International Journal of Emerging Trends & Technology in Computer Science (IJETTCS)
Web Site: www.ijettcs.org Email: editor@ijettcs.org
Volume 6, Issue 4, July- August 2017 ISSN 2278-6856

EFFICIENT REVOCATION AND SECURED DATA ACCESS CONTROL IN CLOUD

[1]P.NAGA USHA SREE,[2]P.N.V.S PAVAN KUMAR

[1]PG Student, Computer Science and Engineering Dept, GPREC, Kurnool (District), Andhra Pradesh-518004, INDIA.

[2] Assistant Professor, Computer Science and Engineering Dept, GPREC, Kurnool (District), Andhra Pradesh-518004, INDIA.

Abstract

Identity -Based Encryption (IBE) is an interesting and foremost replacement for Public Key Infrastructure (PKI). Public Key Encryption and Certificate organization will be normalized using IBE. Due to this absence of PKI, revocation problem will be raised in IBE settings. To solve this problem, many IBE schemes have been proposed. One of the IBE scheme that is proposed with Key Update Cloud Service Provider (KU-CSP) by employing outsourced computation method into IBE. Some of the drawbacks of this scheme are computation and communication costs which are more than the previous proposed revocable schemes. It has another drawback that is inefficiency and lack of scalability because KU-CSP must keep a secret value for each user. During user revocation, the overhead computation occurs at Private Key Generator (PKG) which is the major drawback of this IBE. So, an IBE scheme is proposed with Cloud Revocation Authority (CRA), in which the revocation process can be done by CRA, to deduce the load of the PKG. To solve these shortcomings, where CRA holds only one master key for all users.So that more security will be provided and the performance will be significantly improved and increased. The proposed scheme will be extended with multiple CRAs and multiple PKGs to reduce the load.

Keywords: Identity Based Encryption, Outsourced, Revocation, Authority,Cloud Revocation Authority , Private key Generator

1. INTRODUCTION

Identity based Public Key System Encryption (ID-PKS) is a significant alternative to Public key Cryptography. It is proposed to make the public key management and certificate organization easier in Public Key Infrastructure. Identity Based Encryption is an attractive way to public key Encryption in which it eradicates the necessity of Public Key Infrastructure (PKI). IBE is completely based upon the human identities (like Email, Unique name, IP address etc). It uses the user's identities as Public keys. ID-PKS consists of users and a third party called PKG. Private Key Generator is responsible to generate the private keys for users by using corresponding identities. There will be no need of PKI's system in ID-PK systems

User needs to convert the message/data into cipher text by using public key of receiver without checking the certificates of the users. Public key of a receiver may be the email, IP address, unique name etc. There is no need for a user to look for the certificate and public keys and due the absence of PKI, revocation problem will raise. In PKI, if a user gets public key , he/she used to validate in Certificate Revocation List (CRL)whether if the user public key is revoked or not. But, in IBE settings, this process is not required. Identity Based Encryption found to use in Email encryption, Web applications, Electronic Voting, Mobile Phone Calls.

This paper proposes a identity based encryption scheme for efficient revocation and for secure data and they are organized as follows. Section I gives an Introduction. Section II gives the Related work .Section III provides the Architecture. Section IV describes Implementation and Results and Section V describes comparison of various IBE schemes and Section VI Security notations and Section VII concludes the paper with Conclusion and Future Enhancements

2. RELATED WORK

Shamir [1] introduce an Identity based cryptographic scheme, which has a pair of users to communicate securely without verifying the signatures, issuing certificates, exchanging private or public keys, keeping key directories and not using the services of a thirdparty and only have Key Generator.
Girish[2] discuss the comparison of traditional Public Key Infrastructure (PKI) and Identity based Cryptography(IBC), in which it proves the advantages of IBC over PKI.

Boneh [3] introduced a fully functional identity-based encryption scheme (IBE) based upon Weil pairing. It assumes a variant of the computational Diffie Hellman problem that has Chosen cipher text security in the random oracle model. The Weil pairing is an example of a bilinear map between groups. In this scheme, a process is proposed in which each user should get a private key from PKGand PKG need a secure channel to transfer the keys to the users and this will produce some additional load on PKG. To revoke users, PKG should stop issuing keys to that particular user.

