Distributed Multi-authority Attribute-Based Encryption for Secure Friend Discovery and Data Sharing in Mobile Social Networks

Fang Qi, Wenbo Wang, and Zhe Tang(✉)

School of Information Science and Engineering,
Central South University, Changsha 410083, China
{wb_wang,csqifang,tz}@csu.edu.cn

Abstract. With the rapid development of mobile social networks and cloud servers, more and more people will outsource their personal profiles for sharing in cloud. Compared to traditional web-based online social networks, the mobile social networks can assist users to easily discover and make new social interaction with others. To keep the shared data confidential against untrusted cloud service providers and solve the problem of single point failure as well as performance bottleneck, we propose a secure distributed multi-authority attribute-based encryption scheme without central authority, so as to provide not only fine-grained access control, but also high security and performance. By employing this scheme, users can achieve fine-grained access control and privacy preserving.

Keywords: Attribute-based encryption · Multi-authority · Mobile social networks · Friend discovery · Data sharing

1 Introduction

With the explosive growth of mobile social networks and cloud services, users can remotely access the data shared in cloud anytime and anywhere, using any device. Outsourcing data into the cloud provides great convenience to users for they do not need to consider the large investment in both the deployment and management of the hardware infrastructure. In mobile social networks, sharing data in cloud offers users opportunities to enjoy the online activities, for example, by sharing photos, users can appreciate the beauty of other places without actually being there. However, allowing the cloud servers to take part in the computation and communication processes, raises underlying security and privacy issues that will result in a series of unexpected consequences. For instance, the untrustworthy third parties may collude to get the confidential information about a user and sell it to make a profit. Hence, a natural way to keep sensitive data confidential is to store only the encrypted data in cloud.

Fang Qi and Wenbo Wang are co-first authors. These two authors contribute equally to this study.

G. Wang et al. (Eds.): SpaCCS 2016, LNCS 10066, pp. 374–382, 2016.
DOI: 10.1007/978-3-319-49148-6_31

In recent years, many private matching schemes have been proposed to solve this problem. Among these schemes, some protect user's privacy based on trusted third party (TTP) [10,11,13,18], the other is TTP-free [8,14,17]. Although, this kind of approaches can achieve profile matching without the support of TTP, they have some disadvantages. The reliance on public-key crytosytem and homomorphic encryption [4,10,12,18] requires multiple rounds of interaction which causes high communication and computation overhead. Moreover, matched and unmatched users are all involved in the expensive computation and learn the matching result. Many schemes have been proposed to protect the privacy information. The technique of group signature [3,9] is widely used. In this kind of schemes, each visitor needs to be allocated a special group signature, which will cause huge amount of computation cost. Li et al. [8] propose a private matching scheme based on the common interests, which is not fine-grained. Zhang et al. [18] present a fine-grained private matching scheme but fail in considering the priority related to every attribute and they employ the homomorphic encryption which is resource consuming on mobile devices. Qi et al. [14] employ an asymmetric-scalar-production based on kNN query, but the presentation of interests is too single to get an accurate result. Moreover, the widely used technique of group signature [7,15] always costs huge volume of computational resources on users' hand-held devices, and the access control based on the key-policy attribute-based encryption [5] is not efficient enough. In addition, if any server or TTP is compromised, the confidentiality of the stored data may be compromised, too. Therefore, considering the powerful computational as well as storage ability of the TTP and cloud server, the main point of our work is to design an efficient privacy-preserving and fine-grained friend discovery system based on the combination of TTP and cloud server.

In this paper, the flexible encryption scheme, ciphertext-policy attribute-based encryption (CP-ABE) [2], is adopted to provide a fine-grained access control for the encrypted data. CP-ABE allows to encrypt data specifying an access policy over attribute, so that only users who satisfying the policy can decrypt the corresponding data [16]. For example, the access policy is designed as $(a_1 \wedge a_2) \vee a_3$ means that a user who has attribute a_1 and a_2 or a user with attribute a_3 can decrypt the data.

