# Extensible Conditional Privacy Protection Authentication Scheme for Secure Vehicular Networks in a Multi-Cloud Environment

Jie Cui, Xiaoyu Zhang, Hong Zhong, Jing Zhang, Lu Liu

***Abstract*—With an increasing number of cloud service providers (CSPs), research works on multi-cloud environments to provide solutions to avoid vendor lock-in and deal with the single-point failure problem have expanded considerably. However, a few schemes focus on the conditional privacy protection authentication of vehicular networks under a multi-cloud environment. In this regard, we propose a robust and extensible authentication scheme for vehicular networks to fulfil the ever-growing diversified service demands from users. According to our solution, the vehicles need to register with the trusted authority (TA) only once to achieve a fast and efficient authentication with CSPs. Additionally, as long as the new CSP is successfully registered in TA, it can participate in vehicular service. A cloud broker, which is managed by the TA, is responsible for connecting all the cloud services; consequently, the complexity involved in the selection of CSPs is hidden from the users' view. A detailed security analysis establishes that our scheme can fulfil conditional privacy protection and achieve the security objectives of vehicular networks. Our scheme is based on elliptic curve cryptography and does not employ the complex bilinear pairing operation. An evaluation of performance of the proposed scheme indicates that it is suitable for applications involving vehicular networks.**

***Index Terms*—Vehicular networks, multi-cloud environment, authentication, elliptic curve**

## I. Introduction

As an indispensable part of the Internet of Things, vehicular networks play an ever-increasing important role in our daily life. Vehicular networks are employed by the vehicles with the aid of advanced on-board units that demonstrate excellent sensing, communication, and network functions to communicate with neighboring vehicles or infrastructure for achieving two primary applications [1]. Firstly, the vehicular network ensures safety by providing the drivers with information on road conditions and traffic conditions to improve the traffic efficiency. Secondly, it delivers infotainment by providing the users with map downloads, online entertainment information, and other services to enhance the driving experience and travel pleasure [2].

Although vehicular networks present significant advantages in our everyday life, there are several challenges in achieving their large-scale deployment. First, vehicular communication in a wireless environment is vulnerable to malicious attacks by adversaries, which can cause the information be intercepted, forged, or tampered with [3]. It is, therefore, important to ensure the privacy and integrity of the messages [4]. Second, the explosive increase in the number of vehicles and the diversified demands for new vehicular services require the researchers to critically explore relevant novel solutions in this field [5].

Some researchers have proposed the concept of vehicular clouds. A vehicular cloud is a temporary cloud that comprises many volunteer vehicles [1], [6]. Although this approach of building a cloud exploits the redundant power of vehicles and expands the computing, processing, and storage capabilities of traditional clouds to some extent, some unresolved problems still persist. For instance, there is no specific tactic to effectively select the relay vehicles. Moreover, this approach results in new security and privacy risks. For example, intermittent short-range communication in high-dynamic network environments can pose difficulties in providing a reliable commitment to the computation-intensive and delay-sensitive applications [7].

Therefore, optimizing and expanding the traditional vehicular cloud architecture demonstrates greater practical significance [8]. Nevertheless, simply adopting the previous vehicles and the single cloud service provider (CSP) mutual authentication scheme under the new situation is impossible mainly because they do not consider the need for users to switch and choose among multiple cloud service providers [9], [10]. Therefore, in this study, we consider the authentication scheme of vehicular networks in a multi-cloud environment. The term "multi-cloud" signifies different cloud services provided by multiple CSPs. Multi-cloud is essentially a strategy rather than a technology [11]. Studies on this strategy have been increasingly prevalent in recent times [12]. The key reason is that it not only provides users with more flexible choices and highly diverse services but also prevents the vendor lock-in and risk of a single-point failure [8].

Meanwhile, the users encounter difficulties in effectively considering one appropriate CSP due to the emergence of several service providers [13]. To address this problem, we use the cloud broker (CB), which refers to an entity that manages the application, performance, and delivery of the cloud services [14]. And according to the National Institute for Standards and Technology (NIST), cloud brokering services are mapped into three general areas: service intermediation, service aggregation and service arbitrage [15], [16]. In our scheme, CB mainly manages the negotiation between the CSPs

J. Cui, X. Zhang, H. Zhong, J. Zhang are with the School of Computer Science and Technology, Anhui University, Hefei 230039, China, the Anhui Engineering Laboratory of IoT Security Technologies, Anhui University, Hefei 230039, China, and the Institute of Physical Science and Information Technology, Anhui University, Hefei 230039, China (e-mail: zhongh@ahu.edu.cn).

L. Liu is with the Department of Informatics, University of Leicester, LE1 7RH, UK (email: ll297@leicester.ac.uk).

and vehicles by acting as an intermediary for providing users with superior service experience [17].

The aforementioned analysis signifies the importance of studying the authentication scheme of vehicular networks over multi-cloud environments. Therefore, in this study, we present an extensible conditional privacy protection authentication scheme based on the proposed novel vehicular network model in a multi-cloud environment. It is worth mentioning that this scheme is suitable for the 3G, 4G, and emerging 5G networks environments, as it does not require the roadside base stations to participate in the authentication process.

### A. Our Motivations

Firstly, references [18] and [19] make us realize that the research on a multi-cloud environment is important and of great practical significance. Secondly, the existing research on mobile phones and mobile medical devices in a multi-cloud environment [20], [21], [22], [23] lets us focus on the vehicular networks which is a sub-category of mobile Internet of Things. In addition, the reference [24] mentions that the multi-cloud environment is beneficial to solving server management problems in vehicular networks. All in all, the above references strengthen our determination to study vehicular networks in a multi-cloud environment.

### B. Our Contributions

To the best of our knowledge, this is the first authentication scheme for secure vehicular networks in a multi-cloud environment with a CB that acts as an intermediary. The main contributions are summarized as follows:

- We propose a novel vehicular network architecture for a multi-cloud environment. The CB which is managed by the trusted authority (TA) selects appropriate CSPs for vehicles; consequently, the complexity in the selection of CSPs is hidden from the users' view and the dependence of vehicles on a single CSP is eliminated.
- The vehicles and CSPs need to register with the TA only once for mutual authentication and session key agreement. The proposed scheme alleviates the hassle of key management of vehicles and eliminates the trouble of repeated registrations of vehicles with different CSPs. Moreover, it does not require the CSPs to maintain the considerable amount of redundant registration information of vehicles.
- An in-depth security analysis confirms that the proposed scheme can achieve the security objectives of vehicular networks. Furthermore, during the entire authentication phase, the vehicles can remain anonymous to CSPs resulting in better privacy protection. The scheme employs the elliptic curve encryption algorithm, and the comparison results with recent related schemes indicates that it is suitable for deployment in real-world applications.

### C. Organization of the Rest Paper

Section II introduces the related work. Section III provides the background knowledge used in this study. In Section IV, the specific scheme is presented. Then, Section V shows the detailed security proof and analysis. In Section VI is the performance analysis and comparison from the aspects of computation and communication costs. Finally, some concluding remarks is provided in Section VII.

## II. Related Work

The increasing number of vehicles and the urgent demands for diversified vehicular services have already motivated the global academic and business community devoted exclusively to introduce novel pragmatic paradigms in the new situation.

In 2010, Olariu *et al.* [6] first proposed the concept of Autonomous Vehicular Cloud (AVC), which means that underutilized autonomous vehicles gather together to form a temporary cloud for dynamically allocating available resources to authorized users.

Later, Bitam *et al.* [25] proposed that integrating traditional permanent clouds with temporary clouds formed by static vehicles. Through the combination of these two sub-modules, vehicular ad hoc network cloud (VANET-Cloud) is constructed to further expand the traditional cloud resources and better satisfy the needs requested by road users.

Bhoi *et al.* [26] also considered that the resources of static vehicles in the parked lots as the data centers, providing storage services for the vehicles, and proposed a new task scheduling policy. However, the proposed system is based only on resources within the vehicles, ignoring the advantages of traditional cloud computing [27].

It is noteworthy that in the above schemes, the entry and departure of vehicles in the parking lot makes the network environment dynamic, so it is very challenging to efficiently assign tasks to vehicles [28].

Recently, Shao *et al.* [29] reduced the computing burden of task-requesting vehicles by outsourcing time-consuming bilinear pairing operations to connected vehicular cloud computing (CVCC) which integrates computing resources from traditional clouds, the roadside units (RSUs) and vehicles with underutilized resources. However, this model poses new challenges, such as data security and computational security, due to it allowing potential malicious vehicles to participate in CVCC, while the solution lacks a clear protocol on how to manage server vehicles that leaving CVCC before finishing the task.

In the scheme of Wang *et al.* [7], a novel dynamic vehicle-based cloudlet relaying scheme was proposed for the first time to alleviate the burden of mobile computing and make a reliable commitment to delay-sensitive applications to a certain extent. However, the scheme does not consider how to select vehicles in the cloudlet to cope with the rapid change of network topology.

According to [30], VANET-based clouds have three main architectural frameworks: vehicular clouds (VCs), vehicles using clouds (VuCs), and hybrid vehicular clouds (HVCs). The mentioned [6], [26] and [25], [29] belong to the first and third types respectively. In addition, through the previous analysis, we can find that even though the above schemes improve the resource utilization rate of idle vehicles and reduce service response time, there are still a series of problems to be addressed, especially the selection, management and task allocation of participating vehicles [31].

Therefore, we propose a novel vehicular network authentication scheme which can be attributed to the extension of VuCs, the second combination type, in a multi-cloud environment. In fact, multi-cloud has received widespread attention in the past few years [29], [32]. The existing literatures signify that it is imperative to construct a multi-cloud environment under the new situation [33], [34], [35].

We pursue the multi-cloud strategy because of the following advantages of vehicular network deployed in a multi-cloud environment:1) No longer limited to the limited choices offered by a single CSP, multi-cloud can provide users with more flexible choices. While meeting the upsurge diversified demand of a large number of users, it can avoid vendor lock-in and reduce users' over-dependence on a single CSP [11]; 2) The multi-cloud environments can increase the flexibility of the entire system, reduce the risk of vehicle data loss, and avoid a single-point failure of CSP in the process of vehicle access to the service, which results in service interruption [34].

Meanwhile, in order to cope with the problem of the selection of CSPs caused by multi-cloud environments [13], [35], we also introduce the entity of cloud broker [36]. As an crucial part of the cloud architecture, the main role of cloud broker in this study is reflected in: 1) Enable users to interact through a single interface that connects to multiple CSPs; 2) Concealing the complexity of the selection of CSPs from the perspective of the vehicle users; 3) Manage the use, performance and delivery of cloud services, effectively allocate and manage resources, and negotiate the relationship between CSPs and vehicles [14].

