International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 1 | ISSN : 2456-3307

Secure Data Sharing in Cloud Computing using Revocable-Storage Identity-Based Encryption

Rutu Manmode, Hemlata Dakhore
Department of Computer Science and Engineering, G. H. Raisoni College of Engineering and Technology, Wadi, Nagpur, Maharashtra, India

ABSTRACT

The Cloud computing gives a least difficult method for information sharing, it gives different advantages to the clients. Be that as it may, specifically outsourcing the mutual information to the cloud server will bring security issues as the information which may contain profitable data. Hence, it is necessary to place cryptographically enhanced access control on the shared data, named Identity-based encryption to build a practical data sharing system. 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. Thus, we propose a notion called revocable-capacity identity based encryption (RS-IBE), which introducing the functionalities of user revocation and cipher text update simultaneously

Keywords : Revocation, Encryption, Key Exchange, Private Key Generator, Cipher Text.

I. INTRODUCTION

Cloud computing is a model for empowering on request arrange access to a mutual pool of figuring assets (eg. Systems, servers, stockpiling and services).In the most starting phase of distributed computing security is given by Certificate Based Encryption which encode the information in light of declaration which is given to the information client. Unauthorized user may duplicate the certificate which may lead to security issue. To solve the issue, Identity Based Encryption replaces this strategy. In which the client's id (name, email address, ip address, port number, and so on.) is utilized to produce the keys which are utilized to scramble the information. This does not provide security to data shared in cloud because the data is stored for a longer period by then the data is accessible to the third party very easily. To avoid this Identity Based Encryption with Efficient Revocation was introduced. In this approach the data provider can provide the life time of the key provided to the user. Towards the finish of the life time the client can deny the key with the assistance of focal specialist called Private Key Generator (PKG). After this Revocable Storage Identity Based Encryption is proposed, this gives both forward and in reverse security which is missing in past procedure. This technique allows the data provider to specify the life time of the data shared as well as the private key provided to the data user. Once this time expires the private key generator (pkg) is responsible for revoking the cipher text and private key of each user. This system of giving security in both the closures is called as forward and in reverse security.

Brief Literature Survey

A certificate, namely a signature acts not only as a certificate but also as a decryption key. A key holder needs the its secret key and a mode authentication from its CA to decode a message. Authentication

based encryption consolidates the best parts of identity based encryption and open key encryption. Endorsement incorporate at any rate the name of a client and its open key.

Sometimes, the authority includes a serial number as well as the certificate issue date and expiration date. On the off chance that a client coincidentally uncovers its secret key or an aggressor effectively bargains it, the client might be asked for the disavowal of its endorsement. Further the client's organization may ask for disavowal if the client leaves the organization or changes position and is never again qualified for utilize the key. If a certificate is revocable, then the third parties cannot relay on that certificate unless the CA distributes certificate status information indicating whether the certificate is currently valid.

Identity Based Encryption (IBE) takes a effective approach to the problem of encryption key management. IBE can utilize any string as an open key, empowering information to be ensured without the requirement for authentications. Security is given by a key server that controls the age of private unscrambling 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

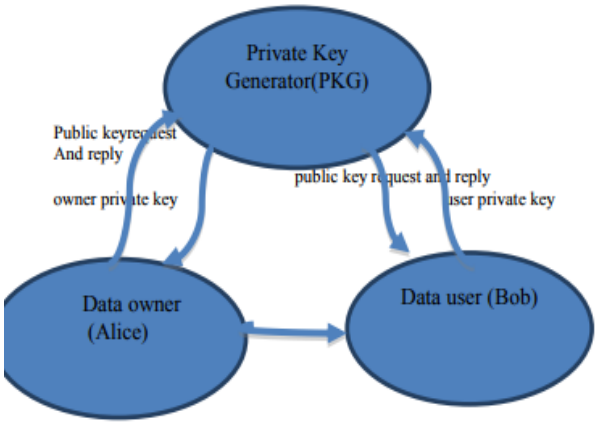


Fig 1:Identity based encryption

Identification-based systems allow any user to generate a public key from a known identity value such as an ASCII string. A trusted party, called the Private Key Generator (PKG), creates the comparing private keys. To work, the PKG first distributes an ace open key, and holds the comparing expert private key. Given the master public key, any user can compute a public key corresponding to the identity ID by combining the master public key with the identity value.

