Secure Real-Time Traffic Data Aggregation With Batch Verification for Vehicular Cloud in VANETs

Jian Shen, Dengzhi Liu, Xiaofeng Chen, Jin Li, Neeraj Kumar, and Pandi Vijayakumar

***Abstract*—The vehicular cloud provides many significant advantages to Vehicular ad-hoc Networks (VANETs), such as unlimited storage space, powerful computing capability and timely traffic services. Traffic data aggregation in the vehicular cloud, which can aggregate traffic data from vehicles for further processing and sharing, is very important. Incorrect traffic data feedback may affect traffic safety; therefore, the security of traffic data aggregation should be ensured. In this paper, by using the property of data recovery in the message recovery signature (MRS), we propose a secure real-time traffic data aggregation scheme for vehicular cloud in VANETs. In the proposed scheme, the validity of vehicles' signatures are verified, and then the original traffic data is recovered from signatures. Moreover, the proposed scheme supports batch verification for multiple vehicles' signatures. Due to advantages of the MRS, security features such as data confidentiality, privacy preservation and reply attack resistance are preserved. In addition, the comparison and simulation results indicate that the proposed scheme is superior in comparison to previous schemes with respect to the communication and computational cost.**

***Index Terms*—Vehicular cloud, VANETs, traffic data aggregation, message recovery signature, batch verification.**

Manuscript received May 31, 2019; revised August 4, 2019; accepted October 3, 2019. Date of publication October 11, 2019; date of current version January 15, 2020. This work was supported in part by the National Natural Science Foundation of China under Grants 61922045, U1836115, 61572382, and 61672295, in part by the Natural Science Foundation of Jiangsu Province under Grant BK20181408, in part by the Foundation of State Key Laboratory of Cryptology under Grant MMKFKT201830, in part by the Peng Cheng Laboratory Project of Guangdong Province under Grant PCL2018KP004, in part by the Open Foundation of State key Laboratory of Networking and Switching Technology (Beijing University of Posts and Telecommunications) under Grant SKLNST-2019-2-02, in part by the Postgraduate Research & Practice Innovation Program of Jiangsu Province, in part by the CICAEET fund, and in part by the PAPD fund. The review of this article was coordinated by Prof. C. Zhang. *(Corresponding author: Neeraj Kumar.)*

J. Shen and D. Liu are with the Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science and Technology, Nanjing 210044, China, and the Cyberspace Security Research Center, Peng Cheng Laboratory, Shenzhen 518000, China, and also with the State Key Laboratory of Cryptology, Beijing 100878, China (e-mail: s_shenjian@126.com; liudzdh@126.com).

X. Chen is with the State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China (e-mail: xfchen@xidian.edu.cn).

J. Li is with the School of Computer Science, Guangzhou University, Guangzhou 510006, China (e-mail: jinli71@gmail.com).

N. Kumar is with King Abdul Aziz University, Jeddah, Saudi Arabia and the Department of Computer Science & Engineering, Thapar Institute of engineering and technology (Deemed to be University), Patiala 147004, India (e-mail: neeraj.kumar@thapar.edu).

P. Vijayakumar is with the Department of Computer Science & Engineering, University College of Engineering Tindivanam, Tindivanam 604001, India (e-mail: vijibond2000@gmail.com).

Digital Object Identifier 10.1109/TVT.2019.2946935

I. Introduction

THE rapid development of vehicular technology has spawned many vehicular applications. The vehicular cloud is one of the applications that combines the technologies of cloud computing and VANETs [1]. It is generally known that cloud computing can provide a virtual resource pool to the end users. In cloud computing, many distributed servers are connected through the Internet. Various cloud services can be provided to users through numerous servers in cloud computing [2], [3]. Meanwhile, users can remotely access the cloud anytime to enjoy infinite storage space and strong computing power, as well as entertainment services through the Internet. The distributed cloud servers are managed by a Cloud Service Provider (CSP), and users need to pay the CSP for the cloud usage using the pay-per-use [4]. Using VANETs, vehicles on the road can communicate with the neighboring vehicles and roadside units (RSUs) via inter-vehicle communication modules to exchange traffic data [5]–[7]. In the VANETs system, every vehicle is equipped with various sensors [8]. Due to the abovementioned numerous advantages of cloud computing, a vehicular cloud can be constructed such that vehicles can upload their traffic data to the cloud servers and enjoy various services through VANETs [9]. Since many vehicles and RSUs can communicate with each other at any time, the vehicular cloud can provide many potential applications, such as video surveillance, traffic flow management, real-time navigation, remote traffic management and traffic monitoring [1], [10].

The vehicular cloud is a third party service offered to the end users; therefore, we are not confident that traffic data stored in the cloud is always secure and complete. Similar to the feature of the cloud server, the vehicular cloud cannot be completely trusted. As the traffic data is sent through the Internet so the vehicular cloud requires a security assurance mechanism to ensure the storage security of the traffic data so as to resist malicious attacks from adversaries. Data security can be achieved via the method in cloud computing that encrypts the data before outsourcing it to the cloud [11]–[14]. System security can be ensured through an authentication protocol or verification mechanism to check the trustworthiness of entities in the vehicular cloud. For example, in [15], an authentication protocol is proposed by Kumar *et al.* for the vehicular cloud, which is designed based on the RFID. Note that the ECC-based key generation method was used in Kumar *et al.*'s protocol to authenticate servers and tags in the

system. In [16], a mutual authentication protocol is proposed by Sharma *et al.*, which can authenticate the server and the sender simultaneously based on the ECC.

All vehicular cloud services are provided based on data from vehicles, so the system should provide a mechanism that enables the vehicular cloud to aggregate traffic data from vehicles. The data can be collected by wireless sensor networks (WSNs) [17]–[19]. Due to the constrained storage space and energy of sensor nodes, data aggregation schemes should be designed keeping in view of the energy-efficiency of the nodes. In [20], a secure data aggregation scheme is proposed to avoid transmission of redundant data. The data aggregation approach in WSNs cannot be directly used in the vehicular cloud due to the specific characteristics of the vehicular cloud. There have been many studies on traffic data aggregation in the vehicular cloud [21]–[23]. Although the existing studies proposed efficient methods for traffic data aggregation, security of traffic data in the system has not been considered. In [24], a cryptography based traffic data aggregation scheme is proposed by Du *et al.* to enhance the traffic data security; however, the scheme did not consider attacks from illegal entities. Hence, a secure real-time traffic data aggregation scheme should be designed to provide a mechanism for the system to authenticate vehicles and to verify the validity of the data before aggregation.

A. Contributions

In this paper, a secure real-time traffic data aggregation scheme is proposed for vehicular cloud in VANETs. The contributions of the proposed scheme are three folds.

- We use the MRS to construct a traffic data aggregation scheme for the vehicular cloud. Due to the usage of the MRS, the proposed scheme has low computational cost compared to previous schemes.
- To ensure the security of the traffic data recovery, the proposed scheme provides a mechanism to verify the validly of the vehicle's signature. Moreover, batch verification is supported, which enables the RSU in the system to simultaneously verify multiple vehicles' signatures.
- The proposed scheme is proved to be correct, as it provides security features, including data confidentiality, privacy preservation and reply attack resistance.

B. Related Work

The data aggregation schemes are significant to distributed systems to ensure that an aggregation server or sink node can aggregate data from distributed clients or sensor nodes. Data aggregation was originally used in WSNs [17]. In 2004, Mahimkar *et al.* proposed a secure data aggregation scheme based on secret key sharing for sensor networks. Mahimkar *et al.*'s scheme supports aggregated data integrity checking through the use of Merkle-Hash-Tree. The data aggregation scheme can be executed with less energy consumption for the sensor nodes; however, the redundant data in the WSNs violates the energy efficiency of data aggregation. In order to alleviate the influence of redundant data on the system, Sanli *et al.* designed a secure data aggregation scheme that requires the nodes to transmit the de-duplicate data to the sink node or the server [20]. By taking advantage of deployment estimation, Sanli *et al.*'s scheme also provides secure communication for sensors without requiring key distribution. To reduce the energy consumption, a data aggregation scheme designed based on hop-by-hop was proposed by Yang *et al.* in [18], which uses the probabilistic grouping to divide the nodes into multiple groups. Moreover, a commitment-based hop-by-hop aggregation mechanism is executed in each sensor nodes group to aggregate the data. It is worthy noting that the proposed scheme in [18] can highly improve the efficiency of data aggregation in WSNs.

