Future Generation Computer Systems 49 (2015) 104–112

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

A lightweight attribute-based encryption scheme for the Internet of Things

Xuanxia Yao [a,*], Zhi Chen [a], Ye Tian [b,c]

[a] School of Computer and Communication Engineering, University of Science and Technology Beijing, Beijing, 100083, China
[b] Computer Network Information Center, Chinese Academy of Sciences, Beijing, 100190, China
[c] DNSLAB, China Internet Network Information Center, Beijing, 100190, China

HIGHLIGHTS

- Propose a lightweight no-pairing ECC-Based ABE scheme for the Internet of Things.
- The security depends on the ECDDH assumption instead of bilinear Diffie–Hellman based assumptions.
- The criteria and metrics for measuring the overhead are defined uniformly.
- Comparisons with the existing ABE schemes in efficiency illustrate its lightweight.

ARTICLE INFO

Article history:
Received 30 April 2014
Received in revised form
2 August 2014
Accepted 8 October 2014
Available online 18 October 2014

Keywords:
Internet of Things
Attribute-based encryption
Elliptic curve cryptography
Decision Diffie–Hellman problem
Selective-set model

ABSTRACT

Internet of Things (IoT) is an emerging network paradigm, which realizes the interconnections among the ubiquitous things and is the foundation of smart society. Since IoT are always related to user's daily life or work, the privacy and security are of great importance. The pervasive, complex and heterogeneous properties of IoT make its security issues very challenging. In addition, the large number of resources-constraint nodes makes a rigid lightweight requirement for IoT security mechanisms. Presently, the attribute-based encryption (ABE) is a popular solution to achieve secure data transmission, storage and sharing in the distributed environment such as IoT. However, the existing ABE schemes are based on expensive bilinear pairing, which make them not suitable for the resources-constraint IoT applications. In this paper, a lightweight no-pairing ABE scheme based on elliptic curve cryptography (ECC) is proposed to address the security and privacy issues in IoT. The security of the proposed scheme is based on the ECDDH assumption instead of bilinear Diffie–Hellman assumption, and is proved in the attribute based selective-set model. By uniformly determining the criteria and defining the metrics for measuring the communication overhead and computational overhead, the comparison analyses with the existing ABE schemes are made in detail. The results show that the proposed scheme has improved execution efficiency and low communication costs. In addition, the limitations and the improving directions of it are also discussed in detail.

1. Introduction

With the booming of wireless communications, micro-electro-mechanical systems (MEMS), digital electronics and mobile computing, IoT has developed vigorously, and been applied not only in the academic research and industrial fields but also in daily life [1], such as smart grid [2], e-health [3], e-home, environment monitoring [4], smart city and so on. By connecting sensors, tiny smart devices and intelligent everyday items with the Internet, the data can be collected or distributed automatically and the virtual information world can be integrated seamlessly with the physical world [5]. Applications based on IoT not only make people live easily and smartly, and also bring many challenges. For one aspect, according to the novel system architecture proposed by H. Ning and H. Liu [6], ubiquitous data collection is indispensable in the perception layer. Moreover, whether the unit or ubiquitous IoT, the application layer should be responsible for data processing, which may require sharing the collected data among users. For the other aspect, with more and more sensors available and able to be linked to the user for gathering data, individuals want to control their

* Corresponding author. Tel.: +86 13671086439.
E-mail address: yaoxuanxia@163.com (X. Yao).

http://dx.doi.org/10.1016/j.future.2014.10.010
0167-739X/

personal data and make high requirements for data security and privacy preservation. The two conflicting aspects make the data collection, distribution and utilization bring severe security challenges for the IoT applications.

For instance, in the ubiquitous IoT application such as smart city, data is usually gathered from various sources owned by different administrative domains (e.g., smart phones, and public or private transportation providers). The data collection may be out of the user's knowledge and data transmitting may be in plaintext. Since the massive collected data is shared among different departments, which may be accessed by unauthorized users to cause serious problems or even be used to harm the owners of the data if no security restriction is made on it. Another example is a unit IoT application, that is health or medical monitoring. Normally, the data collected by the body sensors applied to an elderly person or patient should be always sent to the server of the medical center or hospital and accessible only by the specified doctors, because the body data are all sensitive data. The privacy may be broken if it is transmitted in plaintext or there is no appropriate access control made on it, which may lead to serious result. In addition, the multi-hop wireless broadcast communication mode in IoT is also vulnerable to eavesdropping.

Similar to the traditional (wire or wireless) networks, data security in IoT also includes confidentiality, integrity, authenticity and privacy. As for the privacy and confidentiality, since data are always transmitted in broadcast communication mode in the IoT, storage and dynamically shared through the heterogeneous and distributed networks, encryption and preventing unauthorized entities from accessing are very important [7], which can be achieved by cipher-text based access control mechanism. For data integrity and authenticity, authentication is a fundamental and efficient approach. For instance, H. Ning et al. put forward an aggregated-proof based hierarchical authentication scheme for the Internet of Things [8] in 2013. For the sake of practicability, the lightweight authentication approach should be the first choice of IoT.

