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

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

CCA-secure ABE with outsourced decryption for fog computing☆

Cong Zuo, Jun Shao *, Guiyi Wei, Mande Xie, Min Ji

College of Computer and Information Engineering, Zhejiang Gongshang University, PR China

HIGHLIGHTS

- The CCA security model for ABE with outsourced decryption is proposed.
- A concrete CCA-secure ABE scheme with outsourced decryption is proposed.
- The security analysis and experimental results show that our proposal is secure and practical for fog computing.

ARTICLE INFO

Article history:
Received 3 June 2016
Received in revised form
17 September 2016
Accepted 27 October 2016
Available online xxxx

Keywords:
Fog computing
IoT
Attribute-based encryption
Chosen ciphertext security
Outsourced decryption

ABSTRACT

Fog computing is not a replacement but an extension of cloud computing for the prevalence of the Internet of Things (IoT) applications. In particular, fog computing inserts a middle layer named fog into the infrastructure of cloud computing to obtain the low latency, mobility and location-awareness. Due to the fog layer, the sensitive data stored in fog computing is facing more sophisticated attacks, such as chosen ciphertext attacks, than that in cloud computing. Currently, the attribute-based encryption (ABE) with outsourced decryption is the best solution for data protection in cloud computing for IoT applications. However, none of the existing schemes are CCA secure. To fill this gap, we firstly propose the CCA security model for ABE with outsourced decryption, and then present a concrete CCA-secure ABE scheme with outsourced decryption. The security analysis and experimental results show that our proposal is secure and practical for fog computing.

1. Introduction

Cloud computing is now the dominant computing paradigm for the Internet, since it can provide elastic computing resources in an on-demand way to users from its computing resource center. It has been reported by Cisco Cloud Index (2013–2018) that most of the current Internet traffic has come from or went to a data center. However, the prevalence of the Internet of Things (IoT) applications are now changing the main factor of computing. The centralized computing systems is starting to suffer from the unbearable transmission latency and degraded service due to the extraordinary huge volume traffic between IoT devices and cloud [1–3].

To solve the above problems, Cisco proposed the concept of fog computing in 2014, where a new layer consisted by fog devices (such as hardened routers, switches, and IP video cameras) inserted into the middle of the cloud and end users [4], as shown in Fig. 1. The fog devices are geo-distributed and implemented at the edge of networks with plentiful computing resources and wireless communication facility. As a result, fog devices are much closer to end users than cloud servers, and some of the workloads and services taken in the cloud are moved to the fog devices. In other words, fog computing is not a replacement but an extension of cloud computing, and it bridges the IoT devices and cloud.

On the other hand, cloud storage is the most popular application among the cloud applications. Since the cloud server is not always fully trusted, the fine-grained access control on the encrypted data is quite desired from the viewpoint of users. Attribute-based encryption (ABE), introduced by Sahai and Waters [5], is a promising solution for this requirement. There exist two types of ABE schemes: key-policy ABE (KP-ABE) [6] and ciphertext-policy ABE (CP-ABE) [7–10]. In the former type, the access policy is embedded into the user's private key. While in the latter one, the access policy is embedded into the ciphertext. Only if the user's attributes satisfy the access policy, the ciphertext can be decrypted by the user's private key.

☆ The extended abstract of this paper is published at ACISP 2016 (Zuo et al., 2016) [35].

* Correspondence to: Room 537, 18♯ Xuezheng Street, SCIE building, Zhejiang Gongshang University, Hangzhou, Zhejiang Province, 310018, PR China. Fax: +86 571 28008303.

E-mail addresses: zuocong10@gmail.com (C. Zuo), chn.junshao@gmail.com (J. Shao), weigy@zjgsu.edu.cn (G. Wei), xidmd@zjgsu.edu.cn (M. Xie), jimin@zjgsu.edu.cn (M. Ji).

http://dx.doi.org/10.1016/j.future.2016.10.028
0167-739X/

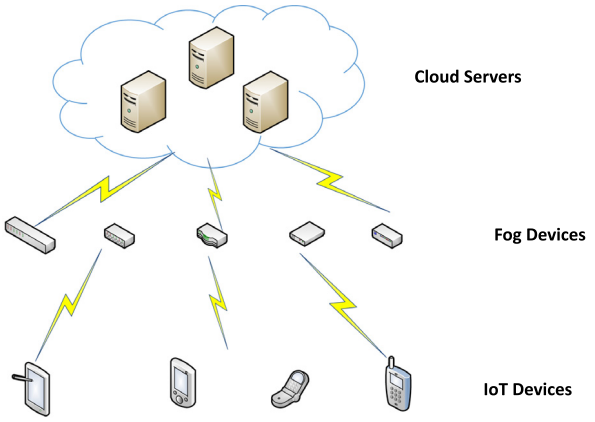

Fig. 1. The infrastructure of fog computing.

Although ABE is a very useful cryptographic tool to realize fine-grained access control, the inefficient performance is its Achilles' Heel. In particular, the size of ABE ciphertext and decryption cost are usually proportional to the complexity of the access policy. This impedes the use of ABE in IoT devices due to the limited resources [11]. As we mentioned above, the IoT is starting to rapidly expand the traditional IT industry [12]. To solve this conflict, Green et al. [13] proposed the concept of attribute-based encryption with outsourced decryption (OD-ABE), where it allows a proxy (such as the cloud) with a transformation key to transform ABE ciphertexts into simple and constant size ciphertexts, while the proxy cannot obtain the corresponding plaintext. By using OD-ABE, the most of the decryption cost on ABE ciphertexts can be moved from the IoT devices to the cloud.

