www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 6 Issue 3 March 2017, Page No. 20558-20563
Index Copernicus value (2015): 58.10 DOI: 10.18535/ijecs/v6i3.29

Revocable-Storage Identity-Based Encryption: Secure Data Sharing In Cloud

Sonia Jenifer Rayen[1], Bharathi P[2], Renuka V[3], Saranya R[4]
[1] Assistant profesor,
Department of information technology,
Jeppiaar Institute of technology,chennai.
soniya@jeppiaarinstitute.org
[2] Jeppiaar Institute of technology,chennai.
bharathi.pandian@yahoo.com
[3] Jeppiaar Institute of technology,chennai.
renukaanura20@gamil.com
[4] Jeppiaar Institute of technology,chennai.
saranyaraman30@gmail.com

Abstract: ***Cloud computing provides a simplest way of data sharing, it provides various benefits to the users. But directly outsourcing the shared data to the cloud server will bring security issues as the data may contain valuable information. 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-storage 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.**

1.INTRODUCTION

Cloud computing is a model for enabling convenient, on demand network access to a shared pool of computing resources (eg. Networks,servers,storage and services).In the earliest stage of cloud computing security is provided by Certificate Based Encryption which encrypt the data based on certificate which is provided to the data user.

Unauthorized user may duplicate the certificate which may lead to security issue. To overcome the issue, Identity Based Encryption replaces this technique. In which the user's id (name, email address, ip address, port number, etc.) is used to generate the keys which are used to encrypt the data. 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. At the end of the life time the user can revoke the key with the help of central authority called Private Key Generator (PKG). After this Revocable Storage Identity Based Encryption is proposed, this provides both forward and backward security which is absent in previous technique. 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 mechanism of providing security in both the ends is called as forward and backward security.

2. LITERATURE SURVEY:

2.1CERTIFICATE-BASED ENCRYPTION: A certificate, namely a signature acts not only as a certificate but also as a decryption key. A key holder needs both its secret key and an up-to-date certificate from its CA to decrypt a message. Certificate-based encryption combines the best aspects of identity-based encryption and public key encryption. Certificate include at least the name of a user and its public key.

Often, the certificate authority includes a serial number as well as the certificate issue date and expiration date. if a user accidentally reveals its

secret key or an attacker actively compromises it, the user may be requested for the revocation of its certificate. Futherly, the user's company may request revocation if the user leaves the company or changes position and is no longer entitled to use 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.

2.2 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.

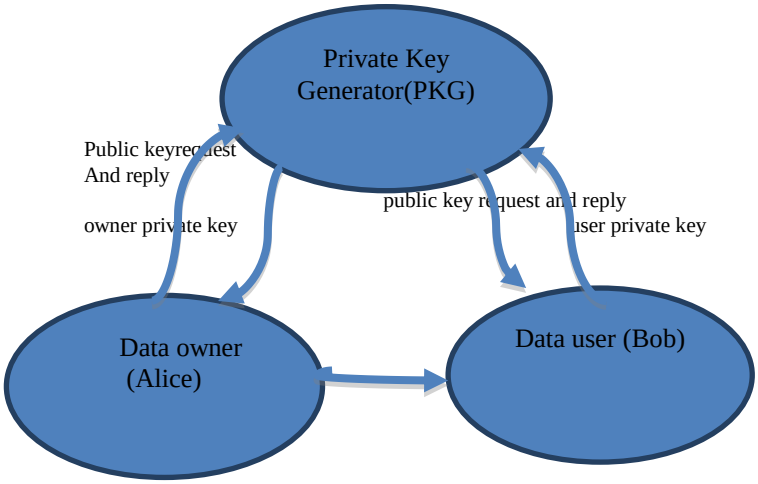


Fig 1:Identity based encryption

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 operate, the PKG first publishes a master public key, and retains the corresponding master 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 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 I dentity*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.

2.3 IDENTITY BASED ENCRYPTION WITH EFFICIENT REVOCATION: there is a security issue in IBE, to avoid it efficient revocation 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 means that all users, regardless of whether their keys have been exposed or not, should regularly get in contact with the PKG, prove their identity 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 note 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 every non-revoked user in the system, the PKG is required to perform one key generation and one encryption operation per key update. We note that this solution, just as the original suggestion, requires the PKG to do work linear in the number of users, and does not scale well as the number of users grow.

