‘‘Identity Based cryptography with Outsourced Revocation in cloud computing for Feedback Management System for Educational Institutes’’

Mr. Butkar Umakant Dinkar
Miss.Kanchan S.Gade. Miss.Rohini K.Gaikwad.
Miss.Karishma V.Kadam Miss.Kirti D. Tarate.

ABSTRACT

IBE which simplifies public key and certificate management at Public Key Infrastructure (PKI) .Identity Based Encryption scheme is best to the public key encryption. One of the main Disadvantage of Identity Based Encryption (IBE) is overhead computation at private key generator during user revocation. In Proposed system use outsourcing computation in IBE and propose a revocable IBE scheme in server aided Our proposed scheme offload key generation related operations during key issuing and key updating using Key update cloud service provider (KU-CSP).using Constant number of calculation. This gaol achieve by utilizing novel collusion resistance technique. We generate private key for every user and use AND logic to connect identity component and time component. Propose another construction which provable secure under the recently formalized referenced Delegation of computation model.

Keywords:-*IBE, Cloud computing, revocation, outsourcing,Authentication.*

1.INTRODUCTION:

IBE scheme is a best alternative to the public key encryption. In IBE scheme use human intelligible as Identities such as use the user’s unique name, email address and IP address as public key. Sender uses IBE scheme does not need look up public key, but directly encrypt the message with receiver identities as public key and generator private key based on identities , receiver take the private key from private key generator and decrypt the message. In revocation technique are used in the IBE scheme to secure sensitive data from unrevoked user. Revocation every user can see data but it cannot update the information only revoked person can update the data. First time use outsourcing in the IBE scheme in outsourcing we can update the data, delete data, and download the data based on their identities .Introducing the cloud services into IBE scheme revocation to fix the efficiency and storage overhead. AND logic is used to connect the identity component and time component. Cloud computing is also known as on demand computing. Cloud provide the services and share the resources to the user.it provides three types of services Infrastructure as service (IaaS),Platform as services (PaaS),Software as services (SaaS). In our proposed System we use key Update cloud Service Provider (KU-CSP) to provide the infrastructure as service, KU-CSP provides the raw materials of cloud computing like processing, storage and hardware resources in virtual manner in via internet. During the key update PKG is offline that means PKG is offline after sending revocation list to the KU-CSP. The KU-CSP store list of all file and also the list of all user in the cloud.

2.LITERATURE SURVEY

- W. Lou etcatal [2] presents as cloud computing becomes prevalent, more and more sensitive data is centralized into cloud for sharing, which brings new challenges for outsourced data security and privacy. Attribute based encryption (ABE) is best cryptographic primitive for designing the fine-grained access control. ABE is criticized being as the computational cost grows with the complexity of the access formula. The drawback is more serious for mobile devices because they have constrained computing resources.
- K. B. Frikken [6], presents Use linear algebra techniques in this system but disadvantage of this system is time complexity the number of user increases the it is difficult to maintain private key size.
- D. Vergnaud [7] presents that Identity-Based Encryption (IBE) offers a best alternative to PKI-enabled encryption as it eliminates the need for digital certificates. The most convenient one was to augment identities with period of the numbers at encryption. It is used only for selective id .This scheme has disadvantage of

bottleneck.

- V. Kumar [9] presents the new scheme based on fuzzy IBE scheme but use binary tree data structure to records user's identities at leaf nodes. PKG has to generate the key for all the nodes on the path from the based on 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. The size of private key increases in logarithmic in the number of users in system, which makes it difficult in private key storage for users. As the number of users in system grows, PKG has to maintain a binary tree with a large amount of nodes, which introduces another bottleneck for the global system.
- Franklin [14] presents 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 their identities and update new private keys. 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

3.EXISTING SYSTEM:

There exists g1, g2 ∈ G with e(g1, g2) 1, in other words, the map does not send all pairs in G×G to the identity in GT. Upon receiving a key update request on ID, KU-CSP firstly checks whether ID exists in the revocation list RL, if so KU-CSP returns ⊥ and key-update is aborted.In RDoC model, the client is able to interact with multiple servers and it has a right output as long as there exists one server that follows the proposed protocol. One of the most advantages of RDoC over traditional model with single server is that the security risk on the single server is reduced to multiple servers involved in. As the result of both the practicality and utility, RDoC model recently has been widely utilized in the literature of outsourced computation.Identity-Based Encryption (IBE) is an interesting alternative to public key encryption, which is proposed to simplify key management in a certificate-based Public Key Infrastructure (PKI) by using human-intelligible identities (e.g., unique name, email address, IP address, etc) as public keys.

- Boneh and Franklin suggested that users renew their private keys periodically and senders use the receivers' identities concatenated with current time period.

- Hanaoka et al proposed a way for users to periodically renew their private keys without interacting with PKG

- Lin et al. proposed a space efficient revocable IBE mechanism from non-monotonic Attribute-Based Encryption (ABE), but their construction requires times bilinear pairing operations for a single decryption where is the number of revoked users.