To reduce the load on the PKG, Boneh proposed a method called Immediate Revocation method. It includes online authority that will assist the load of the PKG and decrypt the cipher text. If the user is revoked, then authority will stop to issue the keys to the particular user.

Boldyreva[4] proposed the most prominent solution that the senders needs to use time periods during encrypting, and allthe receivers (regardless of whether their keys have been misbehaving or not) to update their private keys regularly by consulting the trusted authority. But this solution does not perform well because as the number of user's increases, the key updates of various users also increases. So, it becomes a bottleneck .So, an IBE scheme is proposed that increases effectiveness of the key-updates on the side of the trusted party to the users. This scheme is constructed on the ideas of the Fuzzy IBE and binary tree data structure which is probably secure.

This revocable IBE scheme is based on the concept of the Fuzzy IBE [5] and which takes the complete sub tree method to reduce the number of key updates from linear to logarithmic for the number of users and by using the binary tree data structure, the scheme efficiently alleviates the key-update load of the PKG. Some IBE and HIBE[6][7][8][9][10][11] schemes are proposed in this schema, but these schemes used sub tree to reduce the updates from logarithmic for the users and it uses secure channel for transmission of the private keys to the users.

In all schemes, no other authority will share the responsibility of user revocation. In Tseng and Tsai's propose a revocable IBE scheme [12], in which a public channel will be used instead of secure channel to transmit the private keys to the users. User's private key consists of two component keys one is an identity key and another one is time update key where as an identity key is fixed and time update key will change depending upon time periods. In order to alleviate the load of the PKG, Li *et al.*[13] employed a key update cloud service provider (KU-CSP) to share the responsibilityof user revocation.

Wherever, one of the main problems of IBE is the overhead computation at Private Key Generator (PKG) during user revocation. An outsourcing computation of IBE revocation scheme is a proposed to deduce all the key generation related operations like key-issuing and key-update and leaving only a consistent number of normal and elementary operations for PKG and eligible users to perform locally. There are several existing schemes which are based upon the concept called Attribute Based Encryption (ABE). In this context, this particular scheme uses attributes sets for encrypting data and uses attributes keys with the access structures for decrypting the data. Several ABE schemes are proposed which are completely based on the binary tree for reissuing and uses a secure channel to transmit the user's keys

3. .ARCHITECTURE OF PROPOSED SYSTEM

This section will explain the complete architecture of the proposed system.

3.1 Basic Concepts

Bilinear pairings [15] and notations are needed to build the proposed revocable scheme.

3.1.1 Bilinear Pairings

Let A, M are two cyclic groups. A be the additive cyclic group and M is Multiplicative cyclic group of same order and P be the generator of A

The mapping e: A, M be admissible map when it possesses three properties:

1) Bilinearity : e(aP, bQ)= e(P,Q)abwhere a,b belongs to Z and P,Q belongs to A.
2) Non degeneracy:e(P,P)is not equal to 1
3) Computable: 'e' be calculated in significant manner.

3.1.2 Hypothesis

Decisional Bilinear Diffie-Hellman (DBDH) problem:

Let A, M are two cyclic groups and P be the generator of A. Let e be the mapping that is A X A maps to M .The problem exists in mapping (A, M, e) where P,aP, bP,cP belongs to A and any values like a,b,c belongs to Z and T may be any value belongs to M if declare $T=e(P,P)^{abc}$

3.1.3 DBDH Notation

The notion exists in <A,M,e> where any polynomial time algorithm may solve DBDH problem with some advantage.

Polynomial-time algorithm.

Polynomial time algorithm is an algorithm in which the no of steps taken for running an algorithm is completely depends upon the size of the input in which it may be a negligible integer and nonnegative integer. The polynomial time is the time taken by computer system and calculations like additions, multiplication and other mathematical operations can be performed in polynomial time These algorithms may be applied only to small systems. It does not depend upon large scale machines. By contrast, demonstration of computers could exactly motivate chemical reactions in polynomial time. This algorithm explicitly motivates all electron-nuclear and interelectronic interactions exactly in time.

