IEICE TRANS. INF. & SYST., VOL.E103–D, NO.2 FEBRUARY 2020

PAPER Special Section on Security, Privacy, Anonymity and Trust in Cyberspace Computing and Communications

A Novel Structure-Based Data Sharing Scheme in Cloud Computing

Huiyao ZHENG[†a)], **Jian SHEN**[†,††], **Youngju CHO**[†††], ***Nonmembers***, **Chunhua SU**[††††], ***and*** **Sangman MOH**[†††††], ***Members***

SUMMARY Cloud computing is a unlimited computing resource and storing resource, which provides a lot of convenient services, for example, Internet and education, intelligent transportation system. With the rapid development of cloud computing, more and more people pay attention to reducing the cost of data management. Data sharing is a effective model to decrease the cost of individuals or companies in dealing with data. However, the existing data sharing scheme cannot reduce communication cost under ensuring the security of users. In this paper, an anonymous and traceable data sharing scheme is presented. The proposed scheme can protect the privacy of the user. In addition, the proposed scheme also can trace the user uploading irrelevant information. Security and performance analyses show that the data sharing scheme is secure and effective.

key words: *data sharing, anonymous and traceable, cloud computing, key generation*

1. Introduction

In recent years, with the rapid development of information technology, the public's demand for the network has been increasing. Various forms of data has penetrated almost every field of daily life, and the amount of data has increased exponentially. With the increasing demand for storage and computing, the traditional local computing model has been unable to meet the growing demand. Cloud computing will play an irreplaceable role in the future network development. Cloud computing is a distributed computing model that provides services to users through Internet technology [1]. According to the statistics, the global cloud computing market has reached 260.2 billion dollars in 2017 and is expanding steadily. The emergence of cloud computing has enabled these data to be used in product production, facility construction and life improvement as shown in Fig. 1, for instance, in medicine [2], [3], education, transportation [4] and communication [5], which has improved

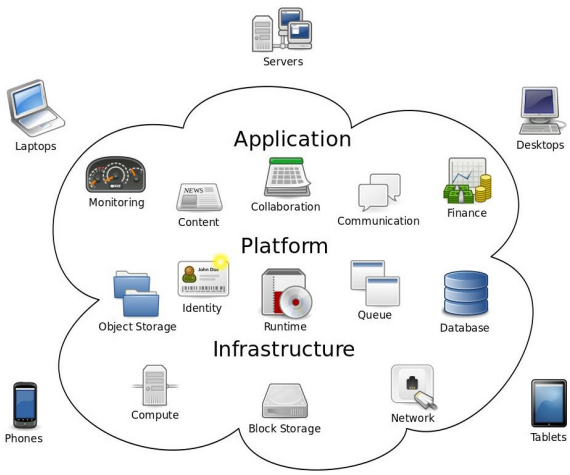

Fig. 1 Cloud application.

the production and living standards of the public. Many researchers also have been attracted by the convenience and high efficiency of cloud computing [6]. It has unique advantages in resource sharing and data collaboration, and is the product of sustainable development of information construction. Cloud computing improves resource utilization and reduces user equipment investment and use costs. Because of the unlimited computing resources and storage resources of the cloud, a lot of data appears in cloud. Users can freely upload and download data in cloud.

In cloud computing environment, data sharing is a way to improve data utilization and increase data value [7]. Introducing the shared process into the cloud environment can solve the problems and challenges brought by local storage and computing, and save the cost of enterprises, institutions and individuals. And by data sharing in cloud computing, computers and other equipment can obtain shared software resources, hardware resources and information, which greatly reduces the costs of extraction and management data. For instance, in intelligent transportation system, the real-time road condition can be shared with drivers, so traffic congestion can be reduced by cloud data sharing. There are two types of users in data sharing in cloud. One is who share data with all users in cloud. The other one is who shares data for specific group. In this paper, a group data sharing scheme is proposed in cloud computing.

Manuscript received March 10, 2019.
Manuscript revised August 7, 2019.
Manuscript publicized November 15, 2019.

[†]The authors are with Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science & Technology, Nanjing, China.
[††]The author is with Cyberspace Security Research Center, Peng Cheng Laboratory, Shenzhen 518000, China.
[†††]The author is with SW Convergence Education Institute, Chosun University, Gwanju 61452, Republic of Korea.
[††††]The author is with Division of Computer Science, University of Aizu, Aizuwakamatsu-shi, 965–0107 Japan.
[†††††]The author is with The Department of Computer Engineering, Chosun University, Gwangju 61452, Republic of Korea.
a) E-mail: liao_zhenghy@126.com
DOI: 10.1587/transinf.2019INP0014

1.1 Contribution

In this paper, an anonymous and traceable data sharing scheme in cloud computing is proposed. The main contributions of this paper are listed as follows.

- **A effective session key agreement protocol is proposed.** In this paper, a based on matrix structure session key agreement protocol is design. By two-part calculation, a group key can be derived used for data sharing in cloud. Moreover, the matrix structure can reduce the communication cost.
- **Anonymity and traceability are supported in data sharing scheme.** Anonymity is ensured by using phony-ID in this paper, which can protect the user's real identity. When a user uploads irrelevant information to cloud, the trusted third party can trace the real identity even though the user uses phony-ID sharing data. The users' privacy and the system security are guaranteed due to anonymity and traceability.
- **The authentication of the message is satisfied.** In this paper, each message is verified by receiver in session key generation phase, which ensures the correctness of the session key and ciphertext. The authenticated message can derive symmetric key used in encrypted the shared data.