With the development of data aggregation and VANETs, some studies of traffic data aggregation [21]–[24] have been researched. In 2009, Shafiee *et al.* in [21] used ad hoc communication and VANETs to construct a protocol for traffic data transmission to avoid traffic congestion. An aggregation algorithm is used in [21] to securely transmit the traffic data. In [22], Han *et al.* proposed a secure probabilistic data aggregation scheme that is designed based on the philosophies of the Flajolet-Martin sketch and the sketch proof. Compared to previous schemes, the traffic data aggregation scheme in Han *et al.*'s scheme has low computational overhead that can be used in VANETs for real-time traffic monitoring. To improve the accuracy of data aggregation in VANETs, Shoaib *et al.* proposed a data aggregation scheme based on particle swarm optimization (PSO) [23]. Compared to previous similar schemes, Shoaib *et al.*'s scheme has a high aggregation accuracy and can reduce the processing time of traffic data. Note that previous studies on traffic data aggregation focused only on improving the accuracy and the efficiency of the scheme but the security of the system is not considered. Du *et al.* in 2003 proposed a secure traffic data aggregation scheme using the method of syntactic aggregation and the cryptographic aggregation. Moreover, the technologies of the Flajolet-Martin sketch and the sketch proof [22] were considered in the scheme to improve the efficiency and the accuracy of the traffic data aggregation. However, the lack of verification before data aggregation increases the risk of malicious attacks to the system. Hence, the proposed scheme in Han *et al.*'s scheme [22] cannot be used in the vehicular cloud for the real-time traffic data aggregation.

C. Organization

The remainder of this paper is organized as follows. Section II introduces the preliminaries. Section III presents the system model and the design goals. Section IV provides the proposed scheme in detail. Section V and Section VI analyze the security and the performance evaluation, respectively. Finally, the paper is concluded in Section VII.

II. Preliminaries

In this section, the preliminaries of the proposed scheme are presented. First, the technology of bilinear pairing is described. Then, the MRS is briefly introduced.

A. Bilinear Pairing

The technology of bilinear pairing has been widely used in the construction of cryptography protocols since 2001 [25]. Due to the properties of bilinear pairing, the implementation of bilinear pairing during protocol construction can make the protocol more secure. Here, bilinear pairing is briefly introduced. Suppose that $\mathbb{G}_1$ and $\mathbb{G}_2$ are two cyclic groups with large prime order q. The equation of bilinear pairing can be constructed as $\widehat{e}$: $\mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$. Let $\mathcal{P}$ and $\mathcal{Q}$ be two different generators of $\mathbb{G}_1$. Moreover, we randomly select two security parameters a and b from $\mathbb{Z}_q^*$ for further bilinear pairing computation, where $\mathbb{Z}_q^*$ is a set of integers 1 to q-1 with modulo q. Bilinear pairing has three properties that are listed as follows:

- Bilinear: $\widehat{e}(a\mathcal{P}, b\mathcal{Q}) = \widehat{e}(\mathcal{P}, \mathcal{Q})^{ab}$.
- Non-degenerate: $\widehat{e}(\mathcal{P}, \mathcal{Q}) \neq 1$.
- Computable: $\widehat{e}(\mathcal{P}, \mathcal{Q})$ can be efficiently computed by an existing algorithm $\mathcal{A}$.

B. Message Recovery Signature

The MRS can not only authenticate the validity of a message's signature but can also recover the corresponding message. The MRS was first proposed by Nyberg *et al.* in [26]. Recently, some researches of the MRS have been proposed by researchers [27], [28]. In 2006, a secure ID-based signature scheme is proposed by Tso *et al.* to support message recovery [29]. Note that Tso *et al.*'s scheme is constructed based on bilinear pairing. The MRS consists of four phases. Here, the process of the MRS is briefly introduced.

1) *Setup*: This phase generates the necessary security keys and parameters for the system. Generally, setup is executed by a fully trusted server. First, the system selects a security parameter θ from $\mathbb{Z}_q^*$ as the input. Then, the server chooses a parameter s from $\mathbb{Z}_q^*$ as its secret key. Finally, the public key can be computed according to secret key s.
2) *Extract*: This phase is executed by the abovementioned server, which authenticates the validity of the user's signature. The goal of this phase is to select a secret key for the user. We assume that the identity number of the user is ID_u. First, the user sends his/her identity number ID_u to the server. When the server receives corresponding identity number ID_u, a secret key can be computed according to ID_u.
3) *Sign*: In this phase, the user computes a signature for his/her message m. The input of this phase is the user's secret key sk_u and data message m. The output is the signature of σ. The signature is sent to the server side in a secure channel.
4) *Verify*: When the server receives the signature of σ, the server can verify the validity of it. The input of this phase is user's identity number ID_u and signature σ. If the verification of signature σ is successful, the signature is valid. Then, the server can correctly recover the original message from the valid signature. Otherwise, the original user's message cannot be recovered by the server according to the signature.

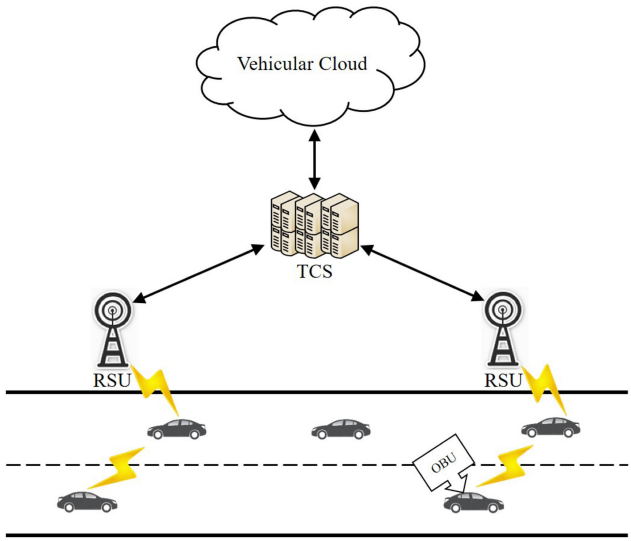


Fig. 1. The System model.

III. Problem Statement

This section introduces the system model of the vehicular cloud in the proposed scheme. Then, the design goals that the proposed scheme must to finish are presented.

A. System Model

We refer to the VANET system [30] and the traditional vehicular cloud [9], [31] to design a new vehicular cloud system. To satisfy the real-world usage requirements and to protect the security of the traffic data aggregation, we add a traffic center server to the system. The system model of the proposed vehicular cloud is shown in Fig. 1. Note that there are four entities in the system: **Vehicular Cloud**, **Traffic Center Server**, **Road Side Unit** and **On Board Unit**. A detailed description of the system model is given from the following four points.

- **Vehicular Cloud (VC):** The VC is an emerging concept that is developed from VANETs and cloud computing. The original intention of developing the vehicular cloud was to enrich applications and process the large data in VANETs [10]. Similar to cloud computing, the VC has unlimited storage and computing resources. Vehicles can access servers from the VC anywhere and anytime via the network. Note that the VC not only provides storage, computing and entertainment services but also supports the traffic warnings, such as road congestion, accidents, fatigued driving and exhaust pollution [1]. Hence, implementing the VC in VANETs can improve the traffic flow efficiency on the road and reduce the occurrence of traffic accidents [32], [33]. In this case, the development of vehicular technology can be promoted.
- **Traffic Center Server (TCS):** The TCS can be seen as the administrator of the system, and it is a fully trustworthy entity. In our scheme, the TCS can recover the original traffic data from the signature and aggregates all the data from RSUs. The transmission channel between the TCS and the RSU is sufficiently secure. Suppose that the TCS

is never compromised. The aggregated data is outsourced to the VC by the TCS for further VANET services.

- **Road Side Unit (RSU):** The RSU in the vehicular cloud system is responsible for aggregating data from nearby vehicles. Moreover, the RSU can broadcast real-time traffic data to vehicles in its communication range. Note that the wireless communication range of the RSU is larger than that of vehicle to vehicle [34]. In addition, compared to the OBU on the vehicle, the RSU is fully trusted, and its computation and storage capabilities are very powerful [30]. Therefore, the RSU can authenticate the identity of the vehicle that will communicate with the RSU. To ensure the correctness and the integrity of the received traffic data, the RSU can also verify the validity of the data received from vehicles.
- **On Board Unit (OBU):** The OBU is an entity that utilizes the communication technique of DSRC (Dedicated Short Range Communication) to communicate with the neighboring RSU and vehicles [30]. In VANETs, every vehicle is equipped with an OBU to ensure traffic data can be transmitted among vehicles and RSUs.

