IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received July 11, 2018, accepted September 25, 2018, date of publication October 8, 2018, date of current version October 31, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2874622

Secure and Membership-Based Data Sharing Scheme in V2G Networks

GANG SHEN[1], YIXIN SU[1], AND MINGWU ZHANG[2,3,4]

[1]School of Automation, Wuhan University of Technology, Wuhan 430070, China
[2]Hubei Key Laboratory of Intelligent Geo-Information Processing, China University of Geosciences, Wuhan 430074, China
[3]Hubei Key Laboratory of Transportation Internet of Things, Wuhan University of Technology, Wuhan 430070, China
[4]School of Computers, Hubei University of Technology, Wuhan 430068, China

Corresponding author: Yixin Su (suyixin@whut.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 61672010, in part by the Open Research Project of The Hubei Key Laboratory of Intelligent Geo-Information Processing under Grant KLIGIP-2017A11, and in part by the Fund of Hubei Key Laboratory of Transportation Internet of Things under Grant WHUTIOT-2017B001.

ABSTRACT Vehicle-to-grid (V2G) network is an emerging network environment that can improve grid efficiency and alleviate fluctuations caused by renewable energy access to the grid. However, security and efficiency of V2G network is a very challenging and important factor in the case of large-scale electric vehicles (EVs) access to the grid. In this paper, we propose a secure and membership-based data sharing scheme in V2G networks. This scheme employs the online/offline ciphertext policy attribute-based encryption mechanism combined with fog computing, thus preserving data privacy and saving system resources. Concretely, the heavy computational operations of encryption and decryption are performed by the fog devices in offline encryption phase and decryption phase, respectively. What's more, the service information is divided into multiple parts in term of different membership levels and is encrypted by the control center (CC) through different access policy. The ciphertext can only be decrypted when the EV has a set of attributes that satisfy the corresponding membership level of access policy. Security and performance analyses demonstrate that the proposed scheme not only protects data privacy, but also saves the computational costs of CC and EV. Therefore, our scheme is more suitable for the deployment and adoption of V2G networks.

INDEX TERMS V2G networks, fog computing, access policy, membership-based data sharing, attribute-based encryption.

I. INTRODUCTION

With the popularity of electric vehicles (EVs), Vehicle-to-grid (V2G) network is extensively used. In fact, V2G is a technology that uses a large number of EVs' batteries as buffers of grid and new energy to realize two-way communication and power exchange between the EVs and the grid [1]. In this way, EVs can supply electricity to grid during peak periods of electricity consumption to meet load demand and store electricity during consumption trough to improve energy utilization rate. Therefore, V2G network has brought us some benefits. However, due to the uncertainty of charging time, capacity, location and charging/discharging behavior, disorderly access of a large number of EVs not only poses a challenge to the security of the grid, but also reduces the utilization rate of power equipment [2]. Thus, it is imperative to consider an orderly mechanism for EVs to access the grid.

Typically, the control center (CC) uploads and shares the service information on the cloud of V2G network for EVs access. EVs should be authenticated before they interact with the grid to protect the privacy of V2G network. For example, an authorized EV may obtain a recharge card with EV user's information from the electricity supplier. If an adversary obtains the service information, he/she can tamper with the data to gain personal benefits, and even infer the EV user's lifestyle and routine action from the information [3]. In addition, heavy computational cost of the CC will affect the accuracy of the charging/discharging planning of the entire V2G network EV, and reduce the operational efficiency of the grid. Therefore, how to securely and efficiently manage service information in V2G network is a key element to smart grid supporting large-scale access of EVs, and also ensures the implementation of two-way, real-time and large-capacity data exchange between EVs and grid.

In general, access control, a key technology for improving information security, can not only prevent unauthorized users from illegally accessing resources in the system,

but also obviate creating public key infrastructure (PKI) certificate. In order to achieve a fine-grained data sharing in V2G networks, attribute based encryption (ABE) usually be deployed [4]–[12]. Especially, ciphertext-policy attribute-based encryption (CP-ABE) [13] is a cryptographic technology of ensuring fine-grained data access control and data confidentiality. Compared with key-policy attribute-based encryption (KP-ABE) [14], CP-ABE is more suitable for the data sharing system because the access policy decision is subject to the data owners. In the V2G network scenario, an authorized EV can only extract service information when its possessed attributes satisfy the access structure of the service information.

Since the extraordinary huge volume traffic between EVs and cloud server of V2G network, the CC in the traditional system suffers from transmission delay and declining service quality. Fortunately, a new technique named fog computing can solve above issues. Fog computing is presented by Cisco in 2012 [15], which provides storage, computing and network services for data by using fog devices that exist between CC and terminal equipment. That is, it can process part of the work in advance rather than handing all the work to the CC. As an extension of cloud computing, fog computing possesses network edge computing capabilities that not only provide low latency and location awareness, but also improve network quality of service [16], [17], [31].

At present, many security schemes on V2G networks have been proposed [18]–[22]. However, there are few schemes that consider encrypting the service information of V2G networks by using an access structure. Moreover, some existing ABE schemes [4], [5], [11] do not consider the user's hierarchical access, that is, users satisfying the conditions can extract all the shared information, resulting in a waste of system resources. In addition, the level-based access granted in the existing scheme [23] can complicate the data sharing method in the cloud because the number of user attributes increases exponentially as the number of levels increases. In order to solve above-mentioned issues, protect the privacy of service information, reduce the computational cost of the CC and improve the efficiency of V2G networks, we first propose a secure and membership-based data sharing scheme in V2G networks. The main contributions of this paper are generalized as follows:

- At first, the proposed scheme uses the online/offline ciphertext policy attribute-based encryption (CP-ABE) mechanism [24] combined with fog computing to preserve the data privacy. To our best knowledge, our work is the first efficient and secure fine-grained data access control framework for V2G networks on fog-aided. In order to improve the security of the system, the access structure of proposed scheme is created based on the linear secret sharing mechanism [25], which can effectively prevent the loss of the key and the attack of malicious EVs, and reduce the risks and responsibilities among the secret sharing users. Additional, since the heavy encryption operation is carried out by the fog devices, it is significantly reduced the online encryption cost of the CC and decryption cost of EV in the proposed scheme.
- Secondly, considered by the issue that the resources of CC are very limited in ABE scheme, the proposed scheme divides the service information into multiple parts of different membership levels. Each level of information is associated with a different LSSS access structure. An EV can obtain the service information of some level when it has the correct membership. The scenarios mentioned in this study are high level EVs (e.g., platinum card member) that can obtain more advanced information (e.g., long charge time, large charge capacity or value-added service) from the grid than low level EVs (e.g., ordinary member). In this way, it is not only significantly reduced the computational costs of the CC, but also facilitated the optimization control of the EVs' charge/discharge.
- Finally, we analyze the security and performance of the proposed scheme. The results demonstrate that our scheme is very secure and efficient, and is suitable for V2G networks.

The rest of this paper is organized as follows. In Section II, the related work is presented. In Section III, the preliminaries are described outlining some basic theories used for our scheme. Next, we introduce the system model, security model and design goals in problem formulation of Section IV. In Section V, the proposed scheme is presented in details, following by the security analysis and the performance evaluation in Section VI and Section VII, respectively. Finally, we conclude this paper in Section VIII.

II. RELATED WORK

In this section, we review some of the previous research works related to this paper.

The concept of V2G networks was first proposed by Kempton and Tomić [26] in 2004. Subsequently, Guille and Gross [27] studied the implementation framework of V2G and discussed the practical approaches for key implementation steps. Until 2011, studies on the security and privacy issues of V2G networks began to be focused. Stegelmann and Kesdogan pioneered the study of the privacy and security issues in V2G networks, presenting the issue of anonymous and location privacy of EVs in [19]. After then, many novel schemes have been proposed to solve various security issues of V2G networks. Wang *et al.* [20] presented a traceable privacy-preserving communication by using ID-based restrictive partially blind signatures. In order to reduce system resources, a lightweight security and privacy-preserving scheme for V2G connection was proposed by [22]. Later, Shen *et al.* [18] introduced a privacy-preserving and lightweight key agreement protocol for V2G that is more efficient compared with the protocols based on elliptic curve encryption (ECC-based).

