Identity-Based Encryption with CloudRevocation 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 inIBE settings. Several revocable IBE schemes have been proposed regarding this issue. Quite recently, by embedding an outsourcingcomputation 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 previousrevocable IBE schemes. The other shortcoming is lack of scalability in the sense that the KU-CSP must keep a secret value for eachuser. In the article, we propose a new revocable IBE scheme with a cloud revocation authority (CRA) to solve the two shortcomings,namely, the performance is significantly improved and the CRA holds only a system secret for all the users. For security analysis, wedemonstrate that the proposed scheme is semantically secure under the decisional bilinear Diffie-Hellman (DBDH) assumption. Finally,we extend the proposed revocable IBE scheme to present a CRA-aided authentication scheme with period-limited privileges formanaging a large number of various cloud services.

EXISTING SYSTEM:

- Li *et al*. introduced an outsourcing computation technique into IBEto propose a revocable IBE scheme with a key-update cloudservice provider (KU-CSP). They shifts the key-update proceduresto a KU-CSP to alleviate the load of PKG.
- Li *et al*.also used the similar technique adopted in Tseng and Tsai'sscheme, which partitions a user's private key into anidentity key and a time update key.
- The PKG sends a userthe corresponding identity key via a secure channel. Meanwhile,the PKG must generate a random secret value (timekey) for each user and send it to the KU-CSP.
- Then the KUCSPgenerates the current time update key of a user by usingthe associated time key and sends it to the user via a publicchannel.

DISADVANTAGES OF EXISTING SYSTEM:

- ID-based encryption (IBE) allows a sender to encrypt message directly by using a receiver's ID without checking the validation of public key certificate.
- In existing system misbehaving/compromised users in an ID-PKS setting is naturally raised.
- Immediaterevocation method employs a designated semi-trusted andonline authority (i.e. mediator) to mitigate the managementload of the PKG and assist users to decrypt ciphertext.
- The computation andcommunication costs are higher than previous revocable IBEschemes.

- The other shortcoming is un-scalability inthe sense that the KU-CSP must keep a time key for eachuser so that it will incur the management load.

PROPOSED SYSTEM:

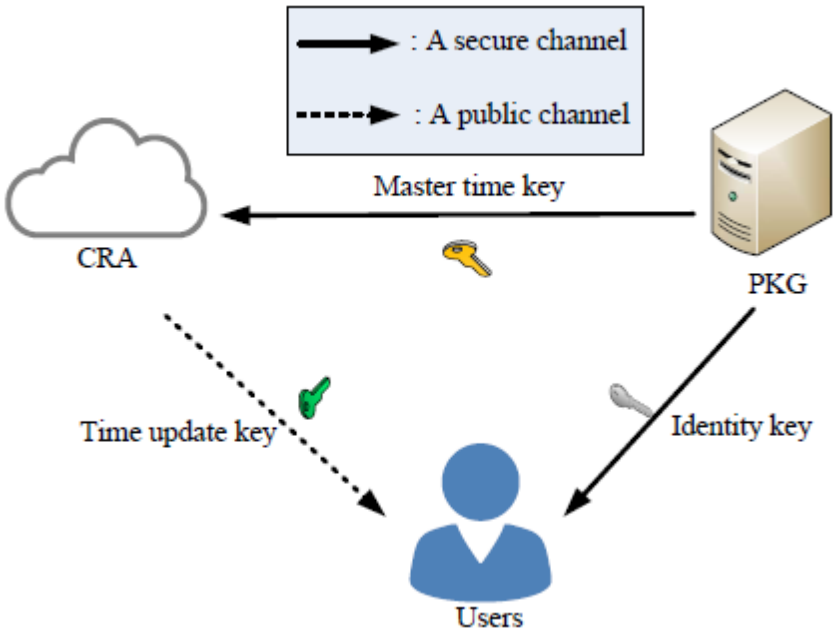
- In order to solve both the un-scalability and the inefficiency in Li *et al*.'s scheme, we propose a new revocable IBE scheme with cloud revocation authority (CRA).
- In particular, each user's private key still consists ofan identity key and a time update key. We introduce acloud revocation authority (CRA) to replace the role ofthe KU-CSP in Li *et al*.'s scheme. The CRA only needs tohold a random secret value (master time key) for all theusers without affecting the security of revocable IBE scheme.
- The CRA uses the master time key to generate the currenttime update key periodically for each non-revoked user andsends it to the user via a public channel. It is evident thatour scheme solves the un-scalability problem of the KU-CSP.
- We construct a CRA-aided authentication scheme with period-limited privileges formanaging a large number of various cloud services.

ADVANTAGES OF PROPOSED SYSTEM:

- The proposed scheme possesses the advantages of both Tsengand Tsai's revocable IBE scheme and Li et al.'s scheme.
- The proposed present the framework of ourrevocable IBE scheme with CRA and define its securitynotions to model possible threats and attacks

- CRA-aidedauthentication scheme with period-limited privileges formanaging a large number of various cloud services.

SYSTEM ARCHITECTURE:



SYSTEM REQUIREMENTS:

HARDWARE REQUIREMENTS:

- System : Pentium Dual Core.
- Hard Disk : 120 GB.
- Monitor : 15''LED
- Input Devices : Keyboard, Mouse
- Ram : 1GB.

SOFTWARE REQUIREMENTS:

- Operating system : Windows 7.
- Coding Language : JAVA/J2EE
- Tool : Netbeans 7.2.1
- Database : MYSQL

REFERENCE:

Yuh-Min Tseng, Tung-Tso Tsai, Sen-Shan Huang, and Chung-Peng Huang, "Identity-Based Encryption with CloudRevocation Authority and Its Applications", **IEEE TRANS. CLOUD COMPUTING 2017.**