Identity-Based Encryption with Outsourced Cloud Revocation Authority

Mr. Mayur D. Waghmare[1], Prof. Sachin K. Korde[2]
[1, 2] Department of Computer Engineering
[1, 2] PREC, Loni.

Abstract- *Identity based encryption (IBE) is an public key cryptosystem and takes out the need of public key infrastructure (PKI)and certificate administration in ordinary public key settings. Because of the nonappearance of PKI, the revocation issue is a difficult issue in IBE settings. Various revocable IBE schemes have been proposed about this issue. By inserting an outsourcing computation system into IBE, Li et al. proposed a revocable IBE scheme with a KU-CSP (key-update cloud service provider) But, that scheme has two weaknesses. Initial one is that the computation and communication costs are higher than prior revocable IBE scheme and second is absence of versatility ie. lack of scalability means the KU-CSP must keep a secret value for every client. In this paper, we propose another revocable IBE scheme with a cloud revocation authority (CRA) to solve the above two shortcomings, namely, the performance is significantly improved and the CRA holds only a system secret for all the clients.*

Keywords- Encryption, authentication, cloud computing, outsourcing computation, revocation authority.

I. INTRODUCTION

Identity based public key system (ID-PKS) is an option for public key cryptography. ID-PKS setting eliminates the demands of public key infrastructure (PKI) and certificate administration in conventional public key settings. An IDPKS setting consists of trusted third party (i.e. private key generator, PKG) and a clients. The PKG is responsible to create every client's private key by utilizing the related ID data (e.g.name, email address, or government managed savings number). so, requirement of certificate and PKI are not necessary in the associated cryptographic mechanisms under ID-PKS settings. ID-based encryption (IBE) permits a sender to encrypt message straightforwardly by utilizing a receivers ID without checking the approval of validation of public key certificate. Appropriately the receiver uses the private key associated with her/his ID to decrypt such ciphertext. Since an public key setting needs to give a client provide a user revocation mechanism, the research issue on how to revoke misbehaving or compromised users in an ID-PKS setting is naturally raised. In routine public key settings, certificate revocation list (CRL) is a known revocation approach. In the CRL approach, if a gathering gets an public key and its related declaration, she/he first approves them and afterward turns upward the CRL to guarantee that people in general key has not been renounced. In such a case, the methodology requires the online help under PKI with the goal that it will bring about correspondence bottleneck. To enhance the execution, a few proficient revocation mechanism for public key settings, we have been considered for PKI.

II. RELATED WORK

D. Boneh and M. Franklin, To propose a completely useful identity based encryption scheme (IBE). The scheme has picked ciphertext security in the arbitrary prophet display expecting a variation of the computational Diffie Hellman is be conveyed so that the master key is never accessible in a solitary area. Dissimilar to normal edge frameworks, demonstrates that power for our conveyed PKG is free. [2]

Alexandra Boldyrev, Vipul Goyal, Virendra Kumar, proposed the most practical solution requires the senders to also use time periods when encrypting, and all the receivers to update their private keys regularly by contacting the trusted authority, this solution does not scale well as the number of users increases, the work on key updates becomes a bottleneck. So propose an IBE scheme that significantly improves key-update efficiency on the side of the trusted party (from linear to logarithmic in the number of users), while staying efficient for the users. This scheme builds on the ideas of the Fuzzy IBE primitive and binary tree data structure, and is provably secure.[6]

Yuh-Min Tseng and Tung-Tso Tsai Proposed a new revocable IBE scheme to remove the usage of secure channel between each user and the authority and use a public channel instead to transmit users periodic private keys. This scheme partitions a users private key into an identity key and a time update key. The initial secret key is fixed and unchanged, while the time update key is changed along with time. In the proposed RIBE, the PKG periodically generates new time update keys for non-revoked users, then the PKG sends them to users using a public channel. Non-revoked users update their own private keys, but the revoked users are unable to update their private keys because the PKG stops issuing the new time update keys of those revoked users. Issue, The key update efficiency is linear in the number of users so that the computation burden of PKG is still enormous. [7]