In [21], Eiza *et al*. used restrictive partially blind signature technology and certificateless public key cryptography to maintain the session continuity between EV and the charging services while ensuring the EV's location privacy. Au *et al*. [28] presented a scheme that supports both location privacy protection and traceability of EVs. In addition, in order to protect the data privacy in the smart grid, Liu *et al*. [29] proposed a practical privacy-preserving data aggregation scheme that does not rely on a trusted third party. Shen *et al.* [30] also presented a secure and fine-grained electricity consumption aggregation scheme with forward-backward *security*.

To improve the computational efficiency of the system, Guo *et al.* [32] presented the first identity-based online/offline encryption that can be used where the computational power of a device is limited. Although their scheme can be implemented without knowing the identity of the recipient, the identity-based encryption (IBE) can hardly satisfy many application scenarios. Attribute-based encryption (ABE) is a public key encryption scheme that uses user attributes as private keys, which was originally formed on the basis of fuzzy identity-based encryption (FIBE) introduced by Sahai and Waters [33]. In 2006, Goyal *et al*. [14] presented a key-policy attribute-based encryption (KP-ABE), which is a key that is associated with access control, and a ciphertext with a set of attributes. Subsequently, Bethencourt *et al*. [13] proposed another fine-grained access control technology, namely ciphertext-policy attribute-based encryption (CP-ABE). In 2013, a scheme of attribute-based secure data sharing of hidden policies in smart grid was proposed by Hur [4], which protects the data privacy and policy privacy by obfuscating. The first online/offine ABE scheme [24] was proposed by Hohenberger *et al*., which uses a method of ''pooling'' work done offline. The method means that an encryptor can continuously create offline ciphertext fragments and add them to the pool in the system. In their proposed online/offline CP-ABE scheme, the ciphertext is associated with a linear secret sharing scheme (LSSS) matrix. Specifically, the random exponent is divided into secret shares according to the LSSS structure at each encryption, and each share is assigned to an attribute.

Recently, the application of fog computing attracts increasing attention. A service-oriented architecture for fog computing in telehealth applications is presented by Dubey *et al.* [9], but the analysis of the raw data is performed by a low power embedded computer. In [10], Truong *et al.* introduced a new vehicular ad hoc network architecture that integrates fog computing and software-defined. The delay-sensitive and location-aware services that are provided by fog computing can optimize resource utility and reduce service latency. Lu *et al*. proposed a lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT, which solves the problem of failing to aggregate hybrid IoT device's data into some real IoT applications. Zuo *et al*. [8] proposed a CCA-secure ABE with outsourced decryption for fog computing. They used fog computing to cloud computing infrastructure for low latency of data transmission. Zhang *et al.* [5] proposed a CP-ABE scheme supporting outsourcing capability and attribute update for fog computing. Concretely, the fog nodes are responsible for performing the computational operations of encryption and decryption to eliminate the computational overhead of encryption and decryption. In addition, Zhang *et al.* [36] presented two public key encryption schemes that can effectively limit key and/or random leakage. Next, we will consider using their proposed encryption schemes to realize privacy protection of data in V2G networks.

III. PRELIMINARIES

A. BILINEAR PAIRING

Let $\mathbb{G}_1$ and $\mathbb{G}_2$ be two multiplicative cyclic groups of the same prime order p. Let $g_1, g_2 \in \mathbb{G}_1$ be a generator in $\mathbb{G}_1$. The function $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ is a bilinear map that demonstrates properties as follows:

- Bilinearity: For any $a, b \in \mathbb{Z}_p$, $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$.
- Non-degeneracy: $e(g_1, g_1) \neq 1$.
- Computability:There exists an efficient algorithm to compute $e(g_1, g_2)$.

B. ACCESS STRUCTURE

Access structure [13] is usually used in attribute-based encryption and its definition is as follows: Let $\{P_1, P_2, \cdots, P_n\}$ be a set of participants of secret sharing and define $\mathbb{P} = 2^{\{P_1, P_2, \cdots, P_n\}}$, then access structure Γ is a non-empty subsets of $\{P_1, P_2, \cdots, P_n\}$, i.e., $\Gamma \subseteq \mathbb{P}\backslash\{\oslash\}$. For $\forall A, B$, if $A \in \Gamma$ and $A \subseteq B$, then $B \in \Gamma$, which means that access structure is monotonic.

In our scheme, the attributes are represented by participants.

C. LINEAR SECRET SHARING SCHEMES (LSSS)

LSSS [35] meets the following two aspects:

1) The shares of all participants make up a vector on $\mathbb{Z}_p$.

2) There exists a matrix $\mathbb{M}$ with $l \times n$. The i-th row of $\mathbb{M}$ corresponds to function $\rho(i)$, for $i = 1, 2, \cdots, l$, where ρ is a mapping function from $\{1, 2, \cdots, l\}$ to $\mathbb{P}$. Randomly select column vector $\vec{v} = (s, r_2, \cdots, r_n)$, where $s \in \mathbb{Z}_p$ is the secret to be shared, then $\mathbb{M}\vec{v}^T$ is a vector of l shares of s, and $M_i \cdot \vec{v}^T$ belongs to party $\rho(i)$.

LSSS also has linear reconstruction property, which is defined as follows: Let $S \in \Gamma$ be any authorized set, and define $I = \{i : \rho(i) \in S\}$ and $I \subseteq \{1, 2, \cdots, l\}$. Then, there exist constants collections $\{w_i \in \mathbb{Z}_p\}_{i \in I}$ such that $\sum_{i \in I} w_i M_i = (1, 0, \cdots, 0)$ holds, then $\sum_{i \in I} w_i M_i \vec{v}^T = s$.

D. ONLINE/OFFLINE CP-ABE SCHEME

The proposed scheme is based on online/offline CP-ABE scheme [24] that is a cryptographic technology of ensuring

fine-grained data access control and reducing computational costs, which consists of the following five algorithms:

Algorithm 1 Setup

Input: A security parameter κ

Output:

1: Choose a bilinear group $\mathbb{G}_1$ of prime order p and random generators $g, h, u, v, w \in \mathbb{G}_1$

2: Pick $\alpha \in \mathbb{Z}_p$

3: **Return** the public key $PK = (\mathbb{G}_1, p, g, h, u, v, w, e(g, g)^{\alpha})$ and the master key $MSK = (PK, \alpha)$

Algorithm 2 Extract

Input: The master key MSK and a set of attributes $S = \{A_1, \cdots, A_k\} \subseteq \mathbb{Z}_p$

Output:

1: Choose $r, r_1, r_2, \cdots, r_k \in \mathbb{Z}_p$

2: Compute $K_0 = g^{\alpha} w^r$, $K_1 = g^r$, and compute $K_{i,2} = g^{r_i}$, $K_{i,3} = (u^{A_i} h)^{r_i} v^{-r}$ for $i = 1$ to k

3: **Return** the key $SK = (S, K_0, K_1, \{K_{i,2}, K_{i,3}\}_{i \in [1,k]})$

Algorithm 3 Offline.Encrypt

Input: PK

Output:

1: Choose a random $s \in \mathbb{Z}_p$

2: Compute key$=e(g, g)^{\alpha s}$, $C_0 = g^s$

3: Choose random $\lambda'_j, x_j, t_j \in \mathbb{Z}_p$ and compute $C_{j,1} = w^{\lambda'_j} v^{t_j}$, $C_{j,2} = (u^{x_j} h)^{-t_j}$, $C_{j,3} = g^{t_j}$

4: **Return** the intermediate ciphertext ICT=(key, s, C_0, $\{\lambda'_j, t_j, x_j, C_{j,1}, C_{j,2}, C_{j,3}\}_{j \in [1,P]}$)

Algorithm 4 Online.Encrypt

Input: PK, ICT, and access structure $(\mathbb{M}, \rho)$, where $\mathbb{M}$ is an $l \times n$ matrix and $l \leq P$ (P denotes the maximum bound of rows)

Output:

1: Compute $C_{j,4} = \lambda_j - \lambda'_j$, $C_{j,5} = t_j \cdot (\rho(j) - x_j)$ for $j = 1$ to l

2: **Return** the $CT = ((\mathbb{M}, \rho), C_0, \{C_{j,1}, C_{j,2}, C_{j,3}, C_{j,4}, C_{j,5}\}_{j \in [1,k]})$

Algorithm 5 Decrypt

Input: SK, CT

Output:

1: Compute Set $I = i : \rho(i) \in S$ and compute $w_i \in \mathbb{Z}_p$ such that $\sum_{i \in I} w_i \cdot M_i = (1, 0, \cdots, 0)$, where M_i is the i-th row of the matrix $\mathbb{M}$

2: **Return** the key$=e(g, g)^{\alpha s}$

IV. PROBLEM FORMULATION

In this section, we present the system model, security model and design goals of this paper.