We design a distributed multi-authority scheme without central authority, the scheme can significantly relieve the users' trust on a single authority and is secure against collusion attack as well as chosen-plaintext attack. The applicability of system also has been increased. Our contributions are as follows:

- We propose a distributed multi-authority attribute-based encryption scheme without central authority, which can significantly reduce the risk of single point failure and performance bottleneck.
- The proposed scheme can achieve fine-grained access control, only the user who satisfies the access policy can decrypt the corresponding ciphertext.
- By combining the powerful computation and storage ability of cloud, the overhead on users' ends can be largely decreased.

The remainder of this paper is organized as follows. Preliminaries are introduced in Sect. 2. We propose our scheme in Sect. 3, followed by the performance evaluations in Sect. 4. Finally, we conclude our work.

2 Preliminaries

2.1 System Model

We assume that the system is composed of the following parts: the cloud servers, attribute authority (AA), data owner and visitor. The shared data which is outsourced in the encrypted form into the cloud by data owner, each visitor has a global identifier $gid \in GID$, where the GID is the identity set of all registered users. The cloud servers that store huge volumes of shared data and operate the computation process, and n attribute authorities $(AA_1, ..., AA_n)$ manage a set of attributes $U_i (U_i \cap U_j = \emptyset \wedge U = \cup_{i=1}^{n} U_i)$ $(i, j \in \{1, 2, ..., n\} \wedge i \neq j)$ and are responsible for generating keys for users. Each visitor with attribute set Λ will obtain their keys from the corresponding AA_n. We assume that all the authorities are run by different organizations and governed by the government. Figure 1 illustrates the system model.

2.2 Bilinear Mapping

Suppose p is a prime number, both $\mathbb{G}$ and $\mathbb{G}_T$ are multiplicative cyclic groups of the order p, g is the generator of $\mathbb{G}$. e is a bilinear map: $e : \mathbb{G} \times \mathbb{G} \rightarrow \mathbb{G}_{\mathbb{T}}$. Bilinear mapping possesses the following characteristics:

1. bilinearity: $\forall x, y \in \mathbb{G}_1$ and $a, b \in Z_q$, there is $e(x^a, y^b) = e(x, y)^{ab}$
2. computability: $\forall u_1, u_2, v \in \mathbb{G}_T$, there exists a computable algorithm $e(x^a, y^b) = e(x, y)^{ab}$
3. non-degeneracy: for $g \in \mathbb{G}$, $e(g, g) \neq 1$

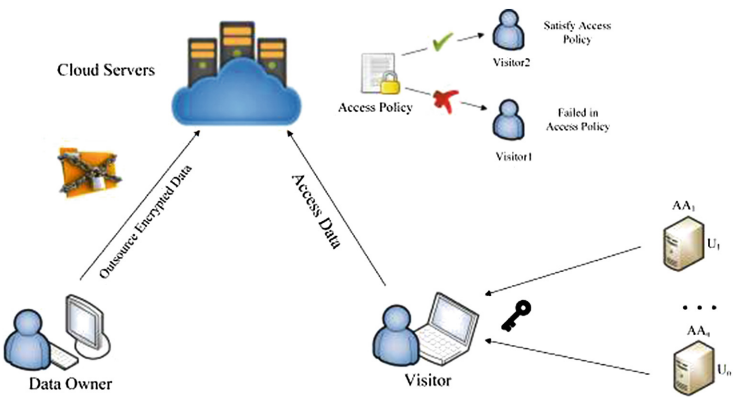

Fig. 1. Data sharing in mobile social networks

2.3 Adversary Model

In the profile matching process, there usually exist two main adversary models: honest but curious adversaries model [19] and malicious model [6].

The honest-but-curious adversary is a legitimate user who will honestly follow the protocol but will try to learn more information than allowed from legitimately received message. In this paper, we assume that the attacker is more interested in the private information of mobile social network users. At the same time, we suppose the data owner and visitor are honest-but-curious users.

The malicious adversary is a user who does not honestly obey the protocol and launch some active attacks to learn more information than allowed. These adversaries behave arbitrarily such as denial-of-service (DoS) and continuous fake-profile attacks.

In this paper, we mainly focus on the honest-but-curious adversaries; those active attacks are not in the scope of this paper.

