A SCHEMATIC APPROACH IN FINDING THE SECURE DATA SHARING IN CLOUD COMPUTING USING RSI- BASED ENCRYPTION- A STUDY

PULI SUNITHA
M. Tech, Assistant professor,
Bandari Srinivas Institute of Technology

ABSTRACT:

Nowadays regularly use cloud services in our daily life. There are various services provided by cloud such as a service, Platform as a service, and Infrastructure asa service. The used to keep our data, documents, and files on cloud. We have developed secure data sharing in cloud computing system using revocable storage identity based encryption. Identity-based encryption is a promising crypto graphical primitive to build a practical data sharing system. However, access control is not static. That is, when some user's authorization is expired, there should be a mechanism that can remove him/her from the system. Consequently, the revoked user cannot access both the previously and subsequently shared data. In this paper we used AES (Advanced Encryption standard) technique to encrypt data as well as decrypt data. In this paper, we used RS- IBE (Revocable Storage Identity- Based Encryption) and KU Node algorithm for the security as well as recognized all members in whole system. This approach acquaints the utilities of user repudiation and cipher text update concurrently. Additionally, we provide a detailed structure of RS-IBE, which certifies its secrecy in the described security model. The realistic and cost-effective system of data sharing is achieved by this RS-IBE scheme which has tremendous benefits of operability and capability. Finally, we provide implementation results of the proposed scheme to demonstrate its practicability.

Keywords: *Cloud computing, Identity-based encryption, data sharing, cipher text.*

INTRODUCTION:

Cloud computing enables outsourcing of data and provides enormous space for memory by which it presents the computational capacity massively. Cloud provides the most flexible way of storing the data, for example, programs, images etc. and accessing them in the easiest way over the Internet rather than storing in hardware components and retrieving that information from the computer. In cloud storage, data integrity is one of the main aspects. Cloud provides the easiest way of outsourcing the data. Obviously, the outsourcing gives rise to the data which is out of control of the user which leads to hesitation as the information may be valuable. This is the major security threat to the information that is stored in the cloud. Also the data in the cloud cannot be accessed by the user, if his/her authentication is terminated.

A natural solution to conquer the aforementioned problem is to use cryptographically enforced access control such as identity-based encryption (IBE).In this paper, advance security provides in cloud computing using the re-encryption technique. Cloud Storage server is responsible for storing the data. Data Provider is nothing but the serverand data provider is responsible for the upload the data or files to storage sever. Number of user access the uploaded data of files or download the files using the key as well as opt code.

LITERATURE REVIEW:

Sandhia, G.K et al (2016) Cipher text attribute based encryption plays a major role in providing security and integrity with the help of access tree structure. The main objective is to provide the security using asymmetric encryption and access control structure for authentication and data integrity. The size of the cipher text will be constant even though the numbers of attributes are increased. The constant size cipher text can be achieved through

integrated access structures. The proposed work provides confidentiality, authentication and data integrity. The personal health records are encrypted using ABE scheme.

Mazhar Ali(2015) Cloud storage is an application of clouds that liberates organizations from establishing in-house data storage systems. We implement a working prototype of the SeDaSC methodology and evaluate its performance based on the time consumed during various operations. We formally verify the working of SeDaSC by using high-level Petri nets, the Satisfiability Modulo Theories Library, and a Z3 solver. The results proved to be encouraging and show that SeDaSC has the potential to be effectively used for secure data sharing in the cloud

Anjali Patel et al (2016) In cloud based storage concept, data owner does not have full control over own data because data controlled by the third party called cloud service providers (CSP).Here, we propose system model for secure data sharing on cloud with intension to provides data confidentiality, access control of share data, removes the burden of key management and file encryption/decryption by users, support dynamically changes of users membership, owner not be always online when the user wants to access the data.