1.2 Related Work

At present, the research results in the field of the secure data sharing are quite rich.

In 2006, Ateniese *et al.* proposed a proxy re-encryption scheme [8]. The scheme attempts to achieve secure data storage in a semi-trusted environment, but the scheme is vulnerable to collusion attacks.

In 2007, Bethencourt and others first proposed the encryption scheme based on ciphertext-policy attributes (CP-ABE) [9]. Yu *et al.* proposed a scheme to prevent revoked malicious user collusion attacks, but the scheme can only be used for one-to-one data sharing, not for multi-party data sharing in cloud environment [10]. Based on attribute encryption, the scheme also provides effective access control. Xu proposed a certificateless proxy re-encrypted data sharing scheme in cloud environment [11]. In the scheme, the data owner encrypts the data using a symmetric key. Chen and Tzeng proposed a secure method of data sharing among group members based on shared key deduction method [12]. The method uses binary tree to calculate the key. However, because the key update mechanism is widely used in the proposed scheme, the computational cost of the proposed scheme is very high. In addition, because some operations need centralized scheduling, this scheme is not suitable for public cloud systems.

Afterwards, Khan *et al.* used El-Gamal encryption system and bilinear pairing to share sensitive data in cloud environment by using trusted third parties as agents [13].

In 2016, Wei *et al.* present revocable-storage identity-based encryption scheme used in data sharing in cloud computing. And the security of the scheme is proved [14].

In 2018, Li *et al.* propose a based on CP-ABE lightweight data sharing scheme for mobile cloud computing, which can reduce the overhead on the mobile device side [15]. Ehab *et al.* propose a multilevel organizational data-sharing scheme that introduces privilege-based access structure into an attribute-based encryption mechanism [16]. Xu *et al.* present a fine-grained access control and data sharing scheme for dynamic user groups, which allow the KGC updating user credentials. In addition, the scheme includes a revocable ABE structure by adopting the property of ciphertext delegation by exploiting [17].

In the cloud environment data sharing problem, how to realize anonymous traceable data sharing still needs to give a more perfect solution.

1.3 Our Organization

The remainder of this paper is organized as follows. Section 2 introduces preliminary knowledge used later. Section 3 describes the model of data sharing scheme including system model and threat model. Section 4 presents the proposed scheme in detail. Section 5 and Sect. 6 analyze the security and performance respectively. Section 7 concludes this paper and our work.

2. Preliminary

2.1 Bilinear Pairing

Let G_1, G_2 and G_T be cyclic groups of prime order q. G_1 is generated by g, G_2 is generated by $\hat{g}$. A bilinear pairing is a map $e : G_1 \times G_2 \leftarrow G_T$, which satisfies the following properties:

Bilinearity. For all $g \in G_1$, $\hat{g} \in G_2$ and $a, b \in Z_p^*$, $e(g^a, \hat{g}^b) = e(g, \hat{g})^{ab}$. For $P, Q \in G_1$ and $R \in G_2$, $e(P, R)e(Q, R) = e(P + Q, R)$.

Non-degeneracy. If g is a generator of G_1 and $\hat{g}$ is a generator of G_2, $e(g, \hat{g}) \neq 1$.

Computability. e is efficiently computable.

Non-commutative. For any $P, Q \in \mathbb{G}_1$, $e(P, Q) \neq e(Q, P)$.

2.2 Short Signature

Signature guarantees that only the sender of information can produce a string which can not be forged by others. The string is also an effective proof of the authenticity of the information sent by the sender [18]–[20]. In this paper, a short signature is adopt. The description is presented as follows [21].

- **Setup**(k): Given the security parameter k, **Setup** outputs public parameters $p.p \leftarrow (p, G_1, G_2, G_T, e)$. In the following descriptions, we denote $G_1^* = G_1 \backslash 1_{G_1}$.

- **Keygen**$(p.p)$: It selects $g \leftarrow G_2$ and $(x, y) \leftarrow Z_p^2$, computes $(X, Y) \leftarrow (g^x, g^y)$ and sets sk as (x, y) and pk as (g, X, Y).
- **Sign**(sk, m): It selects a random number $r \leftarrow G_1^*$ and outputs signature $\sigma \leftarrow (r, r^{x+y \cdot m})$ on a message m.
- **Verify**$((pk, m, \sigma))$: It parses σ as (σ_1, σ_2) and checks whether $\sigma_1 \neq 1_{G_1}$ and $e(\sigma_1, X \cdot Y^m) = e(\sigma_2, g)$ are both satisfied. If positive, it outputs 1, and 0 otherwise.

3. System Model and Threat Model

Our scheme is an anonymous and traceable data sharing scheme in cloud. By using the session key, the security of messages is ensured. In this section, the system model and threat model of the proposed data sharing scheme are presented as follows.

3.1 System Model

In this section, the adopted system model in this paper is shown in Fig. 2. Three entities are involved in the data sharing model, which are Group, Cloud and the Trusted Third Party. The detail description about the three entities is presented as follows [22].