B. Design Goals

The aim of this paper is to construct a secure real-time traffic data aggregation scheme for the vehicular cloud. The design philosophy is based on the technology of the MRS. Moreover, batch operation is considered in our scheme. Therefore, the proposed scheme is applicable to real-world vehicular cloud traffic data aggregation. Here, the design goals are presented, which are divided into two parts: functionality and security.

1) Functionality:

- *Data Signature Verification.* To ensure data security and avoid malicious attacks to the system, the proposed scheme should provide a mechanism to verify the validity of signatures.
- *Original Data Recovery.* The original traffic data of the signature can be recovered by the TCS. Moreover, the system should ensure that only the TCS can recover the original data from valid signatures.
- *Data Integrity Checking.* After the traffic data in the signature is recovered, the proposed scheme can provide a mechanism for the TCS to check the storage integrity of the recovered traffic data.
- *Batch Verification.* In addition, the proposed scheme should support batch verification. In other words, the RSU can simultaneously verify the validity of signatures from multiple vehicles.

2) Security:

- *Data Confidentiality.* In the phase of signature verification, the proposed scheme should guarantee the confidentiality of one vehicle's traffic data; that is to say, no one other than the TCS in the system should be able to obtain the original traffic data.
- *Privacy Preservation.* The identity information of one vehicle in the system should be preserved in the process of signature verification and data recovery.

TABLE I
NOTATIONS

Symbol	Description
θ	The system setup security parameter
sk_R, pk_R	The RSU's secret key and public key
q	The prime order of $\mathbb{Z}$
s	The secret key of the RSU
$\mathcal{G}$	The generator of $\mathbb{G}_1$
H_0, H_1, H_2, H_3	The collision resistant one-way hash function
ID_i	The identity number of the vehicle
sk_i, pk_i	The vehicle's secret key and public key
$Info_i$	The traffic data of vehicle ID_i
σ	The signature of the traffic data
r_1, r_2	The auxiliary parameter for signature generation
b_1, b_2	The bit length of the selected value
m	The auxiliary parameter for signature verification
$\|$	The concatenation operation
$\oplus$	The exclusive-or operation
A, B	The security parameter for signature generation
η	The component of the signature

- *Reply Attack Resistance.* The proposed scheme should ensure that vehicles cannot use the previous security parameters and signatures to pass the RSU's verification and then access the vehicular cloud.

IV. The Proposed Scheme

Our scheme is introduced in detail in this section. Note that our scheme includes two parts: the basic scheme and the batch operation. First, the basic scheme is present in subsection A. The basic scheme explains how traffic data aggregation is performed. Then, the batch operation of the proposed scheme, which satisfies the practical usage requirements of traffic data aggregation, is presented in subsection B. The notation that appears in the proposed scheme is shown in Table I. **Algorithm 1** presents the main flow of the proposed traffic data aggregation scheme.

A. The Basic Scheme

The basic scheme is constructed on the basis of the idea in Tso *et al.*'s scheme [29]. In order to suit the vehicular cloud and enhance the system's security, the proposed traffic data aggregation scheme is constructed with the assist of a third fully trusted server. Similar to VANETs, RSUs and OBUs are also considered in the system. The process of the basic scheme is given in detail as follows:

1) *Setup* $(\theta) \rightarrow (sk_R, pk_R)$: In the vehicular cloud system, the protection of keys and parameters determines the security of the system. As mentioned in Section III, the TCS is a fully-trusted entity that should never be compromised. In the proposed scheme, the system needs to select a security parameter θ from $\mathbb{Z}_q^*$ as the input for the TCS. Here, θ determines the mathematical complexity of the parameter that is selected by the TCS. In the key generation phase, the TCS randomly selects parameter s from $\mathbb{Z}_q^*$ as the RSU's secret key. Then, the RSU's public key can be computed as $pk_R = s \cdot \mathcal{G}$. Here, the parameter of $\mathcal{G}$ is a generator of group $\mathbb{G}_1$. After that, the public parameters of the system can be denoted as $\{\mathbb{G}_1, \mathbb{G}_2,$

Algorithm 1: Traffic Data Aggregation.

TCS:
- selects s from $\mathbb{Z}_q$ as the RUS's scret key
- computes the public key $pk_R = s{\cdot}\mathcal{G}$ for the RSU

RSU:
- computes $sk_i = (H_0(ID_i) + sk_R))^{-1}{\cdot}\mathcal{G}$ and $pk_i = H_0(ID_i){\cdot}\mathcal{G} + pk_R$ for the vehicle

Vehicle ID_i**:**
- selects r_1 from $\mathbb{Z}_q^*$
- computes $m = \widehat{e}(\mathcal{G},\mathcal{G})^{r_1}$ and $A = H_1(m)$
- computes $B = H_2(Info_i)\|(H_3(H_2(Info_i))\oplus Info_i)$
- computes $r_2 = A\oplus B$ and $\eta = (r_1 + r_2){\cdot}sk_i$
- sends signature $\sigma_i = (m, r_2, \eta)$ to the **RSU**.

RSU:
if $\widehat{e}(\eta, pk_i)\cdot\widehat{e}(\mathcal{G},\mathcal{G})^{-r_2} = m$ **then**
The signature of vehicle ID_i is valid
end if

RSU:
- sends signature $\sigma_i = (m, r_2, \eta)$ to the **TCS**

TCS:
- computes $A^* = H_0(m)$ and $B^* = r_2\oplus A^*$
- recovers the data as $Info_i^* = |B^*|_{b_1}\oplus H_3({}_{b_2}|B^*|)$

if ${}_{b_2}|B^*| = H_2(Info_i^*)$ **then**
The recovered data is the original data
end if

$\widehat{e}$, pk_R, H_0, H_1, H_2, H_3, b_1, $b_2\}$. Here, the symbols of b_1 and b_2 are the values of bit length and $|q| = b_1 + b_2$. Note that H_0: $\{0,1\}^*\rightarrow\mathbb{Z}_q^*$, H_1: $\mathbb{G}_1\rightarrow\{0,1\}^{(b_1+b_2)}$, H_2: $\{0,1\}^{b_1}\rightarrow\{0,1\}^{b_2}$ and H_3: $\{0,1\}^{b_2}\rightarrow\{0,1\}^{b_1}$ are four collision-resistant one-way hash functions. Finally, the public parameters are broadcast by the RSU to all vehicles in its communication range.

2) *Extract* (ID_i, sk_R, pk_R) $\rightarrow$(sk_i, pk_i): When one vehicle enters the RSU's communication range and receives the broadcast signal from the RSU, the OBU of the vehicle sends the vehicle's identity number to the RSU using the DSRC protocol. Suppose that the DSRC protocol is embedded in the OBU module by the vehicle manufacturer. The identity number of each vehicle is unique. Here, we use ID_i to denote the identity number of the current vehicle. Upon receiving the vehicle's identity number, the RSU computes the key pair for the corresponding vehicle. The secret key and the public key of the current vehicle are computed as $sk_i = (H_0(ID_i) + sk_R))^{-1}{\cdot}\mathcal{G}$ and $pk_i = H_0(ID_i){\cdot}\mathcal{G} + pk_R$, respectively.

3) *Sign* ($Info_i$, sk_i) $\rightarrow\sigma_i$: In VANETs, various sensor nodes are deployed on the vehicle. These nodes can collect the data of the vehicles' driving status. Moreover, an OBU is configured on every vehicle, which can communicate with nearby vehicles at any time; that is to say, a vehicle on the road can not only send its own data to the RSU but also work as a communication transfer station to transmit other vehicles' data to another vehicle or the RSU. Suppose that the traffic data at the vehicle side is $Info_i \in \{0, 1\}^{b_1}$. First, the vehicle randomly selects a security parameter r_1 from $\mathbb{Z}_q^*$. Then, the OBU computes $m = \widehat{e}(\mathcal{G},\mathcal{G})^{r_1}$ and $A = H_1(m)$, where $A \in \{0, 1\}^{(b_1+b_2)}$. Next, the OBU computes $B = H_2(Info_i)\|(H_3(H_2(Info_i))\oplus Info_i)$ and $r_2 = A\oplus B$. The OBU calculates security parameter $\eta = (r_1 + r_2){\cdot}sk_i$ according to r_1, r_2 and the current vehicle's secret key. The signature of the vehicle's message can be denoted as $\sigma_i = (m, r_2, \eta)$. Finally, the signature is forwarded to the RSU in a secure channel.

