Computer Networks 133 (2018) 141–156

Contents lists available at ScienceDirect

Computer Networks

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

PHOABE: Securely outsourcing multi-authority attribute based encryption with policy hidden for cloud assisted IoT

Sana Belguith[a,b,*], Nesrine Kaaniche[c], Maryline Laurent[c], Abderrazak Jemai[d], Rabah Attia[a]

[a] SERCom Lab, Ecole Polytechnique de Tunisie, Université de Carthage, Tunisie
[b] Telnet Innovation Labs, Telnet Holding, Tunisie
[c] SAMOVAR, CNRS, Télécom SudParis, CNRS, Université Paris-Saclay, France
[d] Laboratory LIP2, University of Sciences of Tunis, Tunisia

ARTICLE INFO

Article history:
Received 20 June 2017
Revised 3 December 2017
Accepted 18 January 2018

Keywords:
Attribute based encryption
Hidden policy
Decryption outsourcing
Cloud computing
Privacy
Data security

ABSTRACT

Attribute based encryption (ABE) is an encrypted access control mechanism that ensures efficient data sharing among dynamic group of users. Nevertheless, this encryption technique presents two main drawbacks, namely high decryption cost and publicly shared access policies, thus leading to possible users' privacy leakage.

In this paper, we introduce PHOABE, a Policy-Hidden Outsourced ABE scheme. Our construction presents several advantages. First, it is a multi-attribute authority ABE scheme. Second, the expensive computations for the ABE decryption process is partially delegated to a Semi Trusted Cloud Server. Third, users' privacy is protected thanks to a hidden access policy. Fourth, PHOABE is proven to be selectively secure, verifiable and policy privacy preserving under the random oracle model. Five, estimation of the processing overhead proves its feasibility in IoT constrained environments.

1. Introduction

The Internet of Things (IoT) refers to connecting different kinds of devices (things), mainly sensors, RFID tags, PDAs or smartphones to build a network. The deployment of these IoT devices is gaining an expanding interest in the academic research and industrial areas as well as in daily life [1] such as smart grid [2], e-health [3], smart city, etc.

Currently, applications based on IoT can be found everywhere. According to Yao et al. [4], IoT is classified into Unit IoT and Ubiquitous IoT categories according to the number of the involved applications or domains [5]. The unit IoT category is involved in a single application, where only one authority is required. However, in the ubiquitous IoT category, IoT is used in cross domain applications, where local, national and industrial IoTs are interacting, thus requiring multiple authorities across domain applications. Both unit IoT and Ubiquitous IoT are becoming popular, and there is a strong need for both of them to handle data processing and sharing among different IoT devices.

The significant growth of involved IoT devices imposes high requirements for data security and privacy preservation. Hence, security problems have become a hurdle in fulfilling the vision for IoT [6,7].

In IoT applications, data are always transmitted, stored and dynamically shared through the heterogeneous and distributed networks [8]. Consequently, encryption and access control mechanisms are important in order to prevent unauthorized entities from accessing data [9–13].

Attribute based encryption schemes is a promising cryptographic primitive that ensures efficient encrypted access control to outsourced data. Indeed, recently, several attribute based encryption mechanisms have been proposed in literature [14–20].

Most of the proposed attribute based schemes have focused on designing expressive access control policies and providing low communication overheads, through short or constant size ciphertexts [21–23]. Though these solutions present low storage and communication costs, they are still not suitable to be used on resource-constrained devices such as mobile devices and sensors. For instance, the construction of ABE schemes is based on the use of bilinear maps which present expensive computation costs. Moreover, the number of these expensive bilinear operations increases along with the number of attributes involved in the access structure, mainly in the decryption procedure [24]. Hence, the most relevant challenge is to reduce the decryption processing cost of the introduced ABE mechanism while providing fine-grained access control for users [25].

* Corresponding author.
E-mail address: sbel452@aucklanduni.ac.nz (S. Belguith).

https://doi.org/10.1016/j.comnet.2018.01.036
1389-1286/

Green et al. [24] proposed, in 2011, the first attribute-based encryption scheme with outsourced decryption. This scheme consists in securely offloading the decryption process of ABE to an external cloud based provider. This solution ensures that most of the decryption cost can be released from the IoT devices to the cloud.

In most attribute based encryption schemes, the access structure is shared publicly with the related ciphertext. Hence, any user who get the ciphertext can see its content. This exposure of data's access structure will disclose sensitive information about the decryption or encryption party. Meanwhile, in order to avoid disclosing these sensitive information, the access structure should be hidden [26–28].

In addition, in single-authority ABE schemes, a central attribute authority is responsible for managing and issuing all users' attributes and related secret keys. Although this setting facilitates the key management, it can be a bottleneck since central attribute authority is able to achieve a key escrow attack, due to its knowledge of the users' private keys. To solve this problem, many multi-attribute authority ABE schemes have been proposed. These solutions rely on multiple parties to distribute attributes and private keys to users. Such approach offers the scalability for the system even if the number of users becomes important [21,29,30].

