ISSN 2395-1621

Identity-based Encryption with Outsourced Revocation in Cloud Computing

[#1]Sameer Sawardekar, [#2]Mayuresh More, [#3]Rajeshwari Thakare,
[#4]V.S.Nandedkar

[1]sameersawardekar1293@gmail.com

[#1234]Department of Computer

Padmabhooshan Vasantdada Patil Institute of Technology,
Savitribai Phule, Pune University
Pune, India

ABSTRACT

Identity based encryption define the public key and certificate management at the public Identity based encryption define the public key infrastructure is an important alternative of public key encryption. Here we are going to introduce the new outsourcing computation IBE. Key upload and key generation is an important key generation during cloud service provider.

Keywords: Revocation, Outsourcing, Identity based Encryption(IBE)

ARTICLE INFO

Article History

Received: 14th March 2017

Received in revised form :

14th March 2017

Accepted: 16th March 2017

Published online :

17th March 2017

I. INTRODUCTION

By using human intelligible identities, IBE is simplify the key management in a certificate based public key Infrastructure for example unique ID and email address.
It encrypts the messages of receiver's identity according to receiver and private key decrypted is able to decrypt such cipher text.

Arbitrary string is allowed by IBE which is used as a public key. This consider as an advantage of PKI, always it demand as the efficient revocation mechanism. Then we must have to provide to revoke such user from system.

From all revocation based study describe the only few revocation mechanism know what is IBE setting. Boneh and Franklin are invented it, and they always said users to renew their private key periodically.

Sender always uses the receiver identity which is concatenate with the current time period. key have been revoked because key have to contact with PKG periodically to prove their identities mechanism would result in an overhead load at PKG. In another word, all the users regardless of whether their keys have been revoked or not, have to contact with PKG periodically to prove the identities and update new private keys. PKG creates a bottleneck for ibe which is maintained for all transaction as number of system user grows therefore PKG should be online.

We used binary tree introduction which is able to achieve the high performance and conclude another problem:

1) PKG will generate the key pair for all node of the path from the identity leaf node to the root node, which will result in complexity logarithmic in the number of users in system which will result in complexity logarithmic in number for issuing a single private key.
2) The size of private key will grow in logarithmic no of user system which results into difficult key storage.

3) As the number of user in the system grows. This will maintain the binary tree with a more amount of nodes.

There is development of cloud computing has ability to merge for user the buy on demand computing from the cloud based service such as Amazon an Microsoft's Windows Azure.

Key Update cloud service provider:

1) With the aid of KU-CSP, user needs not to contact with PKG Key update onto 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.
We consider to realize revocable IBE with semi honest KU-CSP.
To achieve this goal, we present a security enhanced construction.

II. IDENTITY-BASED ENCRYPTION

An IBE scheme which involves two entities, PKG and users (including sender and receiver) is consisted of the following four algorithms:

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

KeyGen: The private key generation algorithm is run by PKG, which takes as input the master key and user's identity. It returns a private key corresponding to the identity.

Encrypt: The encryption algorithm is run by sender, which takes as input the receiver's identity and a message to be encrypted. It outputs the cipher text.[1]

Decrypt: The decryption algorithm is run by receiver, which takes as input the cipher text and his/her private key. It returns a message or an error.

III. RELATED WORK

Firstly implemented by Boneh and Franklin as well as IBE has been researched intensively in cryptographic community.

User periodically renew their private key without interact with PKG.

In this process, there is a third party which is semi-trusted present that is caller as mediator.

Who helps to decrypt each cipher text and if the identity is revoked then the mediator is instructed to stop from helping the user. So it is impractical since all us are unable to decrypt on their own and they need to communicate with mediator.

IV. PROPOSED WORK

We introduce outsourcing computation into IBE revocation, and formalize the security definition of outsourcing revocation IBE for the first time to the best of our knowledge. We proposed scheme offload all the key generation related operation during key-issuing and key update, leaving only a constant number of simple operation for PKG and eligible users to perform locally.
We realize revocation trough updating the private key of the unrevoked users. But unlike that work which travelly concatenate the time period with identities for key generation/ update and require 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 context and bound two sub-components, namely the identity component and the time component.
At first user is able to obtain the identify components (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 Services Provider (KU-CSP).