As stated in [13], OD-ABE solves the fine-grained access control on the encrypted data for resource-constraint devices in cloud computing quite well. However, the fog computing has changed the underlying infrastructure. In particular, the data is physically stored much closer to the users and has many copies in many fog devices. This new infrastructure allows the adversary to launch more sophisticated attacks than ever. On the other hand, it is well-known that the chosen ciphertext security is generally considered as the highest[1] security notion for a cryptosystem, and it can resist the unknown sophisticated attacks to the sensitive data in fog computing. Nonetheless, none of the existing OD-ABE schemes achieve CCA security. The traditional CCA security of public key encryption guarantees that any ciphertext cannot be malleable. Nevertheless, the ciphertext transformation is expected as a regular functionality in OD-ABE, which makes the definition of CCA security tricky. In this paper, to fill the gap between the security requirement of fog computing and the security of OD-ABE, we will propose the CCA security for OD-ABE by following the spirit of the traditional CCA security as close as we can. Furthermore, we will propose a concrete CCA secure OD-ABE scheme by applying the CHK [14] and FO [15] techniques on the ABE scheme in [8]. As we can see later, the design approach used in this paper can be applied to other ABE schemes, such as [16,7,17,18,9,19,20].

1.1. Related work

The main contribution of this paper is to propose the CCA security for OD-ABE and a concrete CCA-secure OD-ABE to resist unknown sophisticated attacks to the sensitive data in fog computing. Hence, in this section, we would like to review the works related to ABE and OD-ABE. Besides that, we would also like to review some other techniques that deal with the data sharing problem in Cloud.

To achieve a fine-grained data sharing in IoT networks, Attribute Based Encryption (ABE) usually be deployed. Sahai et al. [5] first introduced the notion of ABE and further discussed in [21]. Later, in 2006, Goyal et al. [6] formalized two complementary flavors of ABE: key-policy ABE (KP-ABE) and ciphertext-policy ABE (CP-ABE). In [6], the proposed ABE scheme only supports monotonic access structure. Later, a new KP-ABE scheme supporting non-monotonic access structure is proposed by Ostrovsky et al. [17]. They also gave a CP-ABE construction based on the technical of [7] where a CP-ABE secure in the random oracle model is proposed. In 2007, Cheung et al. [8] proposed a CP-ABE scheme with non-monotonic access structure in the standard model. Later, many efficient, secure and expressive ABE schemes were proposed [19,20]. While, the user revocation problem prohibit the deployment of ABE. To circumvent this obstacle, Yang et al. [22] proposed an extended proxy-assisted approach, which supported the revoke of users and significantly reduced the trust of the Cloud. Later, to make the data sharing in Cloud supports fine-grained delegation of decryption rights, Yang et al. [23] proposed a ciphertext-policy attribute based conditional proxy re-encryption scheme which also can offer a more efficient solution to the user revocation problem.

However, the most significant drawback of ABE for the use in fog computing is the computational cost in the decryption phase which is linear with the complexity of policy. So, there is an increasing need to improve the efficiency of decryption. To solve this problem, Green et al. [13] introduced the attribute-based encryption with outsourced decryption (OD-ABE) to outsource the large amount of computation to a third party. As a result, the computational cost of decryption can be significantly decreased.

In [13], to outsource the large computation of decryption while keeping the confidentiality of the underlying plaintexts from the proxy (an adversary), they introduced a key blinding technique. In particular, the proxy can transform an ABE ciphertext by using a secret named transformation key generated from the intending decryptor into a constant-size ElGamal type ciphertext and return it to the intending decryptor. Finally, the intending decryptor applies a secret named retrieving key corresponding to the transformation key to decrypt the ElGamal type ciphertext. However, the validity of the ElGamal type ciphertext in [13] cannot be guaranteed. In order to verify the outsourced computation, Lai et al. [24] proposed an attribute based encryption with verifiable outsourced decryption and further discussed in [25]. In [24], they added an extra component into the ABE ciphertext that is used to verify the ciphertext which was generated by the transformation key. Nevertheless, the extra component doubled the size of the ciphertext of the underlying ABE ciphertext and ElGamal type ciphertext. Hence, their scheme is not so efficient as expected in resource constraint environments.

To improve the efficiency of verifiable OD-ABE, Lin et al. [26] introduced a new technique. Specially, they combined an attribute-based key encapsulation mechanism, a commitment scheme and a symmetric-key encryption scheme to achieve efficient verifiability. Besides that, they also proposed an unified model for the OD-ABE with verifiability. At the same time, many other research efforts also have been dedicated to design more efficient (verifiable) OD-ABE schemes [27,28]. However, none of aforementioned scheme can achieve CCA security. As we mentioned before, fog computing demands that the applied OD-ABE schemes are CCA secure to sophisticated attacks that rarely happen in cloud computing.

We note that OD-ABE has the similar situation with proxy re-encryption (PRE) [29], where a proxy with a re-encryption key can also do ciphertext transformation. However, the intending decryptor changes after the ciphertext transformation in PRE,

[1] In this paper, we do not consider attacks by quantum computer or key leakage.

Please cite this article in press as: C. Zuo, et al., CCA-secure ABE with outsourced decryption for fog computing, Future Generation Computer Systems (2016), http://dx.doi.org/10.1016/j.future.2016.10.028