2.4 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 challenges. Note that the process of decrypt-then-re-encrypt necessarily involves users' secret key information, which makes the overall data sharing system vulnerable to new attacks. In general, 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 update the cipher text of the shared data, the data provider has to frequently carry out the procedure of download-decrypt-re-encrypt-upload. This process brings great communication and computation cost, and thus is cumbersome and undesirable for cloud users with low capacity of computation and storage.

Fig 2: Revocable storage identity based encryption

One method 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. In addition, the technique of proxy re-encryption can also be used to conquer the problem of efficiency.

3. PROPOSED SYSTEM:

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

The security goals are:

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 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 subsequentlyshared 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 previouslyaccessed 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.

3.1 PRELIMINARIES:

1. DECISIONAL ℓ-BDHE ASSUMPTION:

The decisional ℓ-BDHE problem is formalized as follows. Choose a group $G_1$with 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, g^s, f_1, ..., f_ℓ, $f_{\ell+2}$, ..., $f_{2\ell}$) and an element D∈G_2 to a probabilistic polynomial-time (PPT) algorithm C, it outputs 0 to indicate that D = e(g^s, $g^{a\ell+1}$), and outputs 1 to indicate that D is a random element from G_2.

2. 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.

DOI: 10.18535/ijecs/v6i3.29

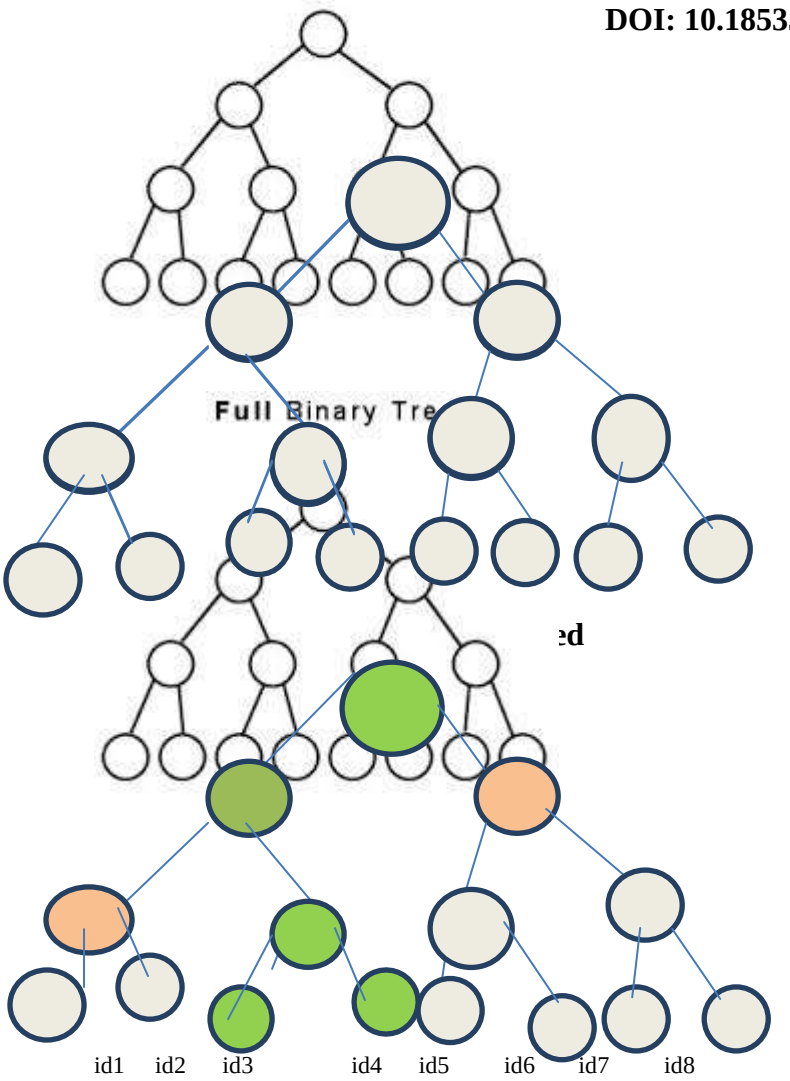


Fig :user id3 is revoked

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)

```
X,Y←−∅
for all (η_i,t_i)∈RL do
  if t_i≤t then
    Add Path(η_i) to X
  end if
end for
for all θ∈X do
  if θ_l∈/X then
    Add θ_l to Y
  end if
  if θ_r∈/X then
    Add θ_r to Y
  end if
end for
if Y=∅ then
  Add the root node ε to Y
end if
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(1^{λ}, 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 generationalgorithm takes as input P P , M SK and an identity ID ∈**I**, and it generates a private key $SK_{ID}$for 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 revocationlist RL, the key update time t≤T and the state st, it outputs the key update KU_t.