A. SYSTEM MODEL

The Fig. 1 shows the architecture of a secure and membership-based data sharing scheme in V2G networks. There are four tiers in the V2G networks architecture: smart grid tier, fog tier, cloud tier and user tier. In the smart grid tier, the CC encrypts the data and sends to the fog devices in fog tier. The fog devices will perform the fog computing to the received data and then send the results to the cloud server in cloud tier. The authorized EVs in user tier can decrypt the ciphertext on the cloud server through the partial key computed by fog devices. Specifically, the system model includes the following five entities.

- Key generation center (KGC): KGC is a full trusted entity that initializes the system, grants private keys to corresponding EVs, and updates attribute sets for the updated EVs.
- Control center (CC): CC is a trusted entity with huge service information. It can divide service information into different levels and share it with EV that has the corresponding membership level.
- Cloud server (CS): The CS is a trusted entity for storing encrypted data.
- Fog device (FD): The FD is a trusted entity, which is a critical part for fog computing. Specifically, the FD will help CC to complete the heavy encryption operation in the offline phase and complete the EVs' partial decryption in the decryption phase.
- Electric vehicle (EV): A data user is an authorized EV that has a membership level. EVs with different membership levels can only obtain service information of the corresponding level on the CS.

B. SECURITY MODEL

Since our work is based on the scheme [24], we can define the adaptive chosen-ciphertext attacks (CCA2) security of a secure and membership-based data sharing scheme (Π) via the security game as follows:

Setup. The challenger $\mathcal{C}$ runs the Setup algorithm, and sends the public key PK to the adversary $\mathcal{A}$.

Phase 1. In this phase, an empty table T and set D, and an integer counter $j = 0$ are initialized by the challenger $\mathcal{C}$. The adversary $\mathcal{A}$ can make any of the following queries:

- Create (S): First, the challenger $\mathcal{C}$ runs the key generation algorithm to obtain the private key SK and stores (j, S, SK) in table T, then sets $j = j + 1$.
- Corrupt (i): If the i^{th} entity (i, S, SK) does not exist in T, then it returns $\perp$. Otherwise, challenger $\mathcal{C}$ obtains (i, S, SK) and sets $D = D \cup S$, then sends the private key SK to the adversary $\mathcal{A}$.
- Decrypt (i, CT): If the i^{th} entity (i, S, SK) does not exist in T, then it returns $\perp$. Otherwise, challenger $\mathcal{C}$ obtains (i, S, SK) and sends the output of the decryption algorithm to the adversary $\mathcal{A}$.

Challenge. In challenge phase, adversary $\mathcal{A}$ provides a challenge access structure $\mathbb{A}^*$ such that for all $S \in D$, $S \notin \mathbb{A}^*$. Next, challenger $\mathcal{C}$ runs the algorithm

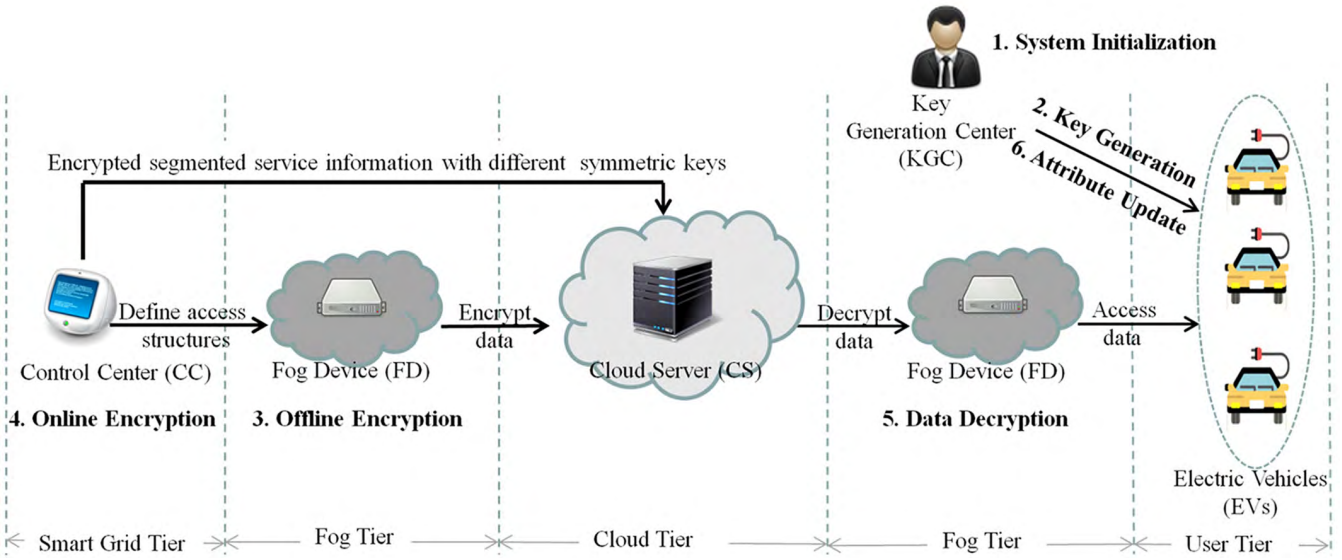

FIGURE 1. System model.

Online.Encrypt $(PK, \mathbf{Offline.Encrypt}\ (PK), \mathbb{A}^*)$ to obtain the ciphertext (key^*, CT^*). It then randomly chooses a bit $b \in \{0, 1\}$. If $b = 0$, challenger $\mathcal{C}$ sends (key^*, CT^*) to $\mathcal{A}$, else if $b = 1$, it chooses a random number R and sends (R, CT^*) to $\mathcal{A}$.

Phase 2. Adversary $\mathcal{A}$ can repeatedly make the queries of phase 1. However, it cannot obtain the S (such that $S \in \mathbb{A}^*$) that can decrypt the challenge ciphertext CT^* by making a Corrupt query.

Guess. Adversary $\mathcal{A}$ outputs a guess b' of b. If $b = b'$, then Adversary $\mathcal{A}$ wins the game.

Definition 1: A membership-based ABE scheme is adaptive chosen-ciphertext attacks (CCA2) secure if all probabilistic polynomial time (PPT) adversaries $\mathcal{A}$ can win the above mentioned game with a negligible probability:

$$Pr[Game_{\mathcal{A},\Pi}(\lambda, U) = 1] \leq \frac{1}{2} + negl(\lambda)$$

where, λ is a security parameter, U denotes the set of attributes allowed in the system.

C. DESIGN GOALS

According to the aforementioned system model and security model, our design goal is to present a secure and membership-based data sharing scheme in V2G networks. Specifically, we are going to fulfill following four goals:

- *Membership-Based Access.* Service information is shared in a hierarchical method based on EV's membership. EVs with more high memberships (e.g., platinum card member) are granted access to more advanced service information than those with lower memberships (e.g., ordinary member).
- *Fine-grained access control.* The proposed scheme should have the advantage of fine-grained access control. That is, the CC can use different defined access policies to encrypt each part of the service information, and only the EV member that meets the access policy can obtain the corresponding service information.
- *Confidentiality of service information.* In the proposed scheme, all service information in V2G networks is protected by the CC. That is, the EVs that do not have enough attributes to satisfy the access policy are denied access to the plaintext of the service information.
- *Efficiency.* In the proposed scheme, the computational costs on the CC and the EVs should be lower than those in the existing related schemes.