Group. A data sharing group consists of some users who want to share information of the same or similar topic. Users can join a interested group and share their information about the topic or obtain some messages from other group members.

Trusted Third Party (TTP). TTP is a trusted entity that initializes the system, generate system parameters. And users send their real ID to TTP for registering the valid group member identity. In addition, the users may upload some irrelevant information about group topic leading to message redundancy. TTP can trace the source of the irrelevant information according to the stored pairs even though users adopt phony-ID. Moreover, before users upload the ciphertext message, TTP checks the validity of the signature on plaintext message, namely, only the verified message can be upload to cloud by users.

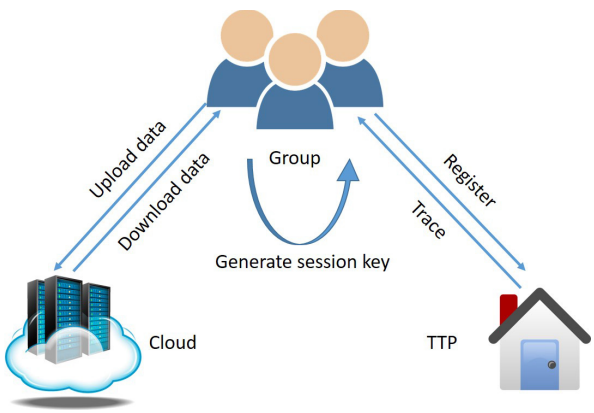

Fig. 2 System model.

Cloud. Cloud is an entity having unlimited computing resources and storage resources. Users can store a large quantity of data in cloud. Meanwhile, users can download the shared data by other users. In the same group, users can upload the own encrypted message by the session key to cloud. And other users use the same session key decrypting the shared data after downloading the message from cloud.

In the proposed scheme, first, users need obtain a valid identity from TTP. Then, the group members generate a session key based on the matrix structure in order to ensure secure data sharing. After that, uploader adopts symmetric encryption algorithms using the session key to encrypt the message and upload the ciphertext to cloud. All users in cloud can download the ciphertext message, however, they cannot decrypt the data. The users in the same group with uploader can successfully get plaintext message. Note that all users employ phony-ID when uploading and downloading messages so as to protect their privacy. In addition, when a user report the irrelevant information to TTP, TTP can trace the information uploader by comparing equation.

3.2 Threat Model

The threat model about the proposed scheme is presented in detail as follows.

A. An attacker can intercept messages communicated between two legal vehicles, and then temper with or regenerate messages. The attacker poses falsely as a legitimate vehicle to communicate with other vehicles.

B. An attacker tries to obtain the previous session key, if it obtains the long-term private key of one or more vehicle and learns some public information of other vehicles. The attacker can be a curious vehicle in the current session or an external attacker.

C. An attacker obtains a long-term key of a user or the previous complete session keys and disguises as a user to communicate.

4. The Proposed Scheme

In this section, an anonymous and traceable data sharing scheme is introduced in detail.

4.1 System Initialization

A trusted third party (TTP) initializes the system and registers users. First, TTP chooses two random number $(x, y) \leftarrow Z_q^*$ as its private key pair, computes $X = g^x$, $Y = g^y$, and sets (X, Y) as its public key pair. Then, TTP chooses three hash functions: $H_1 = \{0,1\}^* \rightarrow \{0,1\}^*$, $H_2 = \{0,1\}^* \rightarrow G_1$, $H_3 = \{0,1\}^* \rightarrow Z_q^*$. Finally, each user sent its $ID \in \{0,1\}^*$ to TTP via a secure channel.

TTP selects a random number $s_0 \leftarrow Z_q^*$, computes s_1 which satisfies $s_0 s_1 = 1 \bmod q$ and sets (s_0, s_1) as user's private key pair [23]. TTP computes $S = s_1 H_2(ID)$, $W = (S + X)$ and each user's public key pair (P_0, P_1), where $P_0 = g^{s_0}$ and $P_1 = g^{s_1}$. TTP publishes the system parameters

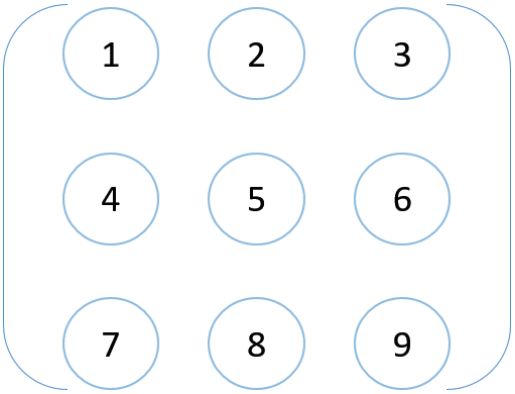

Fig. 3 Matrix structure.

$\{q, G_1, G_2, e, g, X, Y, H_1, H_2, H_3\}$, while keeping (x, y) secret. In addition, TTP sends the private key pair (s_0, s_1), W and S to each user via a secure channel.