3 Proposed Scheme

3.1 System Initialization

$\mathbb{G}$ and $\mathbb{G}_N$ are bilinear cyclic groups with the order $N = p_1 p_2$, where p_1, p_2 are distinct big prime numbers. $\mathbb{G}_{p_i}$ is the subgroup of $\mathbb{G}_N$ with order p_i, g_1 is the generator of $\mathbb{G}_{p_1}$ and g_2 is the generator of $\mathbb{G}_{p_2}$. On input the security parameter λ, the initialization algorithm randomly chooses $h \in_R \mathbb{G}_{p_1}$ and the global parameter is published as:

$$GP = (N, g_1, g_2, h) \tag{1}$$

For each AA_k, inputs GP, AA_k's index k and the attribute universe U_k belonging to AA_k. For each att in U_k, AA_k randomly selects $s_{att}, v_k, \alpha_k, a_k \in_R \mathbb{Z}_N$, then computes $T_{att} = g^{s_{att}}$ and $V_k = g^{v_k}$. The master key is:

$$MK_k = (v_k, \alpha_k, a_k, \{s_{att} | att \in U_k\}) \tag{2}$$

and the public key is published as:

$$PK_k = (V_k, g^{a_k}, e(g,g)^{\alpha_k}, \{T_{att} | att \in U_k\}) \tag{3}$$

where $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_{\mathbb{N}}$ is a bilinear map.

3.2 Encryption

This algorithm is performed on the data owner's end. The data owner designs the access policy that defines the special attributes that the visitors need to satisfy. The access policy is embedded in the ciphertext so that before decrypting the decryption can verify whether the visitor is qualified.

Data owner inputs GP, PK_k, the plaintext of data M and access policy $\mathbb{A} = (A, \rho)$. (A, ρ) a linear secret-sharing scheme (LSSS) [1] matrix, where A is a $l \times n$ matrix and ρ will map each row A_x in A to get an attribute $\rho(x)$. ρ is required that when mapping different row, the attribute must not be the same. Randomly chooses a vector $\boldsymbol{v} = (s, v_2, ..., v_n) \in \mathbb{Z}_N^n$. These valuses will be used to share the encryption exponent s. For each $x \in \{1, 2, ..., l\}$, the algorithm randomly selects $r_x \in \mathbb{Z}_N$. The ciphertext is:

$$\begin{aligned} CT = (M \prod_{k=1}^{n} e(g,g)^{\alpha_k s}, C' = g^s, C_k'' = g^{\alpha_k s}, \\ \forall x \in 1, 2, ..., l: \quad \{C_x = h^{A_x \boldsymbol{v}} T_{\rho(x)}^{\frac{1}{r_x}}, C_x' = g^{r_x}\}) \end{aligned} \tag{4}$$

Along with the access policy $\mathbb{A}$, data owner outsources the ciphertext to the cloud.

3.3 Key Generation

Suppose a visitor wants to visit some data with certain characteristics, he/she will set up an attribute set Λ. To meet the security and efficiency requirements, all attributes in Λ will be split into n different shares and distributed to n different attribute authorities.

Visitor submits his/her identifier gid, attribute set Λ to the attribute authority AA_k for requesting a pair of secret keys $< SK_k^1, SK_k^2 >$. AA_k randomly selects $c_k \in \mathbb{Z}_N^*$, $r_k \in \mathbb{Z}_N$, $\beta_k, \beta_k', \beta_k'' \in \mathbb{G}_{p_2}$. Then it creates the SK_k^1 as:

$$\begin{aligned} SK_k^1 &= (g^{\frac{a_k}{\alpha_k + c_k}} h_k^{r_k} \beta_k, c_k, \\ L_k &= g_k^{r_k} \beta_k', L_k' = (g^{a_k})^{r_k} \beta_k'') \end{aligned} \tag{5}$$

For each attribute $att \in U_k \cap \Lambda$, AA_k randomly chooses $\Gamma_k \in \mathbb{G}_{p_2}$, $\beta_{att}' \in \mathbb{G}_{p_2}$, AA_k computes

$$\begin{aligned} SK_{att,k} &= (V_k^{(a_k + c_k) r_k} \Gamma_k)^{\frac{s_{att}}{v_k}} {\beta'}_{att} \\ &= T_{att}^{(a_k + c_k) r_k} \Gamma_k^{\frac{s_{att,k}}{v_k}} {\beta'}_{att} \end{aligned} \tag{6}$$