V. THE PROPOSED CONCRETE SCHEME

In this section, we propose a concrete construction for a secure and membership-based data sharing scheme in V2G networks. In the proposed scheme, the CC first divides the plaintext files of service information according to different membership levels. Assume that each level of service information contains different service items, such as charging time, value-added services, etc., and a certain level of EVs can only access the corresponding level of service information. For example, an authorized EV that recharges more than 10000 yuan at a time is upgraded to be a platinum card member, the authorized EV who recharges 5000–10000 yuan will become a gold member, and the authorized EV of recharging Less than 5000 yuan can only become an ordinary members. The platinum card member can obtain quality services (e.g., the charging time is not limited or more value-added services can be enjoyed), but the gold card members or ordinary members can only obtain some low-level services (e.g., obtaining limited charging time). Specifically, the CC splits data files $\mathcal{DF}$ into m data file sets, that is $\mathcal{DF} = \{DF_1, DF_2, \cdots, DF_m\}$. We suppose that the service information in DF_1 is the highest level and the service information in DF_m is the lowest level. Then, each data file

$DF_i \in \mathcal{DF}$ is individually encrypted with a secret key sk_i of symmetric encryption algorithm (e.g., AES [34]) to generate an encrypted data file $CDF_i = Enc_{sk_i}(DF_i)$.

In this paper, the symmetric key sk_i is encrypted under online/offline CP-ABE scheme [24] that can be accessed only by the authorized EVs with associated attribute set. For the sake of simplicity, the CC defines different levels of LSSS access structures $\{(\mathbb{M}_1, \rho_1), (\mathbb{M}_2, \rho_2), \cdots, ((\mathbb{M}_m, \rho_m))\}$ for encrypting the symmetric keys $\{sk_1, sk_2, \cdots, sk_m\}$ respectively. When the attribute set of the authorized EV satisfies one of the access structures, he/she can decrypt the corresponding symmetric key. In other word, an authorized EV obtains key sk_i, he/she can decrypt the data files CDF_i to obtain the corresponding level of service information.

The proposed scheme is composed of six phases: system initialization, key generation, data offline encryption, data online encryption, data decryption and attribute update. For convenience, we summarize the main notations of this paper in Table 1.

TABLE 1. Notations summary.

Symbol	Definition
sk_i	The i-th symmetric key used to encrypt DF_i
DF_i	The i-th data file
CDF_i	The i-th encrypted DF_i under sk_i
P_i	The i-th participant in a set of participants of secret sharing
S_j	The j-th authorized EV's attribute set
$A_{j,k}$	The k-th attribute within the attribute set S_j
$\mathbb{M}$	An $l \times n$ matrix and $l \leq P$, P is the maximum number of rows of matrix $\mathbb{M}$
$(\mathbb{M}, \rho)$	LSSS access structure
$(\mathbb{M}_i, \rho_i)$	LSSS access structure corresponding to the EV of level i
M_i	The i-th row of the matrix $\mathbb{M}$
M_{i_i}	The i-th row of the matrix $\mathbb{M}_i$
M_{i_j}	The j-th row of the matrix $\mathbb{M}_i$
t	The time taken for an EV to extract each service information

A. SYSTEM INITIALIZATION

KGC is a full trusted entity which bootstraps the whole system by running setup algorithm. Given the security parameter κ, the KGC chooses a bilinear group $\mathbb{G}_1$ of prime order p, and random generators $g, h, u, v, w \in \mathbb{G}_1$. It also picks a random exponent $\alpha \in \mathbb{Z}_p$, then calculates the public/secret key pair as $(PK = (\mathbb{G}_1, p, g, h, u, v, w, e(g,g)^\alpha), MSK = (PK, \alpha))$. Finally, PK is published as the public parameter, and master key MSK is stored by the KGC.

B. KEY GENERATION

Let's define $S_j = \{A_{j,1}, A_{j,2} \cdots, A_{j,k}\} \subseteq \mathbb{Z}_p$, where S_j denotes the j-th authorized EV's attribute set, and $A_{j,k}$ represents the k-th attribute within the set. Input the master key MSK and an authorized EV's attribute set S_j, the KGC chooses random numbers $r, r_1, r_2, \cdots, r_k \in \mathbb{Z}_p$, then computes $K_0 = g^\alpha w^r$, $K_1 = g^r$. For $i = 1$ to k, it also calculates $K_{i,2} = g^{r_i}$, $K_{i,3} = (u^{A_{j,i}} h)^{r_i} v^{-r}$. So the j-th authorized EV's private key is defined as:

$$SK_j = (S_j, K_0, K_1, \{K_{i,2}, K_{i,3}\}_{i\in[1,k]}) \quad (1)$$

C. OFFLINE ENCRYPTION

In our scheme, to reduce the computational costs of the CC, the fog devices first perform offline encryption that contains the heavy computations (e.g., pairing and group operations) and calculates as much as possible in the offline encryption phase. Specifically, fog device picks a random $s \in \mathbb{Z}_p$ and calculates $key = e(g,g)^{\alpha s}$, $C_0 = g^s$. Next, it chooses random $\lambda'_j, x_j, t_j \in \mathbb{Z}_p$ and calculates $C_{j,1} = w^{\lambda'_j} v^{t_j}$, $C_{j,2} = (u^{x_j} h)^{-t_j}$, $C_{j,3} = g^{t_j}$, for $j = 1$ to P_i, where P_i is assumed to be the maximum number of rows of matrix $\mathbb{M}_i$. Then the intermediate ciphertext ICT_j is constructed as:

$$ICT_j = (key, s, C_0, \{\lambda'_j, x_j, t_j, C_{j,1}, C_{j,2}, C_{j,3}\}_{j\in[1,P_i]}) \quad (2)$$

D. ONLINE ENCRYPTION

In the proposed scheme, the symmetric keys $sk = \{sk_1, sk_2, \cdots, sk_m\}$ are the objects that need to be encrypted. Each sk_i is encrypted with the corresponding access structure $(\mathbb{M}_i, \rho_i)$, where $\mathbb{M}_i$ is an $l \times n$ matrix and $l \leq P_i$. So the online encryption algorithm will run m times. In the stage of encrypting sk_i, the CC chooses random $y_{i,2}, \cdots, y_{i,n} \in \mathbb{Z}_p$, sets the vector $\vec{y_i} = (s, y_{i,2}, \cdots, y_{i,n})^T$ and calculates a vector of shares of s as $(\lambda_1, \cdots, \lambda_l)^T = \mathbb{M}_i \vec{y_i}$ (i.e., $\lambda_j = M_{i_j} \vec{y_i}$), where T denotes the transpose. For j=1 to l, the CC also calculates $C'_0 = sk_i \cdot e(g,g)^{\alpha s}$, $C_{j,4} = \lambda_j - \lambda'_j$, $C_{j,5} = t_j \cdot (\rho_i(j) - x_j)$. So the ciphertext is calculated as:

$$CT_j = ((\mathbb{M}_i, \rho_i), C_0, C'_0, \{C_{j,1}, C_{j,2}, C_{j,3}, C_{j,4}, C_{j,5}\}_{j\in[1,k]}) \quad (3)$$

E. DATA DECRYPTION

If the j-th authorized EV's attribute set S_j satisfy the LSSS access structure $(\mathbb{M}_i, \rho_i)$, he/she can decrypt the ciphertext CT_j by running the decryption algorithm and obtain the symmetric key sk_i. Then he/she can obtain the service information DF_i by using sk_i to decrypt the encrypted data files CDF_i.

The specific decryption is accomplished by the fog devices and the authorized EV, respectively.

- *Step-1*: Fog devices obtain the ciphertext CT_j for LSSS access structure $(\mathbb{M}_i, \rho_i)$ and the part of private key $SK'_j = (K_0, K_1, \{K_{i,2}, K_{i,3}\}_{i\in[1,k]})$ from the authorized EV.
- *Step-2*: If the j-th authorized EV's attribute set S_j cannot satisfy the LSSS access structure $(\mathbb{M}_i, \rho_i)$, the algorithm stops. Otherwise, fog devices set $I = \{i : \rho(i) \in S_j\}$ and chooses constants $w_i \in \mathbb{Z}_p$ such that $\sum_{i\in I} w_i \cdot M_{i_i} = (1, 0, \cdots, 0)$, then $\sum_{i\in I} w_i \cdot M_{i_i} \cdot \vec{y_i} = \sum_{i\in I} w_i \cdot \lambda_i = s$, where M_{i_i} denotes the i-th row of the matrix $\mathbb{M}_i$, and calculate

$$\begin{aligned} key &= \frac{e(C_0, K_0)}{e(w^{\sum_{i\in I} C_{i,4} w_i}, K_1) \cdot \prod_{i\in I} e(C_{i,1}, K_1)^{w_i}} \\ &\quad \cdot \frac{1}{\prod_{i\in I} (e(C_{i,2} \cdot u^{C_{i,5}}, K_{j,2}) \cdot e(C_{i,3}, K_{j,3}))^{w_i}} \\ &= e(g,g)^{\alpha s} \end{aligned} \quad (4)$$

Then, fog devices send key and C'_0 to the EV.

