IDENTITY-BASED ENCRYPTION WITH CLOUD REVOCATION AUTHORITY AND ITS APPLICATIONS

ABSTRACT

Identity-based encryption (IBE) is a public key cryptosystem and eliminates the demands of public key infrastructure (PKI) and certificate administration in conventional public key settings. Due to the absence of PKI, the revocation problem is a critical issue in IBE settings. Several revocable IBE schemes have been proposed regarding this issue. Quite recently, by embedding an outsourcing computation technique into IBE, Li et al. proposed a revocable IBE scheme with a key-update cloud service provider (KU-CSP). However, their scheme has two shortcomings. One is that the computation and communication costs are higher than previous revocable IBE schemes. The other shortcoming is lack of scalability in the sense that the KU-CSP must keep a secret value for each user.

EXISTING SYSTEM

The first practical IBE scheme from the Weil pairing and suggested a simple revocation method in which each non-revoked user receives a new private key generated by the PKG periodically. A period can be set as a day, a week, a month, etc. A sender uses a designated receiver's ID and current period to encrypt messages while the designated receiver decrypts the ciphertext using the current private key.

DISADVANTAGES

- The scheme also results in enormous computation workload for encryption and decryption procedures.
- It is enormous load for PKG to maintain the binary tree with a large amount of users.
- Un-scalability in the sense that the KU-CSP must keep a time key for each user so that it will incur the management load.

PROPOSED SYSTEM

In order to solve both the un-scalability and the inefficiency in Li et al.'s scheme,we will propose a new revocable IBE scheme with cloud revocation authority (CRA). The proposed scheme possesses the advantages of both Tseng and Tsai's revocable IBE scheme and Li et al.'s scheme . In particular, each user's private key still consists of an identity key and a time update key.

ADVANTAGES

- Revocable IBE scheme with CRA and define its security notions to model possible threats and attacks.
- We have demonstrated that our scheme is semantically secure against adaptive-ID attacks under the decisional bilinear Diffie-Hellman assumption.
- we constructed a CRAaided authentication scheme with period-limited privileges for managing a large number of various cloud services.

SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

Processor - Pentium –III

Speed - 1.1 Ghz

RAM - 256 MB(min)

Hard Disk - 20 GB

Floppy Drive - 1.44 MB

Key Board - Standard Windows Keyboard

Mouse - Two or Three Button Mouse

Monitor – SVGA

SOFTWARE REQUIREMENTS:

Operating System - Windows 7/8

Application Server - Tomcat 5.0

Front - End - Java Back – End - MySQL