So the SK_k^2 is defined as:

$$SK_k^2 = (g^{\frac{\alpha_k - a_k}{\alpha_k + c_k}} h_k^{r_k} \beta_k, \{SK_{att,k} | att \in \Lambda\}) \tag{7}$$

3.4 Decryption

When a visitor wants to visit certain data, first, he/she must satisfy the access policy designed by the data owner. If the visitor's attribute set Λ satisfies the access policy $\mathbb{A} = (A, \rho)$, which means there exists constants $\omega_x \in \mathbb{Z}_N$ and $\sum_{\rho(x) \in \Lambda} \omega_x A_x = (1, 0, ..., 0)$. If Λ fails in the access policy, the algorithm will output $\perp$, which means Λ dose not satisfy the access policy, the visitor cannot decrypt the ciphertext and continue the following steps.

If the verification is passed, then the visitor will input $< SK_k^1, SK_k^2 >$, then computes:

$$\begin{aligned}
&\frac{e((C')^{c_k}, g^{\frac{a_k}{\alpha_k + c_k}} h_k^{r_k} \beta_k)}{\prod_{\rho(x)\in\Lambda} (e(C_x, L_k^{c_k}) e(C'_x, SK_{\rho(x),k}))^{\omega_x}} \\
&= \frac{e((g^s)^{c_k}, g^{\frac{a_k}{\alpha_k + c_k}} h_k^{r_k} \beta_k)}{\prod_{\rho(x)\in\Lambda} \left(e(h^{A_x \boldsymbol{v}} T_{\rho(x)}^{\frac{1}{r_x}}, (g_k^{r_k} \beta'_k)^{c_k}) e(g^{r_x}, SK_{\rho(x),k})\right)^{\omega_x}} \\
&= e(g,g)^{a_k s}
\end{aligned} \tag{8}$$

and computes

$$\begin{aligned}
&\frac{e((C')^{c_k}, g^{\frac{\alpha_k - a_k}{\alpha_k + c_k}} h_k^{r_k} \beta_k)}{\prod_{\rho(x)\in\Lambda} (e(C_x, L_k^{c_k}) e(C'_x, SK_{\rho(x),k}))^{\omega_x}} \\
&= \frac{e((g^s)^{c_k}, g^{\frac{\alpha_k - a_k}{\alpha_k + c_k}} h_k^{r_k} \beta_k)}{\prod_{\rho(x)\in\Lambda} \left(e(h^{A_x \boldsymbol{v}} T_{\rho(x)}^{\frac{1}{r_x}}, (g_k^{r_k} \beta'_k)^{c_k}) e(g^{r_x}, SK_{\rho(x),k})\right)^{\omega_x}} \\
&= e(g,g)^{(\alpha_k - a_k)s}
\end{aligned} \tag{9}$$

Finally, the visitor can recover the plaintext:

$$\begin{aligned}
M &= \frac{CT}{\prod_{k=1}^{n} (e(g,g)^{a_k s} e(g,g)^{(\alpha_k - a_k)s})} \\
&= \frac{M \prod_{k=1}^{n} e(g,g)^{\alpha_k s}}{\prod_{k=1}^{n} (e(g,g)^{a_k s} e(g,g)^{(\alpha_k - a_k)s})} \\
&= M
\end{aligned} \tag{10}$$

4 Performance Analysis

In this section, we evaluate the proposed scheme with several existing works in terms of efficiency and practicability. Since the cloud is generally assumed to be resource abundant, we mainly focus on the computation and communication overhead loaded on both the data owner and visitor's ends.

We conduct the experiments on a laptop with 1.6 GHz processor and 2 GB RAM, and the simulation code was written in C++. We perform the comparisons between Boyen [3], Liang [9] and our scheme. The size of attributes set is fixed in 30 and n denotes the number of participated visitors.