Devi D et al (2014)A number of attribute based encryption schemes are proposed for providing confidentiality and access control to cloud data storage where the standard encryption schemes face difficulties. So, this paper extends HASBE with privacy preserving public auditing concept which additionally allows owners to securely ensure the integrity of their data in the cloud. We are using homomorphic linear authenticator technique for this purpose.

PROPOSED SYSTEM

We introduce a notion called revocable storage identity-based encryption (RS-IBE) for building a cost-effective data sharing system that fulfils the three security goals. More precisely, the following achievements are captured in this paper:

• We provide formal definitions for RS-IBE and its corresponding security model;

• We present a concrete construction of RS-IBE. The proposed scheme can provide confidentiality and backward/forward2 secrecy simultaneously;

• We prove the security of the proposed scheme in the standard model, under the decisional ℓ-Bilinear Diffie-Hellman Exponent (ℓ-BDHE) assumption. In addition, the proposed scheme can withstand decryption key exposure.

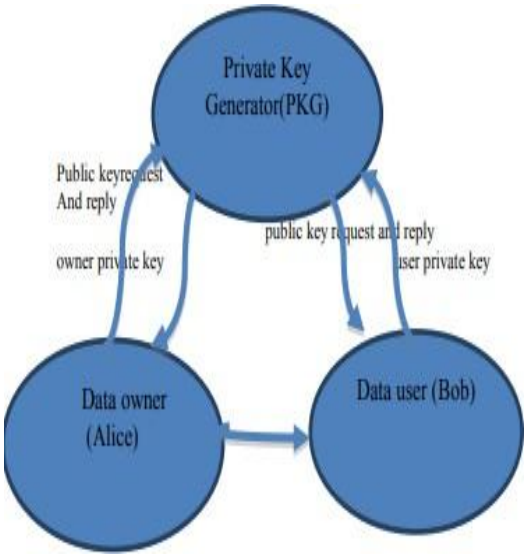
REVOCABLE IDENTITY-BASED ENCRYPTION

The concept of identity-based encryption was introduced by Shamir and conveniently instantiated by Boneh and Franklin. IBE eliminates the need for providing a public key infrastructure (PKI). Regardless of the setting of IBE or PKI, there must be an approach to revoke users from the system when necessary, e.g., the authority of some user is expired or the secret key of some user is disclosed. In the traditional PKI setting, the problem of revocation has been well studied and several techniques are widely approved, such as certificate revocation list or appending validity periods to certificates. However, there are only a few studies on revocation in the setting of IBE. Boneh and Franklin first proposed a natural revocation way for IBE. They appended the current time to the cipher text, and non-revoked users periodically received private keys for each time from the key authority. Unfortunately, such a solution is not scalable, since it requires the key authority to perform linear work in the number of non revoked users. In addition, a

secure channel is essential for the key authority and non-revoked users to transmit new keys. To conquer this problem, Boldyreva, Goyal and Kumar introduced a novel approach to achieve efficient revocation. They used a binary tree to manage identity such that their RIBE scheme reduces the complexity of key revocation to logarithmic (instead of linear) in the maximum number of system users. However, this scheme only achieves selective security.

IDENTITY BASED ENCRYPTION:

Identity Based Encryption (IBE) takes a effective approach to the problem of encryption key management. IBE can use any string as a public key, enabling data to be protected without the need for certificates. Protection is provided by a key server that controls the generation of private decryption keys. By separating authentication and authorization from private key generation through the key server, permissions to generate keys can be controlled dynamically on a granular policy driven basis, facilitating granular control over access to information in real time.



Identity-based systems allow any user to generate a public key from a known identity value such as an ASCII string. A trusted third party, called the Private Key Generator (PKG), generates the corresponding private keys. To obtain a corresponding private key, the user authorized to use the identity ID contacts the PKG, which uses the master private key to generate the private key for Identity ID. Thus, users may encrypt messages with no prior distribution of keys between individual participants. This is extremely useful in cases where pre-distribution of authenticated keys is inconvenient or infeasible due to technical restraints. However, to decrypt or sign messages, the authorized user must obtain the appropriate private key from the PKG.