4) *Verify* (m, σ_i) $\rightarrow$0/1: When the RSU receives the signature from the vehicle, the signature is verified by the RSU. The validity of the signature can be determined by checking whether Eq. (1) holds. As mentioned above, the vehicle's public key pk_i is calculated by the RSU. Note that m, r_2 and η are components of the signature. Hence, the RSU can check the correctness of Eq. (1).

$$\widehat{e}(\eta, pk_i)\cdot\widehat{e}(\mathcal{G},\mathcal{G})^{-r_2} \stackrel{?}{=} m \tag{1}$$

If the verification is successful, it is concluded that the signature was generated by vehicle ID_i; that is to say, the signature contains the correct traffic data $Info_i$ of vehicle ID_i. In this case, the RSU transmits signature σ_i to the TCS for further original traffic data recovery.

5) *Data Recovery* (σ_i) $\rightarrow Info_i^*$: The TCS can recover the original data successfully according to the correct signature. First, the TCS computes $A^* = H_0(m)$. As above-mentioned in the *Sign* phase, we have $r_2 = A\oplus B$. Hence, we can get $B^* = r_2\oplus A^*$ according to A^* and r_2. The original data of the signature can be recovered as $Info_i^* = |B^*|_{b_1}\oplus H_3({}_{b_2}|B^*|)$. Note that $|B^*|_{b_1}$ denotes the value of b_1 bits from the right side of B^*. Contrary to $|B^*|_{b_1}$, ${}_{b_2}|B^*|$ presents the value of b_2 bits from the left side of B^*. Moreover, the integrity and the correctness of the recovered data can be checked by determining whether ${}_{b_2}|B^*|$ equals $H_2(Info_i^*)$. If the signature is valid, the TCS can correctly recover the original data of vehicle ID_i from the signature.

B. Supporting Batch Verification

Under real-world conditions, there are many vehicles on the road. It is possible that many vehicles are in the RSU's communication range and need to communicate with the RSU simultaneously. If the RSU handles each vehicle's data signature one by one, the problem of delay will emerge. Instant traffic data is important to drivers. On the one hand, delayed traffic data may influence drivers' judgment about the vehicle's driving situation. On the other hand, non-real-time traffic data may cause many traffic problems, such as traffic congestion and accidents, and may even threaten the lives of drivers and pedestrians. To improve the signature verification efficiency, we consider batch operation [35], [36] and extend the verification of the proposed scheme to support batch verification. We introduce only the three phases of *Extract*, *Sign* and *Verify* that are different from the phases in the basic scheme. Here, the symbol of n is used to denote the number of vehicles in the current round.

The introduction of the corresponding three phases is given as follows:

- *Extract*: Suppose that n vehicles are running in the RSU's communication range and all vehicles have received the broadcast signal simultaneously. Hence, these n vehicles generate signatures of their own data and transmit the signatures to the RSU for verification. When the RSU receives multiple signatures from vehicles at a time, it executes the batch verification algorithm. The identity numbers of these vehicles can be denoted as $\{ID_1, ID_2, \ldots, ID_n\}$. First, the n vehicles send their identity numbers to the RSU. Then, the RSU calculates the secret-public key pair as $sk_t = (H_0(ID_t) + sk_R))^{-1} \cdot \mathcal{G}$ and $pk_t = H_0(ID_t) \cdot \mathcal{G} + pk_R$, where $1 \leq t \leq n$. The RSU transmits each vehicle's secret key to the corresponding vehicle.
- *Sign*: Upon receiving secret keys from the RSU, the vehicles compute the signature for their own traffic data. The traffic data of each vehicle can be denoted as $Info_t \in \{0,1\}^{b_1}$ $(1 \leq t \leq n)$. For signature generation, each vehicle needs to randomly select a security parameter $r_{1,t}$ and compute $m_t = \widehat{e}(\mathcal{G}, \mathcal{G})^{r_{1,t}}$. Then, each vehicle computes $A_t = H_1(m_t)$. Similar to *Sign* in the basic scheme, the vehicle computes another auxiliary parameter and $r_{2,t}$ as $B_t = H_2(Info_t) \| (H_3(H_2(Info_t)) \oplus Info_t)$ and $r_{2,t} = A_t \oplus B_t$, respectively. After the above security parameter generation, each vehicle computes $\eta = (r_{1,t} + r_{2,t}) \cdot sk_i$ for their signature. The signature of each vehicle can be denoted as $\sigma_t = (m_t, r_{2,t}, \eta)$. The OBUs on the vehicles transmit their signatures to the RSU via a secure channel.
- *Verify* $(m_t, \sigma_t)_{(1 \leq t \leq n)} \rightarrow 0/1$: The RSU can verify the validity of all the vehicles' signatures utilizing vehicles' public keys through batch verification. The batch verification equation is shown in Eq. (2).

$$\sum_{t=1}^{n} \widehat{e}(\eta_t, pk_t) \cdot \widehat{e}(\mathcal{G}, \mathcal{G})^{-r_{2,t}} \stackrel{?}{=} \sum_{t=1}^{n} m_t \tag{2}$$

  Similar to the description of the *Verify* phase in the basic scheme, if Eq. (2) holds, the signatures of all the vehicles are valid. Then, the RSU sends the signatures to the TCS via a secure channel for original traffic data recovery.

V. Security Analysis

The security analysis of our scheme is introduced in this section. First, the theorem of the proposed scheme's correctness and the corresponding proof are presented. Then, the security properties of our scheme are provided, including data confidentiality, privacy preservation and reply attack resistance.

A. Correctness Proof

Theorem 1: Suppose that all entities in the system can generate security parameters correctly and compute the security keys successfully, the correctness of proposed scheme can be proved.

Proof of Theorem 1: In the phase of the signature verification, the validity of the signature can be judged by checking the verification equation. In the basic scheme, the verification equation is Eq. (1). The RSU executes the signature verification phase. In Eq. (1), m, η and r_2 are components of the vehicle's signature. The left-hand side of Eq. (1) is elaborated using pk_i and σ_i as follows:

$$\begin{aligned}
&\widehat{e}(\eta, pk_i) \cdot \widehat{e}(\mathcal{G}, \mathcal{G})^{-r_2} \\
&= \widehat{e}((r_1 + r_2) \cdot sk_i, pk_i) \cdot \widehat{e}(\mathcal{G}, \mathcal{G})^{-r_2} \\
&= \widehat{e}(sk_i, pk_i)^{(r_1 + r_2)} \cdot \widehat{e}(\mathcal{G}, \mathcal{G})^{-r_2} \\
&= \widehat{e}((H_0(ID_i) + s)^{-1} \cdot \mathcal{G}, (H_0(ID_i) + s) \cdot \mathcal{G})^{(r_1 + r_2)} \\
&\quad \cdot \widehat{e}(\mathcal{G}, \mathcal{G})^{-r_2} \\
&= \widehat{e}(\mathcal{G}, \mathcal{G})^{r_1}.
\end{aligned}$$

Note that the right-hand side of Eq. (1) is m. In *Extract* phase, we can find that $m = \widehat{e}(\mathcal{G}, \mathcal{G})^{r_1}$. Hence, Eq. (1) holds; that is to say, the correctness of the basic scheme can be proved.