Jin Li , Jingwei Li, Xiaofeng Chen, Chunfu Jia and Wenjing Lou, Introduced an outsourcing calculation method into IBE to propose a revocable IBE scheme with a key-update cloud service provider (KU-CSP). This scheme offloads the vast majority of the key related operations amid key-issuing and key-upgrade procedures to a KU-CSP, leaving just a consistent number of basic operations for PKG and clients to perform locally. Propose a novel intrigue safe key issuing strategy: utilize a half and half private key for every client, in which an AND gate is included to connect and bound two sub-parts, to be specific 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. A short time later, so as to look after decryptability, unrevoked clients needs to occasionally ask for on key-update for time component called KU-CSP. [11]

III. EXISTING SYSTEM

More customers might want to store their information to PCS (public cloud servers) alongside the quick advancement of distributed computing. New security issues must be explained with a specific end goal to help more customers process their information in public cloud. At the point when the customer is confined to get to PCS, he will assign its intermediary to process his information and transfer them. Then again, remote information respectability checking is additionally a critical security issue in public cloud storage. It makes the customers check whether their outsourced data is kept intact without downloading the entire information/data.

- Identity Based Encryption (IB) is an intriguing other option to public key encryption, which is proposed to simplify key management in a certificate-based Public Key Infrastructure (PKI) by utilizing human understandable characters (e.g., one of a kind name, email address, IP address) as public keys.
- To proposed that users renew their private keys periodically and senders use the receivers identities concatenated with current time period.
- To Proposed a way for clients to occasionally renew their private keys without cooperating with PKG.

IV. PROBLEM STATEMENT

The Problem is to determine how to handle Remote Data Integrity Checking as well as isolate Anonymous & Anonymous Control User.

V. PROPOSED SYSTEM

Propose another revocable IBE Technique with a cloud revocation authority (CRA) to understand the two deficiencies in particular, computation and communication costs and lack of scalability. Present a cloud revocation authority CRA) to replace the part of the KU-CSP in Li et al's. scheme. The CRA just needs to hold a random secret value (master time key) for every one of the clients without influencing the security of revocable IBE conspire. The CRA utilizes the master time key to produce current time update key intermittently for each non-revoked client and sends it to the client by means of an public channel. It is apparent that our scheme tackles the unadaptability(un-scalability) issue of the KU-CSP.

A. Advantages :

Compared with the past work, our scheme does not need to re-issue the entire private keys, however simply need to update a lightweight segment .

- In order to solve both the un-scalability and the inefficiency we will propose a new revocable IBE scheme with cloud revocation authority (CRA).
- With the aid of CRA, 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 CRA.
- No secure channel or user authentication is required during key-update between user and CRA.
- Finally, To provide extensive experimental results to demonstrate the efficiency of our proposed construction.

VI. SYSTEM ARCHITECTURE

Our system has three roles, namely, a private key generator (PKG), a cloud revocation authority (CRA) and users (senders and receivers). In our revocable IBE scheme, we employ a cloud revocation authority (CRA) to perform user revocation. The CRA in our scheme holds only one master time key for all the users. The PKG selects a master secret key, a master time key and a total number of periods, and sends the master time key to the CRA. The PKG uses the master secret key to compute the identity key of the user with identity, and sends the identity key to the user via a secure channel. On the other hand, the CRA is responsible to produce the time update keys for all the non-revoked users by using the master time key When a sender wants to transmit a message to a receiver with identity at period i, the sender produces a ciphertext and sends it to the receiver, Upon receiving the ciphertext, the receiver uses the identity key and time update key to decrypt the ciphertext. The following diagram show that the system architecture.

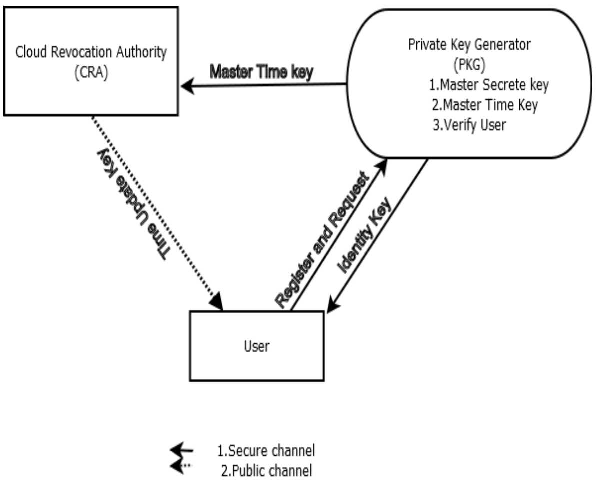


Figure 1. Shows that the System Architecture

A. Modules :

1. Original Client Module
2. Public Cloud Server Module
3. Proxy Module
4. Key Generation Center (KGC)

1. Original Client Module :

An element, which has massive data to be uploaded to PCS by the delegated proxy, can perform the remote data integrity checking.