3.2System Overview

In this system, the data owner wants to store file in the cloud. User needs a identity key from third party generator so that he/she can access he/her home. It can generate the private keys by using receiver identities. By using the private key only user can upload to file. The uploaded file is in the encrypted form .If any other user wants to download a file then he/she needs a time update key.

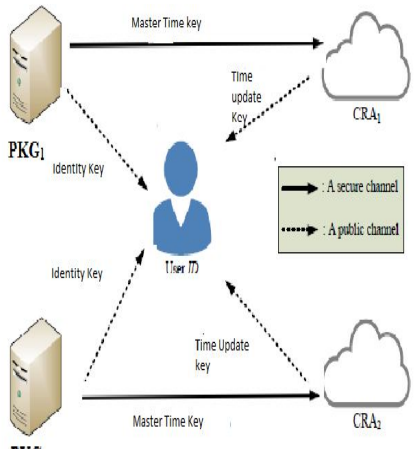

Fig 1 Architecture of the ProposedSystem

Time update keys will be send to the user mails by CRA on the request of PKG. Finally, by using time update keys the user can download the files.In this scheme, CRA can revoke the misbehaving users and activate the users Revocation and Activation procedure completely depends upon the CRA.

This scheme consists of two CRAs and two PKGs .User has a choice to choose any CRA and should choose corresponding PKG. The proposed scheme possesses the advantages of various IBE schemes. The proposed system will present the structure of our revocable IBE scheme with CRA and explain its security notions to model feasible threats and attacks. It solves both the un-scalability and the inefficiency.

3.3Modules

There are some modules in this scheme. Lets us mention about them

Cloud Revocation Authority

Computation and communication costs are more in previouslyproposed IBE schemes than our scheme. The other drawback is unscalability because that the KU-CSP is needed to keep a secret value for each user. To eradicate these problems, a new authority which is named as Cloud Revocation Authority (CRA) is proposed. So that the performance is significantly improved and the CRA holds a one only one master key for all the users.

b)Private Key Generator:

This is third party generator which is used to generate the private keys that are identity keys and time updates keys. It generates these keys by using master time keys and master secret keys. Multiple CRA's and PKG's will be used to reduce the load when there are more number of users..

3.4 Algorithms

The Proposed IBE scheme consists of five Algorithms[14]. These algorithms are mentioned below

System set up Algorithm

This is an algorithm which is performed by the PKG and it takes secret parameter and time periods and returns master secret key with itself and secret time key to CRA.

START:
- Let S be the Secret parameter and T be the time Period
- It outputs time key be the Master Secret Key A and Master Key B

END:

Identity Key Algorithm

This is an algorithm performed by PKG and takes master secret key and receivers as inputs and return identity key.

START:
- Random s = new Random()
- int a = s.nextInt() +any number;
- System.out.print(a);
- return a

END:

Time key update Algorithm

This is an algorithm which is performed by the CRA and uses the master time key and user's identity and a periodto compute the user's time update keyfor that period and CRA returns the time update keyto the user via a public channel (e.g. e-mail).

START:
- ResultSetrs
- String email
- If rs.next()
- String time=rs.get String(time)
- String tkey=new.TripleDes().encrypt(time)
- Http session timekey=request.getsession(true)
- timekey.setAttribute(tkey)
- timekey.setAttribute(fname)
- new mailSender.Sendmail(mail, tkey)

END:

Encryption Algorithm

Encryption is algorithm which is performed by a user. The user takes message, a receiver's identity and a current period i as input and gives a cipher text .

START:
function encrypt(String unencryptedString)

- String encryptedString := NIL

try

- cipher.init(Cipher.ENCRYPT_MODE, key)
- plainText := unencryptedString.getBytes(UNICODE_FORMAT)
- encryptedText := cipher.doFinal(plainText)
- encryptedString := new String(Base64.encodeBase64(encryptedText))

catch (Exception e)
e.printStackTrace()
returnencryptedString
END:

Decryption Algorithm

Decryption is an algorithm which is performed by a user. User takes ciphertext and the private keys consists of identity key and time update keys as inputs and outputs the corresponding plaintext .