4.2 Session Key Generation

In this subsection, the detailed session key generation is described. A matrix structure is employed in key generation. Let $k = \sqrt{n}$, where n is the user number of a data sharing group [24]. In this paper, a 9-group is chosen. All users are presented in a 3×3 matrix, where a node is corresponding to a user as Fig. 3.

The session key generation is divided into two parts. In the first part, the row users in the matrix communicate with each other. In the second part, the column users in the matrix exchange the information got in the first part with each other.

Part 1. Each user U_i need select a random number $\alpha_i \leftarrow Z_q^*$ and compute the phony-ID $PID_i = H_1(ID_i \| \alpha_i)$ for hiding the real ID. Then, U_i computes $Q_i = H_3(PID_i)S_i$, and $M_i = e(Q_i, P_{j0})$ as a part of the session key, where P_{j0} is the public key of the receiver U_j. In addition, in order to authenticate the validity of the information, each user need compute $T_i = e(H_3(PID_i)W_i, g)$ and select a time stamp t_i. Each user U_i sends the message $\{M_i, T_i, t_i, PID_i\}$ to the users in the same row in matrix structure. We present the detail session key generation process form the viewpoint of U_1 as follows. U_1 will receive two messages $\{M_2, T_2, t_2, PID_2\}$ and $\{M_3, T_3, t_3, PID_3\}$ form U_2 and U_3 respectively. U_1 checks whether the time stamp t_2 and t_3 are valid. If they are within the validity period, U_1 decrypts M_2 and M_3 by using its private key, otherwise, closure.

$$M_2' = M_2^{s_{21}} = e(H_3(PID_2)s_{11}H_2(ID_2), g)$$
$$M_3' = M_3^{s_{31}} = e(H_3(PID_3)s_{11}H_2(ID_3), g)$$

Then, U_1 integrates the received message form U_2 and U_3 as follows.

$$\begin{aligned} D_1 &= M_1' M_2' M_3' \\ &= \prod_{i=1}^{3} e(H_3(PID_i)s_{i1}H_2(ID_i), g) \\ &= e(\sum_{i=1}^{3} H_3(PID_i)s_{i1}H_2(ID_i), g) \end{aligned}$$

Finally, similar to U_1, other users do the same operations.

Part 2. Each user U_i sends the integrated information $\{M_i, T_i, t_i, PID_i, D_i\}$ to the column users in matrix structure. From the viewpoint of U_1, the session key generation process is described in detail as follows. U_1 received the messages $\{M_4, T_4, t_4, PID_4, D_4\}$, $\{M_7, T_7, t_7, PID_7, D_7\}$ from U_4 and U_7 respectively. U_1 derives the session key as

$$K = D_1 D_4 D_7.$$

From the Part 1,$D_4 = e(\sum_{i=4}^{6} H_3(PID_i)s_{i1}H_2(ID_i), g)$ and $D_7 = e(\sum_{i=7}^{9} H_3(PID_i)s_{i1}H_2(ID_i), g)$. Namely, the session key is computed as follows.

$$\begin{aligned} K &= D_1 D_4 D_7 \\ &= e(\sum_{i=1}^{3} H_3(PID_i)s_{i1}H_2(ID_i), g) \\ &\quad e(\sum_{i=4}^{6} H_3(PID_i)s_{i1}H_2(ID_i), g) \\ &\quad e(\sum_{i=7}^{9} H_3(PID_i)s_{i1}H_2(ID_i), g) \\ &= e(\sum_{i=1}^{9} H_3(PID_i)s_{i1}H_2(ID_i), g) \end{aligned}$$

If all users implement the above items, they will derives the same session key contained secret information of all users for encrypted the shared data.

In order to ensure the validity of the information, the receiver need not only check the time stamp, but also guarantee that the message is not tampered by attacker [24]. Before integrating the information, U_i computes $E_j = e(H_3(PID_j)X, g)$ using the received message $\{M_j, T_j, t_j, PID_j\}$. Then, U_i checks the validity of the information by determine the equation as follow.

$$\begin{aligned} M_j' E_j &\stackrel{?}{=} T_j \\ M_j' E_j &= e(H_3(PID_j)s_{j1}H_2(ID_j), g)e(H_3(PID_j)X, g) \\ &= e(H_3(PID_j)(s_{j1}H_2(ID_j) + X), g) \\ &\stackrel{?}{=} T_j \end{aligned}$$

If the equation holds, the message is valid; otherwise, it is tampered with attacker.

4.3 Data Sharing and Identity Disclosing

Users in a group can share their information with each other

in cloud. However, the information is related to users' privacy. In order to prevent privacy disclosure, all data need be encrypted before uploading to cloud [25], [26]. In this paper, we use the session key derived in Sect. 4.2 to encrypting the data with classical encryption algorithms.

