Future Generation Computer Systems 52 (2015) 61–66

Contents lists available at ScienceDirect

Future Generation Computer Systems

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

Server-aided anonymous attribute-based authentication in cloud computing

Zhusong Liu [a,*], Hongyang Yan [b], Zhike Li [a]

[a] Department of Computer Science, Guangdong University of Technology, Guangzhou, China
[b] Department of Computer Science, Guangzhou University, Guangzhou, China

HIGHLIGHTS

- A new attribute-based signature with outsourcing compuation was proposed.
- The security model was formalized.
- The security and efficiency analysis has been given.

ARTICLE INFO

Article history:
Received 21 July 2014
Received in revised form
17 November 2014
Accepted 3 December 2014
Available online 2 February 2015

Keywords:
Attribute-based signature
Cloud computing
Privacy
Outsourcing

ABSTRACT

The notion of attribute-based signature is one of the important security primitives to realize anonymous authentication. In an attribute based signature (ABS), users can generate a signature on a message with their attributes. With this signature, any verifier will be convinced that such a signature is generated from a signer with these attributes. However, the identity of the signers will be hidden from the verifier. ABS are useful to design anonymous authentication and attribute-based messaging system. However, existing work of attribute-based authentication usually requires huge computation during signing, which grows linearly with the size of the attributes. Thus, these methods result in heavy computation overhead on the users and are not suitable for devices with only small computation ability.

Cloud computing is an emerging computing paradigm in which resources of the computing infrastructure are provided as outsourcing services over the Internet. In this paper, we first address the challenging issue of securely outsourcing ABS, which enables users to largely eliminate the computational costs of ABS generation. The security model is formally defined to protect the privacy of users' signing key while outsourcing the computation of signing. An efficient and secure outsourcing algorithm of ABS is also proposed. Extensive analysis shows that our scheme is secure in the proposed model and saves more than 90% computation overhead on the user side.

1. Introduction

Attribute-based signature [1–3] is an important variation of digital signature, which extends the identity-based signature [4] and in which a signer is defined by a set of attributes instead of single string representing the signer's identity. In ABS, a user obtains a certificate for a set of attributes from the attribute authority. The verifier of ABS is convinced that a signer, whose set of attributes satisfies a complex predicate, has endorsed the message.

ABS has found many important applications and is a related notion to attribute based encryption [5]. For instance, ABS can be used for fine-grained access control in anonymous authentication. And another important application of ABS can be found in attribute based messaging system, in which the receiver has to be sure that the received message was sent by a user with appropriate attributes. Also considering the application scenario of ABS in an online e-book service (such as Safari online), which allows users to use the service for 30 days for free. To be eligible as a customer, the current solution is that one should provide a valid email address with two independent proofs of his identity, such as a bank account, a passport, or a credit card. Note that in this scenario, it is required to give supporting items for the purpose of proving a valid identity as any valid identity would qualify. That is, convincing the possession of a valid identity without revealing the related identity information itself. With this in mind, one can create a signed statement stating that the possession of two required supporting items without revealing items themselves by applying the ABS technique.

* Corresponding author.
E-mail address: 25421944@qq.com (Z. Liu).

http://dx.doi.org/10.1016/j.future.2014.12.001
0167-739X/

ABS can be used in many important applications, however, the generation of ABS requires huge computation because it grows linearly with the number of attributes. All the previous ABS schemes have this flaw, such as [2,3,6,1]. For traditional computing devices such as desktop computers, these computation can be easily processed. However, for the popular and emerging mobile devices such as mobile phone, such computational overhead will be a challenge.

Cloud computing [7–9] is a new computing paradigm and is able to provide huge resources and computing ability to users. With cloud computing technique, the users are able to outsource their computing and storage tasks to the cloud servers. As a result, even for users only with mobile devices of limited computational ability, this new computing paradigm is able to help users finish these tasks. The cloud computing has attracted much attention because of these properties. Promising as it is, this paradigm also brings forth new challenges when users intend to utilize the untrusted cloud for outsourcing computations. The challenge becomes even grimmer when users want to delegate private operations to the cloud, such as signature generation.

A simple and naive approach would be for a user to handle and send his private key to the cloud provider. With the key, the cloud server could generate the signature and return it to the user. However, this requires complete trust of the cloud. The cloud can generate signatures of any messages on behalf of the user. Thus, the straightforward approach is not secure when the cloud is not fully trusted. A second approach is utilizing the method used in the server-aided signature schemes [10,11]. However, previous server-aided signature schemes are designed to reduce the computational overhead by improving the computational algorithm using untrusted servers. By using these methods in ABS will cause inefficiency. A third approach is to use the outsourcing methods [12–19] with homomorphic encryption or interactive proofs systems. But Gentry [14] has [14] showed that the homomorphic operation technique is not practical currently and required around 30 s on a high performance machine. Therefore, with these methods, the privacy of inputs and outputs can be protected by using the homomorphic encryption, the overhead of these techniques is impractical. There are also some works on outsourcing computation for specific computation problems such as [20–22].