To acquire a relating private key, the client approved to utilize the personality ID contacts the PKG, which utilizes the ace private key to create the private key for IdentityID. 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 unscramble or sign messages, the approved client must acquire the proper private key from the PKG.

There is a security issue in IBE, to avoid it efficient regeneration of keys is suggested that users renew their private period. Only the PKG's public key and the receiver's identity are needed to encrypt, and there is no way to communicate to the senders that an identity has been revoked, such a mechanism to regularly update users' private keys seems to be the only viable solution to the revocation problem. This implies all clients, paying little mind to whether their keys have been uncovered or not, ought to consistently get in contact with the PKG, demonstrate their personality and get new private keys.

The PKG must be online for all such transactions, and a secure channel must be established between the PKG and each user to transmit the private key. Taking scalability of IBE deployment into account, we observe that for a very large number of users this may become a bottleneck. We observe that alternatively, to avoid the need for interaction and a

secure channel, the PKG may encrypt the new keys of non-revoked users under their identities and the previous time period, and send the cipher texts to these users (or post them online)

With this approach, for each non-repudiated client in the framework, the PKG is required to perform one key age and one encryption operation for each key refresh. We take note of that this arrangement, similarly as the first recommendation, requires the PKG to do work straight in the quantity of clients, and does not scale well as the quantity of clients develop.

Revocable storage identity based encryption

The non-revocable data sharing system can provide confidentiality and backward secrecy. Furthermore, the method of decrypting and re-encrypting all the shared data can ensure forward secrecy. However, this brings new difficulties. Note that the procedure of decode then re-encode fundamentally includes clients' mystery key data, which makes the general information sharing framework helpless against new assaults. Practically, the use of secret key should be limited to only usual decryption, and it is inadvisable to update the cipher text periodically by using secret key.

Another challenge comes from efficiency. To upgrade the figure content of the mutual information, the information supplier needs to much of the time do the method of download-unscramble re-scramble transfer. This process brings great communication and computation cost, and thus is cumbersome and undesirable for cloud users with low capacity of computation and storage.

The steps we follow to avoid this problem is to require the cloud server to directly re-encrypt the cipher text of the shared data. However, this may introduce cipher text extension, namely, the size of the cipher text of the shared data is linear in the number of times the shared data have been updated. Moreover the method of intermediary re-encryption can likewise be utilized to vanquish the issue of productivity.

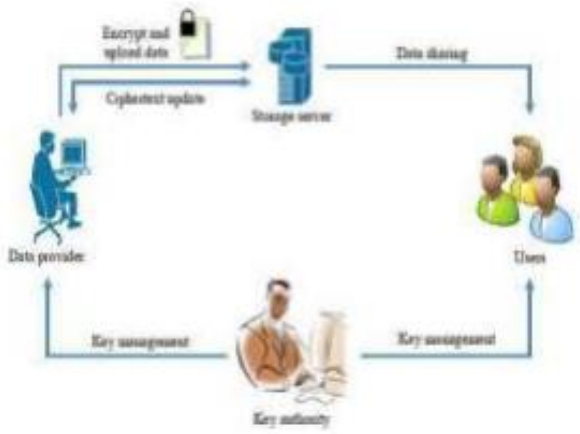


Fig 2: Revocable storage identity based encryption

Proposed System

In the proposed system, we used a concept called revocable-storage identity-based encryption (RSIBE) for developing a cost-effective data sharing system that fulfills the three security goals.

The security goals are:

Data confidentiality: non-permitable users should be prevented from accessing the plaintext of the shared data stored in the cloud server. Moreover, 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 says 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. The proposed system attains the following characteristics:

We can provide formal definitions for RS-IBE and its corresponding security model; and backward/forward secrecy simultaneously.
We prove that the security of the proposed scheme in the standard model, under the decisional ℓ-Bilinear Diffie-Hellman Exponent (ℓ-BDHE) assumption.

In addition to security, this system will reduce the time complexity and provide a better performance.

Preliminaries

Decisional ℓ-BDHE assumption

The decisional ℓ-BDHE problem is formalized as follows. Choose a group G1with prime order p according to the security parameterλ..select a generator g of G1 and a, s<- R ZP and let f i=g a i. .T Provide the vector f= (g, gs , f1, ..., fℓ, fℓ+2, ..., f2ℓ) and an element D∈G2 to a probabilistic polynomial-time (PPT) algorithm C, it outputs 0 to indicate that D = e(gs , g aℓ+1), and outputs 1 to indicate that D is a random element from G2.