Attribute-based encryption (ABE) system has the nature that any user can decrypt the cipher-text as long as it meets the required attributes, which makes it very suitable for cipher-text based access control and broadcast encryption. Unfortunately, it is very difficult to implement the existing ABE schemes in the resources-constraint IoT, because they are all based on the expensive bilinear pairing operations. In order to keep the data privacy and confidentiality in IoT, a lightweight attribute-based encryption scheme is indispensable.

In this paper, considering the fact that ECC algorithm has much stronger bit security than RSA as well as other exponential-based public key cryptographic algorithm, and it is easy to be realized on hardware or a chip, we propose a no-pairing ECC-Based ABE scheme to deal with the data security and privacy issues in IoT. Since it replaces the expensive bilinear pairing operation with point scalar multiplication on elliptic curve, it can meet the lightweight requirement and is suitable for IoT.

The main contributions are as follows: (1) A lightweight no-pairing ECC-Based ABE scheme is proposed to address the data security and privacy issues in the IoT. (2) The proposed ABE scheme's security depends on the ECDDH problem instead of bilinear Diffie–Hellman assumption, which can reduce the computation overhead and communication overhead. The security proof is performed in attribute based selective-set model. (3) The criteria and metrics for measuring the communication overhead and computational overhead are defined uniformly. (4) The lightweight feature is illustrated by comparing it with the existing ABE schemes, which indicates that it is more practical for IoT than others.

The remainder of this paper is organized as follows: In Section 2, we review the related works on attribute-based encryption and the related applications in IoT. Section 3 presents the preliminaries related to the proposed ABE scheme. Section 4 gives a detail description of the lightweight ABE scheme for IoT. The security proof is made in Section 5, and the performance is analyzed in Section 6. Finally, Section 7 draws a conclusion.

2. Related work

The concept of attribute-based encryption was first introduced in Advances in Cryptology EUROCRYPT 2005 [9]. It is an extension or generalization of identity-based cryptosystem, which can realize fuzzy identity by combining the user's identity with a series of attributes and achieve the aim of privacy preserving. In ABE system, a user's identity is composed of a set of strings which serve as descriptive attributes of the user. Messages are encrypted under a set of attributes describing the intended receivers, and the secret or private key of these users is also associated with the attributes set for encryption. Attribute-based encryption schemes allow any user to decrypt cipher-text as long as it has the attributes satisfying a threshold policy. This feature makes ABE a very popular solution to provide data security in loosely coupled, distributed environments and can be used as a perfect cryptographic building block to realize broadcast encryption [10] and cipher-text access control.

According to whether the private key or the cipher-text being associated with the access control policy, attribute-based encryption schemes can be further classified into Key-Policy ABE schemes (KP-ABE) [11] and Ciphertext-Policy ABE (CP-ABE) [12]. In KP-ABE, the message is encrypted under an attributes set, the access control policy that the receivers' attributes set should satisfy is embedded into the private keys. For basic KP-ABE, only the threshold gates can be used to express the access policy. In order to express the access policy flexibly, Goyal et al. also extends the KP-ABE to allow users' private keys to include any policy consisting of AND, OR threshold gates [11]. Ostrovsky et al. further extended KP-ABE to allow access policy including negative constraints [13]. In CP-ABE, the access policy is specified by the sender and embedded into the cipher-text, the encryption attributes set is associated with the private key [12]. CP-ABE is conceptually closer to the role based access control model, which make it more appealing than KP-ABE.

In recent years, the ABE based access control has drawn many researchers attention and many schemes have been proposed. Most of them focus on establishing expressive access control policies [11,13–15] to deal with the challenges in expressing access control policy, constructing constant size cipher-text [15–17] to limit the size of the cipher-text. Although some achievements have been made at the expense of increasing overheads, they do not meet the lightweight requirement of IoT yet. Meanwhile, as the broadcast is a main communication mode in perception layer of IoT, ABE based broadcast encryption is also hot topic [18,19]. Compared with existing one-to-one encryption schemes, these ABE based broadcast encryption schemes are efficient, because they can avoid sending messages encrypted with each individual recipient's public key. Considering the decryption efficiency, there are some researches on speeding up decryption [20] and improving efficiency. In addition, considering that different attributes are usually issued by different authorities, Chase proposed a multi-authority ABE scheme [21]. As far as security, all the ABE schemes are all proved selective security.

At present, ABE is mainly used to prevent unauthorized users from accessing the confidential data in cloud. Cloud computing is a main support technology of IoT. In addition, broadcast encryption is always required to secure data transmission in IoT. Although the existing traditional cryptography based solutions can meet the requirements in theory, they are usually realized by combining public key cryptography and/or symmetric cryptography and