In this paper, we introduce a novel Policy-Hidden Outsourced Attribute Based Encryption (PHOABE) scheme. Our proposed mechanism is multifold.

First, we extend the original multi-authority CP-ABE scheme proposed by Lewko et al. [29] to support the outsourced decryption in order to better fit processing and communication requirements of resource-constrained devices. For instance, our scheme consists in delegating the expensive computations during the decryption phase, to a Semi Trusted Cloud Server, referred to as STCS.

Second, we apply policy-hidden techniques to ensure users' privacy and access policy confidentiality preservation.

Third, we introduce a secure mechanism consisting in verifying that the partially decrypted ciphertext was correctly generated by the remote cloud server referred to as the verifiability concept.

Fourth, we show that our proposed mechanism is selectively secure, verifiable and policy privacy preserving under the random oracle model.

Paper Organisation **–** The remainder of this paper is organized as follows. First, Section 2 highlights security considerations and design goals. Then, Section 3 reviews related work and introduces attribute based mechanisms. In Section 4, we describe the system model and the threat model of the system. Afterwards, we detail the framework design and we introduce the construction of our proposed scheme in Section 5. In Section 6, we perform security analysis of PHOABE based on security games. Finally, a theoretical performance analysis is provided in Section 7, before concluding in Section 8.

2. Problem statement

As e-health systems are witnessing increased popularity, several health organisations are using these systems in order to centralize and share medical data in an efficient way.

Let us consider the following example, where a medical organisation relies on cloud based services to collect and share Electronic Health Records (EHRs) among the medical staff. Note that the medical staff can belong to different organisations such as hospitals, research laboratories, pharmacies, health ministry as well as doctors. The use of a cloud architecture enables the hospital employees to access the data using their smart devices (such as PDAs, smartphones ⋯), considered as resource-constrained devices.

Health Insurance Portability and Accountability Act (HIPAA) [31] states that access policies must finely precise different access privileges of authorized users to the shared outsourced data. In fact, a health-care information system based on cloud services is required to protect medical records from unauthorized access. Hence, the system must restrict access of protected data to eligible doctors. For instance, hospital employees, mainly doctors, have to share patients' health information, in order to collaborate with the involved hospital employees to properly prescript treatments. Thus, they usually form dynamic sharing groups with different granted privileges.

As data are always shared through the heterogeneous and distributed networks, the proposed security mechanisms should provide lightweight processing at the client side, while supporting flexible sharing of encrypted outsourced data among dynamic group of users.

To support all these features with efficiency, we propose to design a multi-attribute authority ABE scheme with outsourced decryption to be run at the client side.

Thus, the proposed scheme PHOABE must fulfill the following properties:

- ***low computation overhead*** **–** PHOABE must introduce cryptographic algorithms with low processing complexity especially at the client side in order to ensure access by different resource-constrained devices.
- ***data confidentiality*** **–** PHOABE has to protect the secrecy of outsourced and encrypted data contents against both curious cloud service providers and malicious users.
- ***flexible access control*** **–** our proposal should ensure fine grained access control to allow authorized users to access data.
- ***privacy*** **–** PHOABE must protect group members' access patterns privacy, while requesting access to outsourced data.

3. ABE-related work

Attribute Based Encryption (ABE) was first designed by Sahai and Waters to ensure encrypted access control [32]. In ABE schemes, the ciphertext is encrypted for many users instead of encrypting to a single user as in traditional public key cryptography. In attribute based encryption schemes, user's private keys and ciphertext are associated with an access policy or a set of attributes [33]. Thus, a data user is able to decrypt the ciphertext if his private key matches the ciphertext. ABE schemes are classified into two categories, namely: Key-Policy Attribute Based Encryption (KP-ABE) and Ciphertext-Policy Attribute Based Encryption (CP-ABE) [34].

In KP-ABE, the ciphertext are labeled with a set of attributes while the users' private keys are associated with an access policy which can be any monotonic tree. The user is able to decrypt the ciphertext if its access policy is satisfied by the attributes embedded in the ciphertext. Although the KP-ABE scheme offers fine-grained access control feature, it has one main disadvantage. Indeed, the data owners cannot decide on who has access to their encrypted data, except by their choice of descriptive attributes for the data, as the access policy is embedded in the user's private keys. Consequently, the data owners have to trust the key issuer. Ciphertext-policy ABE schemes remove such inconvenience by directly embedding the access policy on the ciphertext. As such, the data owners can now authorize who can have access on their encrypted data [21,29,34].

CP-ABE schemes allow the data owner to precise the users authorized to access the data, by embedding the access policy to the ciphertext [21,26,35,36]. In order to issue private keys related to the user's set of attributes, ABE schemes rely on trusted authorities. ABE schemes can be categorized into two types namely single-authority ABE schemes and multi-authority ABE schemes.

In a single-authority ABE scheme, the attributes and their related private keys are issued by a central attribute authority. Al-