Figure 2 represents the communication overhead comparison among Boney's scheme [3], Liang's scheme [9] and ours. It is obvious that the communication cost of Boney's and Liang's schemes sharply increase as the number of visitors grows from 50 to 500. However, the proposed scheme is significantly lower than Boney's and Liang's schemes. Moreover, with the increasing number of visitors,

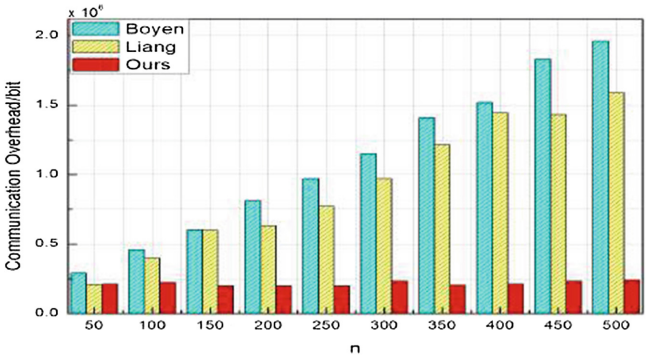

Fig. 2. Communication overhead

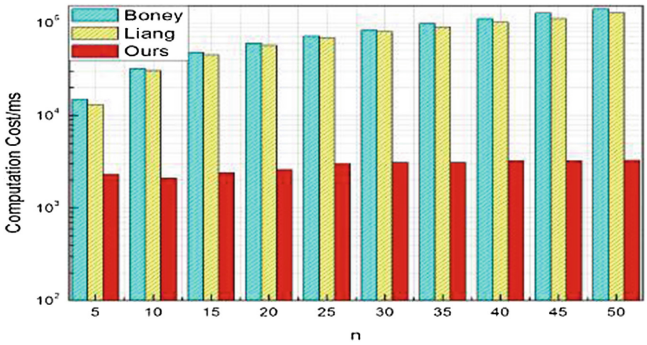

Fig. 3. Computation cost on data owner's end

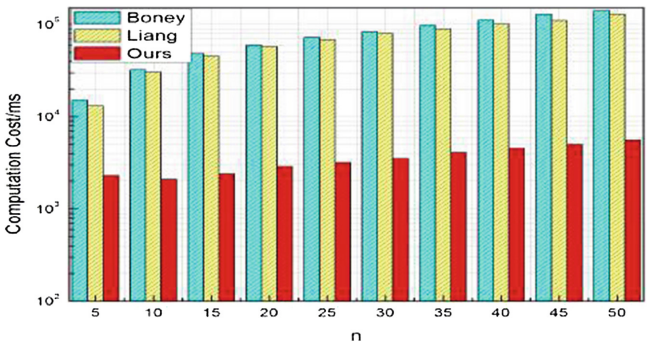

Fig. 4. Computation cost on visitor's end

the communication overhead keeps low and stable, which is really important in massive users enviroment.

Figure 3 illustrates the computation cost comparison among Boyen's scheme [3], Liang's scheme [9] and ours on the data owner's ends. From the curve, we can know that the computation cost in Boney's and Liang's schemes increases quickly as the number of visitors grows. Because the technique of group signatures is adopted, and to achieve privacy preserving, it is required for the data owner to generate one group signature for each visitor, which would bring about intolerable computation complexity on users' ends. Significantly from [3,9], our scheme requires no extra signature to protect privacy information.

Figure 4 shows the computation cost comparison among Boyen's shceme [3], Liang's scheme [9] and ours on the data's ends. It is obvious that the proposed scheme consumes less. When there are many visitors, each of them needs to wait for a special group signature, which is time-consuming. When $n = 50$, both Boyen [3] and Liang [9] need 129.07 ms to complete the computation processes on visitor's end. But in our scheme, the whole processes on visitor's end only consumes 5.54 ms.

From the above analysis, the proposed scheme is superior in both communication and computation overhead. With the increasing number of participated visitors, the system cost only grows slightly, especially in the massive users enviroment the communication overhead can be small and stable.

5 Conclusion

For the sake of enjoying a more comprehensive and high quality service, a distributed multi-authority attribute-based encryption is proposed for secure friend discovery and data sharing, which simultaneously achieves flexibility, high performance and security. The proposed scheme is collusion resistant and can decrease the work pressure and reliance on a single point. In the future work, we will design a more expressive encryption scheme to achieve better performance.

Acknowledgments. This work is supported by the National Natural Science Foundation of China under Grant No. 61632009 and Grant No. 31470028, and Fundamental Research Funds for the Central Universities of Central South University under Grant No. 2016zzts337.