Additionally, considering the unique characteristics of the vehicular networks, existing encryption authentication schemes applied to multi-cloud environments in other fields such as medical care can not be directly applied to the vehicular networks. For instance, highly dynamic network topology and limited computing power of on-board units require the scheme has low time overhead, and because the vehicular networks involves significant property and privacy security, the solution must be able to withstand a variety of common types of attacks and meet the requirement of conditional privacy protection [37], [38]. Therefore, in order to fill this gap, researchers need to devote special attention to this issue.

## III. System Model

In this section, the proposed vehicular network model in a multi-cloud environment along with its system assumptions are introduced firstly. Then we present the specific security objectives.

### A. Network Model and Assumptions

Fig. 1 illustrates our system model over a multi-cloud environment. It mainly contains the trusted authority (TA), cloud broker (CB), cloud service providers (CSPs), vehicles, and base stations. The main functions of each entity and the system assumptions are described below.

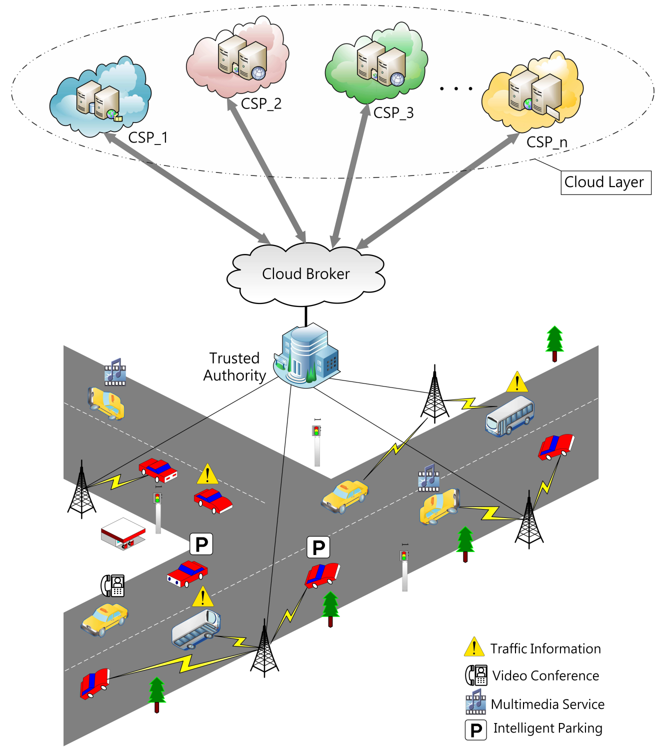



Fig. 1. The vehicular network model in a multi-cloud environment.

1) ***TA***: It is a widely accepted, reliable, independent and highly secure entity, which is undertaken by an Intelligent Transport System (ITS) department of government [39]. The TA equipped with tamper-resistant hardware has sufficient storage space and excellent computing capacity [40]. Its services are provided and underwritten by technical, legal, financial and/or structural means [41]. The TA is responsible for generating system parameters, and the registration of vehicles and CSPs. It is the only entity that can track the real identity of vehicles. It is assumed that the TA will never be compromised.
2) ***CB***: It is governed by the TA and acts as an intermediary between vehicles and CSPs. The CB comprised of a partitioner, encryptor, decryptor, hash key generator, verifier and local database manager [42]. It is assumed that the CB will not be compromised. The CB is in charge of managing the application, performance and delivery of the cloud services, and assisting vehicle users in selecting the CSP that best suits their needs.
3) ***CSP***: It provides vehicles with route recommendation, video-conferencing and driving assistance services, etc. Additionally, data in the tachograph can be stored in CSPs to alleviate the burden of content storage of vehicles, and prevent data loss due to the malfunction of the on-board equipment. The trusted computing platform (TCP) which is based on trusted platform module (TPM) is integrated into the cloud computing system [43]. And the TCP is used in authentication, confidentiality and integrity in cloud computing environment [44]. It is

assumed that the CSP is honest-but-curious, that is, it will faithfully enforce the scheme but is curious about vehicles' privacy data.

4) ***Vehicle***: Vehicles are equipped with advanced on-board units (OBUs), which have good wireless communication capabilities, and limited computing power and storage space. The embedded TPM is a tamper-proof equipment that will not be broken. It is responsible for storing secret information related to vehicular communications and performing basic encryption and decryption operations [45]. Besides, the OBU possesses the functions for dedicated short-range communications (DSRC) communication, a wide area network connection, the electronic control units (ECU) connection, etc [46], [47].
5) ***Base station***: It is deployed on both roadside as well as hotspots, and only responsible for relaying the messages in the vehicular networks. Since it does not involve any cryptographic operations, even if the base stations are compromised, no valuable information will be leaked. It is assumed that base stations are able to provide seamless coverage for vehicular communications with super-fast speed.

Note that, in view of the considerable amount of vehicles, the redundant TAs which have identical functionalities can be deployed based on the size of service area, to avoid becoming a single fault or a bottleneck [48]. Geographically distributed TAs collaborate for the network.

### *B. Security Objectives*

The scheme is supposed to achieve the following security objectives:

1) ***Anonymity***: In order to realize the privacy protection of vehicle's identity, the attackers cannot calculate its real identity from the messages. The real identity of vehicle keeps anonymous to all entities.
2) ***Traceability***: When the vehicle or cloud service provider misbehaves, the TA can derive the real identity of these participating entities through the messages.
3) ***Mutual authentication***: In order to ensure the reliability of the participants, the TA and CSPs as well as vehicles should be able to verify the legitimacy of each other.
4) ***Session key agreement***: The vehicles and CSPs can negotiate a private session key for encrypting and decrypting the subsequent communications.
5) ***Unlinkability***: No third party can link intercepted messages to the same vehicle.
6) ***Forward security***: In order to achieve the secrecy of previous communication, it should be able to ensure that even if the adversary has cracked the current session key, it is impossible to get the session key used in previous communications through the intercepted messages.
7) ***Resistance to common attacks***: The scheme should be able to withstand common types of attacks, such as replay attacks, off-line password guessing attacks, and impersonation attacks to ensure the security of the entire vehicular network.

## IV. Proposed Scheme

In this section, we give a detailed description of our scheme which consists of five phases. Firstly, the TA setups the whole system. The vehicles and CSPs then submit their registrations to the TA separately. Vehicle users must pass the third login phase successfully before they authenticate with CSPs. In the following authentication phases, we introduce the mutual authentication steps among vehicles, CSPs and TA in detail. Finally, it is the password change phase. The proposed scheme has the following advantages: 1) It has good scalability, specifically, the newly added CSPs can participate in the vehicular network service by registering with the TA only once; 2) during the whole mutual authentication and key agreement (AKA) phase, CSPs can not know the real identity of the vehicle, which realizes better privacy protection of vehicle's real identity; 3) it provides users with a quick and convenient password change phase; 4) no bilinear pairing operation is used, which reduces the time consumption of the whole system. Fig. 2 demonstrates our system framework. Notations are listed in Table I.

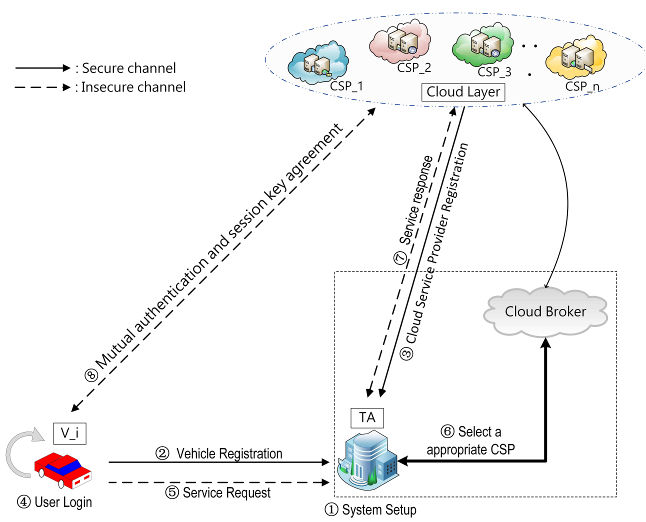



Fig. 2. Framework of the proposed scheme.

### *A. System Setup*

Let $F_p$ be the finite field over $p$, and $p$ is a prime number denotes the size of finite field. The TA generates an additive cyclic group $E$, where $(a, b) \in F_p$ are the parameters of elliptic curve $E$. And $P$ is the generator point of $E$ with a prime order of $q$. $O$ denotes infinity and $P \neq O$. Then the TA chooses two secure hash functions $h : \{0,1\}^* \rightarrow \{0,1\}^l$, $H : \{0,1\}^* \rightarrow \{0,1\}^l$, here $l$ denotes the limit length of bit string. Next, the TA selects a random number $s \in F_p$ to compute its corresponding public key $P_{pub} = sP$. TA keeps $s$ as its private key and publishes $\{P_{pub}, H, P, E\}$ as the public system parameters. Note that in order to further improve the robustness of the scheme, $h$ will not be published and it only stored in the OBU of the registered vehicle.

TABLE I
NOTATIONS

| Notations | Definitions |
|---|---|
| TA | Trusted authority |
| CB | Cloud broker |
| $CSP_j$ | The $j-th$ cloud service provider |
| $V_i$ | The $i-th$ vehicle |
| $s$ | The private key of the TA |
| $P_{pub}$ | The public key of the TA |
| $UID_i$ | The real identity of user |
| $ID_i$ | The real identity of $V_i$ |
| $PID_i$ | The pseudo identity of $V_i$ generated by $V_i$ itself |
| $CID_i$ | The pseudo identity of $V_i$ generated by the TA |
| $ID_j$ | The real identity of $CSP_j$ |
| $PID_j$ | The pseudo identity of $CSP_j$ generated by $CSP_j$ itself |
| $AID_j$ | The pseudo identity of $CSP_j$ generated by the TA |
| $PW_i$ | The password of $V_i$ |
| $M_i$ | A request message of $V_i$ |
| $tt_i$ | The latest timestamp |
| $h, H$ | Two collision-free one-way hash functions |
| $\|$ | Concatenation operation |
| $\oplus$ | Exclusive-OR operation |

### *B. Registration*

In this phase, vehicles and cloud service providers submit their registration applications to the TA respectively.

- ***Vehicle Registration***

Fig. 3 shows the interactions between the vehicle user and the TA during the vehicle registration phase. Details are described as follows.