2. Public Cloud Server Module :

An entity, which is managed by cloud service provider, has significant storage space and computation resource to maintain the clients data.

3. Proxy Module :

Receive all files from the data owner and store all files. Check the data integrity in the cloud and inform to end user about the data integrity. Send request to PKG to Update the private key of the user based on the date parameter (Give some date to update Private Key). List all files, List all updated Private Key details based on the date and users, List all File attackers and File Receive Attackers.

4. Key Generation Center (KGC) Module :

An element, while getting a identity, it creates the private key which corresponds to the received identity.

B. Algorithm :

The AES and DES algorithm are used for encryption and decryption.

Encryption:

Encryption means convert plain text into cipher text. AES algorithm for encryptions as follows.

Input:

- Encryption object as follows,

Encrytedstring ->NULL
Secret key->key

- Literal type as follows,

Byte plaintext, encrypted Text

Output:

1. START
2. Init -> (ENCRYPT MODE, key)
3. Plaintext --> UNICODE FORMAT
4. EncryptedText - do Final (plaintext)
5. EncryptedString-> Base64.encodeBase64 (encryptedText)
6. Return encrypted String.

Decryption:

Decryptions are used to decrypt the message. Convert the cipher text into plain text .

Input:

- Decryption object as follows,

Decrypted String -> NULL
Secret Key -> key

- Literal type as follows,

Byte cipher text, decrypted Text

Output:

1) START
2) Init - (DECRYPT MODE, key)
3) Ciphertext - UNICODE FORMAT
4) DecryptedText - doFinal(ciphertext)
5) DecryptedString - Base64.encodeBase64 (decryptedText)
6) Return decrypted String.

C. Mathematical Model :

a) Uploading file:

U (Z) = {u1, u2,u3......un}
F (Z) = {f1, f2,f3.......fn}
S (Z) = {s1, s2,s3......sn}
MAC (Z) = {m1,m2,m3....mn}
D (Z) = {d1, d2,d3......dn}

Where
U (Z): Total number of users.
F (Z): Total number of files.
S (Z): Total number of secret key.
MAC (Z): Master key.
D (Z): Total data

U (Z) U F(Z): S(Z) U MAC(Z)

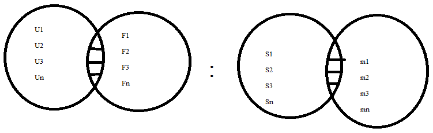


Figure 2. Uploading files

b) Downloading Files :

U (Z) U S(Z) U MAC(Z) : D(Z)

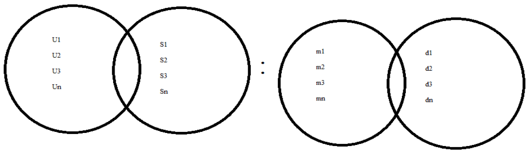


Figure 3. Downloading files

Success Condition :

Properly Maintain key

Failure Condition:

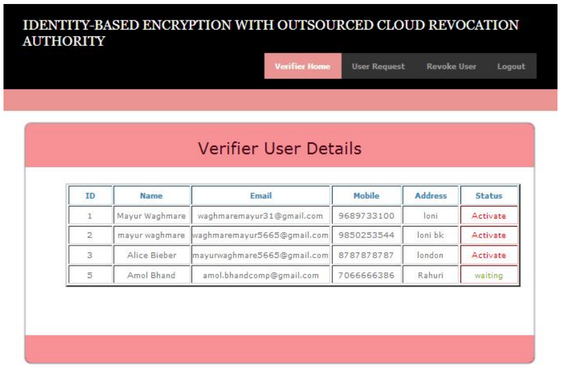
Anonymous User & Anonymous-F User Maintain Authorization.