- **Upload data.** U_i shares the message m to group members. The user obtains the ciphertext C_m by using symmetric encryption algorithms with session key K, namely, $C_m = E_K(m)$[27].
  Then U_i selects a random number $r_i \leftarrow Z_q^*$, and computes $u_{i0} = PID_i^{s_{i0}}$ and $u_{i2} = r_i^{s_{i1}}$. U_i generates the signature $\sigma = (\sigma_1, \sigma_2)$ on message m, where $\sigma_1 = r_i$ and $\sigma_2 = r_i^{s_{i0}+s_{i1}m}$. U_i sends the signature (σ, m) and $\{ID_i, u_{i1}, u_{i2}\}$ to TTP. After TTP checks the validity of σ, U_i will upload the message $\{C_m, PID_i, \sigma_1\}$ in cloud. Meanwhile, TTP stores the information $\{ID_i, u_{i1}, u_{i2}\}$ about U_i. TTP checks the signature as follows.

$$\begin{aligned} &e(\sigma_1, P_{i0}P_{i1}^m) \stackrel{?}{=} e(\sigma_2, g) \\ &e(\sigma_1, P_{i0}P_{i1}^m) = e(r_i, g^{s_{i0}}g^{s_{i1}m}) = e(r_i, g)^{s_{i0}+s_{i1}m} \\ &\qquad = e(r_i^{s_{i0}+s_{i1}m}, g) = e(\sigma_2, g) \end{aligned}$$

- **Download data.** U_j in the same group with U_i can download the message $\{C_m, PID_i, \sigma_1\}$ uploaded by U_i. U_j uses the session key K to decrypt the ciphertext C_m, namely, $m = D_K(C_m)$.
- **Identity Disclosing.** Some members in data sharing group may upload information not conforming to the group topic. When a user downloads the irrelevant information $\{C'_m, PID'_i, \sigma'_1\}$, it can report the situation to TTP with the downloaded message.
  TTP can trace the real ID uploading the irrelevant information according to the messages which all users store in TTP. The user sends the irrelevant information $\{C'_m, PID'_i, \sigma'_1\}$ to TTP. Then, TTP determines the equation whether holding by using $\{ID_i, u_{i1}, u_{i2}\}$ until equation holds.

$$\begin{aligned} &e(u_{i2}, u_{i1}) \stackrel{?}{=} e(\sigma'_1, PID'_i) \\ &e(r_i^{s_{i1}}, PID_i^{s_{i0}}) = e(r_i, PID_i)^{s_{i1}s_{i0}} \\ &\qquad = e(r_i, PID_i) \stackrel{?}{=} e(\sigma'_1, PID'_i) \end{aligned}$$

  When the equation holds, the ID corresponding with (u_{i1}, u_{i2}) is the real identity uploading the irrelevant information $\{C'_m, PID'_i, \sigma'_1\}$.

5. Security Analysis

In this section, the security of the proposed scheme is analyzed.

5.1 Man-in-the-Middle Attack Resistance

A Man-in-the-middle attacker can collect the communication message among users, tamper with messages or regenerate messages. In this paper, we assume that the message can be intercepted in session key generation phase. The description is presented in detail as follows. An attacker disguises a legal user and interrupts the communication message. Then the attacker tampers with the PID_j and selects a new PID'_j in order to access the verification. The receiver can distinguish the validity of the message as follows. The receiver computes $E_j = e(H_3(PID_j)X, g)$ according to the process and decrypts M_j using the session key. Then the receiver checks the validity of the information.

$$\begin{aligned} M'_jE_j &= e(H_3(PID'_j)s_{j1}H_2(ID_j), g)e(H_3(PID_j)X, g) \\ &\neq e(H_3(PID'_j)(s_{j1}H_2(ID_j) + X), g) \\ &\neq T_j \end{aligned}$$

It is clear that the tampered message cannot access the verification. So the proposed scheme can resist man-in-the-middle attack.

5.2 Forward Secrecy

Forward secrecy means that an attacker does not know the previous session key even though the attacker knows the current session key. When group members change, users update the session key. The session key structure is $K = e(\sum_{i=1}^{n} H_3(PID_i)s_{i1}H_2(ID_i), g)$, and ID_i is private. Even though an attacker gets all ID_i of the current session, the attacker cannot know the changed ID. In addition, $PID_i = H_1(ID_i||\alpha_i)$ where α_i is a different random number in each session. So the attacker cannot compute the previous session key, namely, the proposed scheme is characterized by forward secrecy.

5.3 Replay Attack Resistance

Reply attack means that an attacker sends a repeated message to the legal users. In this paper, a time stamp t is included in the sent message. Receivers check the validity of the time stamp. If t is fresh, continue; otherwise, discard the message. Namely, the proposed scheme can resist replay attack.

5.4 Key-Compromise Impersonation

Key-compromise impersonation means that the private key exposure of a user cannot lead to leaking other users' private key. In the proposed scheme, each user's private key is distributed by TTP. The private key is a key pair (s_0, s_1) structure, where s_0 and s_1 are two random numbers and not related to the user information. If a user's private key exposes, an attacker cannot determine other users' private key pair. So other users' key is secure.

5.5 Anonymity

Users' ID is related to the privacy of each user. When the group topic refers to the sensitive information of users, for instance, medical data, body index data and trip route, users

hope that their ID can be protected [28]. In the proposed scheme, users' ID is hidden and exchanged into phony-ID, where $PID_i = H_1(ID_i||\alpha_i)$. Each user uploads the message using phony-ID. The downloader knows the phony-ID included in uploading message of the uploader. In addition, due to the random number α_i and the one-way hash function, receiver cannot recovery the real ID. So the proposed scheme is anonymous.