START :
function decrypt(String encryptedString)

- String decryptedText := NIL

try

- cipher.init(Cipher.DECRYPT_MODE, key)
- encryptedText=Base64.decodeBase64(encryptedString)
- plainText := cipher.doFinal(encryptedText)
- decryptedText := new String(plainText)

catch (Exception e)
e.printStackTrace()
returndecryptedText

END:

4. IMPLEMENTATION AND RESULTS

In this section, the implementation of how IBE can be done and the results of implementation will be presented.

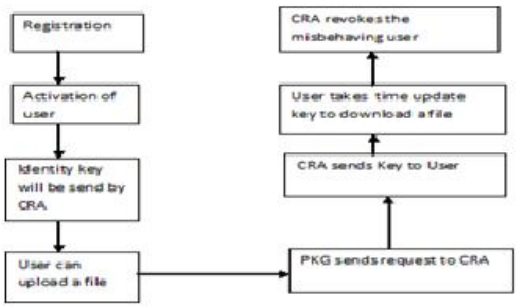

Fig 2: Overview of Implementation

The above figure will represents overall implementation process and various procedure

In registration process, user get registered and obtain user name and password but cannot access even after registration. For login, activation of user should be done.

The activation of user can be done by CRA. For the activation of user, he/she should login in CRA and CRA can activate the user. After activation, if user wants to upload and to view his/her home, user needs a private key called identity key. To get an identity key, he/she should login into PKG

After login into PKG, the PKG will send identity key to user mail and by using identity key. The user makes use of that key and can access login into his/her home.

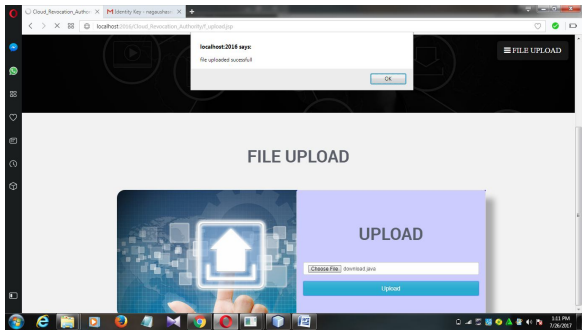

Fig 3:. File Upload

File can be uploaded by the user.

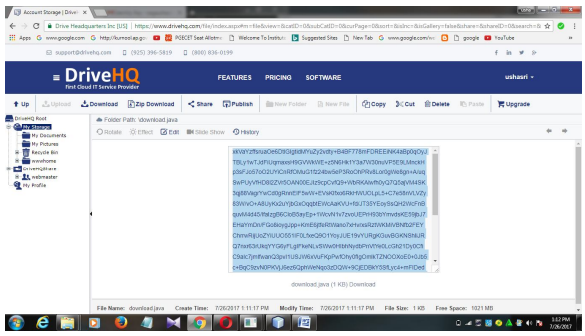

Fig 4: Storage of Encrypted file

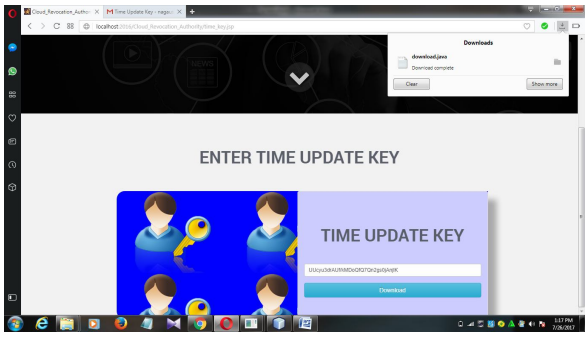

Fig 5: Downloading of file

The file can be stored in encrypted form. User requires time update key for downloading the file and for this PKG send master time key request to CRA. After getting request from PKG, CRA sends the time update key to user mail.