VII. RESULTS AND DISCUSSIONS

Steps for using System:

1. At first time user has to make registration.

2. Registration request are send to PKG(Private key Generator) for user verification. After verification user account make as Activated, then only user can login and send message to another user.

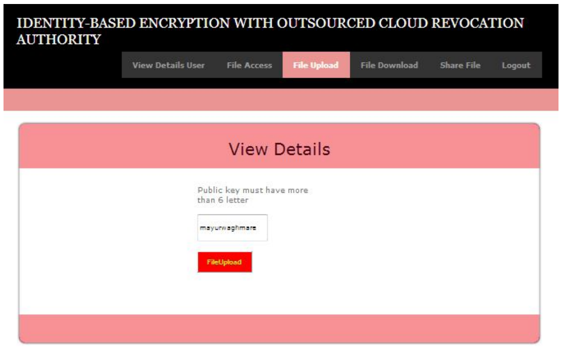

IDENTITY-BASED ENCRYPTION WITH OUTSOURCED CLOUD REVOCATION AUTHORITY

Verifier User Details

ID	Name	Email	Mobile	Address	Status
1	Mayur Waghmare	waghmaremayur31@gmail.com	9689733100	loni	Activate
2	mayur waghmare	waghmaremayur5665@gmail.com	9850253544	loni bk	Activate
3	Alice Bieber	mayurwaghmare5665@gmail.com	8787878787	london	Activate
5	Amol Bhand	amol.bhandcomp@gmail.com	7066666386	Rahuri	waiting

Figure 3.

3. After successfully login user can upload and encrypt file using identity.


IDENTITY-BASED ENCRYPTION WITH OUTSOURCED CLOUD REVOCATION AUTHORITY

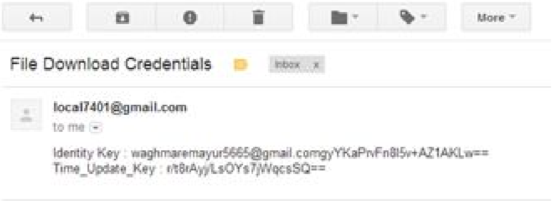
View Details

Public key must have more than 6 letter

mayurwaghmare

Figure 4.

4. Next step is that, sender share or send message to receiver. This share request is send to PKG, after verify PKG generate identity key and this share request is also forwarded to CRA for generating Time update key and these both keys are sending to receiver via email. for downloading and decryption message.

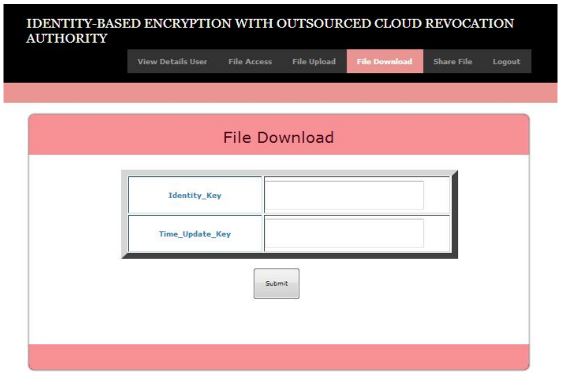


File Download Credentials

local7401@gmail.com
to me

Identity Key : waghmaremayur5665@gmail.comgyYKaPvFn8I5v+AZ1AKLw==
Time_Update_Key : r/t8rAyj/LsOYs7jWqcsSQ==

Figure 5.

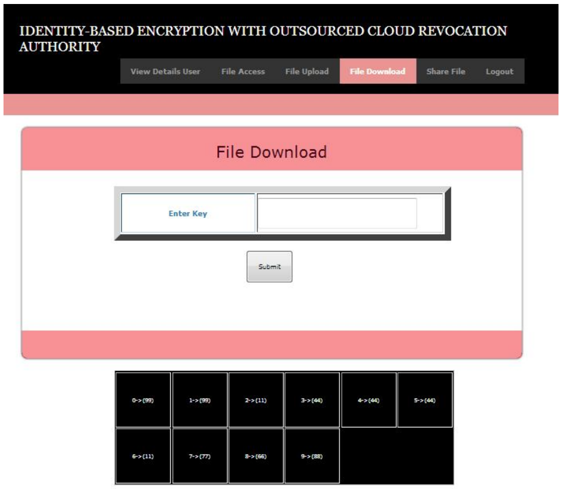


File Download

Identity_Key	
Time_Update_Key	

Figure 6.