1) The vehicle user selects a password $PW_i$ and computes $EPW_i = h(UID_i \| PW_i)$, then $V_i$ sends $\{ID_i, EPW_i\}$ to the TA through the secure channel. What the TA gets is the encrypted login password and the encrypted real identity of user; therefore, the adversary cannot successfully launch a stolen-verified attack.
2) TA computes $A_i = H(ID_i \| s)$, $B_i = A_i \oplus EPW_i$ and stores $\{B_i, P, H, h\}$ into the $V_i$. Meanwhile, the TA locally stores the real identity $\{ID_i\}$ of $V_i$.
3) $V_i$ computes $C_i = h(UID_i \| ID_i \| PW_i)$, and then stores $C_i$ into its on-board unit. At last, $V_i$ is loaded by $\{B_i, C_i, P, H, h\}$.

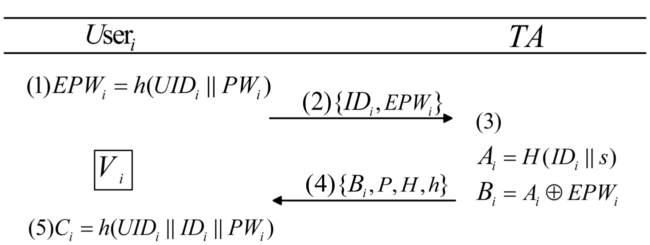



Fig. 3. Vehicle registration phase.

- ***Cloud Service Provider Registration***

Fig. 4 shows the interactions between the cloud service provider and the TA during this registration phase. The following is a detailed description.

1) The cloud service provider $CSP_j$ sends its identity $ID_j$ to the TA via a secure channel.
2) The TA computes $Q_j = H(ID_j \| s)$ and sends it to the cloud service provider $CSP_j$.
3) The cloud service provider $CSP_j$ keeps $Q_j$ secretly.

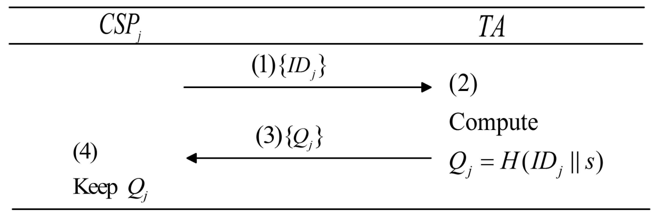



Fig. 4. Cloud service provider registration phase.

### *C. Login*

Fig. 5 shows the user login process. As the first checkpoint, by the following two steps, $V_i$ can verify the legitimacy of the user.

1) The user inputs $UID_i$, $ID_i$ and $PW_i$ to the $V_i$.
2) Vehicle $V_i$ computes $C_i' = h(UID_i \| ID_j \| PW_i)$ and checks if $C_i'$ equals to $C_i$. If the information entered by the user is right, this request will be permitted. Otherwise, this login request will be rejected.

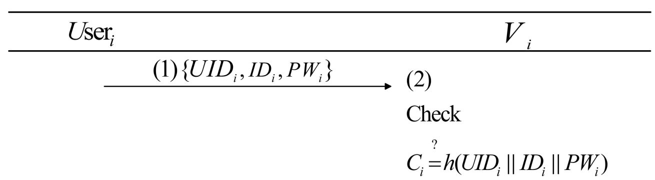



Fig. 5. User login phase.

### *D. Authentication and Session Key Agreement*

As previously described, after successfully passing the login phase, $V_i$ sends its request message $M_i$ to the TA instead of broadcasting the message to CSPs. Then, the TA checks the legitimacy of $V_i$, if the vehicle is legal and has already registered, the cloud broker managed by the TA will recommend the most suitable CSP for $V_i$. Afterwards, $V_i$ and $CSP_j$ complete the authentication with the assistance of the TA. Additionally, a temporary session key is established to encrypt subsequent communications. The interaction processes in the AKA phase are shown in Fig. 6. The following are the detailed descriptions. It is worth noting that, about how to select appropriate cloud service provider is beyond the scope of this study, if you are interested in this issue, you can read the reference [49], [9], [50], and [16].

1) Vehicle $V_i$ computes $EPW_i = h(UID_i \| PW_i)$, $A_i = B_i \oplus EPW_i$, and selects a random nonce $x \in Z_q^*$ to compute $X = xP$, $X^* = xP_{pub}$ and $\eta = H(ID_i \| M_i \| X \| X^* \| A_i)$, where $Z_q^* = \{0, 1, 2, ..., q-1\}$. Then $V_i$ generates a pseudo identity $PID_i$ by itself, where $PID_i = ID_i \oplus H(X^* \| tt_i)$ and $tt_i$ is the

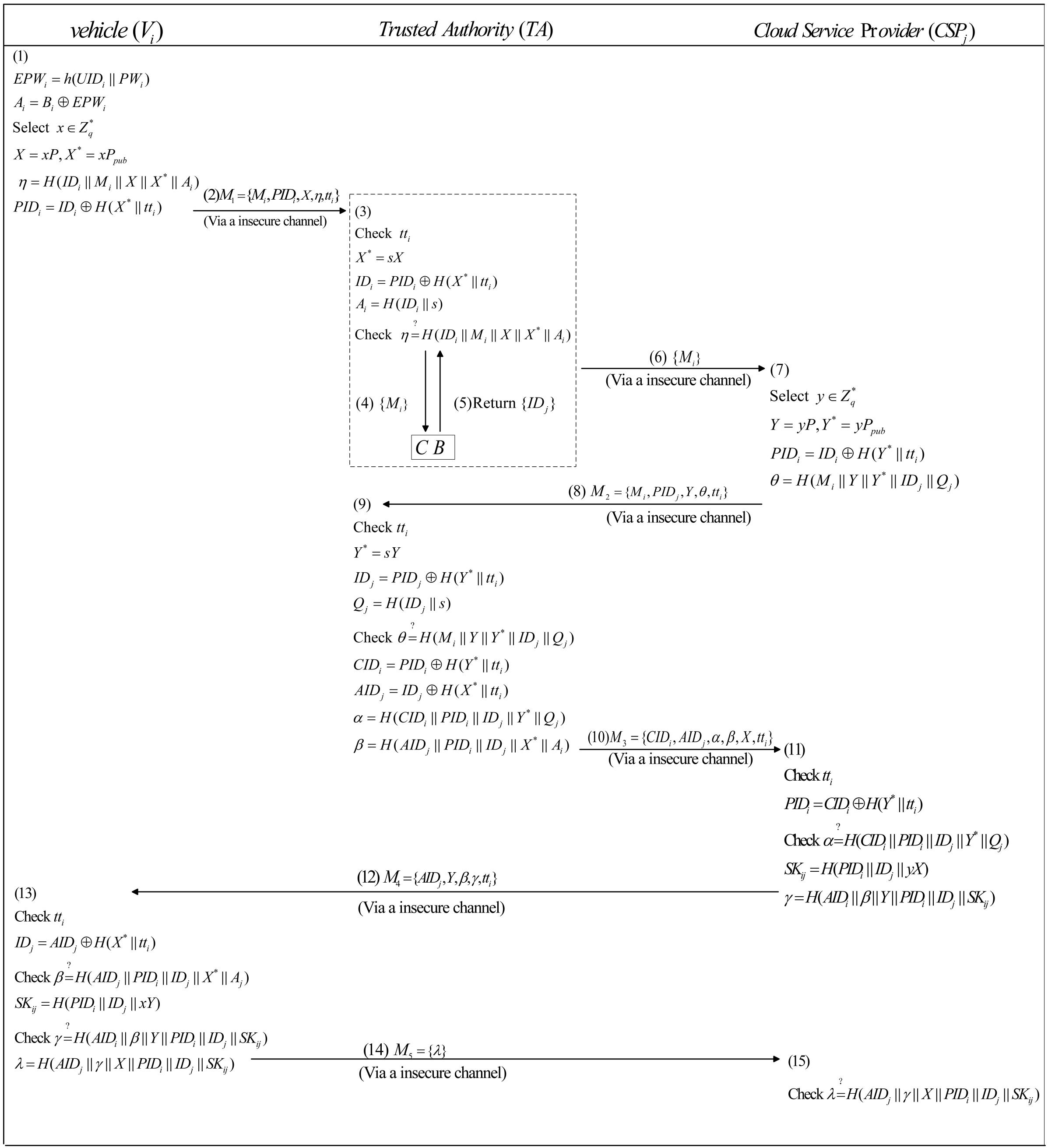



Fig. 6. Authentication and session key agreement phase of our scheme.

latest timestamp. Next, $V_i$ send the message $M_1 = \{M_i, PID_i, X, \eta, tt_i\}$ to the TA.

2) Upon receiving $M_1$ from $V_i$, the TA first checks the timestamp of the message. If $tt_i$ is expired, the TA would terminate the process. Otherwise, the TA computes $X^* = sX$ to get $V_i$'s real identity $ID_i = PID_i \oplus H(X^* \| tt_i)$. If $V_i$ is not in the revocation list, the TA computes $A_i = H(ID_i \| s)$ and checks if $\eta$ and $H(ID_i \| M_i \| X \| X^* \| A_i)$ are equal. If so, TA sends the requests message $M_i$ to the cloud broker. Then the cloud broker finds suitable and reliable $CSP_j$ according to the $M_i$, and returns the real identity of $CSP_j$ to the TA.
3) The TA sends $M_i$ to the cloud service provider $CSP_j$. As a response, $CSP_j$ selects a random nonce $y \in Z_q^*$ to compute $Y = yP$, $Y^* = yP_{pub}$ and $PID_j = ID_j \oplus H(Y^* \| tt_i)$ upon receiving $M_i$ from the TA. Here $PID_j$ is the pseudo identity generated by $CSP_j$ itself. Then $CSP_j$ computes $\theta = H(M_i \| Y \| Y^* \| ID_j \| Q_j)$. Finally, $CSP_j$ sends the message $M_2$ to the TA, where $M_2 = \{PID_j, Y, \theta, tt_i\}$.
4) After receiving $M_2$ from $CSP_j$, TA checks the validity of the timestamp at first. TA would terminate the process if $tt_i$ is expired. If not, TA computes $Y^* = sY$ to get $CSP_j$'s real identity $ID_j$, where $ID_j = PID_j \oplus H(Y^* \| tt_i)$. Next TA computes $Q_j = H(ID_j \| s)$ and checks whether $\theta$ and $H(M_i \| Y \| Y^* \| ID_j \| Q_j)$ are e-

qual. If so, $TA$ computes the authentication message: $CID_i = PID_i \oplus H(Y^*\|tt_i)$, $AID_j = ID_j \oplus H(X^*\|tt_i)$, $\alpha = H(CID_i\|PID_i\|ID_j\|Y^*\|Q_j)$, and $\beta = H(AID_j\|PID_i\|ID_j\|X^*\|A_i)$. Here, TA sends the encrypted pseudo identity of $V_i$ to $CSP_j$ for supporting the requirements of conditional privacy protection in the vehicular networks. Finally, TA sends $M_3 = \{CID_i, AID_j, \alpha, \beta, X, tt_i\}$ to the $CSP_j$.