TABLE 2. The correctness of symmetric key sk_i recovery.

$$\frac{C_0'}{key} = \frac{C_0' \cdot e(w^{\sum_{i\in I} C_{i,4} w_i}, K_1) \cdot \prod_{i\in I} e(C_{i,1}, K_1)^{w_i} \cdot \prod_{i\in I} (e(C_{i,2} \cdot u^{C_{i,5}}, K_{j,2}) \cdot e(C_{i,3}, K_{j,3}))^{w_i}}{e(C_0, K_0)}$$

$$= \frac{C_0' \cdot e(w^{\sum_{i\in I} (\lambda_i - \lambda_i')w_i}, g^r) \cdot \prod_{i\in I} (e(w^{\lambda_i'} v^{t_i}, g^r))^{w_i} \cdot \prod_{i\in I} (e((u^{x_i} h)^{-t_i} \cdot u^{t_i(\rho(i)-x_i)}, g^{r_j}) \cdot e(g^{t_i}, (u^{A_j} h)^{r_j} v^{-r}))^{w_i}}{e(g^s, g^\alpha w^r)}$$

$$= \frac{C_0' \cdot e(g,w)^{r \sum_{i\in I} (\lambda_i - \lambda_i')w_i} \cdot \prod_{i\in I} e(g,w)^{\lambda_i' r} e(g,v)^{t_i r} e(g,u)^{\rho(i) t_i r_j} e(g,h)^{-t_i r_j} e(g,u)^{A_j t_i r_j} e(g,h)^{t_i r_j} e(g,v)^{-t_i r}}{e(g,g)^{\alpha s} \cdot e(g,w)^{sr}}$$

$$= \frac{C_0' \cdot e(g,w)^{r \sum_{i\in I} (\lambda_i - \lambda_i')w_i} \cdot \prod_{i\in I} e(g,w)^{\lambda_i' r}}{e(g,g)^{\alpha s} \cdot e(g,w)^{sr}}$$

$$= \frac{sk_i \cdot e(g,g)^{\alpha s} \cdot e(g,w)^{r \sum_{i\in I} w_i \lambda_i}}{e(g,g)^{\alpha s} \cdot e(g,w)^{sr}}$$

$$\xrightarrow{\because \sum_{i\in I} w_i \lambda_i = s}$$

$$= sk_i$$

- *Step-3*: After receiving *key* and C_0' from fog devices, the EV recovers the symmetric key sk_i by computing

$$\frac{C_0'}{key} = \frac{sk_i \cdot e(g,g)^{\alpha s}}{e(g,g)^{\alpha s}} = sk_i \tag{5}$$

Thus, the authorized EV can obtain the data file DF_i by using sk_i to decrypt the encrypted data file CDF_i as follows:

$$DF_i = Dec_{sk_i}(CDF_i) \tag{6}$$

The correctness of symmetric key sk_i recovery is shown in Table 2.

F. ATTRIBUTE UPDATE

Here, the j-th EV can change its membership through updating his attributes. For instance, the authorized EV's membership level will increase when its recharge amount increases from 5000 to 10000 yuan. Then KGC will update EV's attribute set $S_j = \{A_{j,1}, A_{j,2} \cdots, A_{j,k}\}$ to $S_{uj} = \{A'_{j,1}, A'_{j,2} \cdots, A'_{j,k}\}$. Thus, the updated key is denoted as

$$SK_{uj} = (S_{uj}, K_0 = g^\alpha w^r, K_1 = g^r, \{K_{i,2} = g^{r_i}, K_{i,3} = (u^{A'_{j,i}} h)^{r_i} v^{-r}\}_{i\in[1,k]}) \tag{7}$$

where, S_{uj} is the updated attribute set, and $A'_{j,i}$ represents the i-th updated attribute within S_{uj}.

Note that only the secret key need to be updated while the ciphertext remains unchanged in the proposed scheme.

VI. SECURITY ANALYSIS

In this section, we analyze the security of the proposed scheme, in which a formal proof of security is based on the work presented in [24]. Since all levels of ciphertexts CT_j follow the same rules, as long as a single CT_j is secure, then the whole scheme is proved to be secure.

Theorem 1: The proposed scheme is selectively CPA-secure with respect to Definition 1 under the assumption that the scheme [25] is a selectively CPA-secure CP-ABE system.

Proof: Assume there is an PPT adversary $\mathcal{A}$ can win the game in Section IV-B with a non-negligible advantage, then a PPT simulator $\mathcal{B}$ will can break the selective CPA-security of the scheme [25] (named RW).

Initialization. First, adversary $\mathcal{A}$ sends an LSSS access structure $(\mathbb{M}_i^*, \rho_i^*)$ to simulator $\mathcal{B}$. Then $\mathcal{B}$ gives this access structure to the challenger of RW, where $\mathbb{M}_i^*$ be an $l \times n$ matrix.

Setup. Then, simulator $\mathcal{B}$ receives the public parameters $PK = (\mathbb{G}_1, p, g, h, u, v, w, e(g,g)^\alpha)$ from the challenger of RW and sends them to adversary $\mathcal{A}$ intact.

Phase 1. The RW challenger can obtain the key in the way that adversary $\mathcal{A}$ requests any key generation.

Challenge. Simulator $\mathcal{B}$ chooses two random, distinct messages m_0, m_1, and sends them to the challenger of RW. Next, the challenger of RW returns $\mathcal{B}$ a challenge ciphertext

$$CT_j^* = ((\mathbb{M}_i^*, \rho_i^*), C_0, C_0', \{C_{j,1}, C_{j,2}, C_{j,3}\}_{j\in[1,l]}) \tag{8}$$

where $C_0' = sk_i \cdot e(g,g)^{\alpha s}$ is the encrypted message and $C_0 = g^s$. For each row in $\mathbb{M}_i^*$, there are $C_{j,1} = w^{\lambda_j} v^{t_j}$, $C_{j,2} = (u^{\rho_i^*(j)} h)^{t_j}$ and $C_{j,3} = g^{t_j}$.

Then, Simulator $\mathcal{B}$ chooses random blinding values $z_1, \cdots, z_l, z_1', \cdots, z_l' \in \mathbb{Z}_p$ and calculates the ciphertext $CT_j'^*$ of the proposed scheme as $((\mathbb{M}_i^*, \rho_i^*), C_0)$ followed by

$$C_{j,1}^* = C_{j,1} \cdot w^{-z_j} = w^{\lambda_j - z_j} v^{t_j}$$
$$C_{j,2}^* = C_{j,2} \cdot u^{-z_j'} = (u^{\rho_i(j)^*} h)^{t_j} \cdot u^{-z_j'}$$
$$C_{j,3}^* = C_{j,3} = g^{t_j}$$
$$C_{j,4}^* = z_j$$
$$C_{j,5}^* = z_j'.$$

Next, Simulator $\mathcal{B}$ guesses which of the messages $m_{\mathcal{B}b'}$ ($b' \in \{0,1\}$) is encrypted, and calculates $key_g = \frac{C_0'}{m_{\mathcal{B}b'}}$. Finally, Simulator $\mathcal{B}$ sends $(key_g, CT_j'^*)$ to adversary $\mathcal{A}$.

Phase 2. Same as Phase 1.

Guess. Finally, adversary $\mathcal{A}$ outputs messages $m_{\mathcal{A}b'}$ ($b' \in \{0,1\}$). Assume that $m_{\mathcal{A}0}$ indicates that adversary $\mathcal{A}$ guessed the key_g is the key encapsulated by $CT_j'^*$ and $m_{\mathcal{A}1}$ indicates that adversary $\mathcal{A}$ guessed the key_g is a random number. If the

TABLE 3. Comparison of features.