CLOUD SECURITY

Besides, to overcome the above security threats, such kind of identity-based access control placed on the shared data should meet the following security goals:

- Data confidentiality: Unauthorized users should be prevented from accessing the plaintext of the shared data stored in the cloud server. In addition, the cloud server, which is supposed to be honest but curious, should also be deterred from knowing plaintext of the shared data.
- Backward secrecy: Backward secrecy means that, when a user's authorization is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the subsequently shared data that are still encrypted under his/her identity.
- Forward secrecy: Forward secrecy means that, when a user's authority is expired, or a user's secret key is compromised, he/she should be prevented from accessing the plaintext of the shared data that can be previously accessed by him/her

SYSTEM DESIGN

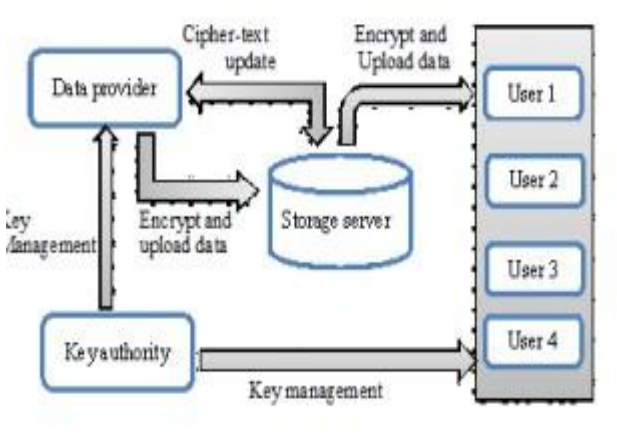


Fig-1: System Architecture

In this system first data provider upload the file. And upload file convert into the encrypted format using key encryption algorithm. i.e. AES algorithm. Then storage server responsible not only storing the data or files but, also give permission for unrevoked user to access the data or files through cloud computing. User send request for accessing data permission to data provider via storage server. Then key authority generates the key as per user requested data. These generated key is send to user. After receiving key, data provider key and user key will be match. If key will be match then user is authorized to download the data. Else it cannot the file. After matching of key again OTP will be send to user for extra security. User can write the OTP within time period. Again user will write the OTP within a time period. Then user can download the required file successfully. Else it cannot download the needed file. This whole process provide large security in cloud computing. In this paper, extra security for data sharing in cloud computing should be provided. There for sharing data through cloud computing is securely.

KUNodes algorithm:

Our RS-IBE scheme uses the same binary tree structure introduced to achieve efficient revocation. To describe the revocation mechanism, we first present several notations. Denote by ε the root node of the binary tree BT , and Path(η) the set of nodes on the path from ε to the leaf node η (including ε and η). For a non-leaf node θ, we let θl and θr stand for its left and right child, respectively. Given a time period t and revocations list RL, which is comprised of the tuples (ηi , ti) indicating that the node ηi was revoked at time period ti , the algorithm KU Nodes(BT , RL, t) outputs the smallest subset Y of nodes of BT such that Y contains an ancestor for each node that is not revoked before the time period t.

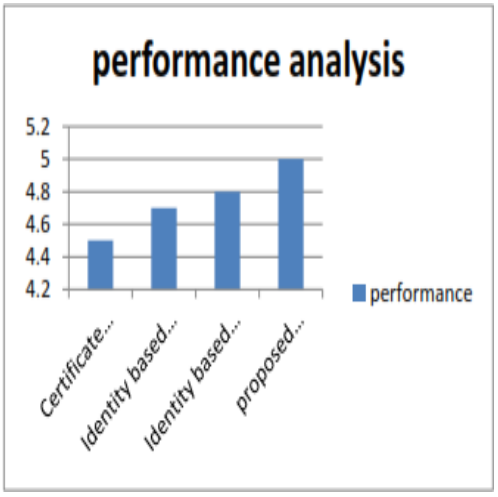
Algorithm 1 KUNodes(BT, RL, t)