5) $CSP_j$ computes $PID_i = CID_i \oplus H(Y^*\|tt_i)$ and verifies whether $\alpha$ and $H(CID_i\|PID_i\|ID_j\|Y^*\|Q_j)$ are equal. If yes, then $CSP_j$ computes the session key $SK_{ij} = H(PID_i\|ID_j\|yX)$ and calculates $\gamma = H(AID_j\|\beta\|Y\|PID_i\|ID_j\|SK_{ij})$. At last, $CSP_j$ sends $M_4 = \{AID_j, Y, \beta, \gamma, tt_i\}$ to $V_i$.
6) Vehicle $V_i$ computes $ID_j = AID_j \oplus H(X^*\|tt_i)$ to get the real identity of $CSP_j$ upon receiving the message $M_4$. And then $V_i$ checks if $\beta = H(AID_j\|PID_i\|ID_j\|X^*\|A_i)$ holds to verify whether the message indeed comes from the TA. If so, $V_i$ computes $SK_{ij} = H(PID_i\|ID_j\|xY)$ to check whether $\gamma$ is equal to $H(AID_j\|\beta\|Y\|PID_i\|ID_j\|SK_{ij})$. If so, $CSP_j$ is authenticated successfully, Consequently, $V_i$ computes $\lambda = H(AID_j\|\gamma\|X\|PID_i\|ID_j\|SK_{ij})$ and sends $M_5 = \{\lambda\}$ to the $CSP_j$.
7) Upon receiving the message $M_5$, $CSP_j$ calculates $H(AID_j\|\gamma\|X\|PID_i\|ID_j\|SK_{ij})$ to verify whether it equals to $\lambda$. If yes, the session key $SK_{ij}$ is assured for future secure communication between $V_i$ and $CSP_j$.

Note that, when the vehicle and other CSPs perform the same steps in this phase, the negotiated session keys enable the vehicle to establish simultaneous links with multiple clouds.

### E. Password Change

Fig. 7 shows our user-friendly password change phase which can be completed on the vehicle whenever users like. The following is a detailed description.

1) The user enters $UID_i$, $ID_i$, $PW_i$ and the new password $PW_i^*$ into $V_i$.
2) Vehicle $V_i$ computes $C_i' = h(UID_i\|ID_i\|PW_i)$ and checks whether the equation $C_i' = C_i$ holds. If the information entered by the user is wrong, this process will be terminated. If not, then $V_i$ performs $B_i^* = B_i \oplus h(UID_i\|PW_i) \oplus h(UID_i\|PW_i^*)$, and $C_i^* = h(UID_i\|ID_i\|PW_i^*)$ for changing $PW_i$ into the new password $PW_i^*$.

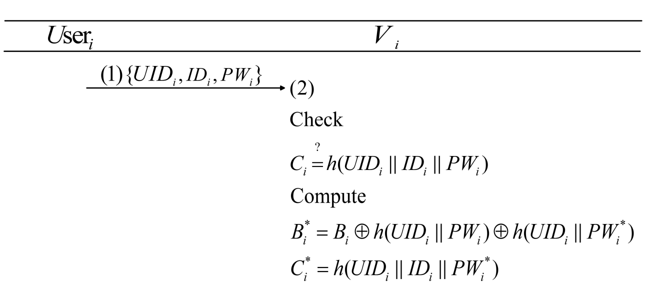



Fig. 7. Password change phase.

## V. Security Analysis

In this section, we first introduce the preliminaries of ECDLP and ECDHP. Then, we define the security model and conduct the formal security proof to show that our scheme is indeed provably secure. Next, based on the safety requirements of the vehicular network, the security analysis is carried out in detail.

### A. Preliminaries

The security of our scheme is based on the following elliptic curve computational problems, namely, Elliptic Curve Discrete Logarithm Problem (ECDLP) and Elliptic Curve Diffie-Hellman Problem (ECDHP).

- ***ECDLP***: $y \in Z_q^*$, $Y = yP$, where $Y \in E_p$ and $P$ is the generator of the $E_p$. Given $Y = yP$, it is not feasible to learn the integer $y$.
- ***ECDHP***: $x, y \in Z_q^*$, and $X = xP$, $Y = yP$, where $X, Y \in E_p$ and $P$ is the generator of the $E_p$. Given $X = xP$ and $Y = yP$, it is not feasible to compute the point $xyP \in E_p$.

### B. Security Model

Assumed that three types of entities are in the authentication scheme $\Gamma$: TA which keeps the secret key $s$; $CSP_j$ which keeps the secret value $D_i$; and $V_i$ that keeps $\{PW_i, OBU_i, UID_i\}$. They all have multiple instances and can execute the authentication scheme $\Gamma$ simultaneously. Each of them can be regarded as an oracle that usually has the following three states: *Accept*, which means the oracle receives a right message; *Reject*, which means the oracle receives a fault message; and $\perp$, which means no answer is output. As we mentioned in Section III. A, the base station does not participate in any encryption operation, and does not store any secret. That is to say, no one can obtain valuable information through the base station, so we do not consider it in this section.

Let $V_i^\alpha$ denote the $\alpha$th instance of $V_i$, similarly, $CSP_j^\beta$ and TA$^\gamma$ denote the $\beta$th and the $\gamma$th instance of $CSP_j$ and TA. We can say that $V_i^\alpha$ and $CSP_j^\beta$ are partners, if either of them reach *Accept* state and a session key $SK_{ij}$ is generated between them.

***Definition 1*** (*Adversary's Capabilities*): Adversary $\mathcal{A}$ can query oracles as follows to learn the session key:

- $Execute-Oracle$: It simulates passive attacks. When $\mathcal{A}$ invokes this query for accessing the honest authentication phase, it replies with $\{M_1, M_2, M_3, M_4, M_5\}$ to $\mathcal{A}$.
- $Send-Oracle$: It simulates active attacks. When $\mathcal{A}$ invokes this query with a valid message $m$ sending to $V_i^\alpha$ or $CSP_j^\beta$ or TA$^\gamma$, this oracle will accept $m$ and reply $\mathcal{A}$ with corresponding answer according to $\Gamma$. Otherwise, the oracle sends *Reject* as a response.
- $Reveal-Oracle$: When $\mathcal{A}$ invokes this query to learn the session key maintained by $V_i^\alpha$, it answers with $SK_{ij}$ only if $V_i^\alpha$ has turned into *Accept* state.
- $Corrupt-Oracle$: It allows $\mathcal{A}$ to get access to the secret information of $V_i^\alpha$.

* $\pi = 0$: $PW_i$ is obtained by $\mathcal{A}$ via this inquiry.
* $\pi = 1$: $\mathcal{A}$ gets all the message stored in $OBU_i$ via this query.
* $\pi = 2$: $\mathcal{A}$ learns the real identity $UID_i$ of $U_i$ via this query.

- $Corrupt-Oracle$: It only used to model forward secrecy, where $\mathcal{A}$ can obtain all the secret values maintained by $V_i^\alpha$, $CSP_j^\beta$ and TA$^\gamma$.
- $Test - Oracle$: It tests the semantic security of the session key, and could be asked by $\mathcal{A}$ at most once. If no session key has been generated or $V_i^\alpha$'s (or $CSP_j^\beta$'s) instance is not fresh (see Definition 2), $\perp$ will be the output. Otherwise, a bit $b$ will be generated by this oracle. If $b = 1$, $\mathcal{A}$ gets the real session key. If $b = 0$, it returns a random binary string as long as $SK_{ij}$ to $\mathcal{A}$.

***Definition 2*** (*Strong Forward Security-fresh*): An instance $V_i^\alpha$ or $CSP_j^\beta$ is strong forward security fresh unless any of the following cases appears:

* A $Reveal$ query sent by $V_i^\alpha$ or $CSP_j^\beta$ appears.
* $Corrupt$ ($\pi = 0, 1, 2$) are all queried by $\mathcal{A}$.
* The situation that $V_i^\alpha$ ( $CSP_j^\beta$/ TA$^\gamma$) has been sent $Corrupt$ queries happens before $Test$.

***Definition 3*** (*Semantic Security*): The ability that $\mathcal{A}$ can defeat the scheme $\Gamma$ is defined as the probability of guessing the $b$ accurately involved in the $Test-Oracle$. That is, the advantage of $\mathcal{A}$ is: $Adv_\Gamma^{ake}(\mathcal{A}) = 2 * Pr[b = b'] - 1$. $\Gamma$ is AKE-secure if $Adv_\Gamma^{ake}(\mathcal{A})$ is ignorably larger than max $\{q_s(\frac{1}{|D|}, \frac{1}{2^{l_b}}, \varepsilon)\}$, where $|D|$ and $q_s$ denote the length of password dictionary and the bound of $Send$-query respectively.

### *C. Formal Security Proof*

***Theorem 1***: Let $E_p$ be an elliptic curve group and D denote a uniformly distributed password dictionary with length is $|D|$. $\Gamma$ represents our proposed scheme, and the advantage for adversary $\mathcal{A}$ breaking $\Gamma$ in upper-bound time $t$ is:

$$\begin{aligned} Adv_\Gamma^{ake}(\mathcal{A}) \leq 2q_h((q_s + q_e)^2 + 1)Adv_\mathcal{A}^{ECDH}(t + t_m(q_e + q_s)) \\ +2\max\{q_s(\frac{1}{|D|}, \frac{1}{2^{l_u}}, \varepsilon)\} + \frac{2q_s + q_h^2 + q_u^2}{2^l} + \frac{(q_s + q_e)^2}{p} \end{aligned} \tag{1}$$

Within the polynomial time $t$, $\mathcal{A}$ can excute at most $q_h$ Hash-queries, $q_u$ Identity-queries, $q_s$ Send-queries, and $q_e$ Execute-queries. Where $\varepsilon$ denotes the case "false positive", $l$ is the length of hash values, $t$ is the time cost of an elliptic curve point multiplication in an additional cyclic group $G$ and $l_u$ is the length of user's identity.