Batch verification makes the scheme more efficient when processing signatures from multiple vehicles. In batch verification, Eq. (2) can verify the validity of signatures from n vehicles simultaneously. That is to say, if Eq. (2) holds, all the signatures are valid. The left-hand side of Eq. (2) is solved as follows:

$$\begin{aligned}
&\sum_{t=1}^{n} \widehat{e}(\eta_t, pk_t) \cdot \widehat{e}(\mathcal{G}, \mathcal{G})^{-r_{2,t}} \\
&= \sum_{t=1}^{n} (\widehat{e}((r_{1,t} + r_{2,t}) \cdot sk_t, pk_t) \cdot \widehat{e}(\mathcal{G}, \mathcal{G})^{-r_{2,t}}) \\
&= \sum_{t=1}^{n} (\widehat{e}(sk_t, pk_t)^{(r_{1,t} + r_{2,t})} \cdot \widehat{e}(\mathcal{G}, \mathcal{G})^{-r_{2,t}}) \\
&= \sum_{t=1}^{n} (\widehat{e}((H_0(ID_t) + s)^{-1} \cdot \mathcal{G}, (H_0(ID_t) + s) \cdot \mathcal{G})^{(r_{1,t} + r_{2,t})} \\
&\quad \cdot \widehat{e}(\mathcal{G}, \mathcal{G})^{-r_{2,t}}) \\
&= \sum_{t=1}^{n} (\widehat{e}(\mathcal{G}, \mathcal{G})^{r_{1,t}}).
\end{aligned}$$

The right-hand side of Eq. (2) is $\sum_{t=1}^{n} m_t$, where $m_t = \widehat{e}(\mathcal{G}, \mathcal{G})^{r_{1,t}}$. Then, we can get that $\sum_{t=1}^{n} m_t = \sum_{t=1}^{n} (\widehat{e}(\mathcal{G}, \mathcal{G})^{r_{1,t}})$. Hence, Eq. (2) can hold. That is to say, batch verification in the proposed scheme is correct.

When the signature of one vehicle is valid, the signature is sent to the TCS by the RSU. Then, the TCS can recover the original traffic data from the signature. In order to check whether the recovered data is correct, we can use the features of hash function and exclusive or operation to check the recovered traffic data integrity. As the introduction in the phase of *Sign*, $B = H_2(Info_i) \| (H_3(H_2(Info_i)) \oplus Info_i)$. In this case, we get ${}_{b_2}|B| = H_2(Info_i)$. In the introduction of the data recovery phase, the system determines that the recovered data is the original data when ${}_{b_2}|B^*| = H_2(Info_i^*)$. Hence, the correctness of the recovered data can be proved.

In summary, the validity of the vehicles' signatures can be proved. Moreover, if the signature is valid, the correctness and

the integrity of the recovered traffic data can be proved [37]; that is to say, the proposed scheme can be proved to be correct. ■

B. Security Properties

Note that the security properties of data confidentiality, privacy preservation and reply attack resistance can be provided by the proposed scheme. A detailed introduction is given as follows:

- *Data Confidentiality*: In a vehicular cloud system, the traffic data can be recovered when the signature is valid; that is to say, the system should ensure that the original data cannot be obtained by entities other than the TCS [38], [39]. Due to the cryptography technologies of the hash function and the exclusive or operation, the original data are blinded in B as $H_2(Info_i)\|(H_3(H_2(Info_i))\oplus Info_i)$. Hence, the original data $Info_i$ cannot be obtained by other entities in the verification process due to the irreversibility of the hash function [40]. Thus, the proposed scheme provides the security property of data confidentiality.
- *Privacy Preservation*: In order to reduce the occurrence of malicious attacks, the private data information of vehicles must be preserved [30], [41], [42]. In our scheme, the vehicle's identity number is used to compute the secret-public key pair as $sk_i = (H_0(ID_i) + sk_R))^{-1}\cdot\mathcal{G}$ and $pk_i = H_0(ID_i)\cdot\mathcal{G} + pk_R$, respectively. From the computation of the keys, the identity of ID_i is concealed in H_0. In the *Setup* phase, H_0 is a hash function. Similar to the description in *Data Confidentiality*, the irreversibility of the hash function H_0 ensures that the vehicles' identity numbers cannot be leaked to other entities in the process of the signature verification and the data recovery. Therefore, the proposed scheme preserves the vehicle's privacy.
- *Reply Attack Resistance*: The proposed scheme can withstand reply attack due to the use of random masking technology [35], [36]. Suppose that one vehicle uses its previous security parameters r_1^*, r_2^*, secret-public keys $sk_i^{'}$ and $pk_i^{'}$ to compute a signature $\sigma_i^{'}$ to try to pass the RSU's verification. Note that $\sigma_i^{'} = (m^{'}, r_2^{'}, \eta^{'})$. As known from the *Sign* phase, the computation of the signature is computed based on r_1 and r_2. In each round, r_1 and r_2 are re-generated. Suppose that the two security parameters are r_1^* and r_2^* in the current round. In the verification equation, the left-hand side can be computed as $\widehat{e}(\eta^{'}, pk_i^{'})\cdot\widehat{e}(\mathcal{G},\mathcal{G})^{-r_2^*}$. The right-hand side can be calculated as $m^* = \widehat{e}(\mathcal{G},\mathcal{G})^{r_1^*}$. Note that the left-hand side of the equation is solved as follows:

$$\begin{aligned}
&\widehat{e}(\eta^{'}, pk_i{}^{'})\cdot\widehat{e}(\mathcal{G},\mathcal{G})^{-r_2^*}\\
&= \widehat{e}((r_1^{'}+r_2^{'})\cdot sk_i^{'}, pk_i^{'})\cdot\widehat{e}(\mathcal{G},\mathcal{G})^{-r_2^*}\\
&= \widehat{e}(sk_i^{'}, pk_i^{'})^{(r_1^{'}+r_2^{'})}\cdot\widehat{e}(\mathcal{G},\mathcal{G})^{-r_2^*}\\
&= \widehat{e}((H_0(ID_i)+s)^{-1}\cdot\mathcal{G}, (H_0(ID_i)+s)\cdot\mathcal{G})^{(r_1^{'}+r_2^{'})}\\
&\quad\cdot\widehat{e}(\mathcal{G},\mathcal{G})^{-r_2^*}\\
&= \widehat{e}(\mathcal{G},\mathcal{G})^{r_1^{'}+r_2^{'}-r_2^*}.
\end{aligned}$$

We can see that the verification equation cannot hold; that is to say, a vehicle cannot use its previous signature to pass the RSU's verification. Hence, our scheme is secure against the reply attack.

From the above description, it can be concluded that our scheme provides the expected security properties, including data confidentiality, privacy preservation and reply attack resistance.

TABLE II
COMPARISON OF COMMUNICATION COST

Scheme	Communication Cost
Han *et al.*'s Scheme [22]	$(p+1)l_{\mathbb{Z}_q}$
Du *et al.*'s Scheme [24]	$12l_{\mathbb{Z}_q} + 1l_{\mathbb{G}}$
Our Scheme	$3l_{\mathbb{Z}_q} + 6l_{\mathbb{G}}$

*p: The number of sketches in [22].
*$l_{\mathbb{Z}_q}$: Bit-length of the parameter in $\mathbb{Z}_q$.
*$l_{\mathbb{G}}$: Bit-length of parameter in $\mathbb{G}$.

VI. PERFORMANCE ANALYSIS

This section analyzes the performance of the proposed scheme. First, the proposed scheme is compared with similar schemes [22], [24]. To determine the efficiency of our scheme, we simulate the proposed scheme and similar schemes on a PBC based experimental platform.

A. Comparison Analysis

In order to indicate the high efficiency of our scheme, the communication and computational costs of our scheme are compared with those of Han *et al.*'s scheme [22] and Du *et al.*'s scheme [24].

Table II shows the comparison of the communication cost of the proposed scheme and previous schemes [22], [24]. Note that $l_{\mathbb{Z}_q}$ and $l_{\mathbb{G}}$ denote the bit-length of the parameters generated in $\mathbb{Z}_q$ and $\mathbb{G}$, respectively. The comparison shows that the communication cost of previous schemes is $(p+1)l_{\mathbb{Z}_q}$ and $12l_{\mathbb{Z}_q} + 1l_{\mathbb{G}}$, respectively. Here, the symbol of p is the number of sketches in [22]. The communication cost of our scheme is $3l_{\mathbb{Z}_q} + 6l_{\mathbb{G}}$. Moreover, the communication cost of Han *et al.*'s scheme will be very high if sketches p is large. Although our scheme has much $l_{\mathbb{G}}$ cost compared to Du *et al.*'s scheme, Du *et al.*'s scheme has high communication cost of the $l_{\mathbb{Z}_q}$ parameter. In addition, we can get that Du *et al.*'s scheme has more $l_{\mathbb{Z}_q}$ parameters compared to the proposed scheme. In other words, the proposed scheme is more efficient than Han *et al.*'s scheme and Du *et al.*'s scheme with respect to communication cost.

