] scheme, while we have $\left|\mathbb{Z}_{N^2}\right|$ overhead, the $\left|\mathbb{G}\right|$ and $\left|H\right|$ communication overhead in Mei et al.' scheme [32] are higher than our scheme. In other words, in terms of communication cost, our scheme is more efficient than the schemes proposed by Shen et al.' scheme [30], Rasheed et al.' scheme [31], and Mei et al.' scheme [32].

C. BLOCKCHAIN PERFORMANCE EVALUATION

Blockchain Performance Parameter Settings: To assess the feasibility of blockchain in the proposed solution, a test on transaction costs within the blockchain was conducted. Since the blockchain in this paper is primarily used for storing and querying uploaded vehicle data, the test focused solely on the storage and retrieval processes of information. A consortium chain was established using FISCO BCOS, deploying four blockchain nodes to simulate the processes of information storage and retrieval. The number of messages was increased from 100 to 1000, and the changes in transaction costs during the storage and retrieval processes were tested as the message quantity varied from 100 to 1000.

For better visualization of the results, the gas fees obtained from the tests were converted into Ether (ETH), where the consumed ETH quantity equals the gas value multiplied by the gas price *(gas price: 42 gwei)*, as shown in Figure 7. The results indicate that the cost of message storage is higher than that of message retrieval. As the number of messages increases, the costs of both message storage and retrieval also increase. When storing 1000 messages, the transaction cost is approximately 0.45486 ETH, and when querying 1000 messages, the transaction cost is approximately 0.31332 ETH. Therefore, the average cost for storing and querying a single message is approximately 0.00076818 ETH, which is considered an acceptable cost.

VIII. SUMMARIES

This paper proposes a secure and efficient multidimensional perception data aggregation solution, addressing the significant computational cost and data security challenges that arise when multiple vehicles simultaneously upload perception data to roadside units in vehicular ad-hoc networks. This scheme enables vehicles to collect multidimensional sensory data at different locations to form a composite database, thus saving communication and computational resources. In addition, blockchain technology is introduced to design a secure and efficient multidimensional sensory data aggregation scheme, improving the system's security. The security of the solution regarding location privacy, data integrity, and resistance to collusion attacks is verified through security analysis, and performance evaluation experiments demonstrate lower computational and communication costs. The cost is validated in the blockchain performance evaluation to be within an acceptable range. Meanwhile, in the following work, we will improve the security scheme against other malicious attacks and improve the efficiency of signature verification under the premise of guaranteeing security to improve the system's overall efficiency.

REFERENCES

[1] Q. Kong, R. Lu, M. Ma, and H. Bao, "A privacy-preserving sensory data sharing scheme in Internet of Vehicles," *Future Gener. Comput. Syst.*, vol. 92, pp. 644–655, Mar. 2019.

[2] D. Liu, J. Shen, A. Wang, and C. Wang, "Secure real-time image protection scheme with near-duplicate detection in cloud computing," *J. Real-Time Image Process.*, vol. 17, no. 1, pp. 175–184, Feb. 2020.

[3] J. Shen, D. Liu, M. Z. A. Bhuiyan, J. Shen, X. Sun, and A. Castiglione, "Secure verifiable database supporting efficient dynamic operations in cloud computing," *IEEE Trans. Emerg. Topics Comput.*, vol. 8, no. 2, pp. 280–290, Apr. 2020.

[4] C. Wang, L. Xiao, J. Shen, and R. Huang, "Neighborhood trustworthiness-based vehicle-to-vehicle authentication scheme for vehicular ad hoc networks," *Concurrency Comput., Pract. Exper.*, vol. 31, no. 21, p. e4643, Nov. 2019.

[5] J. Shen, C. Wang, J.-F. Lai, Y. Xiang, and P. Li, "CATE: Cloud-aided trustworthiness evaluation scheme for incompletely predictable vehicular ad hoc networks," *IEEE Trans. Veh. Technol.*, vol. 68, no. 11, pp. 11213–11226, Nov. 2019.

[6] E. Ahmed and H. Gharavi, "Cooperative vehicular networking: A survey," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 3, pp. 996–1014, Mar. 2018.