***Proof***: Six successive games $G_i (0 \leq i \leq 5)$ are conducted to confirm that our scheme is provably secure. Let $P[s_i]$ represent the probability that $\mathcal{A}$ successfully guesses the value of $b$ which exists in the $Test$ query. Furthermore, $\Delta_i$ denotes the difference between $P[s_i]$ and $P[s_{i-1}]$. Specific proof as follows:

- *Game* $G_0$: $G_0$ is the real protocol under random oracle. According to the definition above, we can easily know: $Adv_\Gamma^{ake}(\mathcal{A}) = 2 \cdot P[S_0] - 1$. In order to prove $Adv_\Gamma^{ake}(\mathcal{A})$ is negligible, we perform the equation transformation:

$$\begin{aligned} Adv_\Gamma^{ake}(\mathcal{A}) &= 2 \cdot P[S_0] - 1 - (2 \cdot P[S_0] - 2 \cdot P[S_5]) \\ &= 2 \cdot P[S_5] - 1 + 2 \cdot \Sigma_{i=1}^5 \Delta_i \end{aligned} \tag{2}$$

- *Game* $G_1$: The hash oracle $H$ maintains a hash list $L_H$, when $\mathcal{A}$ invokes this query using a string $str$, it first exams whether the tuple $\langle str, H(str)\rangle$ already in $L_H$. If so, $H(str)$ will be returned. Otherwise, $H$ returns $\mathcal{A}$ with a random selected value $H(str)$ and stores $\langle str, H(str)\rangle$ into $L_H$. As the difference between $G_0$ and $G_1$ cannot be distinguished by $\mathcal{A}$, we have:

$$\Delta_1 = |P[S_1] - P[S_0]| = 0 \tag{3}$$

- *Game* $G_2$: $G_2$ simulates all the oracles in $G_1$, and based on the birthday paradox there are two collisions:
  * The maximum probability is $\frac{q_h^2+q_H^2}{2^{l+1}}$ for the collision happened on two hash functions $h$ and $H$.
  * The maximum probability is $\frac{(q_s+q_e)^2}{2p}$ for the collision happened on the nonce $x$ and $y$.

  If these two occurs, $P[S_2] = P[S_1]$ and $\mathcal{A}$ wins the game. As the difference between $G_1$ and $G_2$ cannot be distinguished by $\mathcal{A}$, we have:

$$\Delta_2 = |P[S_2] - P[S_1]| \leq \frac{q_h^2 + q_H^2}{2^{l+1}} + \frac{(q_s + q_e)^2}{2p} \tag{4}$$

- *Game* $G_3$: $G_3$ simulates all the oracle in $G_2$. Here, the probability that $\mathcal{A}$ fakes $\langle \eta, \theta, \alpha, \beta, \gamma, \lambda\rangle$ without random oracle be considered. As $\mathcal{A}$ cannot tell the difference between $G_2$ and $G_3$, therefore:

$$\Delta_3 = |P[S_3] - P[S_2]| \leq \frac{q_s}{2^l} \tag{5}$$

- *Game* $G_4$: $G_4$ simulates all the oracle in $G_3$. The premise is that $\mathcal{A}$ can get at most two factors, whereas $\mathcal{A}$ can do nothing if he only own $UID_i$ and $PW_i$. So, assume that $\mathcal{A}$ has carried out the $Corrupt(V_i, 1)$ query. We argue that the ECDH problem could be solved if $\mathcal{A}$ obtains a valid $SK_{ij}$. Following are three cases for $\mathcal{A}$ getting other values:
  * $\mathcal{A}$ executes $q_s$ times $Corrupt(V_i, 2)$ queries for guessing $PW_i$. As there have $|D|$ passwords, the chance for right guessing $PW_i$ is $\frac{q_s}{|D|}$.
  * $\mathcal{A}$ executes $Corrupt(V_i, 0)$ query and chooses one of following two cases for cracking $UID_i$. Note that two cases cannot exist at the same time.
    1. $\mathcal{A}$ guesses $UID_i$ with $q_s$ times $Send$ queries, and the probability is $\frac{q_s}{2^{l_u}}$.
    2. $\mathcal{A}$ provides his own $UID_i$ and the probability of "false positive" is $\varepsilon$.

    Obviously, the maximum probability of above is $q_s \cdot \max\{(\frac{1}{|D|}, \frac{1}{2^{l_u}}, \varepsilon)\}$.

* In order to obtain the true $SK_{ij}$, where $SK_{ij} = H(PID_i \| ID_j \| xyP)$, $\mathcal{A}$ is required to compute $xyP$ using $X$, $Y$ and $P$, where $X = xP$ and $Y = yP$. Hence, the advantage of $\mathcal{A}$ is $Adv_{\mathcal{A}}^{ECDH}(t+t_m(q_e+q_s))$. Consequently, we have:

$$\Delta_4 = |P[S_4] - P[S_3]| \leq q_s \max\{\frac{1}{|D|}, \frac{1}{2^{l_u}}, \varepsilon\} + q_h \cdot Adv_{\mathcal{A}}^{ECDH}(t + t_m(q_e + q_s)) \quad (6)$$

- *Game* $G_5$: According to the *Definition 2*, the $Corrupt-Oracle$ must be queried after the $Test-Oracle$, that is, $G_5$ only affects old simulations. Like the third case in $G_4$, suppose $SK_{ij}$ could be found in the hash oracle, then the probability $x$ and $y$ in one session is $\frac{1}{(q_s+q_e)^2}$. And we can know:

$$\Delta_5 = |P[S_5] - P[S_4]| \leq q_h(q_s + q_e)^2 \cdot Adv_{\mathcal{A}}^{ECDH}(t + t_m(q_e + q_s)) \quad (7)$$

Finally, we get $P[S_5] = \frac{1}{2}$, therefore, $\mathcal{A}$ can not win the game and the theorem is proved.

### D. Security Analysis

1) ***Anonymity***: The real identity $ID_i$ of $V_i$ is hidden in the $PID_i$, where $PID_i = ID_i \oplus H(X^* \| tt_i)$ and $X^* = xP_{pub}$; therefore, others cannot get $ID_i$ unless they are able to solve the ECDH problem.
2) ***Traceability***: In order to prevent malicious vehicles and cloud service providers from misbehaving, TA can track the real identity of $V_i$ and $CSP_j$ by computing $ID_i = PID_i \oplus H(X^* \| tt_i)$ and $ID_j = PID_j \oplus H(Y^* \| tt_i)$. It should be emphasized that only TA can get the true identity of vehicles; consequently, our scheme meets the requirement of conditional privacy protection in vehicular networks.
3) ***Mutual authentication***: By verifying whether $\langle \eta \rangle$ and $\langle \theta \rangle$ are valid, TA can authenticate the $V_i$ and $CSP_j$ accordingly. In the same way, $V_i$ validates TA and $CSP_i$ by verifying whether $\langle \beta \rangle$ and $\langle \gamma \rangle$ are effective. $CSP_j$ can validate TA and $V_i$ through the effectiveness of $\langle \alpha \rangle$ and $\langle \lambda \rangle$. Consequently, the proposed scheme can achieve mutual authentication between $V_i$, $CSP_j$ and TA.
4) ***Session key agreement***: $CSP_j$ and $V_i$ compute $SK_{ji} = H(PID_i \| ID_j \| yX)$ and $SK_{ij} = H(PID_i \| ID_j \| xY)$ independently. Afterwards, $V_i$ and $CSP_j$ confirm the validity of $SK_{ij}$ for subsequent confidential communication by verifying the following equations: $\gamma = H(UID_j \| \beta \| Y \| PID_i \| ID_j \| SK_{ij})$ and $\lambda = H(UID_j \| \gamma \| X \| PID_i \| ID_j \| SK_{ij})$ respectively.
5) ***Un-linkability***: Because the random numbers and timestamps are used in our scheme, the messages transmitted over the network are different. Additionally, the pseudo-ID of $V_i$ and $CSP_j$ are dynamically updated, therefore the adversary cannot distinguish whether two different messages originate from the same sender.
6) ***Perfect forward secrecy***: Due to $SK_{ij}$ equals to $H(PID_i \| ID_j \| xY)$ and $H(PID_i \| ID_j \| yX) = SK_{ji}$, therefore, only the adversary who is able to solve the ECDH problem for getting the random numbers $x$ and $y$, can generate a correct session key. That is, our scheme satisfies perfect forward secrecy.
7) ***Resistant against ordinary attacks***: The proposed scheme protects against the following common attacks:

- ***Replay attack***: Given that timestamp $tt_i$ is attached to the message, by checking the freshness of $tt_i$, participants could discover whether a replay has occurred.
- ***Offline password guessing attack***: During the registration, TA calculates $A_i = H(ID_i \| s)$ with its secret key $s$. Additionally, $PW_i$ could be easily changed by legal users, thus, in polynomial time no one could guess both $s$ and $PW_i$ correctly.
- ***Resistance impersonation of CSP***: Messages sent by $CSP_j$ contain the $Q_j$, where $Q_j$ equals to $H(ID_j \| s)$. Because the system assumes that TA is completely trustworthy and unbreakable, therefore, any other entity can not be successfully forged as $CSP_j$ as they do not know the private key $s$ of TA.
- ***Resistance impersonation of vehicle***: In order to impersonate $V_i$ for sending a legal request message, $\mathcal{A}$ is required to know the correct $A_i$, where $A_i = H(ID_i \| s)$. As we analysed before, the possibility for $\mathcal{A}$ retrieving $ID_i$ and $s$ from the intercepted messages is negligible.

According to Table II, only our scheme can achieve more merits when compared with related schemes [51], [52], [53].

TABLE II
SECURITY COMPARISON

| | [51] | [52] | [53] | Our scheme |
|---|---|---|---|---|
| Anonymity | ⋆ | ⋆ | × | ⋆ |
| Traceability | ⋆ | ⋆ | ⋆ | ⋆ |
| Un-linkability | ⋆ | × | ⋆ | ⋆ |
| Perfect forward secrecy | × | ⋆ | ⋆ | ⋆ |
| Replay attack | ⋆ | × | ⋆ | ⋆ |
| Impersonation attacks | × | ⋆ | ⋆ | ⋆ |

⋆ : The requirement is satisfied.
× : The requirement is not satisfied.

## VI. Performance Evaluation

The dynamic nature of network topology and the limited computing power of OBU make it of great practical significance to realize fast and efficient authentication of vehicular networks. For proving the computation and communication overhead of our scheme can meet the requirements in the vehicular network, we compare it with three other novel authentication schemes. Moreover, we conduct simulation experiment in terms of packet loss ratio and average transmission delay to prove our scheme achieves better performance.

