**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**

As far as we know, though revocation has been thoroughly studied in PKI, few revocation mechanisms are known in IBE setting. In Boneh and Franklin suggested that users renew their private keys periodically and senders use the receivers’ identities concatenated with current time period. But this mechanism would result in an overhead load at PKG. It requires that PKG is online and the secure channel must be maintained for all transactions, which will become a bottleneck for IBE system as the number of users grows. It requires that PKG is online and the  
secure channel must be maintained for all transactions, which will become a bottleneck for IBE system as the number of users grows. For this reason,a challenge on how to design a secure revocable IBE scheme to reduce the overhead computation at PKG with an untrusted CSP is raised.

**PROPOSE SYSTEM**

In this paper, we introduce outsourcing computation into IBE revocation, and formalize the security definition of outsourced revocable IBE for the first time to the best of our knowledge. 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. In our scheme, as with the suggestion that we realize revocation through updating the private keys of the unrevoked users. But unlike that work which trivially concatenates time period with identity for key generation/update and requires to re-issue the whole private key for unrevoked users, we propose a novel collusion-resistant key issuing technique: we employ a hybrid private key for each user, in which an AND gate is involved to connect and bound two sub-components, namely the identity component and the time component. At first, user is able to obtain the identity component and a default time component (i.e., for current time period) from PKG as his/her private key in key-issuing. Afterwards, in order to maintain decrypt ability, unrevoked users needs to periodically request on key-update for time component to a newly introduced entity named Key Update Cloud Service Provider (KU-CSP). Compared with the previous work [4], our scheme does not have to re-issue the whole private keys, but just need to update a lightweight component of it at a specialized entity KU-CSP. We also specify that

1) with the aid of KU-CSP, user needs not to contact with PKG in key-update, in other words, PKG is allowed to be offline after sending the revocation list to KU-CSP.

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

**ALGORITHM:**

**IDENTITY-BASED ENCRYPTION (IBE)**

**MODULE DESCRIPTION:**

**Users:**

**In this system Users will be register and they will encrypt the files with receiver ID (i.e Email) and send to receiver. As well as when any user revoked at time  
period, each unrevoked user needs to send keyupdate request to KU-CSP (Key**  
**Update Cloud Service Provider) to maintain decryptability. The Receiver will decrypt the data using of his Private Key which is generated by PKG (Private Key Generator).**

**PKG (Private Key Generator):**

**In this system PKG will generate the Private Keys for all authorized Users and as well as send Outsourcing Key to KU-CSP. If any User compromised by Attacker then PKG will Revoke that User i.e he can update the time component only for not accessing any resources which is sent to Him.**

**KU-CSP (Key Update Cloud Service Provider):**

**In this system KU-CSP will be update** **upon receiving a keyupdate request on ID, KU-CSP firstly checks whether ID exists in the Revocation List ( *RL)* , if so KU-CSP does not perform KeyUpdation process, Otherwise KU-CSP fetches Updated Key and send to User.**

# SYSTEM CONFIGURATION:

**Hardware requirements:**

Processor : Any Update Processor

Ram : Min 1 GB

Hard Disk : Min 100 GB

**Software requirements:**

Operating System : Windows family

Technology : Java (1.7/1.8)

Web Technologies : Html, Html-5, JavaScript, CSS, JSP

Web Server : Tomcat 7/8

Database : My SQL5.5

**Implemented by**

Development team : Cloud Technologies

Website : <http://www.cloudstechnologies.in/>

Contact : 8121953811, 040-65511811