5. If receiver insert correct Identity key and Time update key then system provide another security mechanism ie. OTP for download message, otherwise user will be revoke.
6. This OTP has dynamic value in system, user has to carefully insert the corrected value regarding this OTP. This value for OTP is not fixed in system they are dynamic for every user at every time.



File Download

Enter Key	

0->(99)	1->(99)	2->(11)	3->(44)	4->(44)	5->(44)
6->(11)	7->(77)	8->(66)	9->(88)		

Figure 7.

Table 1.

Parameter	**Li**'s scheme	**Tseng's** scheme	**Proposed** scheme
Computational cost for time update key	9.1(ms)	5.6(ms)	**4.9(ms)**
No of keys store in cloud authority	**n**	**1**	**1**
Computational cost for encryption	0.446(s)	0.643(s)	**0.58(s)**
Computational cost for decryption	1.176(s)	0.26 (s)	**0.22(s)**
Bit length of ciphertext	**512byte**	**168byte**	**64byte**

VIII. CONCLUSION

Finally conclude that So many existing system is available to handle Identity scheme but, as per CRA technique how auto update PKG of master key as well as identity key. A new revocable IBE scheme with a cloud revocation authority (CRA), in which the revocation procedure is performed by the CRA to alleviate the load of the PKG. Finally, based on the proposed revocable IBE scheme with CRA, we constructed a CRA aided authentication scheme with period-limited privileges for managing a large number of various cloud services.

REFERENCES

[1] A. Shamir, Identity-based cryptosystems and signature schemes, Proc. Crypto84, LNCS, vol. 196, pp. 47-53, 1984.

[2] D. Boneh and M. Franklin, Identity-based encryption from the weil pairing, Proc. Crypto01, LNCS, vol. 2139, pp. 213-229, 2001

[3] R. Housley, W. Polk, W. Ford, and D. Solo, Internet X.509 public key infrastructure certificate and certificate revocation list (CRL) profile, IETF, RFC 3280, 2002.

[4] W. Aiello, S. Lodha, and R. Ostrovsky, Fast digital identity revocation, Proc. Crypto98, LNCS, vol. 1462, pp. 137-152, 1998.

[5] M. Naor and K. Nissim, Certificate revocation and certificate update, IEEE Journal on Selected Areas in Communications, vol.18 , no. 4, pp.561 - 570, 2000.

[6] A. Boldyreva, V. Goyal, and V. Kumar, Identity-based encryption with efficient revocation, Proc. CCS08, pp. 417-426, 2008.

[7] Y.-M. Tseng. and T.-T. Tsai, Efficient revocable ID-based encryption with a public channel, Computer Journal, vol.55, no.4, pp. 475-486, 2012.

[8] V. Goyal, Certificate revocation using fine grained certificate spmaster partitioning, Proc. Financial Cryptography, LNCS, vol. 4886,pp.247-259,2007.

[9] D. Boneh, X. Ding, G. Tsudik, and C.-M. Wong, A Method for fast revocation of public key certificates and security capabilities, Proc.10th USENIX Security Symp., pp. 297-310. 2001.

[10] X. Ding and G. Tsudik, Simple identity-based cryptography with mediated RSA, Proc. CT-RSA03, LNCS, vol. 2612, pp. 193-210,2003

[11] J. Li, J. Li, X. Chen, C. Jia, and W. Lou, Identity-based encryption with outsourced revocation in cloud computing, IEEE Trans. On Computers, vol. 64, no. 2, pp. 425-437, 2015.

[12] Yuh-Min Tseng, Tung-Tso Tsai, Sen-Shan Huang, and Chung-Peng Huang Identity-Based Encryption with Cloud Revocation Authority and Its Applications IEEE TRANS. CLOUD COMPUTING, VOL.pp , NO., 2016