Kunodes algorithm:

By using this algorithm onlynon-revoked user at a time period are able to decrypt the cipher text. INPUT: Binary tree revocation list,Time period OUTPUT: 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.

Steps:1 Data owner upload the file in cloud with validity time

2.Data user access the data.

2.1. if the user tries to access the data within a specified time only he is able to access the data

2.2. Otherwise data owner need to update the key.

3.Data owner update the key used by the user.

4. Then he will update the cipher text. This will provide both forward and backward security to the data stored in a cloud.

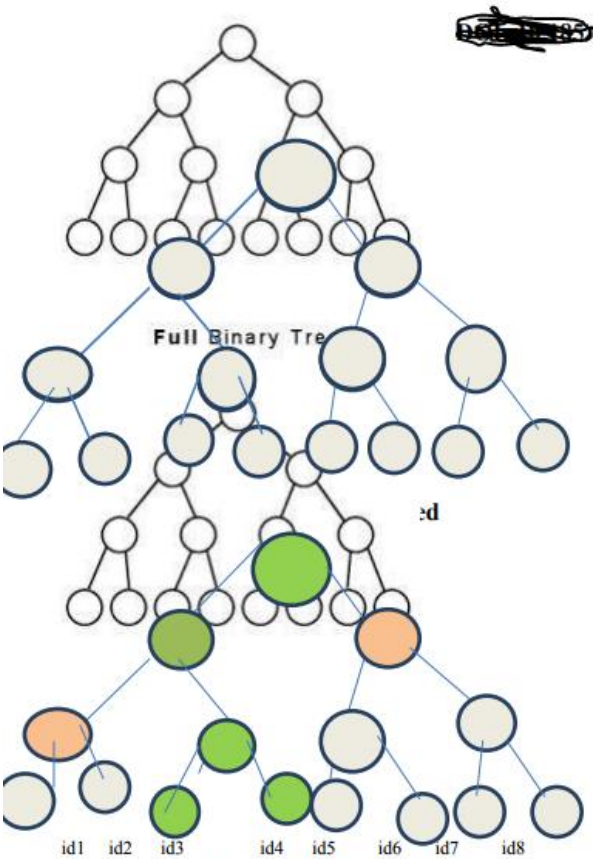


Fig :user id3 is revoked

By this algorithm ,when we rovoke the leaf node(id3) their ancestors also get updated(nodes in green color) and the node which shares the same key of revoked nod(nodes in orange color)e also get updated.

Algorithm 1 KUNodes(**BT**, RL, t)

1: X,Y ← −**ø**
2: **for all** (η_i,t_i)**∈**RL **do**
3: **if** $t_i \leq t$ **then**
4: Add Path(η_i) to X
5: **end if**
6: **end for**
7: **for all** θ**∈**X **do**
8: **if** θ_l**∈/**X **then**
9: Add θ_l to Y
10: **end if**
11: **if** θ_r**∈/**X **then**
12: Add θ_r to Y
13: **end if**
14: **end for**
15: **if** Y**=ø then**
16: Add the root node ε to Y
17: **end if**
18: **return**Y

Definition in RS-IBE:

A revocable-storage identity-based encryption scheme with message space M, identity space I and total number of time periods T is comprised of the following seven polynomial time algorithms

1.setup(1λ , T, N): the setup algorithm takes as input the security parameter λ ,the time bound T and the maximum number of system users N , and it outputs the public parameter P P and the master secret key M SK, associated with the initial revocation list RL=∅ and state st.

2.PKGen(P P, M SK, ID): The private key generation algorithm takes as input P P , M SK and an identity ID ∈I, and it generates a private key SKIDfor ID and an updated state st.

3.KeyUpdate(P P, M SK, RL, t, st): The key update algorithm takes as input P P , M SK, the current revocation list RL, the key update time t≤T and the state st, it outputs the key update KUt .

4.DKGen(P P, SKID, KUt): The decryption key generation algorithm takes as input P P , SKID and KUt , and it generates a decryption key DKID,t for ID with time period t or a symbol ⊥ to illustrate that ID has been previously revoked.

5.Encrypt(P P, ID, t, M): The encryption algorithm takesas input P P , an identity ID, a time period t≤T , and a message M∈M to be encrypted, and outputs a cipher text CTID,t.