### A. Computation Cost Analysis

In the scheme of [51], Liu *et al.* adopted bilinear pairings crypto-operations to design an efficient AKA scheme for V2V communications. In the schemes of Ying *et al.*'s [52], they proposed a lightweight and anonymous authentication based on smart card protocol for secure vehicular networks. In [53], Jiang *et al.* proposed an integrated AKA framework for achieving mutual authentication and secure communications among users, vehicular cloud (VC), and conventional cloud (CC). Note that, both the scheme of Jiang *et al.*'s [53] and the proposed scheme are established on ECC, and Ying *et al.*'s [52] scheme involves modulo exponential operations.

The method of computation evaluation proposed in [2] is adopted in this study. We use MIRACL to get the execution time of cryptographic operations on the hardware platform which contains 8 gigabytes memory, an Intel I7-6700 processor, and runs Windows 7 operating system. Table III shows the details about the involved operations. Due to the time for performing XOR operation is negligible, we do not take this into account in computation time calculation.

Here, we introduce the analysis about Liu *et al.*'s scheme [51] and our scheme in detail only, as the specific computation cost analysis about [52] and [53] can be achieved similarly. From Table IV we can see the detailed computation cost of each entity. As mentioned before, Liu *et al.*'s scheme [51] adopted bilinear pairing crypto-operations. During the AKA phase, it requires OBU to execute two MapToPoint hash operations, one symmetric encryption operation, one bilinear pairing and one point addition operation about the bilinear pairing, that is, the execution time of OBU is $2T_{mtp} + T_s + T_{bp} + T_{ba}$ $\approx$ 8.04 ms. Meanwhile, the RSU is required to perform two MapToPoint hash operations, one bilinear pairing and two symmetric encryption operations, namely, the execution time of RSU is $2T_{mtp} + 2T_s + T_{bp} \approx 5.8364$ ms. As for TA, it needs to carry out three MapToPoint hash operations, one scale multiplication operation and one symmetric decryption operations; consequently, the execution time of TA is $3T_{mtp} + T_s + T_{bm}$ $\approx$ 1.2676 ms. Therefore, the total execution time in [51] for AKA is about 14.144 ms.

In our scheme, the computation time needed in vehicle is eight one-way hash function operations and three scale multiplication about the ECC, accordingly, the execution time is $3T_{em} + 8T_h \approx 0.9734$ ms. The base stations do not participate in the AKA phase. The CSP is required to perform seven one-way hash function operations and three scale multiplication about the ECC, that is, $3T_{em} + 7T_h \approx 0.9724$ ms. The computation time in TA is about 0.6536 ms which equals to ten times of one-way hash function operations and two scale multiplication about the ECC. Consequently, the total time needed in our scheme during AKA is about 2.5994 ms.

For demonstrating the major benefit of our scheme, in Fig. 8, we depict the comparison results from the aspects of time cost on vehicle and the total time cost during the whole AKA phase. Obviously, our scheme achieves better performance when compared with other related authentication schemes [51]-[53].

### *B. Communication Cost Analysis*

As $p$ is 20 bytes and $\overline{p}$ is 64 bytes, the elements in $G$ and $G_1$ are $20 \times 2 = 40$ bytes and $64 \times 2 = 128$ bytes respectively. Besides, without loss of generality, we set the size of timestamp be 4 bytes, the size of of output of general hash function and symmetric encryption/decryption be 20 bytes. Here we only consider the length of messages during AKA phase only. Table V shows the detailed communication costs and the rounds in AKA.

TABLE IV
COMPUTATION COST COMPARISON (MS)

| | Vehicle | R/C/V | TA | Total |
|---|---|---|---|---|
| [51] | $2T_{mtp} + T_{bp} + T_{bpm} + T_s \approx 8.04$ | $2T_{mtp} + T_{bp} + T_s \approx 5.5604$ | $3T_{mtp} + T_{bpm} + T_s \approx 1.2656$ | $7T_{mtp} + 2T_{bp} + 2T_{bpm} + 4T_s \approx 14.144$ |
| [52] | $T_e + T_s + 6T_h \approx 6.296$ | $T_h \approx 0.001$ | $T_e + T_s + 5T_h \approx 6.295$ | $2T_e + 2T_s + 12T_h \approx 12.592$ |
| [53] | $3T_{ecm} + 9T_h + 4T_s \approx 2.0784$ | $(VC)$ : $3T_{ecm} + 4T_h + 5T_s \approx 2.3494$ $(CC) : 3T_h + T_s \approx 0.279$ | $Null$ | $3T_{ecm} + 9T_h + 4T_s \approx 4.7068$ |
| Our | $3T_{ecm} + 8T_h \approx 0.9734$ | $3T_{ecm} + 7T_h \approx 0.9724$ | $2T_{ecm} + 10T_h \approx 0.6536$ | $8T_{ecm} + 25T_h \approx 2.5994$ |

R/C/V: It represents RSU, cloud or another vehicle.
$Null$: The entity is not considered in the system model of the scheme.

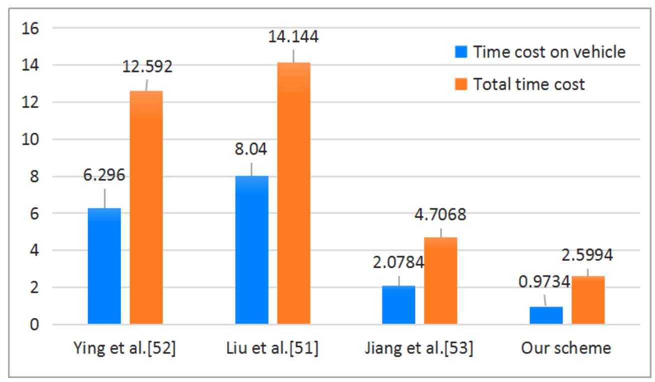



Fig. 8. Computation cost comparison.

TABLE V
COMMUNICATION COST

| | Rounds in AKA | Length of messages |
|---|---|---|
| Liu's scheme [51] | 5 | 2296 bytes |
| Ying's scheme [52] | 5 | 216 bytes |
| Jiang's scheme [53] | 6 | 444 bytes |
| Our scheme | 5 | 416 bytes |

We introduce the analysis about Liu *et al.*'s scheme [51] and the proposed scheme in detail only, due to the specific communication cost analysis about [52] and [53] can be computed in the same way. In Liu *et al.*'s scheme [51], there are five rounds in the AKA process, accordingly, the messages are from $m_0$ to $m_4$, where $m_0 = \{AID_i, A_i, TS_i, r_iP, P_{pub}, query\}$, $m_1 = \{AID_j, A_j, TS_j, r_jP, P_{pub}\}$, $m_2 =$

TABLE III
EXECUTION TIME OF BASIC OPERATIONS (MS)

| Symbol | Description | Format | Time (ms) |
|---|---|---|---|
| $T_{bp}$ | Bilinear pairing operation | $\overline{e}(\overline{S},\overline{T})$, where $\overline{S},\overline{T}\in G_1$ | 5.086 |
| $T_{bpm}$ | Scale multiplication operation related to the bilinear pairing | $\overline{x}\cdot\overline{P}$, where $\overline{P}\in G_1$, $x\in Z_q^*$ | 0.694 |
| $T_{bpa}$ | Point addition operation related to the bilinear pairing | $\overline{S}+\overline{T}$, where $\overline{S}$, $\overline{T}\in G_1$ | 0.0018 |
| $T_{mtp}$ | MapToPoint hash operation related to the bilinear pairing | $H_1:\{0,1\}^*\rightarrow G_1$ | 0.0992 |
| $T_{ecm}$ | Scale multiplication operation related to the ECC | $x\cdot P$, where $P\in G$ and $x\in Z_q^*$ | 0.3218 |
| $T_{eca}$ | Point addition operation related to the ECC | $S+T$, where $S,T\in G$ | 0.0024 |
| $T_h$ | One-way hash function operation | $h:\{0,1\}^*\rightarrow\{0,1\}^l$ | 0.001 |
| $T_e$ | Modular exponentiation operation | $g^x \bmod n$ | 6.014 |
| $T_s$ | Symmetric encryption/decryption operation | AES-CBC | 0.276 |

$\{C, AID_i, AID_j, MAC, TS_r, P_r\}$, $m_3 = \{AID_i, AID_j, TD_i, TD_j, E_{xi}(q^{r_i r_t}), E_{xj}(q^{r_i r_j}), TS_t, \sigma, M\}$, and $m_4 = \{SK_{i-j}, data\}$. Owing to $\langle AID_i, AID_j, r_iP, r_jP, P_{pub}, P_r, MAC, \sigma, M, SK_{i-j}\rangle \in G_1$ $\langle A_i, A_j, C\rangle$ are the outputs of symmetric encryption, $\langle TD_i, TD_j\rangle$ belong to the identity database, $\langle E_{xi}(q^{r_i r_t}), E_{xj}(q^{r_i r_j})\rangle$ are the results of modular exponential operation, and $\langle TS_i, TS_j, TS_r, TS_t\rangle$ denote the timestamp, the total communication cost in Liu *et al.*'s scheme [51] is $128\times 17+20\times 5+5\times 4=2296$ bytes.

Next is the analysis of our scheme. It also contains five rounds in the AKA process and the messages are from $m_1$ to $m_5$, where $M_1 = \{M_i, PID_i, X, \eta, tt_i\}$, $M_2 = \{PID_j, Y, \theta, tt_i\}$, $M_3 = \{CID_i, AID_j, \alpha, \beta, X, tt_i\}$, $M_4 = \{AID_j, Y, \beta, \gamma, tt_i\}$ and $M_5 = \{\lambda\}$. Due to $\langle X, Y\rangle \in G$, $\langle PID_i, PID_j, \eta, \theta, \alpha, \beta, \gamma, \lambda, CID_i, AID_j\rangle$ are the results of one-way hash operation, and $tt_i$ denotes the latest timestamp, consequently, the total communication overhead is $40\times 4+20\times 12+4\times 4=416$ bytes.

According to the above analysis combined with Table V as well as the Fig. 9, we can draw the conclusion that the overall communication cost of our scheme is suitable for applications involving vehicular networks.