	Hur's scheme [4]	Zhang *et al.*'s scheme [5]	Wang *et al.*'s scheme [6]	Our scheme
Access control	CP-ABE	CP-ABE	CP-ABE	CP-ABE
Access structure	Access Tree	Access Tree	Access Tree	LSSS
Level-based access	No	No	No	Yes
Offline/online	No	No	Yes	Yes
Fog computing	No	Yes	No	Yes
Attribute update	No	Yes	No	Yes
Selective security	Yes	Yes	Yes	Yes

TABLE 4. Comparison of computational costs.

	Hur's scheme [4]	Zhang *et al.*'s scheme [5]	Wang *et al.*'s scheme [6]	Our scheme
Key generation	$(1+5k)\mathcal{E}_1+\mathcal{M}_1$	$(4+k)\mathcal{E}_1+\mathcal{M}_1$	$(1+5k)\mathcal{E}_1+\mathcal{M}_1$	$(4+3k)\mathcal{E}_1+(2k+1)\mathcal{M}_1$
Offline encryption	–	–	$C_e+(2+2k)\mathcal{E}_1+\mathcal{M}_1$	$C_e+\mathcal{E}_2+(1+5k)\mathcal{E}_1$ $+2k\mathcal{M}_1$
Online encryption	$C_e+\mathcal{E}_2+(1+2k)\mathcal{E}_1$ $+2\mathcal{M}_1$	$C_e+\mathcal{E}_2+(5+2k)\mathcal{E}_1$ $+3\mathcal{M}_1$	$C_e+\mathcal{E}_2+(2+k)\mathcal{M}_1$	$C_e+\mathcal{E}_2+(1+k)\mathcal{M}_1$
Decryption (fog device)	–	$(2k+2)C_e+k\mathcal{E}_2+2\mathcal{M}_1$	–	$(2+3k)C_e+\mathcal{M}_1$
Decryption (User)	$(3k+1)C_e+k\mathcal{E}_2+2\mathcal{E}_1$ $+k\mathcal{M}_1$	$C_e+2\mathcal{M}_1$	$(2k+1)C_e+3\mathcal{E}_1$ $+(k+1)\mathcal{M}_1$	$\mathcal{M}_1$

output is $m_{\mathcal{A}0}$, then simulator $\mathcal{B}$ outputs 0 to means that the ciphertext is the correct form. Otherwise, simulator $\mathcal{B}$ outputs 1 to means that the ciphertext is the random number. Therefore, if adversary $\mathcal{A}$ can win the game in Section IV-B with a non-negligible advantage, then simulator $\mathcal{B}$ can break the RW system with the same advantage.

Since scheme [25] has been proved to be a selectively CPA-secure CP-ABE system, the proposed scheme is selectively CPA-secure. Therefore, our scheme can ensure the security of service information.

VII. PERFORMANCE ANALYSIS

In this section, we analyze the performance of the proposed scheme in terms of performance characteristics and computational costs, and compare it with related schemes, that is, Hur's scheme [4], Zhang *et al.*'s scheme [5] and Wang *et al.*'s scheme [6].

A. CHARACTERISTICS COMPARISON

The results in Table 3 show the comparison of the performance characteristics between our scheme and other schemes. Although these schemes use the CP-ABE access control, only our scheme's access structure is LSSS, others are access trees. Compared with the access tree, LSSS mechanism can effectively prevent the loss of keys and attacks of malicious users. Additionally, schemes [4]–[6] are based on independent access strategies for handing data sharing, that is, their design does not support hierarchical access structures. However, the encrypt algorithm runs once for each level of information to achieve a membership-based access structure in our scheme. Moreover, Wang *et al.*'s scheme [6] has offline/online encryption function but does not support fog computing and attribute update. Zhang *et al.*'s scheme [5] has fog computing function but cannot perform offline/online encryption. However, the proposed scheme has both offline/online encryption and fog computing. Because of both offline/online encryption and fog computing, our scheme is more powerful than other schemes [4]–[6].

B. EFFICIENCY

Here, we will compare the efficiency of the proposed scheme and other schemes [4]–[6] in term of the computational cost of each phase (including key generation, encryption and decryption). The efficiency comparison results are shown in Table 4. In order to make the analysis more understandable, we describe the meaning of the notations used in Table 4 as follows:

- $\mathcal{E}_1$: An exponentiation in $\mathbb{G}_1$.
- $\mathcal{E}_2$: An exponentiation in $\mathbb{G}_2$.
- $\mathcal{M}_1$: A multiplication in $\mathbb{G}_1$.
- C_e: Bilinear pairing operation.
- k: Number of attributes associated with a EV's secret key.

In the *Key Generation* phase, the authorized EV's private key in our scheme is described as $(K_0 = g^{\alpha}w^{r}, K_1 = g^{r}, \{K_{i,2} = g^{r_i}, K_{i,3} = (u^{A_{j,i}}h)^{r_i}v^{-r}\}_{i\in[1,k]})$. Therefore, the computational cost of key generation is $(4+3k)\mathcal{E}_1+(2k+1)\mathcal{M}_1$. The *Encryption* phase of our scheme consists of two parts: *offline encryption* and *online encryption*. To reduce the computational cost of CC, we delegate the heavy computational operations of the encryption to the fog devices during the offline encryption phase. From Table 4, our scheme's computational cost of CC is greatly reduced compared with scheme [4], [5]. In the *Data Decrypt* phase, both scheme [5] and our scheme employ a fog device to help the user to decrypt, that is, partial decryption is performed by the fog device, thus reducing the computational cost of user. In our scheme, the computational cost of fog device is $(2+3k)C_e+\mathcal{M}_1$, while the computational cost of authorized EV is only $\mathcal{M}_1$. Of course, the fog device in fog tier shares most of the decryption computational overhead for the EV.

From Table 4, we can observe that the computational cost of *Key Generation* in our scheme is higher than other schemes in [4]–[6]. However, the computational costs of CC's encryption and EV's decryption are all less than that in [4]–[6].

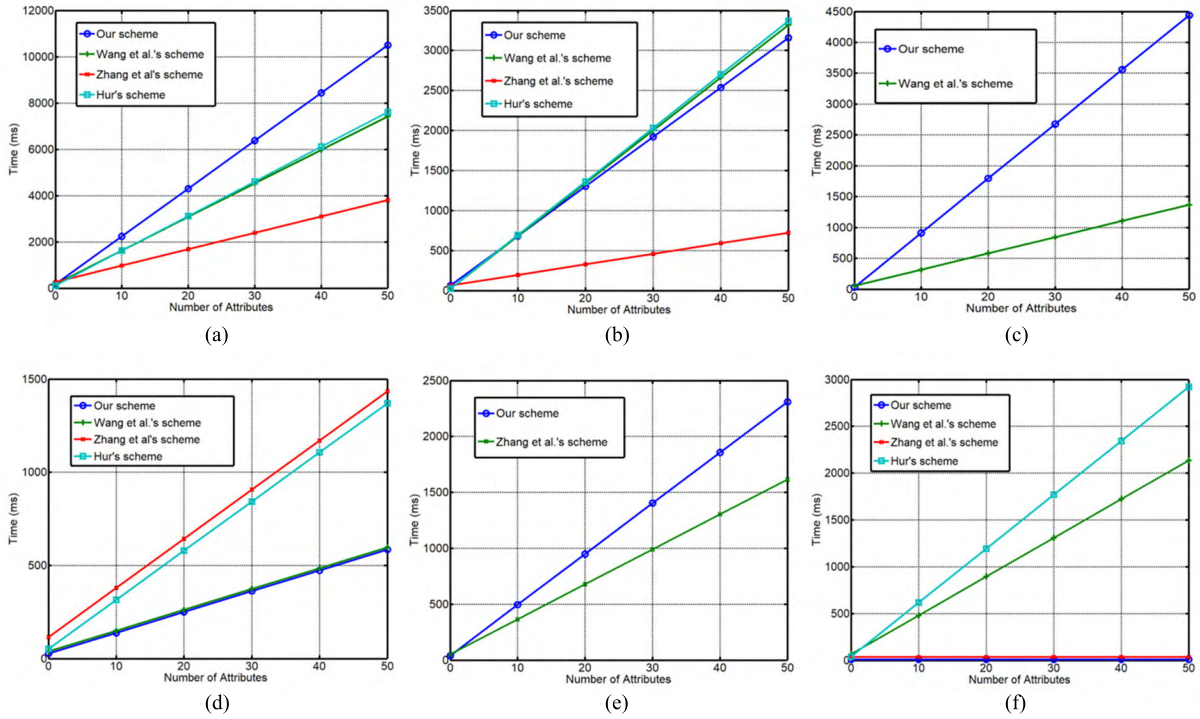

FIGURE 2. Comparison of computational costs of key generation, encryption and decryption. (a) Cost for entire system operation. (b) Cost on system for key generation. (c) Cost for offline encryption. (d) Cost on owner for encryption. (e) Cost on fog device for decryption. (f) Cost on user for decryption.