The computational cost of the proposed scheme is also compared with that of previous schemes [22], [24]. Table III shows the comparison result of the computational cost. To better express the computational cost, we use $T_{H.}$, $T_{E.}$, $T_{Mul.}$, $T_{P.}$, $T_{Add.}$, $T_{C.}$ and $T_{X.}$ to denote the time required to execute hash function, exponentiation operation, multiplication, pairing map, addition, concatenation and xor (exclusive-or). Moreover, the symbols of p and k are the number of sketches and

TABLE III
COMPARISON OF COMPUTATIONAL COST

Schemes / Aspects	Han *et al.*'s Scheme [22]	Du *et al.*'s Scheme[24]	The Proposed Scheme
Server-Side	$kT_{H.}$+$10T_{E.}$+$3T_{Mul.}$+$1T_{Add.}$ +$5T_{C.}$	$4T_{H.}$+$5T_{E.}$+$3T_{Mul.}$+$2T_{C.}$	$3T_{H.}$+$2T_{E.}$+$3T_{Mul.}$+$2T_{P.}$ +$2T_{Add.}$+$3T_{X.}$
Vehicle-Side	$1T_{H.}$+$3T_{E.}$+$1T_{Mul.}$+$pT_{Add.}$	$5T_{H.}$+$2T_{E.}$+$2T_{Mul.}$+$2T_{P.}$ +$3T_{C.}$	$4T_{H.}$+$1T_{E.}$+$1T_{Mul.}$+$1T_{P.}$+$1T_{Add.}$ +$1T_{C.}$+$2T_{X.}$
Total	$(k$+$1)T_{H.}$+$13T_{E.}$+$4T_{Mul.}$+$(p$+$1)T_{Add.}$ +$5T_{C.}$	$9T_{H.}$+$7T_{E.}$+$5T_{Mul.}$+$2T_{P.}$ +$5T_{C.}$	$7T_{H.}$+$3T_{E.}$+$4T_{Mul.}$+$3T_{P.}$ +$3T_{Add.}$+$1T_{C.}$+$5T_{X.}$

*$T_{H.}, T_{E.}, T_{Mul.}, T_{P.}, T_{Add.}, T_{C.}, T_{X.}$: The time required to execute the corresponding operations.
*p, k: The number of sketches and sketch tuples in [22].

sketch tuples in [22], respectively. Note that the computational cost is compared from three aspects, namely, the server-side computational cost, the vehicle-side computational cost and the total computational cost. To make the computational cost is easier to compare, the server-side is composed of entities other than the vehicle in the system. From Table III, we can see that Han *et al.*'s scheme costs $kT_{H.} + 10T_{E.} + 3T_{Mul.} + 1T_{Add.} + 5T_{C.}$ and $1T_{H.} + 3T_{E.} + 1T_{Mul.} + pT_{Add.}$ at the server-side and the vehicle-side, respectively. It is worthy noting that the cost in Han *et al.*'s scheme is determined by sketches and sketch tuples. The computational cost of Han *et al.*'s scheme [22] is linearly increased with the growth of sketches and sketch tuples. Compared to the constant size of the computational cost in similar scheme [24] and the proposed scheme, it can be concluded that Han *et al.*'s scheme [22] is less efficient than similar scheme [24] and the proposed scheme. The computational cost at the server-side in Du *et al.*'s scheme is $4T_{H.} + 5T_{E.} + 3T_{Mul.} + 2T_{C.}$. Correspondingly, the proposed scheme costs $3T_{H.} + 2T_{E.} + 3T_{Mul.} + 2T_{P.} + 2T_{Add.} + 3T_{X.}$ at the server-side. Compared to similar scheme [24], our scheme has additional computational cost of $2T_{P.} + 2T_{Add.} + 3T_{X.}$. However, the computational cost of *H.* and *E.* is increased approximately 1 time compared to that of our scheme. At the vehicle-side, the computational costs of our scheme and Du *et al.*'s scheme is $4T_{H.} + 1T_{E.} + 1T_{Mul.} + 1T_{P.} + 1T_{Add.} + 1T_{C.} + 2T_{X.}$ and $5T_{H.} + 2T_{E.} + 2T_{Mul.} + 2T_{P.} + 3T_{C.}$, respectively. The comparison at the vehicle-side shows that our scheme has additional operations of *Add.* and *X.*. The computational cost of *X.* is small and negligible in the security community. Although the operation of *Add.* may result in high computational cost, the computational cost of the other operations at the vehicle-side in [24] is higher than that in the proposed scheme. In summary, the computational costs of the server-side and the vehicle-side of our scheme are much less than those of Du *et al.*'s scheme. Hence, the total computational cost of our scheme is less than Du *et al.*'s scheme. Table III shows the total cost of our scheme and Du *et al.*'s scheme is $7T_{H.} + 3T_{E.} + 4T_{Mul.} + 3T_{P.} + 3T_{Add.} + 1T_{C.} + 5T_{X.}$ and $9T_{H.} + 7T_{E.} + 5T_{Mul.} + 2T_{P.} + 5T_{C.}$, respectively. Similar to the analysis of the comparison above, it can be summarized that our scheme has lower computational costs than previous schemes [22], [24].

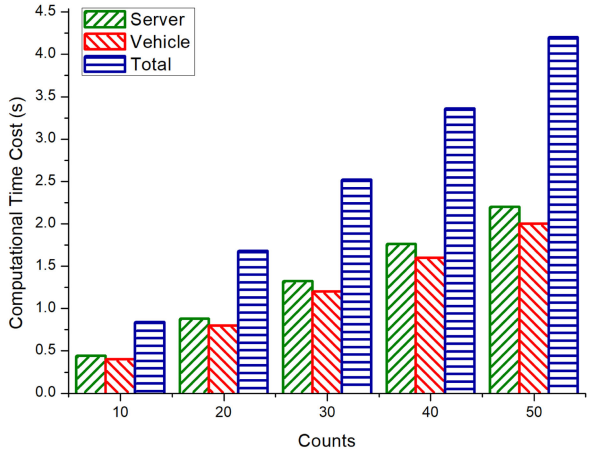


Fig. 2. Simulation of the proposed scheme.

B. Simulation Analysis

The proposed scheme and similar schemes [22], [24] are simulated on an experimental platform constructed based on the cryptographic function libraries of GMP [1] and PBC [2] library. The simulation computer is installed with the Linux system. The RAM is 8 GB, and the CPU is an Intel Xeon E5-2650 v2 at 2.60 GHZ.

The computational time of the proposed scheme is simulated. Fig. 2 is the simulation results. The time cost in Fig. 2 shows that the server-side and vehicle-side, as well as the total time cost, increase with the growth of the experimental count. Moreover, the server-side costs have more time compared to the vehicle-side under the condition of the same count. The main reason for the higher time cost at the server-side is that the server needs to execute the operations of the signature verification and original data recovery. Although the time cost in the proposed scheme increases with the growth of counts, the time is within acceptable range.

We also simulate the computational time of previous schemes [22], [24] at the two sides of server and vehicle, as well

[1]GNU Multiple Precision Arithmetic: http://gmplib.org/
[2]Paring Based Cryptography: http://crypto.stanford.edu/pbc/

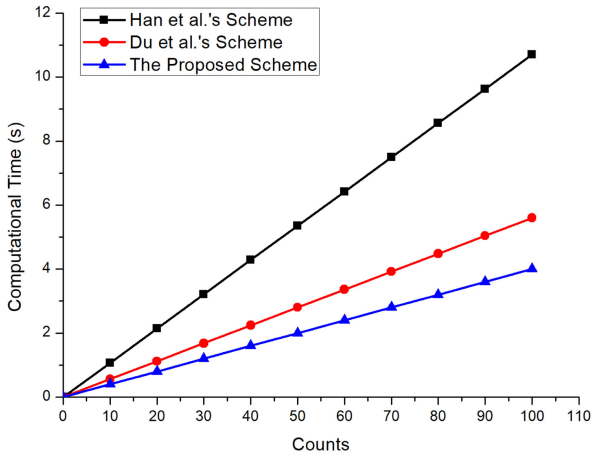


Fig. 3. The simulation result of the computation at the server-side.