Time update Key will be sent to mail and by entering the time update key the user can download the file. Revocation is the main process in IBE and the Cloud Revocation Authority (CRA) is main responsible for this process and it can revoke the misbehaving user .User can download the files and see the details of downloaded files.

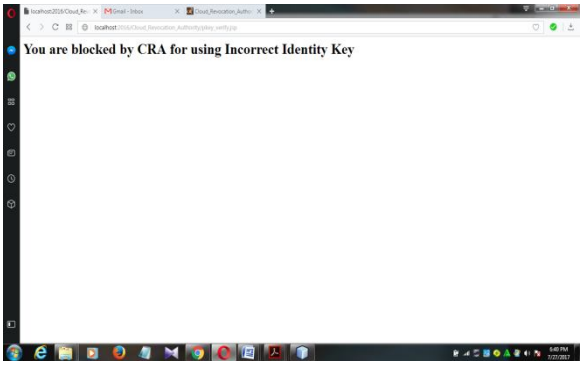

Fig 6: Revocation Process

5. COMPARISON OF VARIOUS IBE SCHEMES

Severalcomparisons are made on different IBE schemes. Table1 mentioned below will describe various comparisons of our scheme. The channels which are used in these all schemes are the Public channels. Public channel which is used in these schemes will be EMAIL. In Tseng scheme, outsourcing computation will not done by other authority and the computation will be completely done by only PKG.So, the load the on the PKG will be more in Tseng scheme than other two schemes .But in Lie and our scheme the computation will be outsourced to third party authority .In these two schemes, many secret time keys are used to generate time update keys in which each user needs one time key to generate their time update keys. But in our scheme, only one master time key will be required to generate time update keys of all users. So, scalability of our scheme is established.

The figure 5.1 shows that cost of computation for key update is more in Li scheme than this scheme

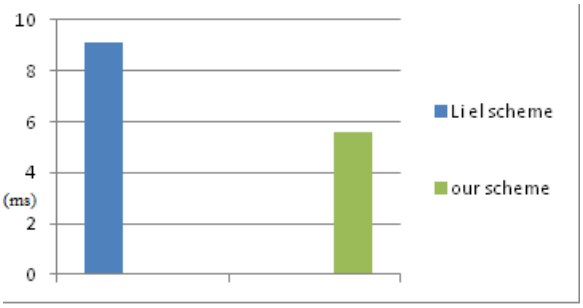

Fig 7: Cost for time update for both schemes

The Figure 5.2 will show that computation encryption for cost is more in ourscheme and computation for decryptioncost will be less in this scheme

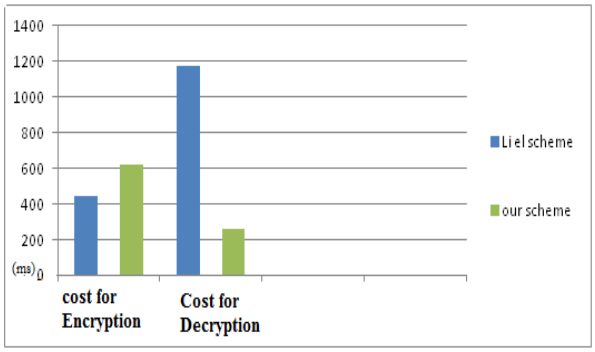

Fig 8: Comparison of Encryption and Decryption cost in both schemes

Table 1 Comparison of All Schemes

	Tseng and Tsai scheme	Li el at scheme	Our scheme
Key issue channel	Public channel	Public channel	Public channel
Outsourced computation to authority	No	Yes	Yes
Work load on PKG	High	Low	Low
No of master time keys	N	N	1
Scalability of authority	No support	Un scalability	Yes

6. SECURITY NOTIONS

This scheme is more secure under attacks because of decisional bilinear Diffie Hellman notion .CRA holds two types Adversaries.

a) Type 1 Adversary (Inside revoke user):

The CRA authority has a right to revoke the user at any time period. User has a unique identity key and time update keys and time update key may be changed at every time.

b) Type 2 Adversary (outside revoke user):

In this type, User can get the unique identity key and time update key which change at relevant time periods .CRA computes time update keys for all users. If this adversary triesto attack a user home and then CRA will block the misbehaving user.