C. EXPERIMENTAL ANALYSIS

We use Java as programming language to run the experiments on the Win7 system of a computer with an Intel(R) Pentium(R) G3240 CPU at 3.10GHz and 4.00GB memory. By applying Java Pairing-Based Cryptography Library [37], the running time of each operation is $\mathcal{E}_1 = 13.179\ ms$, $\mathcal{E}_2 = 1.042\ ms$, $\mathcal{M}_1 = 11.161\ ms$, $C_e = 15.127\ ms$, respectively.

The comparison results of computational cost between our scheme and other schemes [4]–[6] in term of key generation, encryption and decryption are shown in Fig. 2. Fig. 2 (a) and (b) show the comparison of computational cost of entire system operation and the key generation time of system, respectively. We can find that the computational cost of entire system operation in our scheme is much bigger than that in [4]–[6], and the key generation time is much longer than that in [5] too. The reason is that the access structure used in our scheme is LSSS matrix which is more complex than the tree structure. Since scheme [6] and our scheme all adopt offline/online encryption mechanism, we compare the computational cost of the scheme [6] and ours in term of offline encryption, as shown in Fig. 2 (c). Fig. 2 (c) shows that the burden of offline encryption of our scheme is much greater than that of scheme [6]. Fig. 2 (d) shows the comparison of the computational cost on data owner for encryption. It is easy to see that the encryption time of data owner of our scheme is the smallest in all schemes. In decryption aspect, scheme [5] is similar to ours, which uses the fog devices to help users decrypt. Fig. 2 (e) shows that the computational cost of fog devices for decryption in our scheme is higher than that in scheme [5]. However, from Fig. 2 (f), we find that the computational cost of users for decryption in our scheme is much smaller than the schemes [4], [6] and slightly less than scheme [5].

Experimental results show that although our scheme has the highest computational cost for the entire system, we use offline/online encryption mechanisms and fog computing technology to minimize the time required for data owner encryption and user decryption. Therefore, our scheme is more efficient in reducing computational cost than schemes [4]–[6].

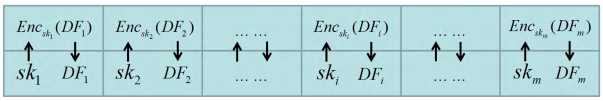

FIGURE 3. Ciphertext structure of partitioned service information.

D. ACCESS EFFICIENCY ANALYSIS

In terms of access efficiency, we mainly consider the time for authorized EV to extract service information. As mentioned earlier, CC first divides the service information into m parts $\mathcal{DF} = \{DF_1, DF_2, \cdots, DF_m\}$, respectively, and then encrypts each part with a symmetric key $sk = \{sk_1, \ldots, sk_m\}$. Here, we suppose that the ciphertext structure is depicted in Fig. 3, which the time taken for an EV to extract each service information is t. For the traditional scheme, the size of service information extracted by an EV is $\mathcal{DF} = (DF_1 + DF_2 + \cdots + DF_m)$. Then, the time for an EV to extract the

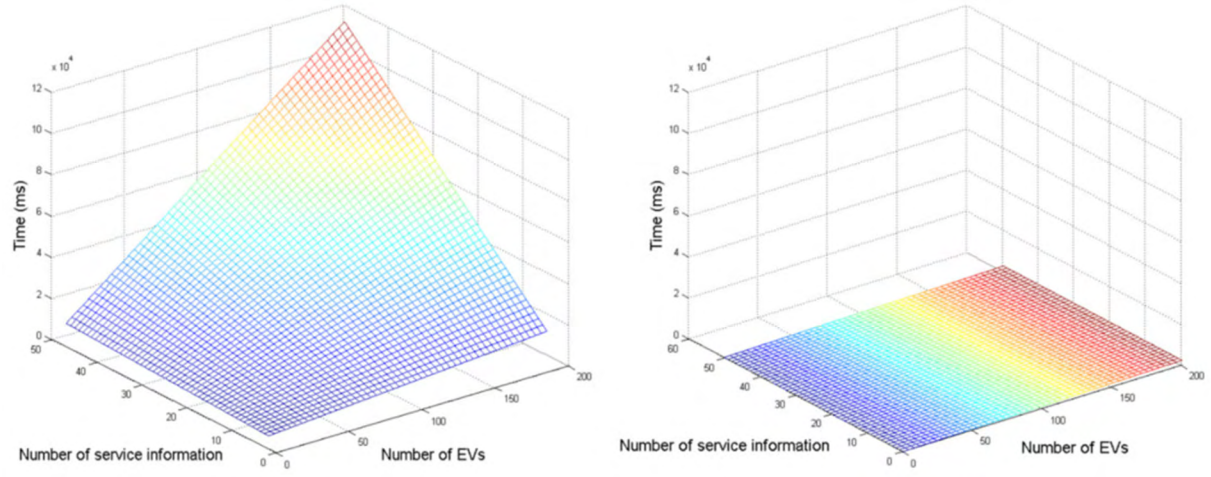

FIGURE 4. Comparison of extraction time of traditional ABE scheme and our scheme. (a) Extraction time of EVs in traditional ABE scheme. (b) Extraction time of EVs in our scheme.

service information is mt. However, the time for an EV to extract service information is t in our scheme. Fig. 4 (a) shows the time consumed for extracting service information when multiple EVs access the grid at the same time in the traditional ABE scheme, and Fig. 4 (b) shows our scheme's time consumed in this situation. Obviously, the access efficiency of our scheme is much higher than of traditional ABE scheme.

VIII. CONCLUSION

In this paper, we propose a secure and membership-based data sharing scheme in V2G networks, which can share service information according to the membership level of the EVs. With the help of the offline/online encryption mechanisms and fog computing technology, the proposed scheme can significantly reduce the time required for data owner encryption and user decryption. Security and performance analyses demonstrate the proposed scheme is selectively CPA-secure and more efficient in reducing computational cost than related schemes. Therefore, the proposed scheme is more suitable for V2G networks. In the future, we will study the privacy protection of V2G networks under the conditions of semi-trusted cloud and fog servers.

REFERENCES

[1] W. Han and Y. Xiao, "Privacy preservation for V2G networks in smart grid: A survey," *Comput. Commun.*, vols. 91–92, pp. 17–28, Oct. 2016.

[2] S. Käebisch, A. Schmitt, M. Winter, and J. Heuer, "Interconnections and communications of electric vehicles and smart grids," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 161–166.

[3] N. Saxena, S. Grijalva, V. Chukwuka, and A. V. Vasilakos, "Network security and privacy challenges in smart vehicle-to-grid," *IEEE Wireless Commun.*, vol. 24, no. 4, pp. 88–98, Aug. 2017.

[4] J. Hur, "Attribute-based secure data sharing with hidden policies in smart grid," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 11, pp. 2171–2180, Nov. 2013.

[5] P. Zhang, Z. Chen, J. K. Liu, K. Liang, and H. Liu, "An efficient access control scheme with outsourcing capability and attribute update for fog computing," *Future Generat. Comput. Syst.*, vol. 78, pp. 753–762, Jan. 2018.

[6] Z. Wang, F. Chen, and A. Xia, "Attribute-based online/offline encryption in smart grid," in *Proc. Int. Conf. Comput. Commun. Netw.*, Aug. 2015, pp. 1–5.

[7] A. Alrawais, A. Alhothaily, C. Hu, X. Xing, and X. Cheng, "An attribute-based encryption scheme to secure fog communications," *IEEE Access*, vol. 5, pp. 9131–9138, 2017.