In this paper, we focus on a concrete outsourcing scheme with respect to ABS. We propose an efficient and secure ABS-Outsourcing (ABSO) protocol that eliminates most computations of signature generation while simultaneously protects the user's privacy and security. In the protocol, the user provides the cloud server a single outsourcing key such that the cloud server is able to generate a half-signature. When the user receives the half-signature, he can transform it into a valid ABS with several multiplications which is far more efficient than that if he generates the signature by himself. For security analysis, first of all, we formally define the security of verifiability and unforgeability. Then we prove that our scheme satisfies the security definitions in the standard model. Our ABSO scheme is based on the most efficient ABS scheme proposed by Li [1,2], however, the approach proposed in this paper can also be extended to other ABS schemes.

This paper is organized as follows. In Section 2 we present the preliminaries of our scheme. In Section 3, the system model and security definition of our scheme are given. The construction of our scheme is presented in Section 4. In Section 5, we show the efficiency analysis and security proof of our scheme. Finally, the conclusion of this paper is given in Section 6.

2. Preliminaries

2.1. Bilinear maps

Let $\mathbb{G}$ and $\mathbb{G}_T$ be (multiplicative) cyclic group of prime order p, g and g_T be the generator of $\mathbb{G}$ and $\mathbb{G}_T$ respectively. A bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_T$ is called a bilinear pairing if the following conditions hold [23]:

- **Bilinearity**: For all $g \in \mathbb{G}^*$, g is a generator of $\mathbb{G}$, and $a, b \in \mathbb{Z}_p$, $e(g^a, g^b) = e(g, g)^{ab}$.
- **Non-degeneracy**: $e(g, g) \neq 1$. That is to say, if g generates the group $\mathbb{G}$, then $e(g, g)$ generates $\mathbb{G}_T$.
- **Efficiency**: There exists an efficient algorithm for computing $e(., .)$.

2.2. Access structure

Definition 1 (*Access Structure [24]*)**.** We define the set $\{P_1, P_2, \ldots, P_N\}$ as the parties involved. $\mathbb{A} \subset 2^{\{P_1, P_2, \ldots, P_n\}}$ is called monotone if for any B, C with the conditions $B \in \mathbb{A}$ and $B \subset C$. We have that $C \in \mathbb{A}$. We define an access structure as $\mathbb{A}$ of $\{P_1, P_2, \ldots, P_n\}$. Then, all the sets given in $\mathbb{A}$ are authorized sets.

In attribute-based systems, the party is defined through the attributes. Based on this definition, all the authorized users are contained in the set of $\mathbb{A}$. In more detail, the new scheme supports all predicates Υ consisting of thresholds gates, which can be described as:

$$\Upsilon_{k,\omega^*}(\omega) = \begin{cases} 1 & \text{if } |\omega^* \cap \omega| \geq k \\ 0 & \text{otherwise} \end{cases} \quad (1)$$

where ω^* and ω are attribute sets and k is a predefined threshold value. Therefore, the authorized sets in this context consist of all the attribute subsets ω that satisfies $\Upsilon_{k,\omega^*}(\omega) = 1$.

2.3. Assumption

Computational Diffie–Hellman Assumption (CDH) The standard CDH assumption is defined as follows. For every probabilistic polynomial time algorithm $\mathcal{A}$, there exists a negligible function $neg(\cdot)$ such that for all n.

$$|Pr[\mathcal{A}(1^n, g, g^x, g^y) = g^{xy}]| \leq neg(\cdot)$$

where g is the generator of a group $\mathbb{G}$ of order p which is a prime of length approximately n, $x, y \in \mathbb{Z}_p$. We say that (t, ϵ)-CDH holds in $\mathbb{G}$ if there is no adversary $\mathcal{A}$ that solves CDH problem with probability ϵ.

3. System model and security definitions

3.1. Model

Three entities are involved in the system, an attribute authority A, a user U and a cloud server S. The attribute authority issues attribute private keys to users. The user outsources most of the computations of signature generation to the cloud server S without breaking the security of the attribute based signature. $\mathbb{U}$ is utilized to represent the attribute universe. In a nutshell, the attribute based signature scheme with outsourcing functionality consists of the following algorithms:

Setup$(\lambda, \mathbb{U})$ The setup algorithm takes security parameter and attribute universe as input. It outputs the public parameters PK and the master key SK for the attribute authority.

Extract$(\mathbf{SK}, \omega)$ The extract algorithm takes the master key and a set of attributes as input. It generates the corresponding private keys sk_ω for the user who is eligible to be issued with these attributes.

KeyGen$_{out}(sk_\omega, \mathbf{T})$ The outsourcing key generation algorithm takes a user's private key sk_ω and a set T which is composed of randomly selected numbers $t_i \in \mathbb{Z}_p$ as input. It generates the outsourcing key sk_{out} for the cloud server S.