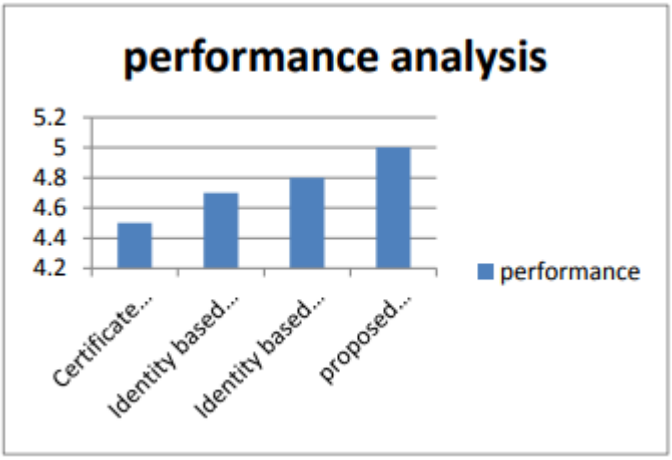
6.CTUpdate(P P, CTID,t, t′): The ciphertext update algorithm takes as input P P , CTID,t and a new time period t ′ ≥ t, and it outputs an updated ciphertextCTID,t′ .

7.Decrypt(P P, CTID,t, DKID,t′): The decryption algorithm takes as input P P , CTID,t, DKID,t′ , and it recovers the encrypted message M or a distinguished symbol ⊥ indicating that CTID,t is an invalid ciphertext.

8.Revoke(P P, ID, RL, t, st): The revocation algorithm takes as input P P , an identity ID∈I to be revoked, the current revocation list RL, a state st and revocation time period t≤T , and it updates RL to a new one.

Performance discussions

In this area, we talk about the execution 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. Moreover, by delegating the generation of re-encryption key to the key authority, the cipher text size of this system also achieves constant. Finally the key authority has to maintain a data table for each user to store the user's secret key for all time periods.



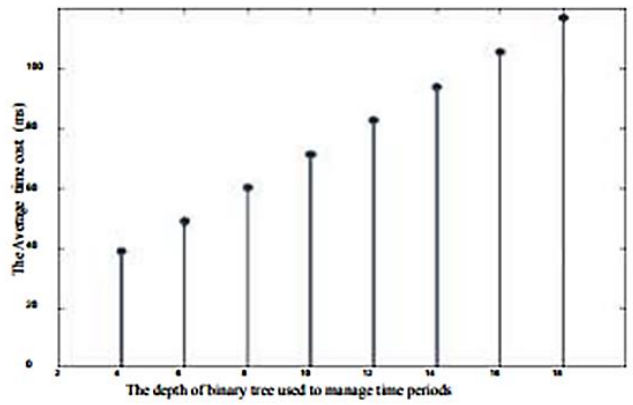
Result analysis and discussions

The proposal (Libert and Vergnaud, Seo and Emura, Liang et al) 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 gives logarithmic capacity of clients character rather than direct capacity for client personality. As the time complexity decreases the number of users involved increases with no effect in performance of the system. Based on the sample data of the table is derived to explain the improvement of performance in terms of time complexity.

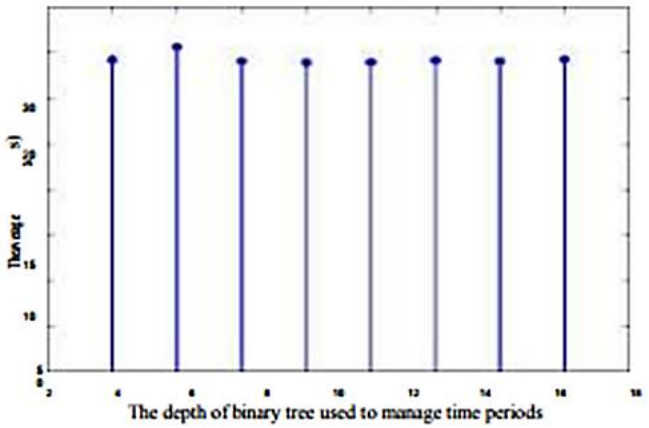
SCHEME	ENCRYPTION	DECRYPTION
Libert	O(1)e+o(1)p	o(1)p
Emura	O(1)e+o(1)p	o(1)p
Liang	O(1)e+o(1)p	o(1)p
Proposed scheme	o(Log T)e+ o(1)p	o(1)p

TABLE: comparison of time complexity

Table is taken using sample inputs. The following graphs (Encrypt, Decrypt) are drawn based on the table data



(a) Encrypt



(b) Decrypt

II. CONCLUSIONS

Cloud computing is a very much convenient 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 so that a revoked user is prevented from accessing previously shared data, as well as subsequently shared data. Evenmore, a concrete construction of RS-IBE is presented. The proposed RS-IBE scheme is proved adaptive-secure in the standard model, under the decisional ℓ-DBHE assumption. The comparison results demonstrate that our scheme has advantages in terms of efficiency and functionality, and thus is more feasible for practical applications.