5.6 Traceability

Traceability means that the trust third party can trace the source of the data in cloud. An effective and secure protocol should not only protect the privacy of group members but also trace the source of the irrelevant messages. Some group members may share the irrelevant information to other users, which is not allowed. When a user discovers this situation and reports to TTP, TTP can trace the real ID of the uploading the information [29]. TTP checks the equation $e(u_{i2}, u_{i1}) \stackrel{?}{=} e(\sigma'_1, PID'_i)$ according to the pair (u_{i1}, u_{i2}) stored in TTP by each user and receiving message (σ'_1, PID'_i) one by one, until the equation holds. The pair that makes the equation hold is the receiver. TTP finds the related to real ID on the basis of the pair (ID_i, u_{i1}, u_{i2}). After identifying the real ID, TTP removes the user. And the all group members restart the data sharing scheme [30], [31].

6. Performance Analysis

In this section, the performance of the proposed scheme is simulated and analyzed.

6.1 Performance Analysis

In this section, the proposed data sharing scheme is analyzed in terms of the session key generation and the process that TTP trace the real ID. In the session key generation phase, the computational cost of each user is equal. In the traceable phase, the computational cost of TTP is unfixed, so it is discussed in two cases, the best case and the worst case.

In the session key generation, each user need do one point multiplication $H_3(PID_i)S_i$ and one weil pairing $e(Q_i, P_{j0})$ for computing the part of the session key. Then, for authentication, each user need compute two point multiplications $H_3(PID_i)W_i$ and $H_3(PID_i)X$, and three weil pairings $e(H_3(PID_i)W_i, g)$, $e(H_3(PID_i)X, g)$ and M'_iE_i. For decrypting the M_i, each user need compute two exponentiations $M_j^{S_{i1}}$. In the process of the session key combination, each user need compute two weil pairings D_i and K. The total cost is listed in Table 1 in detail.

Table 1 The total cost of each user on the session key.

Propagation mode	Point multiplication	Weil pairings	Exponentiation
Multicast	3	6	2

* n: the number of vehicles, t_p: point multiplication by vehicles, t_w: Weil pairings by users, t_e: exponentiation by users.

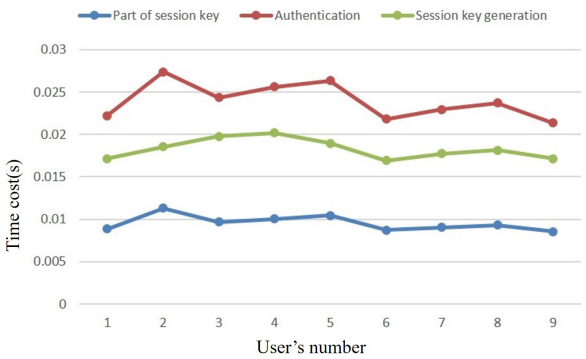

Fig. 4 Computation cost of each user.

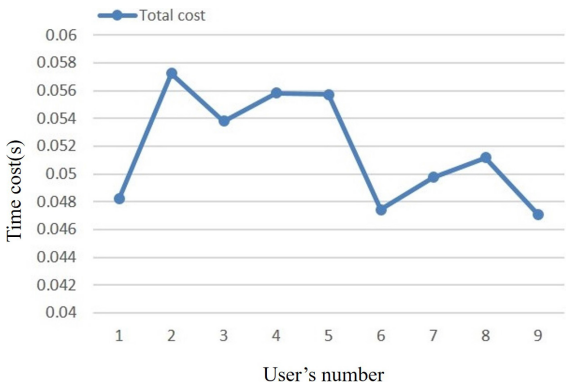

Fig. 5 Total cost of each user.

In the process of tracing the real ID, TTP computes one weil pairing $e(\sigma'_1, PID'_i)$ according to the received message. And in the best case, TTP only computes one weil pairing $e(u_{i2}, u_{i1})$, which satisfies the equation $e(u_{i2}, u_{i1}) = e(\sigma'_1, PID'_i)$. In the worst case, TTP need compute all weil pairings $e(u_{i2}, u_{i1})$.

6.2 Performance Evaluation

In this section, the proposed scheme is simulated in a personal computer by using the pairing-based cryptography (PBC) library and the GUN multiple precision arithmetic (GMP) library. And the simulation environment is presented as follows: 1) CPU: Intel(R) Core(TM) i5-4200U; 2) Random-access Memory: 4 GB (3.89 G available); 3) Read-only Memory: 1 T; 4) OS: Ubuntu 12.04 x64 over VMware workstation full 12.5.2.

The computation cost of each user is presented in Fig. 4. The computation cost of the part of session key, authentication and session key generation is described respectively. The total cost of each user is presented in Fig. 5. In Fig. 6, the computation cost of TTP in tracing real ID is presented. Note that the worst case which TTP traces the real ID is less than 0.06s. So the proposed data sharing scheme is practical.

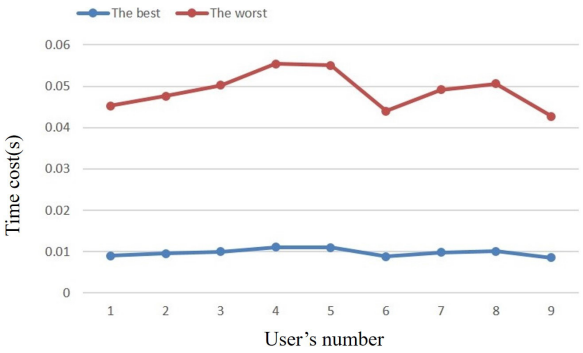

Fig. 6 Computation cost of TTP.