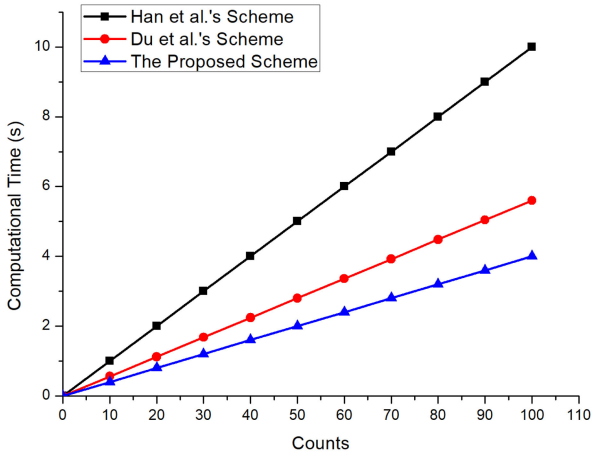


Fig. 4. The simulation result of the computation at the vehicle-side.

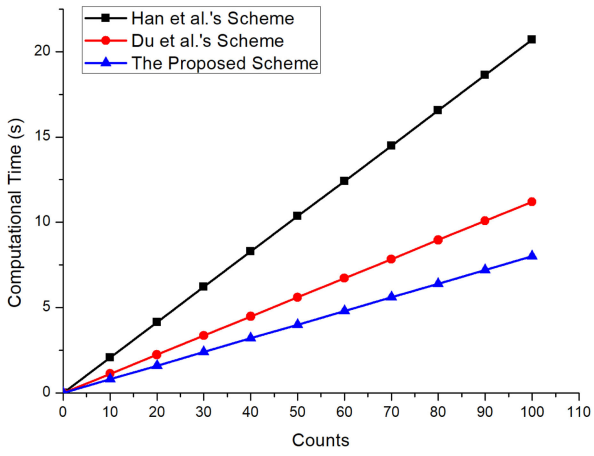


Fig. 5. The simulation result of the total computation.

as the total cost. Here, the number of sketches and sketch tuples in [22] is selected as 100 and 50, respectively. The simulation results at the server-side and the vehicle-side are depicted in Figs. 3 and 4. The total time cost of the proposed scheme and the previous schemes is shown in Fig. 5. It is worthy noting that Figs. 3, 4 and 5 show that the trends of the simulation results are the same. In other words, the time cost of our scheme and the three similar schemes is increased when the number of counts increases. However, the computational time of the proposed scheme increases slower in comparison to the other two schemes. Moreover, the computational time cost of the two similar schemes is always larger than that of the proposed scheme. In summary, the previous schemes [22], [24] have more time as compared to our scheme at the server and vehicle sides. In addition, the total time cost of our scheme is much less than that of previous schemes [22], [24]. Hence, it can be concluded that the proposed scheme is more efficient in comparison to the previous schemes.

VII. Conclusion

With the rapid development of VANETs, the concept of the vehicular cloud has been proposed, and it can be applied to process many traffic issues. In this paper, a secure real-time traffic data aggregation scheme is proposed, which is constructed based on the MRS and can be used for the vehicular cloud in VANETs. The validity of vehicle's signatures can be verified in the proposed scheme. Moreover, the original traffic data can also be recovered from the valid signatures. Note that the basic scheme in the proposed scheme can also be extended to support batch verification. Security analysis shows that our scheme can be proved to be correct. The security properties of data confidentiality, privacy preservation and reply attack resistance can be provided in the proposed scheme. In addition, we compare the proposed scheme with previous schemes in terms of communication and computation. The comparison results show that our scheme cost less operations compared to the previous schemes. To determine the high efficiency of the proposed scheme, an experimental platform is constructed based on GMP and PBC to simulate the proposed scheme and previous schemes. The simulation results demonstrate that our scheme costs less computational time than the previous schemes. Therefore, our scheme can be implemented in the vehicular cloud to aggregate traffic data to provide additional traffic services.

References

[1] E. Lee, E. K. Lee, M. Gerla, and S. Y. Oh, "Vehicular cloud networking: Architecture and design principles," *Commun. Mag.*, vol. 52, no. 2, pp. 148–155, 2014.

[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.*, to be published, doi: 10.1007/s11554-019-00887-6.

[3] X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, "New publicly verifiable databases with efficient updates," *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 5, pp. 546–556, Sep./Oct. 2015.

[4] 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.*, to be published, doi: 10.1109/TETC.2017.2776402.

[5] S. Zeadally, R. Hunt, Y. S. Chen, A. Irwin, and A. Hassan, "Vehicular ad hoc networks (VANETs): Status, results, and challenges," *Telecommun. Syst.*, vol. 50, no. 4, pp. 217–241, 2012.

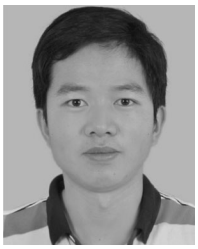
[6] C. Wang, J. Shen, C.-F. Lai, R. Huang, and F. Wei, "Neighborhood trustworthiness based vehicle-to-vehicle authentication scheme for vehicular ad hoc networks," *Concurrency Comput.: Practice Experience*, vol. 31, 2019, Art. no. e4643.