III. EXTENSION

Technology is not constant, the technological advancement day by day changes the advantages to the disadvantages. This project is secure with the revocable functionality where as we can restrict the cloud users at any point of time, by changing the key given to him. The extension to this project is tracking the every action of the cloud user, so that we can maintain utmost security to the system. The cloud user in this project can download the files, the complete tracking of the downloaded files gives a multi-step security to the cloud provider. The tracking of the files is irrespective of the user, whoever is the user the tracking system tracks all the download details of the user. This is the security implementation of the project.

IV. REFERENCES

[1]. Alexandra Boldyreva (Georgia institute of technology, Atlanta, GA, USA), Vipul Goyal (university of California at Los Angeles, CA, USA) and Virendra Kumar (Georgia institute of technology, Atlanta, GA, USA) "Identity-based encryption with efficient revocation" 2008.

[2]. Chul Sur Dept. of IT Convergence &Applic. Eng., Pukyong Nat. Univ., Busan, South Korea, Youngho Park (Dept. of IT Convergence &Applic. Eng., Pukyong Nat. Univ., Busan, South Korea), Sang UK Shin (Dept. of IT Convergence &Applic. Eng., Pukyong Nat. Univ., Busan, South Korea) Kyung Hyune Rhee (Dept. of IT Convergence &Applic. Eng., Pukyong Nat. Univ., Busan, South Korea) "Certificate-Based Proxy Reencryption for Public Cloud Storage 2013".

[3]. Mohan, Prakash, and Ravichandran Thangavel. "Resource Selection in Grid Environment Based on Trust Evaluation using Feedback and Performance." American Journal of Applied Sciences 10.8 (2013): 924.

[4]. Prakash, M., and T. Ravichandran. "An Efficient Resource Selection and Binding

Model for Job Scheduling in Grid." European Journal of Scientific Research 81.4 (2012): 450-458.

[5]. Jin Li (School of Computer Science, Guangzhou University, Guangzhou, China),Wenjing Lou (Virginia Polytechnic Institute and State University, Blacksburg) "Identity based encryption with outsourced revocation in cloud computing" 2015.

[6]. Prakash, M., R. Farah Sayeed, S. Princey, and S. Priyanka. "Deployment of MultiCloud Environment with Avoidance of DDOS Attack and Secured Data Privacy." International Journal of Applied Engineering Research 10, no. 9 (2015): 8121-8124.

[7]. Annamalai, R., J. Srikanth, and M. Prakash. "Integrity and Privacy Sustenance of Shared Large Scale Images in the Cloud by Ring Signature." International Journal of Computer Applications 114.12 (2015).

[8]. 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.

[9]. C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy preserving public auditing for secure cloud storage,"2013.

[10]. G. Anthes, "Security in the cloud," Communications of the ACM, 2010

[11]. S. Ruj, M. Stojmenovic, and A. Nayak, s"Decentralized access control with anonymous authentication of data stored in clouds" 2014

[12]. X. Huang, J. Liu, S. Tang, Y. Xiang, K. Liang, L. Xu, and J. Zhou, "Cost-effective authentic and anonymous data sharing with forward security" 2014.

[13]. C. Gentry, "Certificate-based encryption and the certificate revocation problem," 2003.

[14]. V. Goyal, "Certificate revocation using fine grained certificate space partitioning," 2007.

[15]. J. M. G. Nieto, M. Manulis, and D. Sun, "Forward-secure hierarchical predicate encryption,"2013.

[16]. K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloud based revocable identity-based proxy reencryption scheme for public clouds data sharing," 2014.

[17]. D.-H. Phan, D. Pointcheval, S. F. Shahandashti, and M. Strefler, "Adaptive cca broadcast encryption with constant-size secret keys and ciphertexts," 2013.

[18]. M. Abdalla and L. Reyzin, "A new forward-secure digital signature scheme," 2000.