7. Conclusion

Cloud is effective and provides convenience for our life due to the unlimited computing resource and storage resources. In addition, based on the characteristic of cloud, data sharing greatly reduces the cost of data management and data processing. However, existing data sharing schemes don not consider the privacy of users. In this paper, an anonymous data sharing scheme is proposed. Users' real ID cannot exposed. In addition, in order to remove the dishonest users, TTP can trace the resource of the irrelevant information. Additionally, the simulation shows that the proposed scheme is effective in practice.

Acknowledgments

This work is supported by the National Natural Science Foundation of China under Grants No. 61922045, No. U1836115, No. 61672295, the Natural Science Foundation of Jiangsu Province under Grant No. BK20181408, the Foundation of State Key Laboratory of Cryptology under Grant No. MMKFKT201830, the Peng Cheng Laboratory Project of Guangdong Province PCL2018KP004, the CICAEET fund, and the PAPD fund.

References

[1] T. Zhou, L. Chen, and S. Jian, "Movie recommendation system employing the user-based cf in cloud computing," IEEE International Conference on Computational Science & Engineering, pp.46–50, 2017.

[2] D. Liu, J. Shen, A. Wang, and C. Wang, "Lightweight and practical node clustering authentication protocol for hierarchical wireless sensor networks," International Journal of Sensor Networks, vol.27, no.2, pp.95–102, 2018.

[3] C.-H. Hsia, "Improved finger-vein pattern method using wavelet-based for real-time personal identification system," Journal of Imaging Science & Technology, vol.62, no.3, pp.30402.1–30402.8, 2018.

[4] C. Wang, L. Xiao, J. Shen, and R. Huang, "Neighborhood trustworthiness-based vehicle-to-vehicle authentication scheme for vehicular ad hoc networks," Concurrency and Computation: Practice and Experience, vol.31, no.21, 2018, doi: 10.1002/cpe.4643.

[5] C.-H. Hsia, "New verification method for finger-vein recognition system," IEEE Sensors Journal, vol.18, no.2, pp.790–797, 2018.

[6] M. Zhang, Y. Zhang, Y. Jiang, and J. Shen, "Obfuscating eves algorithm and its application in fair electronic transactions in public clouds," IEEE System Journal, vol.13, no.2, pp.1478–1486, 2019, doi:10.1109/JSYST.2019.2900723.

[7] J. Shen, T. Zhou, X. Chen, J. Li, and W. Susilo, "Anonymous and traceable group data sharing in cloud computing," IEEE Transactions on Information Forensics and Security, vol.13, no.4, pp.912–925, 2018.

[8] G. Ateniese, K. Fu, M. Green, and S. Hohenberger, "Improved proxy re-encryption schemes with applications to secure distributed storage," Acm Transactions on Information & System Security, vol.9, no.1, pp.1–30, 2006.

[9] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," Proceedings of the IEEE Symposium on Security and Privacy, pp.321–334, 2007.

[10] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable, and fine-grained data access control in cloud computing," 2010 Proceedings IEEE INFOCOM, pp.1–9, 2010.

[11] X. Lei, X. Wu, and X. Zhang, "Cl-pre: A certificateless proxy re-encryption scheme for secure data sharing with public cloud," Proceedings of the 7th ACM Symposium on Information, Computer and Communications Security, pp.87–88, 2012.

[12] Y.-R. Chen and W.-G. Tzeng, "Efficient and provably-secure group key management scheme using key derivation," IEEE International Conference on Trust, pp.295–302, 2012.

[13] A.N. Khan, M.L.M. Kiah, S.A. Madani, M. Ali, A.U.R. Khan, and S. Shamshirband, "Incremental proxy re-encryption scheme for mobile cloud computing environment," Journal of Supercomputing, vol.68, no.2, pp.624–651, 2014.

[14] J. Wei, W. Liu, and X. Hu, "Secure data sharing in cloud computing using revocable-storage identity-based encryption," IEEE Transactions on Cloud Computing, vol.6, no.4, pp.1136–1148, 2018.

[15] R. LI, C. Shen, H. He, X. Gu, Z. Xu, and C.-Z. Xu, "A lightweight secure data sharing scheme for mobile cloud computing," IEEE Transactions on Cloud Computing, vol.6, no.2, pp.344–357, 2018.

[16] E. Zaghloul, Z. Kai, and R. Jian, "P-mod: Secure privilege-based multilevel organizational data-sharing in cloud computing," IEEE Transactions on Big Data, 2019.

[17] S. Xu, G. Yang, Y. Mu, and R.H. Deng, "Secure fine-grained access control and data sharing for dynamic groups in the cloud," IEEE Transactions on Information Forensics and Security, vol.13, no.8, pp.2101–2113, 2018.

[18] X. Chen, J. Li, X. Huang, J. Li, Y. Xiang, and D.S. Wong, "Secure outsourced attribute-based signatures," IEEE Transactions on Parallel & Distributed Systems, vol.25, no.12, pp.3285–3294, 2014.