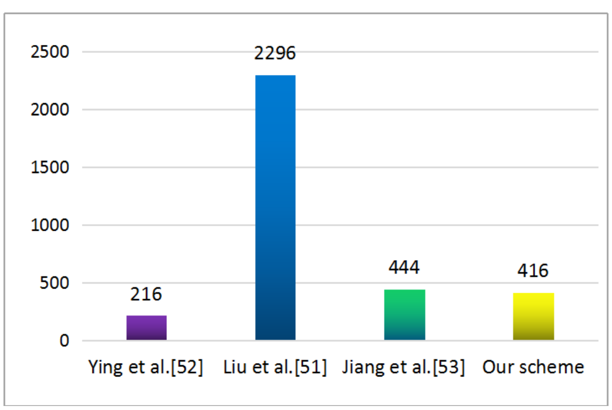



Fig. 9. Communication cost comparison.

### C. Packet Loss Ratio and Average Transmission Delay

In this section, we compare our scheme with the other three schemes [51], [52], [53] on packet loss ratio and average time delay. The simulation platform is composed of Omnet++, Sumo, Veins and Miracl [54]. Among them, Omnet++ is an extensible, modular C++ simulation library and build network simulators supporting the simulation for wired network and wireless mobile ad hoc network. Sumo is an open road traffic simulation package for handling large road networks. Veins is the middleware linking the first two modules. Table VI lists the relevant parameters used in the simulation experiment.

TABLE VI
SIMULATION PARAMETERS

| Parameters | Value |
|---|---|
| Simulation area | $2500\times 2500(m^2)$ |
| Data Transmission Rate | 24 Mbps |
| Transmission Power | 40 mW |
| Sensitivity | -89 dBm |

*1) Packet Loss Ratio:* In equation (8), the packet loss ratio $P_L$ is defined. The so-called packet loss ratio refers to the percentage of lost messages in the total number of messages sent by vehicles, where $A_{vg}(.)$ refers to a averaging function. $n$ represents the number of vehicles. $Num_r^i$ denotes the number of messages received from vehicle $V_i$. And $Num_l^i$ refers to the number of lost messages.

$$P_L = Avg(\Sigma_{i=1}^n Num_l^i(Num_r^i + Num_l^i)^{-1}) \tag{8}$$

We compare our scheme with related schemes [51], [52], and [53] in terms of packet loss ratio. The fixed size of packages sent by vehicles is 400 KB. Fig. 10 shows the relationship between packet loss ratio and vehicle's speed, where the x-axis represents the maximum speed of the vehicle. From Fig. 10, we can see that the trend of packet loss ratio of [52] and [53] is very close, and our scheme achieves the minimum packet loss ratio.

*2) Average Transmission Delay:* We define the average transmission delay $T_D$ of the message between the receiver and the sender in equation (9). Where $n$ represents the number of vehicles. $N^j$ refers to the number of messages received from the vehicle $V_j$. And $T_s^j$, $T_r^j$ represent the time at which the message is sent and the time at which the message is received, respectively. It goes without saying that $T_r^j - T_s^j$ corresponds to the time it takes for the message to perform a one-way transmission between the receiver and the sender.

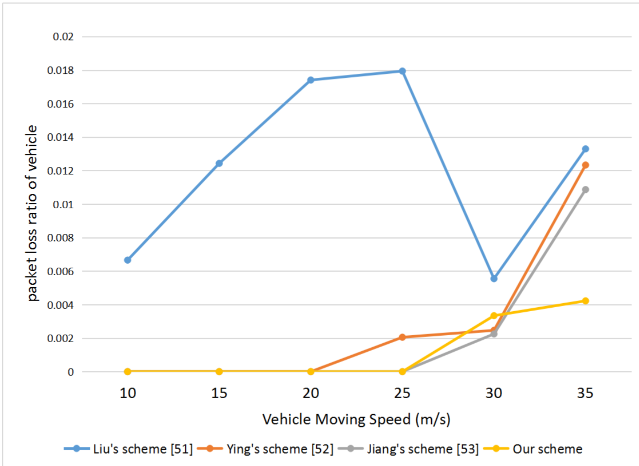



Fig. 10. The relationship between packet loss ratio and vehicle's moving speed

$$T_D = Avg(\Sigma_{i=1}^{n} Avg(\Sigma_{j=1}^{N_j}(T_r^j - T_s^j))) \quad (9)$$

Fig. 11 shows the average packet delay between our scheme and [51], [52], and [53]. Identically, we set the fixed package size be 400 KB. From Fig. 11, we can see that the average packet delay of different schemes tends to be stable at different vehicle speeds, while our scheme achieves the minimum average transmission packet delay, that is to say, our scheme achieves better performance.

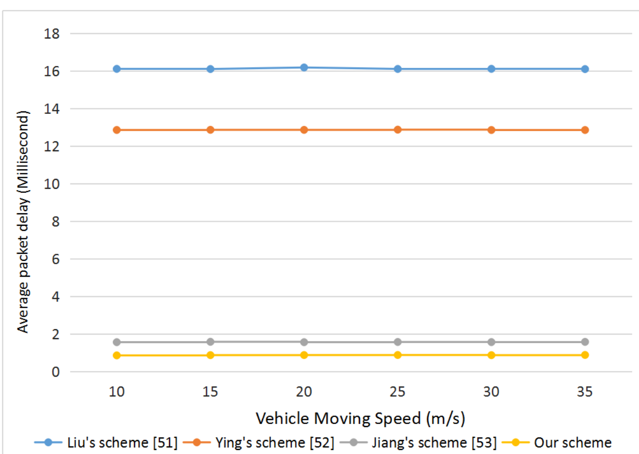



Fig. 11. The relationship between average packet delay and vehicle's moving speed

## VII. Conclusion

In this study, we proposed our novel insights on the vehicular network authentication over a multi-cloud environment. The main objective of this scheme is to propose a vehicular network anonymous authentication scheme that can be practically applied to a multi-cloud environment. The CSPs need to register with the TA only once to participate in the network services; consequently, our scheme demonstrates good scalability. As the TA is responsible for the registration of vehicles, the CSPs do not need to store the considerable amount of redundant vehicles registration information. Moreover, the hassle of public key management is reduced for vehicle users. A detailed security analysis as well as the calculation and communication cost comparisons with related schemes established that our scheme can achieve the security objectives in the vehicular network with lower time consumption. In the future, we will apply reputation mechanism in the model of this scheme and design a multi-level feedback mechanism to evaluate the CSPs to provide improved cloud services for vehicles.

## Acknowledgment

The work was supported by the National Natural Science Foundation of China (No.61872001, No.61572001, No.61702005), the Open Fund of Key Laboratory of Embedded System and Service Computing (Tongji University), Ministry of Education (No. ESSCKF2018-03), the Open Fund for Discipline Construction, Institute of Physical Science and Information Technology, Anhui University and the Excellent Talent Project of Anhui University. The authors are very grateful to the anonymous referees for their detailed comments and suggestions regarding this paper.

## References

[1] A. Botta, W. de Donato, V. Persico, and A. Pescap, "On the integration of cloud computing and internet of things," in *2014 International Conference on Future Internet of Things and Cloud*, Aug 2014, pp. 23–30.
[2] J. Cui, X. Zhang, H. Zhong, Z. Ying, and L. Liu, "Rsma: Reputation system-based lightweight message authentication framework and protocol for 5g-enabled vehicular networks," *IEEE Internet of Things Journal*, pp. 1–1, 2019.
[3] L. Wang and X. Liu, "Notsa: Novel obu with three-level security architecture for internet of vehicles," *IEEE Internet of Things Journal*, vol. 5, no. 5, pp. 3548–3558, Oct 2018.
[4] J. Liu, S. Zhang, W. Sun, and Y. Shi, "In-vehicle network attacks and countermeasures: Challenges and future directions," *IEEE Network*, vol. 31, no. 5, pp. 50–58, 2017.
[5] Q. Jian, Y. He, and X. S. Shen, "Improving video streaming quality in 5g enabled vehicular networks," *IEEE Wireless Communications*, vol. 25, no. 2, pp. 133–139, 2018.
[6] M. Eltoweissy, S. Olariu, and M. Younis, "Towards autonomous vehicular clouds," in *International Conference on Ad Hoc Networks*, 2010.
[7] Z. Wang, Z. Zhong, D. Zhao, and M. Ni, "Vehicle-based cloudlet relaying for mobile computation offloading," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 11, pp. 11 181–11 191, Nov 2018.
[8] S. Azodolmolky, P. Wieder, and R. Yahyapour, "Cloud computing networking: Challenges and opportunities for innovations," *IEEE Communications Magazine*, vol. 51, no. 7, pp. 54–62, 2013.
[9] J. L. Lucas-Simarro, R. Moreno-Vozmediano, R. S. Montero, and I. M. Llorente, "Cost optimization of virtual infrastructures in dynamic multi-cloud scenarios," *Concurrency and Computation: Practice and Experience*, vol. 27, no. 9, pp. 2260–2277, 2015.
[10] M. Louk and H. Lim, "Homomorphic encryption in mobile multi cloud computing," in *2015 international conference on information networking (ICOIN)*. IEEE, 2015, pp. 493–497.
[11] D.-S. Lee, W.-T. Sung, S.-M. Wang, and J.-Y. Shun, "Cloud service enabling architecture for multi-vendor environment," in *2015 17th Asia-Pacific Network Operations and Management Symposium (APNOMS)*. IEEE, Conference Proceedings, pp. 348–351.
[12] I. Benkacem, T. Taleb, M. Bagaa, and H. Flinck, "Optimal vnfs placement in cdn slicing over multi-cloud environment," *IEEE Journal on Selected Areas in Communications*, vol. PP, no. 99, pp. 1–1, 2018.
[13] N. Somu, R. M. R. Gauthama, K. Krithivasan, and S. V. S. Shankar, "A trust centric optimal service ranking approach for cloud service selection," *Future Generation Computer Systems*, vol. 86, p. S0167739X18301262, 2018.

[14] F. Fowley, C. Pahl, P. Jamshidi, D. Fang, and X. Liu, "A classification and comparison framework for cloud service brokerage architectures," *IEEE Transactions on Cloud Computing*, vol. PP, no. 99, pp. 1–1, 2016.

[15] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, "Nist cloud computing reference architecture," *NIST special publication*, vol. 500, no. 2011, pp. 1–28, 2011.

[16] A. Amato, B. Di Martino, and S. Venticinque, "Cloud brokering as a service," in *2013 Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing*. IEEE, 2013, pp. 9–16.

[17] R. Mehrotra, S. Srivastava, I. Banicescu, and S. Abdelwahed, "Towards an autonomic performance management approach for a cloud broker environment using a decompositionccoordination based methodology," *Future Generation Computer Systems*, vol. 54, pp. 195–205, 2016.