[7] E. R. Cavalcanti, J. A. R. de Souza, M. A. Spohn, R. C. D. M. Gomes, and A. F. B. F. D. Costa, "VANETs' research over the past decade: Overview, credibility, and trends," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 48, no. 2, pp. 31–39, May 2018.

[8] A. Munir and F. Koushanfar, "Design and analysis of secure and dependable automotive CPS: A steer-by-wire case study," *IEEE Trans. Dependable Secure Comput.*, vol. 17, no. 4, pp. 813–827, Jul. 2020.

[9] F. Luo and Q. Hu, "Security mechanisms design for in-vehicle network gateway," Tech. Rep., 2018.

[10] H. J. Jo, J. H. Kim, H.-Y. Choi, W. Choi, D. H. Lee, and I. Lee, "MAuth-CAN: Masquerade-attack-proof authentication for in-vehicle networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 2, pp. 2204–2218, Feb. 2020.

[11] M. Bozdal, M. Samie, S. Aslam, and I. Jennions, "Evaluation of CAN bus security challenges," *Sensors*, vol. 20, no. 8, p. 2364, Apr. 2020.

[12] R. Geng, X. Wang, and J. Liu, "A software defined networking-oriented security scheme for vehicle networks," *IEEE Access*, vol. 6, pp. 58195–58203, 2018.

[13] H. Olufowobi, G. Bloom, C. Young, and J. Zambreno, "Work-in-progress: Real-time modeling for intrusion detection in automotive controller area network," in *Proc. IEEE Real-Time Syst. Symp. (RTSS)*, Dec. 2018, pp. 161–164.

[14] S. Yoon, J.-H. Cho, D. S. Kim, T. J. Moore, F. Free-Nelson, and H. Lim, "DESOLATER: Deep reinforcement learning-based resource allocation and moving target defense deployment framework," *IEEE Access*, vol. 9, pp. 70700–70714, 2021.

[15] Q. Jiang, X. Zhang, N. Zhang, Y. Tian, X. Ma, and J. Ma, "Three-factor authentication protocol using physical unclonable function for IoV," *Comput. Commun.*, vol. 173, pp. 45–55, May 2021.

[16] W. Jiang, H. Li, G. Xu, M. Wen, G. Dong, and X. Lin, "PTAS: Privacy-preserving thin-client authentication scheme in blockchain-based PKI," *Future Gener. Comput. Syst.*, vol. 96, pp. 185–195, Jul. 2019.

[17] Y. Zhao, G. Dan, A. Ruan, J. Huang, and H. Xiong, "A certificateless and privacy-preserving authentication with fault-tolerance for vehicular sensor networks," in *Proc. IEEE Conf. Dependable Secure Comput. (DSC)*, Jan. 2021, pp. 1–7.

[18] D. Gabay, K. Akkaya, and M. Cebe, "Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5760–5772, Jun. 2020.

[19] L. Wei, J. Cui, Y. Xu, J. Cheng, and H. Zhong, "Secure and lightweight conditional privacy-preserving authentication for securing traffic emergency messages in VANETs," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 1681–1695, 2021.

[20] R. Yang, Q. Xu, M. H. Au, Z. Yu, H. Wang, and L. Zhou, "Position based cryptography with location privacy: A step for fog computing," *Future Gener. Comput. Syst.*, vol. 78, pp. 799–806, Jan. 2018.

[21] C. Di, L. Hao, and Z. Shilei, "CSEP: Circular shifting encryption protocols for location privacy protection," in *Proc. IEEE/ACIS 16th Int. Conf. Comput. Inf. Sci. (ICIS)*, May 2017, pp. 45–50.

[22] H. Jannati and B. Bahrak, "An oblivious transfer protocol based on elgamal encryption for preserving location privacy," *Wireless Pers. Commun.*, vol. 97, no. 2, pp. 3113–3123, Nov. 2017.

[23] X. Deng, X. Xin, and T. Gao, "A location privacy protection scheme based on random encryption period for VSNs," *J. Ambient Intell. Humanized Comput.*, vol. 11, no. 3, pp. 1351–1359, Mar. 2020.