References

1. Beimel, A., et al.: Secure schemes for secret sharing and key distribution. Int. J. Pure Appl. Math. **85**(5), 933–937 (1996)
2. Bethencourt, J., Sahai, A., Waters, B., et al.: Ciphertext-policy attribute-based encryption. In: Proceedings of the 2007 IEEE Symposium on Security and Privacy, SP 2007, no. 4, pp. 321–334 (2007)
3. Boyen, X., Waters, B., et al.: Full-domain subgroup hiding and constant-size group signatures. In: International Conference on Practice and Theory in Public-Key Cryptography, pp. 1–15 (2007)

4. Costantino, G., Martinelli, F., Santi, P., et al.: Privacy-preserving interest-casting in opportunistic networks. In: Proceedings of Wireless Communications and Networking Conference, pp. 2829–2834 (2012)
5. Goyal V, Pandey O, Sahai A, Waters B, et al.: Attribute-based encryption for fine-grained access control of encrypted data. In: Proceedings of the 13th ACM Conference on Computer, Communications Security, pp. 89–98 (2006). Observation of strains. Infect Dis. Ther. **3**(1), 35–43 (2011)
6. Hazay, C., Toft, T.: Computationally secure pattern matching in the presence of malicious adversaries. In: Abe, M. (ed.) ASIACRYPT 2010. LNCS, vol. 6477, pp. 195–212. Springer, Heidelberg (2010). doi:10.1007/978-3-642-17373-8_12
7. Li, J., Au, M.H., Susilo, W., Xie, D., Ren, K., et al.: Attribute-based signature and its applications. In: Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, pp. 60–69 (2010)
8. Li, M., Cao, N., Yu, S., Lou, W., et al.: FindU: privacy-preserving personal profile matching in mobile social networks. In: Proceedings of IEEE INFOCOM, pp. 2435–2443 (2011)
9. Liang, X., Cao, Z., Shao, J., Lin, H., et al.: Short Group Signature Without Random Oracles. Springer, Heidelberg (2007)
10. Lu, R., Lin, X., Liang, X., Shen, X., et al.: A secure handshake scheme with symptoms-matching for mhealthcare social network. Mobile Netw. Appl. **16**(6), 683–694 (2011)
11. Manweiler, J., Scudellari, R., Cox, L.P., et al.: Smile: encounter-based trust for mobile social services. In: Proceedings of the 16th ACM Conference on Computer and Communications Security, pp. 246–255 (2009)
12. Niu, B., Zhang, T., Zhu, X., Li, H., Lu, Z., et al.: Priority-aware private matching schemes for proximity-based mobile social networks. In: Computer Science, pp. 3170–3175 (2014)
13. Pietiläinen, A.K., Oliver, E., LeBrun, J., Varghese, G., Diot, C., Mobiclique, et al.: middleware for mobile social networking. In: Proceedings of the 2nd ACM Workshop on Online Social Networks, pp. 49–54 (2009)
14. Qi, F., Wang, W., et al.: Efficient private matching scheme for friend information exchange. In: Proceedings of Algorithms and Architectures for Parallel Processing, pp. 492–503 (2015)
15. Shahandashti, S.F., Safavi-Naini, R.: Threshold attribute-based signatures and their application to anonymous credential systems. In: Preneel, B. (ed.) AFRICACRYPT 2009. LNCS, vol. 5580, pp. 198–216. Springer, Heidelberg (2009). doi:10.1007/978-3-642-02384-2_13
16. Wang, G., Liu, Q., Wu, J., et al.: Hierarchical attribute-based encryption for fine-grained access control in cloud storage services. In: Proceedings of ACM Conference on Computer and Communications Security, pp. 735–737 (2010)
17. Zhang, L., Li, X.Y., Liu, Y., et al.: Message in a sealed bottle: privacy preserving friending in social networks. In: IEEE 33rd International Conference on Distributed Computing Systems (ICDCS), pp. 327–336 (2013)
18. Zhang, R., Zhang, R., Sun, J., Yan, U., et al.: Fine-grained private matching for proximity-based mobile social networking. In: Proceedings of IEEE INFOCOM, pp. 1969–1977 (2012)
19. Zhou, J., Cao, Z., Dong, X., Lin, X., Vasilakos, A.V., et al.: Securing m-healthcare social networks: challenges, countermeasures and future directions. Wirel. Commun. **20**(4), 12–21 (2013)