Procedia Computer Science

Volume 80, 2016, Pages 617–626

ICCS 2016. The International Conference on Computational Science

Distributed Multi-authority Attribute-based Encryption Scheme for Friend Discovery in Mobile Social Networks

Wenbo Wang[1], Fang Qi[1], Xiaoqiang Wu[2], and Zhe Tang[1] *

[1] School of Information Science and Engineering, Central South University, Changsha, China, 410083
wb_wang@csu.edu.cn, qi.fangfang@gmail.com, tz@csu.edu.cn
[2] Institute of Software, Chinese Academy of Sciences, Beijing, China, 100190
xiaoqiang2014@iscas.ac.cn

Abstract

In recent years, the rapid expansion of the capability of portable devices, cloud servers and cellular network technologies is the wind beneath the wing of mobile social networks. 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. A challenging task is to protect the privacy of the users' profiles and communications. Existing works are mainly based on traditional cryptographic methods, such as homomorphic and group signatures, which are very computationally costly. In this paper, we propose a novel distributed multi-authority attribute-based encryption scheme to efficiently achieve privacy-preserving without additional special signatures. In addition, the proposed scheme can achieve fine-grained and flexible access control. Detailed analysis demonstrates the effectiveness and practicability of our scheme.

Keywords: Multi-authority, Attribute-based Encryption, Privacy Preserving, Access Control, Profile Matching

1 Introduction

A boom in mobile hand-held devices greatly enriches the social networking application [1]. Many social networking services are available on the mobile devices (e.g., WeChat, QQ, MocoSpace, etc.). According to eMarketer [2], they estimate that the number of US smartphone users will reach 192.4 million by 2016 and 2.28 billion worldwide [3]. Friend discovery and communication are two important basic steps of social networks. When people take part in social networks, they usually begin by creating a profile, then interact with others. The personal profile usually contains a large amount information, such as hobbies, age, education degree, etc. Profile matching is a common and helpful method to make new friend with mutual interests or experience. Unfortunately, a series of unaddressed security and privacy problems dramatically impede its practicability and popularity [4].

*Corresponding author

Selection and peer-review under responsibility of the Scientific Programme Committee of ICCS 2016

doi:10.1016/j.procs.2016.05.350

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) [5, 6, 7, 8], the other is TTP-free [9, 10, 1]. 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 [11, 12, 7, 8] 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. Li et al. [9] propose a private matching scheme based on the common interests, which is not fine-grained. Zhang et al. [8] 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. [10] 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 [13][14] always costs huge volume of computational resources on users' hand-held devices, and the access control based on the key-policy attribute-based encryption [15] 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 computationanl 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, we propose an efficient destributed multi-authority attribute-based encryption scheme, which can achieve privacy preserving and fine-grained access control. By using ciphertext-policy attribute-based encryption (CP-ABE) [16], the encrypted information can kept confidential even if the storage server is not fully-trusted and users can design the their own access policy. Hence, the fine-grained access control can be achieved efficiently. By employing the powerful storage and computational ability of cloud server, the storage and computaion overhead of the client can be greatly reduced. The multi-authorities are designed to be destributed, which can significantly relieves the users' trust on a single authority and is secure against collusion attack as well as chosen-plaintext attack. The main contributions are outlined as follows.

- A multi-authority attribute-based encryption scheme is proposed for fine-grained multi-level access control in cloud friend discovery system. Users can design their own access policy to find the potential friends, which is user friendly.

- User's identity and personal profile are encrypted under the access policy specified by the user himself and outsourced to the cloud server, the client is lightweight.

- The destributed multi-authority model in friend discovery cloud computing system also reduces the risk of a single central authority being compromised for potential privacy leakage.

- Formal security proof and simulation evaluation demonstrate that our scheme is secure against chosen-plaintext attack and collusion attack in the standard model.

The remainder of this paper is organized as follows. Preliminaries are introduced in Section 2. The system architecture and models are presented in Section 3. We propose our scheme in Section 4, followed by the formal security proof and performance evaluations respectively in Section 5 and 6. Finally, we conclude our work.