ARTICLE IN PRESS

Future Generation Computer Systems ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Future Generation Computer Systems

journal homepage: www.elsevier.com/locate/fgcs

An efficient access control scheme with outsourcing capability and attribute update for fog computing

Peng Zhang [a], Zehong Chen [a,*], Joseph K. Liu [b], Kaitai Liang [c], Hongwei Liu [a]

[a] ATR Key Laboratory of National Defense Technology, College of Information Engineering, Shenzhen University, Shenzhen, China

[b] Faculty of Information Technology, Monash University, Melbourne, Australia

[c] Department of Computing, Mathematics and Digital Technology, Manchester Metropolitan University, UK

HIGHLIGHTS

- We propose an access control (CP-ABE) scheme supporting outsourcing capability and attribute update for fog computing.
- The outsourcing method outsources the heavy computation of encryption and decryption to fog nodes, thus the computation for data owners to encrypt and users to decrypt are irrelevant to the number of attributes in the access structure and secret keys respectively.
- We propose an efficient updating method to address the issue of attribute update that we only concentrate on the update of the ciphertext associated with the corresponding updated attribute.
- The experimental results show that fog nodes do the heavy computation operations of encryption and decryption, so that the time of encryption for data owner and decryption for end users are small and constant, even in the resource-constrained smartphones.

ARTICLE INFO

Article history:
Received 2 June 2016
Received in revised form
21 October 2016
Accepted 11 December 2016
Available online xxxx

Keywords:
Fog computing
Access control
Attribute-based encryption
Outsourcing capability
Attribute update

ABSTRACT

Fog computing as an extension of cloud computing provides computation, storage and application services to end users. Ciphertext-policy attribute-based encryption (CP-ABE) is a well-known cryptographic technology for guaranteeing data confidentiality and fine-grained data access control. It enables data owners to define flexible access policy for data sharing. However, in CP-ABE systems, the problems of the time required to encrypt, decrypt and attribute update are long-standing unsolved in the literature. In this paper, we propose the first access control (CP-ABE) scheme supporting outsourcing capability and attribute update for fog computing. Specifically, the heavy computation operations of encryption and decryption are outsourced to fog nodes, thus the computation operations for data owners to encrypt and users to decrypt are irrelevant to the number of attributes in the access structure and secret keys, respectively. The cost brought by attribute update is efficient in the sense that we only concentrate on the update of the ciphertext associated with the corresponding updated attribute. The security analysis shows that the proposed scheme is secure under the decisional bilinear Diffie–Hellman assumption. The proposed scheme is efficient, and the time of encryption for data owners and decryption for users are small and constant. The computational ability of fog nodes are fully utilizing during the access control, so the tiny computing cost is left to end users with resource-constrained devices.

© 2016 Elsevier B.V. All rights reserved.

1. Introduction

Cloud computing is considered as a promising computing paradigm, which delivers services to users in terms of infrastructure, platform and software, and supplies applications with elastic resources at low cost [1–3]. However, as it mainly provides resources distributed in the core network far from users, a primary limitation is delay—the lag between user request and cloud response [4,5]. Fog computing is presented to enable computing directly at the edge of the network [6], which is an extension of cloud computing, meets enhanced network performance requirements by locating data, computing, and networking capabilities closer to users [7–9]. In fog computing, devices that can provide various resource services at the edge of the network are termed fog nodes [7,

* Corresponding author.
E-mail addresses: zhangp@szu.edu.cn (P. Zhang), zhchen@szu.edu.cn (Z. Chen), joseph.liu@monash.edu (J.K. Liu), K.Liang@mmu.ac.uk (K. Liang), liuhw@szu.edu.cn (H. Liu).

http://dx.doi.org/10.1016/j.future.2016.12.015
0167-739X/© 2016 Elsevier B.V. All rights reserved.

Please cite this article in press as: P. Zhang, et al., An efficient access control scheme with outsourcing capability and attribute update for fog computing, Future Generation Computer Systems (2016), http://dx.doi.org/10.1016/j.future.2016.12.015

10], such as access points, routers and base stations. Fog computing has many attractive features, such as low latency, mobility and location-awareness [8,11], and it can be used to the thin-client, highly mobile and geographical distributed applications, e.g., intelligent urban transportation.

Cloud forensic researchers have demonstrated access control protection, but this is outside the scope of this paper. We refer interested readers to [12–14] for a comprehensive overview of the topic. In accord with cloud computing, access control in fog computing is a security guarantee for user data sharing [15], yet the network structures and system models are different. So a new access control scheme with cloud, fog and users should be considered, in which fog nodes should assist user, to make less computational complexity and more flexibility left for users.

Ciphertext policy attribute-based encryption (CP-ABE), one of the most fine-grained access control (encryption) techniques, was first introduced by Bethencourt et al. [16] in 2007. Over the past few years, many CP-ABE schemes have been proposed to achieve various functional purposes. Cheung and Newport [17] presented a CP-ABE scheme in which access structure is AND gate on positive and negative attributes. Horvath [18] proposed a multi-authority CP-ABE scheme with identity-based revocation. Hur [19] constructed a CP-ABE scheme for a data sharing system by applying the characteristic of the system architecture, and the proposed scheme can do an immediate user revocation on each attribute set. The similar technologies that have been introduced in the recent literature for cloud-based data sharing and user revocability, such as [20–23]. Wang et al. [24] proposed a variant of CP-ABE to share the hierarchical files in cloud computing, and the scheme is proved to be secure under DBDH assumption. Ref. [25] revisited attribute-based data sharing scheme to address the key escrow problem and improve the expressiveness of attributes. Nonetheless, CP-ABE schemes are typically computationally intensive, which include a number of pairing operations and exponentiations. This greatly limits their uses on resource-constrained devices, e.g., tablet computers and smartphones.