[8] C. Zuo, J. Shao, G. Wei, M. Xie, and M. Ji, "CCA-secure ABE with outsourced decryption for fog computing," *Future Generat. Comput. Syst.*, vol. 78, pp. 730–738, Jan. 2018.

[9] H. Dubey, J. Yang, N. Constant, A. M. Amiri, Q. Yang, and K. Makodiya, "Fog data: Enhancing telehealth big data through fog computing," in *Proc. ASE BigData Social Informat.*, 2015, Art. no. 14.

[10] N. B. Truong, G. M. Lee, and Y. Ghamri-Doudane, "Software defined networking-based vehicular adhoc network with fog computing," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage.*, May 2015, pp. 1202–1207.

[11] R. Lu, K. Heung, A. H. Lashkari, and A. A. Ghorbani, "A lightweight privacy-preserving data aggregation scheme for fog computing-enhanced IoT," *IEEE Access*, vol. 5, pp. 3302–3312, 2017.

[12] M. Zhang, Y. Zhang, Y. Su, Q. Huang, and Y. Mu, "Attribute-based hash proof system under learning-with-errors assumption in obfuscator-free and leakage-resilient environments," *IEEE Syst. J.*, vol. 11, no. 2, pp. 1018–1026, Jun. 2017.

[13] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *Proc. IEEE Symp. Secur. Privacy (SP)*, May 2007, pp. 321–334.

[14] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in *Proc. ACM Conf. Comput. Commun. Secur.*, 2006, pp. 89–98.

[15] F. Bonomi, R. Milito, J. Zhu, and S. Addepalli, "Fog computing and its role in the Internet of Things," presented at the 1st edition MCC Workshop Mobile Cloud Comput., Helsinki, Finland, Aug. 2012, pp. 13–16.

[16] A. V. Dastjerdi and R. Buyya, "Fog computing: Helping the Internet of Things realize its potential," *Computer*, vol. 49, no. 8, pp. 112–116, Aug. 2016.

[17] H. Freeman and T. Zhang, "The emerging era of fog computing and networking [the president's page]," *IEEE Commun. Mag.*, vol. 54, no. 6, pp. 4–5, Jun. 2016.

[18] J. Shen, T. Zhou, F. Wei, X. Sun, and Y. Xiang, "Privacy-preserving and lightweight key agreement protocol for V2G in the social Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 4, pp. 2526–2536, Aug. 2018.

[19] M. Stegelmann and D. Kesdogan, "Design and evaluation of a privacy-preserving architecture for vehicle-to-grid interaction," in *Proc. Eur. Public Key Infrastruct. Workshop*. Berlin, Germany: Springer-Verlag, 2011, pp. 75–90.

[20] H. Wang, B. Qin, Q. Wu, L. Xu, and J. Domingo-Ferrer, "TPP: Traceable privacy-preserving communication and precise reward for vehicle-to-grid networks in smart grids," *IEEE Trans. Inf. Forensics Security*, vol. 10, no. 11, pp. 2340–2351, Nov. 2015.

[21] M. H. Eiza, Q. Shi, A. Marnerides, and T. Owens, "Secure and privacy-aware proxy mobile IPv6 protocol for vehicle-to-grid networks," in *Proc. IEEE Int. Conf. Commun.*, May 2016, pp. 1–6.
[22] A. Abdallah and X. S. Shen, "Lightweight authentication and privacy-preserving scheme for V2G connections," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2615–2629, Mar. 2017.
[23] S. Wang, J. Zhou, J. K. Liu, J. Yu, J. Chen, and W. Xie, "An efficient file hierarchy attribute-based encryption scheme in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 6, pp. 1265–1277, Jun. 2016.
[24] S. Hohenberger and B. Waters, "Online/offline attribute-based encryption," in *Public-Key Cryptography—PKC*. Berlin, Germany: Springer, 2014, pp. 293–310.
[25] Y. Rouselakis and B. Waters, "Practical constructions and new proof methods for large universe attribute-based encryption," in *Proc. Conf. Comput. Commun. Secur.* Berlin, Germany, 2013, pp. 463–474.
[26] W. Kempton and J. Tomić, "Vehicle-to-grid power fundamentals: Calculating capacity and net revenue," *J. Power Sour.*, vol. 144, no. 1, pp. 268–279, Jun. 2005.
[27] C. Guille and G. Gross, "A conceptual framework for the vehicle-to-grid (V2G) implementation," *Energy Policy*, vol. 37, no. 11, pp. 4379–4390, 2009.
[28] M. H. Au, J. K. Liu, J. Fang, Z. L. Jiang, W. Susilo, and J. Zhou, "A new payment system for enhancing location privacy of electric vehicles," *IEEE Trans. Veh. Technol.*, vol. 63, no. 1, pp. 3–18, Jan. 2014.
[29] Y. Liu, W. Guo, C.-I. Fan, L. Chang, and C. Cheng, "A practical privacy-preserving data aggregation (3PDA) scheme for smart grid," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2018.2809672.
[30] G. Shen, Y. Su, D. Zhang, H. Zhang, B. Xiong, and M. Zhang, "Secure and fine-grained electricity consumption aggregation scheme for smart grid," *KSII Trans. Internet Inf. Syst.*, vol. 12, no. 4, pp. 1553–1571, Apr. 2018.
[31] M. Zhang, Y. Yao, Y. Jiang, B. Li, and C. Tang, "Accountable mobile E-commerce scheme in intelligent cloud system transactions," *J. Ambient Intell. Humanized Comput.*, vol. 9, no. 6, pp. 1889–1899, 2018.
[32] F. Guo, Y. Mu, and Z. Chen, "Identity-based online/offline encryption," in *Financial Cryptography and Data Security*. Berlin, Germany: Springer-Verlag, 2008, pp. 247–261.
[33] A. Sahai and B. Waters, "Fuzzy identity-based encryption," in *Proc. Int. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer-Verlag, 2005, pp. 457–473.
[34] J. Daemen and V. Rijmen, *The Design of Rijndael: AES—The Advanced Encryption Standard*. Springer, 2013.
[35] B. Waters, "Ciphertext-policy attribute-based encryption: An expressive, efficient, and provably secure realization," in *Public Key Cryptography—PKC*. Berlin, Germany: Springer-Verlag, 2011, pp. 53–70.
[36] M. Zhang, W. Leng, Y. Ding, and C. Tang, "Tolerating sensitive-leakage with larger plaintext-space and higher leakage-rate in privacy-aware Internet-of-Things," *IEEE Access*, vol. 6, no. 1, pp. 33859–33870, Jun. 2018.
[37] *The Java Pairing Based Cryptography Library*. Accessed: Apr. 20, 2018. [Online]. Available: http://gas.dia.unisa.it/projects/jpbc/

GANG SHEN received the B.S. degree in electrical automation from the Wuhan Institute of Technology, Wuhan, China, in 2002, and the M.S. degree in control theory and control engineering from the School of Automation, Huazhong University of Science and Technology, Wuhan, in 2009. He is currently pursuing the Ph.D. degree in transportation information engineering and control from the School of Automation, Wuhan University of Technology, Wuhan. His current research interests include cryptography, network security, and privacy preservation.

YIXIN SU received the B.S. degree in process control from Wuhan University, Wuhan, China, in 1985, the M.S. degree in control theory and application from Southeast University, Nanjing, China, in 1988, and the Ph.D. degree in mechanical manufacturing and automation from the Huazhong University of Science and Technology, Wuhan, in 2006. He is currently a Professor with the School of Automation, Wuhan University of Technology, Wuhan, and also with the Deputy Dean of the School of Automation. His current research interests include intelligent controls, evolutionary computation, marine motion control, and cryptography technology for networks.

MINGWU ZHANG was a Japan Society for the Promotion of Science Fellow with the Institute of Mathematics for Industry, Kyushu University, Japan, from 2010 to 2012. From 2015 to 2016, he was a Senior Research Fellow with the Centre for Computer and Information Security, University of Wollongong, Australia. He is currently a Professor with the School of Computers, Hubei University of Technology, Wuhan, China. His current research interests include cryptography technology for networks, secure computations, and privacy preservation.