1:X,Y←−∅
2:for all (ηi ,ti)∈RL do
3: if ti≤t then
4: Add Path(ηi) to X
5: end if
6:end for
7:for all θ∈X do
8: if θl∈/X then
9: Add θl to Y
10: end if
11: if θr∈/X then
12: Add θr to Y
13: end if
14: end for
15: if Y=∅ then
16: Add the root node ε to Y
17: end if
18: returnY

PERFORMANCE DISCUSSIONS

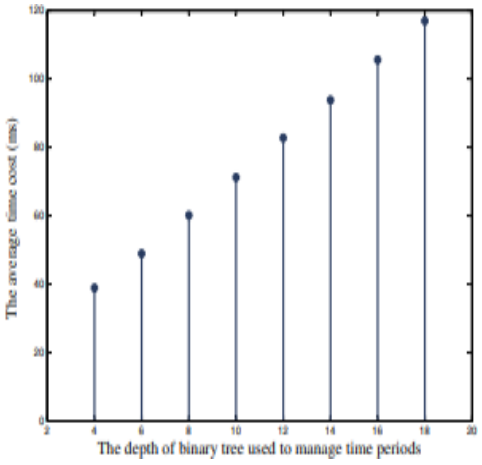
In this section, we discuss the performance of the proposed RS-IBE scheme by comparing it with previous works in terms of communication and storage cost, time complexity and functionalities, these schemes all utilize binary data structure to achieve revocation. Furthermore, by delegating the generation of re-encryption key to the key authority the cipher text size of this system also achieve constant. At this

end, the key authority has to maintain a data table for each user to store the user's secret key for all time periods.

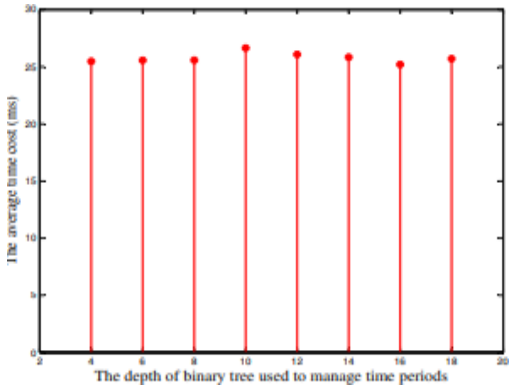


RESULT ANALYSIS

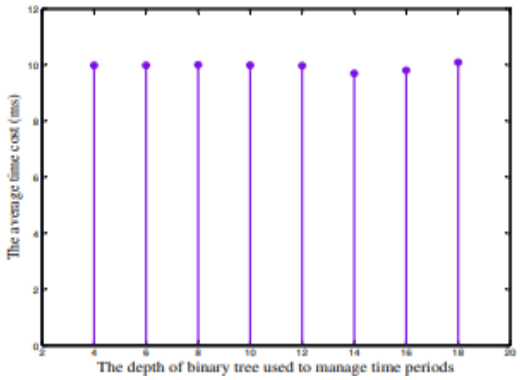
The proposed schemes have same time complexity for encryption whereas the proposed system implements an efficient time complexity. The time complexity of decryption maintain constant in all the systems. The schema provides logarithmic storage of user's identity instead of linear storage for user identity storage. As the time complexity decreases the number of users involved increases with no effect in performance of the system.



(a) Encrypt



(b) KeyUpdate



(c) Decrypt

In this paper, key authority sends the key to data provider and users. Key authority is responsible for generating the key. If the data provider receive key and user receive key is match the user will permitted to download the data. Otherwise her/him is cannot download the needed file. Matching key mechanism provide advanced security to sharing data in cloud computing. Therefore, matching of key in important to secure data sharing in cloud computing. The time period is taken to users to download the data. As per the time period user will write the OTP. Normally, size of OTP code is the 4 to 6 digit. In this paper, 6 digit integer number provided fir OTP. Each and every time OTP will be changed. So for that purpose, more security will provided. In case of within a time period OTP will not write then time will expired. And user cannot download the required files. For all

this time period mechanism provide large security.