Fog nodes, the edge of the cloud and closer to end users, are one of the best choices for the outsourcing proxy, which can be used to do massive computation to reduce the computational overhead required on resource-constrained devices. So, some CP-ABE schemes with outsourcing have been proposed in the literature. Green et al. [26] proposed novel paradigm for outsourcing the decryption of attribute-based encryption (ABE). Zhou and Huang [27] proposed a privacy preserving CP-ABE scheme, which allows portable devices to outsource heavy encryption and decryption operations to the cloud service provider without revealing the data. However, the computational overhead of encryption increases with the complexity of the access structure for the data owner. Asim et al. [28] constructed an CP-ABE scheme with encryption and decryption outsourcing capabilities. In the encryption of their scheme, the data owner first generated the ciphertext and then applied a semi-trusted proxy to re-encrypt the encrypted information associated with the access structure. In the decryption, they send a transformation key to another semi-trusted proxy to decrypt most of the ciphertext, which leaves a constant number of simple computations for the user to decrypt. Mao et al. [29] introduced a generic construction of attribute-based encryption with verifiable outsourced decryption, which also leaves a constant number of simple computations for the user to decrypt the ciphertext.

Due to outsourcing, the demand for the computation power required on user terminals is lower, such that more mobile terminals join the fog computing platform. The attribute update convenience becomes an important need when the user role is changed. For example, the attribute set of an employee may be updated when his working role is changed inside a company, e.g., set A = "Team member, Programming" → set B = "Manager, Product Design". The key generation authority should be requested to issue an updated secret key to the employee, so that the access rights of the employee for new encrypted data should be modified accordingly. At the same time, we need to guarantee that the employee cannot reuse his old and outdated secret key corresponding to "Team member, Programming" to gain access to the ciphertexts with access policy matching the set A. Attribute update is not trivial and straightforward in ABE, since the update of a single attribute will affect a wide range of users obtaining the same attribute. However, the attribute update problem has not been taken into account in the existing access control schemes.

Motivated by the issues of outsourcing and the attribute update, we propose an access control scheme in the context of attribute-based cryptographic encryption. We design a secure outsourced approach to eliminate the computational overhead of encryption and decryption. In the encryption phase, the encryption operations associating with the access structure are outsourced to fog nodes, while the computation for the data owner is simple and constant. In the decryption phase, the user sends part of his secret key to fog nodes to decrypt most of the ciphertext, where the secret key does not need to transform. In addition, we make use of an efficient updating method to address the issue of attribute update. Specifically, we assign distinct updated (key) information for each system user who can update the secret key and the ciphertext that related to the updated attribute using the information. We state that the both approaches introduced in this paper greatly save the computation cost of encryption, decryption and the updated process.

Compared to the conference version [30] of this work, we have the following improvements:

1. We modify the system model and make it more suitable for the practice to the fog computing system, in which fog nodes serve as a bridge between users (contains data owner and end users) and cloud service providers, users have a direct link to fog nodes, and each fog node is linked to the cloud.
2. We propose an efficient outsourced CP-ABE scheme, which achieves both secure outsourced encryption and decryption. In particular, we use fog nodes to implement all access structure and attribute related operations in the encryption and decryption to reduce the computing burden of the data owner and end users, and leave a constant number of operations for the data owner and end users to execute locally.
3. We add the simulation experiment of the proposed scheme. The experimental results show that the time of encryption for data owner and decryption for users are small and constant, even in the resource-constrained smartphones.

The rest sections of the paper are organized as follows. In Section 2, the preliminaries are introduced. The system model and security model are introduced in Section 3. An efficient access control scheme with outsourcing capability and attribute update for fog computing is proposed in Section 4. We analyze the security and efficiency of the proposed scheme in Sections 5 and 6, respectively. The paper is concluded in Section 7.

2. Preliminaries

2.1. Access structure

Definition 1 (*Access Structure [16]*)**.** Let $\{A_1, A_2, \ldots, A_n\}$ be a group of attributes. For $\forall B, C$, if $B \in \mathbb{A}$ and $B \subseteq C$, then $C \in \mathbb{A}$, we say that $\mathbb{A} \subseteq 2^{\{A_1, A_2, \ldots, A_n\}}$ is monotone. An access structure (or monotone access structure) contains a set (or monotone set) $\mathbb{A}$ of non-empty subsets of $\{A_1, A_2, \ldots, A_n\}$. Elements in $\mathbb{A}$ are referred to as authorized elements, otherwise, elements are referred to as unauthorized elements.

In our scheme, $\mathbb{A}$ will include authorized elements. Unless stated in another way, access structure used in this paper is in monotone form.

Please cite this article in press as: P. Zhang, et al., An efficient access control scheme with outsourcing capability and attribute update for fog computing, Future Generation Computer Systems (2016), http://dx.doi.org/10.1016/j.future.2016.12.015

Download English Version:

https://daneshyari.com/en/article/4950202

Download Persian Version:

https://daneshyari.com/article/4950202

Daneshyari.com