4.PROPOSED SYSTEM:

Our proposed system first time introduces outsourcing reckoning into IBE revocation, and formalizes the security definition of outsourced revocable IBE. Our recommend a scheme offload all the key cohort related operations during the time of issuing and update the key, remaining only a simple operation for the PKG and authorised users based on their identity. In our scheme, as with the idea, we realize revocation through updating the private keys of the unrevoked users. But unlike that work which takes time period with identity based component for key generation/update and requires re-issuing the whole private key for unrevoked users, proposing a novel collusion-resistant key issuing technique. In Our propose scheme use AND logic connect two sub-components are date and identity respectively. User first able to obtain the identity component and a default time component from PKG and issue private key based on their identity.In our scheme, as with the suggestion, 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).

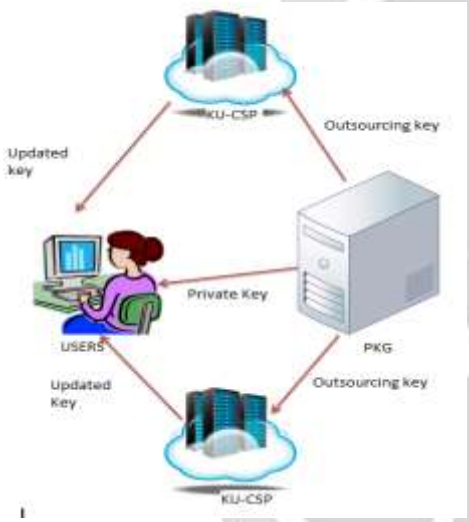
5.ADVANTAGE

- There are only a finite number of users, after all users have been issued with keys the third party's secret can be destroyed.
- Revocation mechanism used
- Provide facility for Key updation
- No secure channel or user authentication is required during key-update between user and KU-CSP.
- Reduce overhead of key computation.
- Make OTP is private.

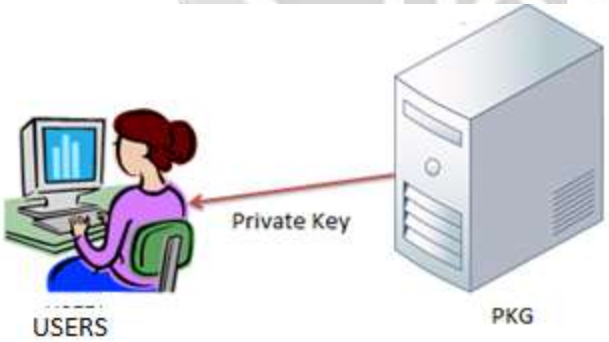
6.PROBLEM STATEMENT

The problem is to determine serious issue of identity revocation. Proposed scheme present outsourcing computation into IBE and recommend revocable scheme in which revocable operation delegated to CSP. Achieve the constant efficiency at both the sides.

7.SYSTEM ARCHITECTURE



8.SYSTEM MODULES:



Four modules in the system architecture are as follows.

1. **Data Owner:**

First User registers with unique name on cloud server and login based on their unique name. After login send request to Private Key generator (PKG) to generate IBE Key based on unique name. Browse file and request Private Key to encrypt the data, Upload data on cloud. Verify the data from the cloud by SHA-512.

2. **PKG:**

Receive request from the users to generate the key based on their unique name, Store all keys based on the user names. Check the username and then provide the private key to accurate end user .File Receiver if they try to hack file in the cloud server and unrevoked the user after updating the private key for the corresponding file based on the user.

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

KU-CSP receives all files from the data owner and store all files on cloud. 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. KU-CSP List all files on cloud, List all the. Updated private key based on the date component and user name, List all File attackers and File Receive Attackers.

4. **End User (Receiver):**

In this module receiver first has to register and login with unique name, Request to PKG for secret key, Request available files in the cloud and after receive the private key end user download the files.

9.ALGORITHMS

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

1.Encryption:

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

- **Input:**

Encryption object as follows,

1. Encrytedstring ->NULL
2. Secret key->key

Literal type as follows,

Byte plaintext, encrypted Text

- **Output:**

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

2.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 /input message
4. DecryptedText - do Final(cipher text)
5. DecryptedString - Base64.encodeBase64 (decrypted Text)
6. Return decrypted String.

10.MATHEMATICAL MODEL:

- **UPLOADING FILE:**

U (Z) = {u1, u2, u3.....fn}

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.

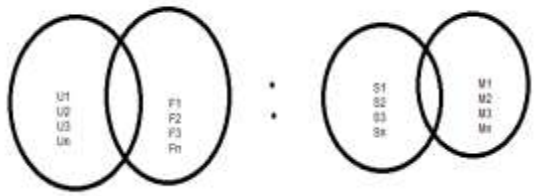
F (Z): Total number of files.