7.CONCLUSION AND FUTURE ENHANCEMENTS

In this paper, identity based encryption scheme is proposed for efficient revocation and data access control. Previously proposed IBE scheme became inefficient because of more load on PKG and has several secret keys for many users which lead to un-scalability. In this context, an IBE scheme with Cloud Revocation Authority (CRA) is

proposed in which CRA hold one master key to produce time update keys. Multiple CRA's and PKG's are used in this proposed system to reduce the load. For future enhancements, this IBE scheme will become more secure if PKG generates new identity keys at each time when user wants to access his/her home and this extended scheme should reduce the computational cost of encryption.

REFERENCES

[1]. A. Shamir, "Identity-based cryptosystems and signature schemes," Proc. Crypto'84, LNCS, vol. 196, pp. 47-53, 1984.
[2]. Girish and Phaneedra H.D "iIdentity-Based Cryptography and Comparison withtraditional Public key Encryption: A Survey"
[3]. D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," Proc. Crypto'01, LNCS, vol. 2139, pp. 213-229, 2001.
[4]. A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryptionwith efficient revocation," Proc. CCS'08, pp. 417-426, 2008.
[5]. A. Sahai and B. Waters, "Fuzzy identity-based encryption," Proc.Eurocrypt'05, LNCS, vol. 3494, pp. 557-557, 2005.
[6]. J.-H. Seo and K. Emura, "Revocable identity-based encryption revisited: security model and construction," Proc. PKC'13, LNCS, vol. 7778, pp. 216-234, 2013.
[7]. S. Park, K. Lee, and D.H. Lee, "New constructions of revocable identity-based encryption from multilinear maps," IEEE Transactions on Information Forensics and Security, vol.10 , no. 8, pp. 1564 - 1577, 2015.
[8]. C. Wang, Y. Li, X. Xia, and K. Zheng, "An efficient and provable secure revocable identity-based encryption scheme," PLoS ONE, vol. 9, no. 9, article: e106925, 2014.
[9]. A. Lewko A and B. Waters, "New techniques for dual system encryption and fully secure hibe with short ciphertexts," Proc. TCC'10, LNCS, vol. 5978, pp. 455-479, 2010.
[10]. J.-H. Seo and K. Emura, "Efficient delegation of key generation and revocation functionalities in identity-based encryption," Proc. CT-RSA'13, LNCS, vol. 7779, pp. 343-358, 2013.
[11]. J.-H. Seo and K. Emura, "Revocable hierarchical identity-based encryption: history-free update, security against insiders, and short Ciphertexts," Proc. CT-RSA'15, LNCS, vol. 9048, pp. 106-123, 2015.
[12]. Y.-M. Tseng.and T.-T. Tsai, "Efficient revocable ID-based encryptionwith a public channel," Computer Journal, vol.55, no.4, pp.475-486, 2012.
[13]. J. Li, J. Li, X. Chen, C. Jia, and W. Lou, "Identity-based encryption with outsourced revocation in cloud computing," IEEE Trans. onComputers, vol. 64, no. 2, pp. 425-437, 2015.
[14]. Girish, Subhash Kumar Gupta, Dr. H. D. Phaneendra"Identity Based Encryption Outsourced Revocation forGroup Data Sharing Via Cloud"
[15]. S. Galbraith, K. Paterson, and N. P. Smart, "Pairings for cryptographers," Discrete Applied Mathematics, vol. 156, no. 16, pp. 3113-3121, 2008..

AUTHOR

P.Nagaushasreewas born in Andhra Pradesh, India. She received the B.Tech Degree in Computer Science and Engineering from Jawaharlal Nehru Technological University Anantapur branch, India in 2015 and M.Tech Degree also in same the branch and University. Her research interests are in the area of Data Security in Cloud computing Techniques

P.N.V.S. Pavan Kumar M.Tech[Ph.D], was born in Andhra Pradesh, India. He is working as Assistant Professor .in Computer Science & Engineering Dept, GPREC Kurnool (district),A.P.518007,INDIA. His research interests are in the areas of Big data.