[24] J. Cui, J. Zhang, H. Zhong, R. Shi, and Y. Xu, "An efficient certificateless aggregate signature without pairings for vehicular ad hoc networks," *Inf. Sci.*, vols. 451–452, pp. 1–15, Jul. 2018.

[25] J. Li, H. Yuan, and Y. Zhang, "Cryptanalysis and improvement of certificateless aggregate signature with conditional privacy-preserving for vehicular sensor networks," *Cryptol. ePrint Archive*, 2016.

[26] E. Wood, "A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper 151, 2014.

[27] M. U. Hassan, M. H. Rehmani, and J. Chen, "Privacy preservation in blockchain based IoT systems: Integration issues, prospects, challenges, and future research directions," *Future Gener. Comput. Syst.*, vol. 97, pp. 512–529, Aug. 2019.

[28] D. Pei, A. Salomaa, and C. Ding, *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography*. Singapore: World Scientific, 1996.

[29] X. Liu, R. H. Deng, K. R. Choo, and J. Weng, "An efficient privacy-preserving outsourced calculation toolkit with multiple keys," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2401–2414, Nov. 2016.

[30] J. Shen, D. Liu, X. Chen, J. Li, N. Kumar, and P. Vijayakumar, "Secure real-time traffic data aggregation with batch verification for vehicular cloud in VANETs," *IEEE Trans. Veh. Technol.*, vol. 69, no. 1, pp. 807–817, Jan. 2020.

[31] I. Rasheed, L. Zhang, and F. Hu, "A privacy preserving scheme for vehicle-to-everything communications using 5G mobile edge computing," *Comput. Netw.*, vol. 176, Jul. 2020, Art. no. 107283.

[32] Q. Mei, H. Xiong, J. Chen, M. Yang, S. Kumari, and M. K. Khan, "Efficient certificateless aggregate signature with conditional privacy preservation in IoV," *IEEE Syst. J.*, vol. 15, no. 1, pp. 245–256, Mar. 2021.

[33] S. Chen, L. Yang, C. Zhao, V. Varadarajan, and K. Wang, "Double-blockchain assisted secure and anonymous data aggregation for fog-enabled smart grid," *Engineering*, vol. 8, pp. 159–169, Jan. 2022.

[34] E. Bresson, D. Catalano, and D. Pointcheval, "A simple public-key cryptosystem with a double trapdoor decryption mechanism and its applications," in *Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur.*, 2003, pp. 37–54.

[35] Z. Liu, J. Weng, J. Ma, J. Guo, B. Feng, Z. Jiang, and K. Wei, "TCEMD: A trust cascading-based emergency message dissemination model in VANETs," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 4028–4048, May 2020.

[36] Y. Cheng, J. Ma, Z. Liu, Y. Wu, K. Wei, and C. Dong, "A lightweight privacy preservation scheme with efficient reputation management for mobile crowdsensing in vehicular networks," *IEEE Trans. Dependable Secure Comput.*, vol. 20, no. 3, pp. 1771–1788, May/Jun. 2023.

[37] Z. Liu, L. Wan, J. Guo, F. Huang, X. Feng, L. Wang, and J. Ma, "PPRU: A privacy-preserving reputation updating scheme for cloud-assisted vehicular networks," *IEEE Trans. Veh. Technol.*, early access, Dec. 8, 2023, doi: 10.1109/TVT.2023.3340723.

RUICHENG YANG was born in 1999. He received the bachelor's degree in communication engineering from the School of Information Science and Technology, Guilin University of Electronic Technology, in 2018. He is currently pursuing the master's degree in information and communication engineering with the School of Electrical Information Engineering, Yunnan Minzu University. His research interests include data aggregation and privacy protection.

GUOFANG DONG (Member, IEEE) received the Ph.D. degree from Kunming University of Science and Technology, Yunnan, China. She is currently an Associate Professor with the School of Electrical Information Engineering, Yunnan Minzu University. Her current research interests include security protocols, the IoT security, and cloud computing security. She is a member of CCF.