S (Z): Total number of secret key.

MAC (Z): Master key.

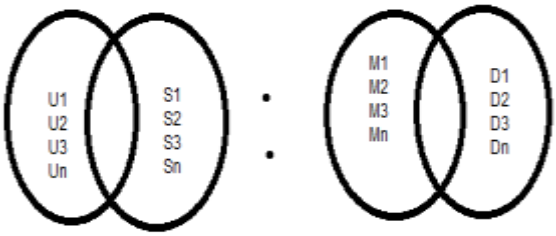
D (Z): Total data

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



- **DOWNLOADING FILES :**

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



In this scheme, focusing on the critical issue of identity revocation, we present outsourcing computation into IBE and a revocable scheme in which the revocation operations are delegated to CSP. With the aid of KU-CSP, this scheme is full-featured: It achieves constant efficiency for both computation at PKG and private key size at user. User needs not to contact with PKG during 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. Realize revocable IBE under a stronger adversary model.

11.REFERENCES

1. Jin Li, Jingwei Li, Xiaofeng Chen, Chunfu Jia, and Wenjing Lou, Identity-Based Encryption with Outsourced Revocation in Cloud Computing, in IEEE Feb2015.
2. J. Li, X. Chen, J. Li, C. Jia, J. Ma, and W. Lou, Fine-grained access control system based on outsourced attribute-based encryption,in Proc. 18th Eur. Symp. Res. Computer Security (ESORICS), 2013, pp. 592609.
3. J. Li, C. Jia, J. Li, and X. Chen,Outsourcing encryption of attribute based en- cryption with mapreduce, in Information and Communications Security. Berlin, Heidelberg: Springer, 2012, vol. 7618, pp. 191201..
4. R. Canetti, B. Riva, and G Rothblum, Two protocols for delegation of computa- tion, in Information Theoretic Security, ser. Lecture Notes in Computer Science, A. Smith, Ed. Springer Berlin / Heidelberg, 2012, vol. 7412, pp. 3761.
5. R. Canetti, B. Riva, and G N. Rothblum, Two 1-round protocols for delegation of computation, Cryptology ePrint Archive, Report 2011/518, 2011.
6. M. J. Atallah and K. B. Frikken, Securely outsourcing linear algebra computa- tions, in Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, ser. ASIACCS 10. New York, NY, USA: ACM, 2010, pp. 4859.
7. B. Libert and D. Vergnaud, Adaptive-id secure revocable identity based encryp- tion,in Topics in Cryptology(CT-RSA09), M. Fischlin, Ed. Berlin, Germany: Springer, 2009, vol. 5473, pp. 115.
8. C. Gentry, C. Peikert, and V. Vaikuntanathan, Trapdoors for hard lattices and new cryptographic constructions, in Proceedings of the 40th annual ACM symposium on Theory of computing, ser. STOC 08. New York, NY, USA: ACM, 2008, pp. 197206.
9. A. Boldyreva, V. Goyal, and V. Kumar, Identity-based encryption with efficient revocation, in Proceedings of the 15th ACM conference on Computer and com- munications security, ser. CCS 08. New York, NY, USA: ACM, 2008, pp. 417426.
10. V. Goyal, Certicate revocation using ne grained certicate space partitioning, in Financial Crypto graphy and Data Security, ser. Lecture Notes in Computer Science, S. Dietrich and R. Dhamija, Eds. Springer Berlin / Heidelberg, 2007, vol. 4886, pp. 247259.
11. C. Gentry, Practical identity-based encryption without random oracles, in Ad- vances in Cryptology - EUROCRYPT 2006, ser. Lecture Notes in Computer Science, S. Vaudenay, Ed. Springer Berlin / Heidelberg, 2006, vol. 4004, pp. 445464.

12. A. Sahai and B. Waters, Fuzzy identity-based encryption, in Advances in Cryp- tology EUROCRYPT 2005, ser. Lecture Notes in Computer Science, R. Cramer, Ed. Springer Berlin / Heidelberg, 2005, vol. 3494, pp. 557557.
13. F. Elwailly, C. Gentry, and Z. Ramzan, Quasimodo: Efficient certificate valida- tion and revocation, in Public Key Cryptography PKC 2004, ser. Lecture Notes in Computer Science, F. Bao, R. Deng, and J. Zhou, Eds. Springer Berlin / Heidelberg, 2004, vol. 2947, pp. 375388.
14. D. Boneh and M. Franklin, Identity-based encryption from the weil pairing, in Advances in Cryptology CRYPTO 2001, ser. Lecture Notes in Computer Science, J. Kilian, Ed. Springer Berlin / Heidelberg, 2001, vol. 2139, pp. 213229.
15. U. Feige and J. Kilian, Making games short (extended abstract), in Proceedings of the twenty-ninth annual ACM symposium on Theory of computing, ser. STOC 97. New York, NY, USA: ACM, 1997, pp. 506516.