CONCLUSION:

Cloud computing brings great convenience for people. Particularly, it perfectly matches the increased need of sharing data over the Internet. In this paper, to build a cost-effective and secure data sharing system in cloud computing, we proposed a notion called RS-IBE, which supports identity revocation and cipher text update simultaneously such that a revoked user is prevented from accessing previously shared data, as well as subsequently shared data. Furthermore, a concrete construction of RS-IBE is presented. We have studied and implement a system for secure data sharing in cloud computing. We have used RS-IBE and AES algorithm to revoke as well as encryption, re-encryption and decryption. We have given time period to users for downloading data.

REFERENCES:

1. *Sandhia, G.K., Bhaskar, G. K (2016), "Secure data sharing using attribute based encryption in cloud computing", Journal of Chemical and Pharmaceutical Sciences, ISSN: 0974-2115, Volume 9 Issue 4, PP: 3296-3299*
2. *Mazhar Ali, Revathi Dhamotharan, Eraj Khan et al (2015), "SeDaSC: Secure data sharing in clouds", IEEE Systems Journal, Vol No: 11, Issue No: 2, PP: 1-10*
3. *Anjali Patel, Nimisha Patel, Dr. Hiren Patel (2016), "Secure Data Sharing Using Cryptography in Cloud Environment", IOSR Journal of Computer Engineering, ISSN: 2278-0661, Volume 18, Issue 1, PP: 58-62*
4. *Devi D, Arun P S (2014), "A Design for Secure Data Sharing in Cloud", International Journal of Engineering Research and General Science, ISSN 2091-2730, Volume 2, Issue 5, PP: 72-77.*
5. *Revocable Identity-Based Encryption Revisited: Security Model and Construction ∗ Jae Hong Seoy and Keita Emuray January 10, 2013*
6. *Identity-based Encryption with Efficient Revocation Alexandra Boldyreva∗ School of Computer Science Georgia Institute of Technology Atlanta, GAaboldyre@cc.gatech.edu*
7. *J. Yu, R. Hao, F. Kong, X. Cheng, J. Fan, and Y. Chen, "Forwardsecure identity-based signature: security notions and construction," Information Sciences, vol. 181, no. 3, pp. 648–660, 2011.*
8. *W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," in Advances in Cryptology–CRYPTO 1998. Springer, 1998, pp. 137–152.*
9. *Boldyreva, A., V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in Proceedings of the 15th ACM conference on Computer and communications security. ACM, 2008, pp. 417–426.*
10. *Yao, D., N. Fazio, Y. Dodis, and A. Lysyanskaya, "Id-based encryption for complex hierarchies with applications to forward security and broadcast encryption," in Proceedings of the 11th ACM conference on Computer and communications security. ACM, 2004, pp. 354–363.*
11. *Shamir, A. "Identity-based cryptosystems and signature schemes," in Advances in cryptology. Springer, 1985, pp. 47–53.*
12. *Ruj, S., M. Stojmenovic, and A. Nayak, s"Decentralized access control with anonymous authentication of data stored in clouds" 2014*
13. *Mohan Prakash, Chelliah Saravanakumar. "An Authentication Technique for Accessing De-Duplicated Data from Private Cloud using One Time Password", International Journal of Information Security and Privacy, 11(2), 1-10, 2017.*
14. *Rupesh Vaishnav, Attribute Based Signature Scheme for Attribute based Encrypted data in cloud, International Journal of Engineering Research & Technology (IJERT), 1 (10), 2012*
15. *Kirubakaramoorthi R, Arivazhagan D, and Helen D, Survey on Encryption Techniques used to secure Cloud storage system, 8 (36), 2015*