Compared with the previous work, 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 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.

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

Furthermore, we consider realizing revocable IBE with a semi-honest KU-CSP. To achieve this goal, we present a security enhanced construction under the recently formalized Refereed Delegation of Computation (RDoC)

V. FIGURE

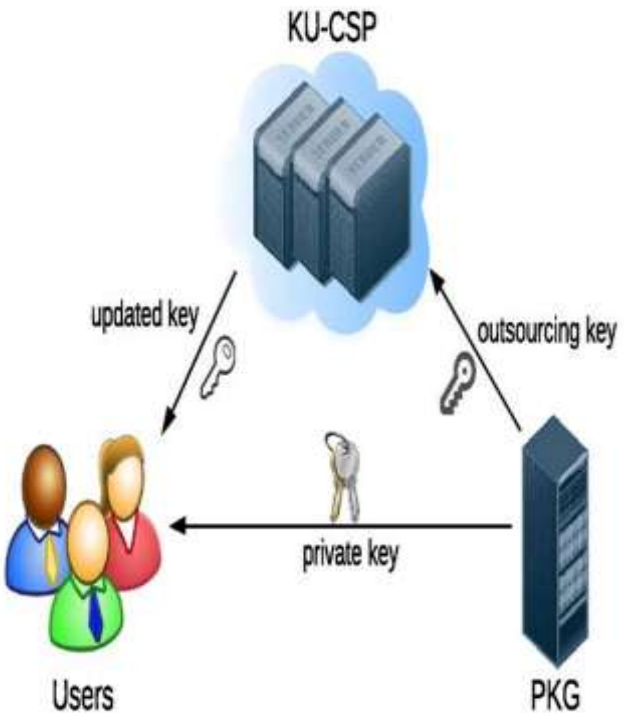

Fig 1. System architecture

VI. MODULE DESCRIPTION

User:
The user module is responsible for the file sharing process with the cloud. The whole process include tree types of key will be shared from PKG to the user. Once the outsourced key distribution to the user with respect to the details receive from the user end such as user is associated with the file download process as well with the collaboration of updated key and private key distribution.

KU-CSP:
It provides computing services in the infrastructure as a service(IAAS) model, which provide the raw material of cloud computing such as processing, storage an the other forms of lower level network raw material and hardware resources in a virtual , on demand manner via the Internet. Differing from traditional hosting services with which physical server or parts there of are rented on a monthly or yearly basis, the cloud infrastructure is rented as virtual machines on a per- use basis and can scale and out dynamically, based on customer needs.
It is responsible for updating key to the user as per the user request.

PKG:
PKG has to generate the key pair for all the nodes on the path from the identity leaf node to the root node, which results in complexity logarithmic in the number of users in system for issuing a single private key.
We employ a hybrid private key for each user, in which an AND gate is involved to connect, namely the identity components and the time components where (i.e., for current time period) from PKG as his or private key in key issuing.

Key Distribution:
At first, user is able to obtain the identity component and default time component and a default time component.
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)

VII.CONCLUSION

PKG is allowed to be offline after sending the revocation list to KU-CSP.
User authentication is required every time during key-update between user and KU-CSP
Online feature are available which recover the limitation of existing system.

REFERANCES

[1]W.Aiello, S.Lodha, and R.Ostrovsky ,“Fast digital identity revocation, ”in Advance sin Cryptology (CRYPTO’98).New York, NY,USA: Springer, 1998, pp. 137–152.

[2] V.Goyal,“Certificate revocation using fine grained certificate space partitioning, ”in Financial Cryptography and Data Security,S.Dietrich and R. Dhamija, Eds. Berlin, Germany: Springer, 2007, vol. 4886, pp. 247–259.