[18] M. A. AlZain, E. Pardede, B. Soh, and J. A. Thom, "Cloud computing security: from single to multi-clouds," in *2012 45th Hawaii International Conference on System Sciences*. IEEE, 2012, pp. 5490–5499.

[19] A. Celesti, M. Fazio, M. Villari, and A. Puliafito, "Adding long-term availability, obfuscation, and encryption to multi-cloud storage systems," *Journal of Network and Computer Applications*, vol. 59, pp. 208–218, 2016.

[20] H. Flores and S. N. Srirama, "Mobile cloud middleware," *Journal of Systems and Software*, vol. 92, pp. 82–94, 2014.

[21] K. Zkik, G. Orhanou, and S. El Hajji, "Secure scheme on mobile multi cloud computing based on homomorphic encryption," in *2016 International Conference on Engineering & MIS (ICEMIS)*. IEEE, 2016, pp. 1–6.

[22] H. Wu, Q. Wang, and K. Wolter, "Mobile healthcare systems with multi-cloud offloading," in *2013 IEEE 14th International Conference on Mobile Data Management*, vol. 2. IEEE, 2013, pp. 188–193.

[23] B. Fabian, T. Ermakova, and P. Junghanns, "Collaborative and secure sharing of healthcare data in multi-clouds," *Information Systems*, vol. 48, pp. 132–150, 2015.

[24] G. L. Junior, R. P. do Nascimentos, M. A. Dantas, and D. D. de Macedo, "A platform for vehicular networks in the cloud to applications in intelligent transportation systems," in *2017 IEEE 26th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*. IEEE, 2017, pp. 101–106.

[25] S. Bitam, A. Mellouk, and S. Zeadally, "Vanet-cloud: a generic cloud computing model for vehicular ad hoc networks," *IEEE Wireless Communications*, vol. 22, no. 1, pp. 96–102, February 2015.

[26] S. Bhoi, S. Panda, S. Ray, R. Sethy, V. Sahoo, B. Sahu, S. Nayak, S. Panigrahi, R. Moharana, and P. Khilar, "Tsp-hvc: a novel task scheduling policy for heterogeneous vehicular cloud environment," *International Journal of Information Technology*, pp. 1–6, 2018.

[27] R. I. Meneguette, A. Boukerche, and R. de Grande, "Smart: An efficient resource search and management scheme for vehicular cloud-connected system," in *2016 IEEE Global Communications Conference (GLOBECOM)*, Dec 2016, pp. 1–6.

[28] R. I. Meneguette, A. Boukerche, and A. H. M. Pimenta, "Avarac: An availability-based resource allocation scheme for vehicular cloud," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–12, 2018.

[29] J. Shao and G. Wei, "Secure outsourced computation in connected vehicular cloud computing," *IEEE Network*, vol. 32, no. 3, pp. 36–41, May 2018.

[30] R. Hussain, S. H. Bouk, N. Javaid, A. M. Khan, and J. Lee, "Realization of vanet-based cloud services through named data networking," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 168–175, August 2018.

[31] X. Chen and L. Wang, "A cloud-based trust management framework for vehicular social networks," *IEEE Access*, vol. 5, pp. 2967–2980, 2017.

[32] Z. Wei, H. Tang, F. R. Yu, M. Wang, and P. Mason, "Security enhancements for mobile ad hoc networks with trust management using uncertain reasoning," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 9, pp. 4647–4658, Nov 2014.

[33] K. Lim, K. M. Tuladhar, X. Wang, and W. Liu, "A scalable and secure key distribution scheme for group signature based authentication in vanet," in *2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, Oct 2017, pp. 478–483.

[34] S. H. Ahmed, S. H. Bouk, M. A. Yaqub, D. Kim, H. Song, and J. Lloret, "Codie: Controlled data and interest evaluation in vehicular named data networks," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 6, pp. 3954–3963, June 2016.

[35] J. A. F. F. Dias, J. J. P. C. Rodrigues, F. Xia, and C. X. Mavromoustakis, "A cooperative watchdog system to detect misbehavior nodes in vehicular delay-tolerant networks," *IEEE Transactions on Industrial Electronics*, vol. 62, no. 12, pp. 7929–7937, Dec 2015.

[36] X. Wang, S. Wu, K. Wang, S. Di, H. Jin, K. Yang, and S. Ou, "Maximizing the profit of cloud broker with priority aware pricing," in *2017 IEEE 23rd International Conference on Parallel and Distributed Systems (ICPADS)*, Dec 2017, pp. 511–518.

[37] D. He, S. Zeadally, B. Xu, and X. Huang, "An efficient identity-based conditional privacy-preserving authentication scheme for vehicular ad hoc networks," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 12, pp. 2681–2691, Dec 2015.

[38] J. Cui, J. Zhang, H. Zhong, and Y. Xu, "Spacf: A secure privacy-preserving authentication scheme for vanet with cuckoo filter," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 11, pp. 10 283–10 295, Nov 2017.

[39] J. Kang, R. Yu, X. Huang, and Y. Zhang, "Privacy-preserved pseudonym scheme for fog computing supported internet of vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 19, no. 8, pp. 2627–2637, Aug 2018.

[40] K. Stamou, J. Aubert, B. Gateau, and J.-H. Morin, "Preliminary requirements on trusted third parties for service transactions in cloud environments," in *2013 46th Hawaii International Conference on System Sciences*. IEEE, 2013, pp. 4976–4983.

[41] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," *Future Generation computer systems*, vol. 28, no. 3, pp. 583–592, 2012.

[42] P. Varalakshmi and H. Deventhiran, "Integrity checking for cloud environment using encryption algorithm," in *2012 International Conference on Recent Trends in Information Technology*. IEEE, 2012, pp. 228–232.

[43] Z. Shen and Q. Tong, "The security of cloud computing system enabled by trusted computing technology," in *2010 2nd International Conference on Signal Processing Systems*, vol. 2, July 2010, pp. V2–11–V2–15.

[44] Huanan Liu and Shiqing Wang, "The analysis and design of trusted computing applied into cloud," in *2012 IEEE Control and System Graduate Research Colloquium*, July 2012, pp. 5–9.

[45] A. Quyoom, R. Ali, D. N. Gouttam, and H. Sharma, "A novel mechanism of detection of denial of service attack (dos) in vanet using malicious and irrelevant packet detection algorithm (mipda)," in *International Conference on Computing, Communication Automation*, May 2015, pp. 414–419.

[46] Y. Hattori, T. Shimoda, and M. Ito, "Development and evaluation of its information communication system for electric vehicle," in *2012 IEEE 75th Vehicular Technology Conference (VTC Spring)*. IEEE, 2012, pp. 1–6.

[47] Q. Luo and J. Liu, "Wireless telematics systems in emerging intelligent and connected vehicles: Threats and solutions," *IEEE Wireless Communications*, vol. 25, no. 6, pp. 113–119, 2018.

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

[49] X. Li, H. Ma, W. Yao, and X. Gui, "Data-driven and feedback-enhanced trust computing pattern for large-scale multi-cloud collaborative services," *IEEE Transactions on Services Computing*, vol. 11, no. 4, pp. 671–684, July 2018.

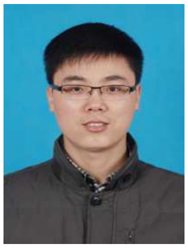
[50] S. Singh and J. Sidhu, "Compliance-based multi-dimensional trust evaluation system for determining trustworthiness of cloud service providers," *Future Generation Computer Systems*, vol. 67, pp. 109–132, 2017.

[51] Y. Liu, Y. Wang, and G. Chang, "Efficient privacy-preserving dual authentication and key agreement scheme for secure v2v communications in an iov paradigm," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 10, pp. 2740–2749, Oct 2017.

[52] B. Ying and A. Nayak, "Anonymous and lightweight authentication for secure vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 66, no. 12, pp. 10 626–10 636, Dec 2017.

[53] Q. Jiang, J. Ni, J. Ma, L. Yang, and X. Shen, "Integrated authentication and key agreement framework for vehicular cloud computing," *IEEE Network*, vol. 32, no. 3, pp. 28–35, May 2018.

[54] J. Cui, D. Wu, J. Zhang, Y. Xu, and H. Zhong, "An efficient authentication scheme based on semi-trusted authority in vanets," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2972–2986, 2019.



**Jie Cui** was born in Henan Province, China, in 1980. He received his Ph.D. degree in University of Science and Technology of China in 2012. He is currently an associate professor and Ph.D. supervisor of the School of Computer Science and Technology at Anhui University. His current research interests include applied cryptography, IoT security, vehicular ad hoc network, cloud computing security and software-defined networking (SDN). He has over 80 scientific publications in reputable journals (e.g. IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Vehicular Technology, IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Network and Service Management, IEEE Transactions on Emerging Topics in Computing, IEEE Transactions on Circuits and Systems and IEEE Internet of Things Journal), academic books and international conferences.

**Xiaoyu Zhang** is currently a research student in the School of Computer Science and Technology, Anhui University, Hefei, China. Her research focuses on vehicle ad hoc network.

**Hong Zhong** was born in Anhui Province, China, in 1965. She received her PhD degree in computer science from University of Science and Technology of China in 2005. She is currently a professor and Ph.D. supervisor of the School of Computer Science and Technology at Anhui University. Her research interests include applied cryptography, IoT security, vehicular ad hoc network, cloud computing security and software-defined networking (SDN). She has over 120 scientific publications in reputable journals (e.g. IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Information Forensics and Security, IEEE Transactions on Parallel and Distributed Systems, IEEE Transactions on Vehicular Technology, IEEE Transactions on Intelligent Transportation Systems, IEEE Transactions on Network and Service Management, IEEE Transactions on Big Data and IEEE Internet of Things Journal), academic books and international conferences.

**Jing Zhang** is currently a PhD student in the School of Computer Science and Technology, Anhui University, Hefei, China. Her research interests include vehicular ad hoc network, IoT security and applied cryptography. She has over 10 scientific publications in reputable journals (e.g. IEEE Transactions on Dependable and Secure Computing, IEEE Transactions on Vehicular Technology, IEEE Transactions on Intelligent Transportation Systems, Information Sciences, Science China Information Sciences and Vehicular Communications) and international conferences.

**Lu Liu** is the Professor of Informatics and Head of Department of Informatics in the University of Leicester, UK. Prof Liu received the Ph.D. degree from University of Surrey, UK and MSc in Data Communication Systems from Brunel University, UK. Prof Lius research interests are in areas of cloud computing, service computing, computer networks and peer-to-peer networking. He is a Fellow of British Computer Society (BCS).