[7] 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.
[8] C. C. Lee, T. H. Lin, and R. X. Chang, "A secure dynamic id based remote user authentication scheme for multi-server environment using smart cards," *Expert Syst. Appl.*, vol. 38, no. 11, pp. 13863–13870, 2011.
[9] M. K. Jiau, S. C. Huang, J. N. Hwang, and A. V. Vasilakos, "Multimedia services in cloud-based vehicular networks," *IEEE Intell. Transp. Syst. Mag.*, vol. 7, no. 3, pp. 62–79, Jul. 2015.
[10] M. K. Sharma and A. Kaur, "A survey on vehicular cloud computing and its security," in *Proc. Int. Conf. Next Gener. Comput. Technol.*, 2016, pp. 67–71.
[11] J. Shen, D. Liu, C.-F. Lai, Y. Ren, J. Wang, and X. Sun, "A secure identity-based dynamic group data sharing scheme for cloud computing," *J. Internet Technol.*, vol. 18, no. 4, pp. 833–842, 2017.
[12] X. Chen, J. Li, J. Li, X. Huang, Y. Xiang, and D. S. Wong, "Secure outsourced attribute-based signatures," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 12, pp. 3285–3294, Dec. 2014.
[13] D. Liu, J. Shen, A. Wang, and C. Wang, "Lightweight and practical node clustering authentication protocol for hierarchical wireless sensor networks," *Int. J. Sensor Netw.*, vol. 27, no. 2, pp. 95–102, 2018.
[14] M. Zhang, Y. Yao, B. Li, and C. Tang, "Accountable mobile e-commerce scheme in intelligent cloud system transactions," *J. Ambient Intell. Humanized Comput.*, vol. 9, pp. 1889–1899, Nov. 2018.
[15] N. Kumar, K. Kaur, S. C. Misra, and R. Iqbal, "An intelligent RFID-enabled authentication scheme for healthcare applications in vehicular mobile cloud," *Peer-to-Peer Netw. Appl.*, vol. 9, no. 5, pp. 824–840, 2016.
[16] M. K. Sharma, R. S. Bali, and A. Kaur, "Dyanimc key based authentication scheme for vehicular cloud computing," in *Proc. Int. Conf. Green Comput. Internet Things*, 2016, pp. 1059–1064.
[17] S. Ozdemir and Y. Xiao, "Secure data aggregation in wireless sensor networks: A comprehensive overview," *Comput. Netw.*, vol. 53, no. 12, pp. 2022–2037, 2009.
[18] Y. Yang, X. Wang, S. Zhu, and G. Cao, "SDAP: A secure hop-by-hop data aggregation protocol for sensor networks," in *Proc. ACM Int. Symp. Mobile Ad Hoc Netw. Comput.*, 2006, pp. 356–367.
[19] Y. Zhang, Y. Yu, M. Nekovee, Y. Liu, S. Xie, and S. Gjessing, "Cognitive machine-to-machine communications: Visions and potentials for the smart grid," *IEEE Netw. Mag.*, vol. 26, no. 3, pp. 6–13, May/Jun. 2012.
[20] H. O. Sanli, S. Ozdemir, and H. Cam, "SRDA: Secure reference-based data aggregation protocol for wireless sensor networks," in *Proc. Veh. Technol. Conf.*, 2005, pp. 4650–4654.
[21] K. Shafiee and V. C. M. Leung, "A novel localized data aggregation algorithm for advanced vehicular traffic information systems," in *Proc. IEEE Int. Conf. Commun. Workshops*, 2009, pp. 1–5.
[22] Q. Han, S. Du, D. Ren, and H. Zhu, "SAS: A secure data aggregation scheme in vehicular sensing networks," in *Proc. Int. Conf. Commun.*, 2010, pp. 1–5.
[23] M. Shoaib and W. C. Song, "Data aggregation for vehicular ad-hoc network using particle swarm optimization," in *Proc. Netw. Oper. Manage. Symp.*, 2012, pp. 1–6.
[24] S. Du, T. Peng, K. Ota, and Z. Haojin, "A secure and efficient data aggregation framework in vehicular sensing networks," *Int. J. Distrib. Sensor Netw.*, vol. 2013, no. 3, pp. 1–10, 2013.
[25] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in *Proc. Int. Cryptology Conf. Adv. Cryptology*, 2001, pp. 213–229.
[26] K. Nyberg and R. A. Rueppel, "A new signature scheme based on the DSA giving message recovery," in *Proc. ACM Conf. Comput. Commun. Secur.*, 1993, pp. 58–61.
[27] J. Zhang, W. Zou, D. Chen, and Y. Wang, "On the security of a digital signature with message recovery using self-certified public key," *Informatica*, vol. 29, no. 3, pp. 343–346, 2005.
[28] R. Lu and Z. Cao, "Designated verifier proxy signature scheme with message recovery," *Appl. Math. Comput.*, vol. 169, no. 2, pp. 1237–1246, 2005.
[29] R. Tso, C. Gu, T. Okamoto, and E. Okamoto, "An efficient id-based digital signature with message recovery based on pairing," *IACR Cryptology ePrint Archive*, vol. 2006, no. 195, pp. 1–15, 2006.
[30] J. Cui, J. Zhang, H. Zhong, and Y. Xu, "SPACF: A secure privacy-preserving authentication scheme for VANET with cuckoo filter," *IEEE Trans. Veh. Technol.*, vol. 66, no. 11, pp. 10283–10295, Nov. 2017.
[31] L. Gu, D. Zeng, and S. Guo, "Vehicular cloud computing: A survey," in *Proc. GLOBECOM Workshops*, 2014, pp. 403–407.
[32] R. Yu, Y. Zhang, S. Gjessing, and W. Xia, "Toward cloud-based vehicular networks with efficient resource management," *IEEE Netw.*, vol. 27, no. 5, pp. 48–55, Sep./Oct. 2013.
[33] K. Mershad and H. Artail, "Finding a star in a vehicular cloud," *IEEE Intell. Transp. Syst. Mag.*, vol. 5, no. 2, pp. 55–68, Apr. 2013.
[34] C. Zhang, X. Lin, R. Lu, and P. H. Ho, "Raise: An efficient RSU-aided message authentication scheme in vehicular communication networks," in *Proc. Int. Conf. Commun.*, 2008, pp. 1451–1457.
[35] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 5, pp. 847–859, May 2011.
[36] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," *IEEE Trans. Comput.*, vol. 62, no. 2, pp. 362–375, Feb. 2013.
[37] T. Zhou, J. Shen, X. Li, C. Wang, and J. Shen, "Quantum cryptography for the future internet and the security analysis," *Secur. Commun. Netw.*, vol. 2018, 2018, Art. no. 8214619.
[38] Y. Zhu, G. Ahn, H. Hu, S. S. Yau, H. G. An, and C. Hu, "Dynamic audit services for outsourced storages in clouds," *IEEE Trans. Services Comput.*, vol. 6, no. 2, pp. 227–238, Apr.–Jun. 2013.
[39] H. Tian *et al.*, "Dynamic-hash-table based public auditing for secure cloud storage," *IEEE Trans. Services Comput.*, vol. 10, no. 5, pp. 701–714, Sep./Oct. 2017.
[40] V. Shoup, "A composition theorem for universal one-way hash functions," in *Proc. Int. Conf. Theory Appl. Cryptographic Techn.*, 2000, pp. 445–452.
[41] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun, and Y. Xiang, "Block design-based key agreement for group data sharing in cloud computing," *IEEE Trans. Dependable Secure Comput.*, vol. 16, no. 6, pp. 996–1010, Nov.–Dec. 1, 2019.
[42] S. Lins, S. Schneider, and A. Sunyaev, "Trust is good, control is better: Creating secure clouds by continuous auditing," *IEEE Trans. Cloud Comput.*, vol. 6, no. 3, pp. 890–903, Jul.-Sep. 2018.

Jian Shen received the M.E. and Ph.D. degrees in computer science from Chosun University, Gwangju, South Korea, in 2009 and 2012, respectively. Since late 2012, he has been a Professor with the Nanjing University of Information Science and Technology, Nanjing, China. His research interests include public cryptography, cloud computing and security, data auditing and sharing, and information security systems.

Dengzhi Liu received the B.S. and M.E. degrees from the Nanjing University of Information Science and Technology, Nanjing, China, in 2014 and 2017, respectively. He is currently working toward the Ph.D. degree with the School of Computer and Software, Nanjing University of Information Science and Technology. He research focuses on the security and privacy issues in cloud computing. His current research interests include applied cryptography, network and data security, and cloud computing security.

Xiaofeng Chen received the B.S. and M.S. degrees in mathematics from Northwest University, Xi'an, China, in 1998 and 2000, respectively, and the Ph.D. degree in cryptography from Xidian University, Xi'an, China, in 2003. He is currently a Professor with Xidian University. His research interests include applied cryptography and cloud computing security. He has authored or coauthored more than 200 research papers in refereed international conferences and journals. His work has been cited more than 7000 times at Google Scholar. He is on the editorial board of the IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, *Security and Privacy*, *Computing and Informatics*, etc. He was the Program/General Chair or Program Committee Member in more than 30 international conferences.



Jin Li received the B.S. degree in mathematics from Southwest University, Chongqing, China, in 2002 and the Ph.D. degree in information security from Sun Yat-sen University, Guangzhou, China, in 2007. He is currently a Professor with Guangzhou University, Guangzhou, China. His research interests include applied cryptography and security in cloud computing. He has authored or coauthored more than 50 research papers in refereed international conferences and journals. He was the Program Chair or Program Committee Member in many international conferences. He has been selected as one of science and technology new star in Guangdong province.

Neeraj Kumar received the Ph.D. degree in computer science and engineering from Shri Mata Vaishno Devi University, Katra, India. He is currently an Associate Professor with the Department of Computer Science and Engineering, Thapar University, Patiala, India. He has authored or coauthored more than 300 technical research papers in leading journals such as the IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS, IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, the IEEE TWPS, IEEE SYSTEMS JOURNAL, IEEE COMMUNICATIONS MAGAZINE, the IEEE WIRELESS COMMUNICATIONS MAGAZINE, the IEEE NETWORK MAGAZINE, and conferences. His research is supported from DST, TCS, and UGC. He has guided many students leading to M.E. and Ph.D. degrees. His research interests include mobile computing, parallel/distributed computing, multiagent systems, service-oriented computing, routing and security issues in mobile ad hoc, and sensor and mesh networks. He is recipient of best papers award from IEEE SYSTEMS JOURNAL in 2018 and IEEE International Conference on Communications (ICC) in 2018. He is a TPC Member/Technical Committee Member of various conferences and organized various workshops in ICC, and Globecom conferences.

Pandi Vijayakumar received the B.Eng. degree from Madurai Kamaraj University, Madurai, India, in 2002, the M.Eng. degree in computer science and engineering from the Karunya Institute of Technology, Coimbatore, India, in 2005, and the Ph.D. degree in computer science and engineering from Anna University, Chennai, India, in 2013. He was the former Dean of the University College of Engineering, Tindivanam, India, and is currently an Assistant Professor with the Department of Computer Science and Engineering. He is guiding many Ph.D. scholars in the field of network and cloud security. He has authored or co-authored various quality papers in reputed journals like IEEE TRANSACTIONS, *Elsevier, Springer, IET, Taylor & Francis, Wiley*, etc. His main research include management in network security and multicasting in computer networks.