[19] B. Dan and X. Boyen, "Short signatures without random oracles and the sdh assumption in bilinear groups," Journal of Cryptology, vol.21, no.2, pp.149–177, 2008.

[20] A.L. Ferrara, M. Green, S. Hohenberger, and M.Ø. Pedersen, "Practical short signature batch verification," Cryptographers Track at the Rsa Conference, vol.5473, pp.309–324, 2009.

[21] D. Pointcheval and O. Sanders, "Short randomizable signatures," Cryptographers Track at the Rsa Conference, vol.9610, pp.111–126, 2016.

[22] J. Shen, A. Wang, C. Wang, and N.N. Xiong, "A RFID based localization algorithm applying trilateration for wireless sensor networks," Journal of Internet Technology, vol.18, no.5, pp.1167–1175, 2017.

[23] X. Chen, J. Li, J. Ma, Q. Tang, and W. Lou, "New algorithms for secure outsourcing of modular exponentiations," IEEE Transactions on Parallel & Distributed Systems, vol.25, no.9, pp.2386–2396, 2012.

[24] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun, and Y. Xiang, "Block design-based key agreement for group data sharing in cloud computing," IEEE Transactions on Dependable and Secure Computing, pp.996–1010, 2017, doi:10.1109/TDSC.2017.2725953.

[25] T. Zhou, J. Shen, X. Li, C. Wang, and J. Shen, "Quantum

Cryptography for the Future Internet and the Security Analysis," Security and Communication Networks, vol.2018, 2018. doi:10.1155/2018/8214619.
[26] C. Wang, J. Shen, Q. Liu, Y. Ren, and T. Li, "A novel security scheme based on instant encrypted transmission for internet of things," Security and Communication Networks, vol.2018, 2018, doi:10.1155/2018/3680851.
[27] T. Zhou, J. Shen, X. Li, C. Wang, and H. Tan, "Logarithmic encryption scheme for cyber physical systems employing fibonacci q-matrix," Future Generation Computer Systems, 2018, doi:10.1016/j.future.2018.04.008.
[28] M. Abe, S.S.M. Chow, K. Haralambiev, and M. Ohkubo, "Double-trapdoor anonymous tags for traceable signatures," International Journal of Information Security, vol.12, no.1, pp.19–31, 2013.
[29] S. Shin and T. Kwon, "Aana: Anonymous authentication and authorization based on short traceable signatures," International Journal of Information Security, vol.13, no.5, pp.477–495, 2014.
[30] X. Chen, L. Jin, X. Huang, J. Ma, and W. Lou, "New publicly verifiable databases with efficient updates," IEEE Transactions on Dependable & Secure Computing, vol.12, no.5, pp.546–556, 2015.
[31] J. Shen, D. Liu, C.F. Lai, Y. Ren, and X. Sun, "A secure identity-based dynamic group data sharing scheme for cloud computing," Journal of Internet Technology, vol.18, no.4, pp.833–842, 2017.

Huiyao Zheng received the B.E. degree from Nanjing University of Information Science and Technology, Nanjing, China, in 2017. She is currently a postgraduate with the School of Nanjing University of Information Science and Technology, Nanjing, China. She focuses on group user authentication scheme in networks. Her research interests include information security, security systems and cryptography.

Jian Shen received the M.E. and Ph.D. degrees in Computer Science from Chosun University, South Korea, in 2009 and 2012, respectively. Since late 2012, he has been a professor at Nanjing University of Information Science and Technology, Nanjing, China. His research interests include public key cryptography, secure data sharing and data auditing in cloud.

Youngju Cho received the SWeducation research professor of the SW Convergence Education Institute at Chosun University and is a head researcher of an annex research institute owned by the SCG corporation. She received her master's degree and PhD both in electronic calculation from Chosun University, specializing in information techologies, education, and mobile ad hoc networks. Her interests include network security, Internet of things, information protection, mobile ad hoc networks, Internet ethics, VR, and AR.

Chunhua Su received the B.S. degree for Beijing Electronic and Science Institute in 2003 and received his M.S. and PhD of computer science from Faculty of Engineering, Kyushu University in 2006 and 2009, respectively. He is currently working as an Associate Professor in Division of Computer Science, University of Aizu. He has worked as a research scientist in Cryptography and Security Department of the Institute for Infocomm Research, Singapore from 2011-2013. From 2013-2016, he has worked as an Assistant professor in School of Information Science, Japan Advanced Institute of Science and Technology. From 2016-2017, he worked as Assistant Professor in Graduate School of Engineering, Osaka University. His research interests include cryptanalysis, cryptographic protocols, privacy-preserving technologies in data mining and IoT security and privacy.

Sangman Moh received the Ph.D. degree in computer engineering from Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Korea in 2002. Since late 2002, he has been a faculty member in the School of Computer Engineering at Chosun University, Gwangju, Korea. From 2006 to 2007, he was on leave at Cleveland State University, Cleveland, Ohio, USA. His research interests include mobile computing and networking, ad hoc networks and systems, ubiquitous sensor networks, network based computing, parallel and distributed computing, and high-performance computer systems.