4.DKGen(P P, SK_{ID}, KU_t): The decryption key generation algorithm takes as input P P , SK_{ID} and KU_t, and it generates a decryption key $DK_{ID,t}$ 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 $CT_{ID,t}$.

6.CTUpdate(P P, $CT_{ID,t}$, t'): The ciphertext update algorithm takes as input P P , $CT_{ID,t}$ and a new time period $t' \geq t$, and it outputs an updated ciphertext$CT_{ID,t}'$.

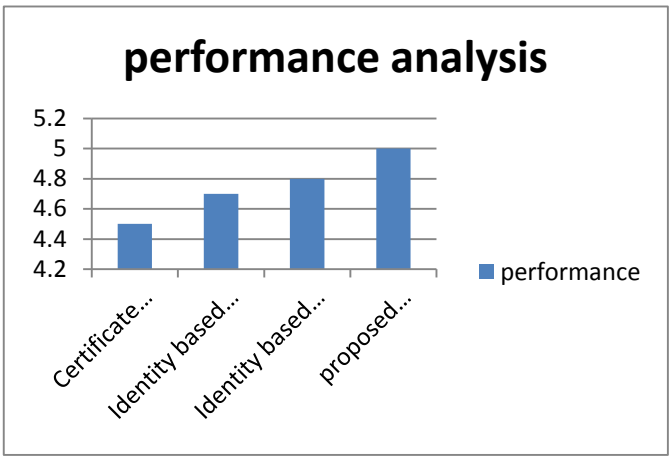
7.Decrypt(P P, $CT_{ID,t}$, $DK_{ID,t}'$): The decryption algorithm takes as input P P , $CT_{ID,t}$, $DK_{ID,t}'$, and it recovers the encrypted message M or a distinguished symbol ⊥ indicating that $CT_{ID,t}$ is an invalid ciphertext.

8.Revoke(P P, ID, RL, t, st): The revocation algorithmtakes 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.

4. 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 achieves 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.



6.RESULT ANALYSIS AND DISCUSSIONS:

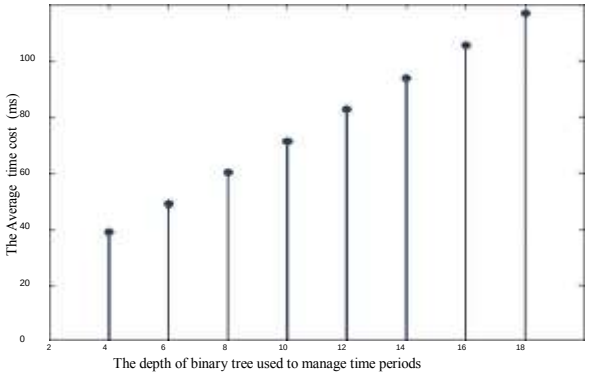
The proposed scheme (Libert and Vergnaud, Seo and Emura, Liang et al) have same time complexity for encryption whereas the proposed system implements a efficient time complexity. The time complexity of decryption maintain constant in all the systems. The scehmae provides logarithmic storage of users 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. Based on the sample data of the table is derived to explain the performance improvement in terms of time complexity.

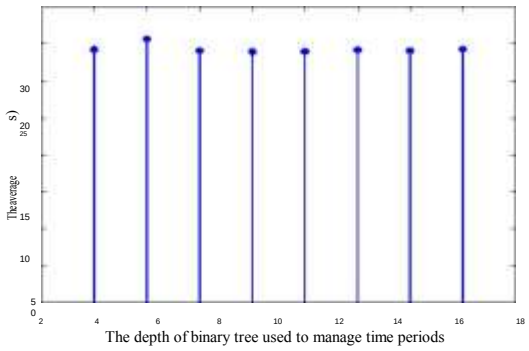
SCHEMES	ENCRYPTION	DECRYPTION
Libert	O(1)e+o(1)p	o(1)p
Emura	O(1)e+o(1)p	o(1)p
Liang	O(1)e+o(1)p	o(1)p
Proposed scheme	o(Log T)e+ o(1)p	o(1)p

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

5. CONCLUSIONS

Cloud computing is a 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 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. 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.

REFERENCE:

[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

120

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 Re-encryption 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] 11. K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, "An efficient cloud based revocable identity-based proxy re-encryption scheme for public clouds data sharing," *2014.*

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

[18] 13. M. Abdalla and L. Reyzin, "A new forward-secure digital signature scheme," 2*000*.