IDENTITY-BASED ENCRYPTION WITH OUTSOURCED REVOCATION IN

CLOUD COMPUTING

ABSTRACT

Identity-based encryption (ibe) which simplifies the public key and certificate management at public key infrastructure (pki) is an important alternative to public key encryption. However, one of the main efficiency drawbacks of ibe is the overhead computation at private key generator (pkg) during user revocation. Efficient revocation has been well studied in traditional pki setting, but the cumbersome management of certificates is precisely the burden that ibe strives to alleviate.

In this paper, aiming at tackling the critical issue of identity revocation, we introduce outsourcing computation into IBE for the first time and propose a revocable IBE scheme in the server-aided setting. Our scheme offloads most of the key generation related operations during key-issuing and key-update processes to a Key Update Cloud Service Provider, leaving only a constant number of simple operations for PKG and users to perform locally. This goal is achieved by utilizing a novel collusion-resistant technique: we employ a hybrid private key for each user, in which an AND gate is involved to connect and bound the identity component and the time component. Furthermore, we propose another construction which is provable secure under the recently formulized Refereed Delegation of Computation model. Finally, we provide extensive experimental results to demonstrate the efficiency of our proposed construction.

EXISTING SYSTEM

There exists g1, g2 ∈ G with e(g1, g2) 1, in other words, the map does not send all pairs in G×G to the identity in GT.

Upon receiving a keyupdate request on ID, KU-CSP firstly checks whether ID exists in the revocation list RL, if so KU-CSP returns ⊥ and key-update is aborted.

In RDoC model, the client is able to interact with multiple servers and it has a right output as long as there exists one server that follows the proposed protocol. One of the most advantages of RDoC over traditional model with single server is that the security risk on the single server is reduced to multiple servers involved in. As the result of both the practicality and utility, RDoC model recently has been widely utilized in the literature of outsourced computation.

.

**PROPOSE SYSTEM**

which is proposed to simplify key management in a certificate-based Public Key Infrastructure (PKI) by using human-intelligible identities (e.g., unique name, email address, IP address, etc) as public keys.

we introduce outsourcing computation into IBE for the first time and propose a revocable IBE scheme in the server-aided setting.

We propose a scheme to offload all the key generation related operations during key-issuing and key-update, leaving only a constant number of simple operations for PKG and eligible users to perform locally.

Based on the system model proposed, we are able to define the outsourced revocable IBE scheme. Compared with the traditional IBE definition, the KeyGen, Encrypt and Decrypt algorithms are redefined as follows to integrate time component.

proposed a way for users to periodically renew their private keys without interacting with PKG.

The authors utilized proxy re-encryption to propose a revocable ABE scheme.

ALGORITHM

The setup algorithm takes as input a security parameter λ and outputs the public key PK and the master key MK. Note that the master key is kept secret at PKG.

The private key generation algorithm is run by PKG, which takes as input the master key MK and user’s identity ID ∈ {0, 1}∗. It returns a private key SKID corresponding to the identity ID.

The encryption algorithm is run by sender, which takes as input the receiver’s identity ID and a message M to be encrypted. It outputs the ciphertext CT.

The decryption algorithm is run by receiver, which takes as input the ciphertext CT and his/her private key SKIDs . It returns a message M or an error ⊥.

# SYSTEM CONFIGURATION

**SOFTWARE REQUIREMENTS**:

Operating System : Windows

Technology : Java and J2EE

Web Technologies : Html, JavaScript, CSS

IDE : My Eclipse

Web Server : Tomcat

Tool kit : Android Phone

Database : My SQL

Java Version : J2SDK1.5

**HARDWARE REQUIREMENTS**:

Hardware : Pentium

Speed : 1.1 GHz

RAM : 1GB

Hard Disk : 20 GB

Floppy Drive : 1.44 MB

Key Board : Standard Windows Keyboard

Mouse : Two or Three Button Mouse

Monitor : SVGA

### IMPLEMENTATION:

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it’s constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

**MODULE DESCRIPTION:**

# Number of Modules;

After careful analysis the system has been identified to have the following modules:

1.Client Module

i.Identity-based Encryption Authentication Module.

ii.Public Key Generator Module.

2.Private Key Generator Module.

3.Server Module

i.Graph Module

1.Client Module

i.Identity-based Encryption Authentication Module.

A trustee-based social authentication includes two phases:.

* Registration Phase:

The system prepares trustees for a user Alice in this phase. Specifically, Alice is first authenticated with her main authenticator (i.e., password),and then a few(e.g., 5) friends, who also have accounts in the system, are selected by either Alice herself or the service provider from Alice’s friend list and are appointed as Alice’s trustees.

ii.Public Key Generator Module.

Authentication is essential for securing your account and preventing upload your data encrypted file store from database. Imagine a phishing email being sent from your mail because someone had forged your information. Angry recipients and spam complaints resulting from it become your mess to clean up, in order to repair your reputation. Identity-based Encryption social authentication systems ask users to select their own trustees without any constraint. In our experiments we show that the service provider can constrain Identity-based Encryption selections via imposing that no users are selected as Identity-based Encryption by too many other users, which can achieve better security guarantees.

2.Private Key Generator.

They are short in storage for both private key at user and binary tree structure at PKG. We specify that in this work we also aim to utilize outsourcing computation technique to deliver overhead computation to KU-CSP so that PKG is able to be offline in keyupdate.

1) It achieves constant efficiency for both computation at PKG and private key size at user;

2) User needs not to contact with PKG during key-update, in other words, PKG is allowed to be offline after sending the revocation list to KU-CSP;

3) No secure channel or user authentication is required during key-update between user and KU-CSP.

3.Server Module

Server module first PKG send the key. After check the keyword user key and sever key is matching server approved the file. Not matching don’t data download. This is work main concept of paper. Keyword matching meaning server send the new key from user.

i.Graph module is using how many key in generator in server collection.

CONCLUSION

In this paper, focusing on the critical issue of identity revocation, we introduce outsourcing computation into IBE and propose a revocable scheme in which the revocation operations are delegated to CSP. With the aid of KU-CSP, the proposed scheme is full-featured: 1) It achieves constant efficiency for both computation at PKG and private key size at user; 2) User needs not to contact with PKG during key-update, in other words, PKG is allowed to be offline after sending the revocation list to KU-CSP; 3) No secure channel or user authentication is required during key-update between user and KU-CSP.

Furthermore, we consider to realize revocable IBE under a stronger adversary model. We present an advanced construction and show it is secure under RDoC model, in which at least one of the KU-CSPs is assumed to be honest. Therefore, even if a revoked user and either of the KU-CSPs collude, it is unable to help such user re-obtain his/her decryptability.

Finally, we provide extensive experimental results to demonstrate the efficiency of our proposed construction