International Journal of Research
Available at https://pen2print.org/index.php/ijr

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 06 Issue 02
February 2019

Multi Cloud Storage of Data with Cost Efficiency Using Data Centric Security

Mr. Kondekar S.S.
P.G. Department(CSIT)
Computer Science and Information Technology
M.B.E.S College of Engineering ,Ambajogai.

Prof. B.M.Patil
Department(CSIT)
Computer Science and Information Technology
M.B.E.S College of Engineering ,Ambajogai.

Abstract: - Cloud computing provides a flexible and convenient way for data sharing, which brings various benefits for both the society and individuals. But there exists a natural resistance for users to directly outsource the shared data to the cloud server since the data often contain valuable information. Thus, it is necessary to place cryptographically enhanced access control on the shared data. Identity-based encryption is a promising cryptographically 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. To this end, we propose a notion called revocable-storage identity-based encryption (RS-IBE), which can provide the forward/backward security of cipher text by introducing the functionalities of user revocation and cipher text update simultaneously. Furthermore, we present a concrete construction of RS-IBE, and prove its security in the defined security model. The performance comparisons indicate that the proposed RS-IBE scheme has advantages in terms of functionality and efficiency, and thus is feasible for a practical and cost-effective data-sharing system. Finally, we provide implementation results of the proposed scheme to demonstrate its practicability.

1. Introduction

Cloud computing is a paradigm in Technology of information(IT) that provides ubiquitous access to shared pools of configurable system resources and often over the internet, Service of higher-level with minimal management effort can be rapidly provisioned[4][5][6]. Cloud computing relies on sharing of resources to achieve coherence and economy of scale, similar to a utility.ID-based encryption, or identity-based encryption (IBE), is an important primitive of ID-based cryptography. Because a type of public-key encryption user of public key has some unique information about the user identity (e.g. email address of user). This means that a sender who has access to the public parameters of the system can encrypt a message using e.g.

the text-value of the receiver's name or email address as a key. From the central authority the decryption keys are obtained to the receiver , which needs to be trusted as it generates secret keys for every user. By knowing the ASCII string in system of Identity Based allow to generate a public key by known identity value by any party[6]. A corresponding private keys are generated by trusted third party, called the Private Key Generator (PKG) . In order to corresponding private key are to be obtain, identity ID contacts the PKG used by the party authorized , to generate the private key for identity ID which uses the master private key. Outsourcing data to cloud server implies that data is out control of users. This may cause users' hesitation since the outsourced data usually contain valuable and sensitive information[5]. Even worse, cloud server itself may reveal users' data for illegal profit. Data sharing is not static. When the authorization of user is expired, he/she could not access the previously and subsequently shared data[9]. Therefore, while outsourcing data to cloud server, users also want to control access to these data such that only those currently authorized users can share the outsourced data[11]. A solution to overcome the problem is to use access control such as identity-based encryption (IBE).

2. Existing System

- Boneh and Franklin first proposed a natural revocation way for IBE. They appended the current time period to the ciphertext, and non-revoked users periodically received private keys for each time period from the key authority.
- 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.
- Subsequently, by using the aforementioned revocation technique, Libert and Vergnaud proposed an adaptively secure RIBE scheme based on a variant ofWater's IBE scheme.
- Chen et al. constructed a RIBE scheme from lattices.

DISADVANTAGES OF EXISTING SYSTEM:

- Unfortunately, existing 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.
- However, existing scheme only achieves selective security.
- This kind of revocation method cannot resist the collusion of revoked users and malicious non-revoked users as malicious non-revoked users can share the update key with those revoked users.

- Furthermore, to update the ciphertext, the key authority in their scheme needs to maintain a table for each user to produce the re-encryption key for each time period, which significantly increases the key authority's workload.

3. PROPOSED SYSTEM

- It seems that the concept of revocable identity-based encryption (RIBE) might be a promising approach that fulfills the aforementioned security requirements for data sharing.
- RIBE features a mechanism that enables a sender to append the current time period to the ciphertext such that the receiver can decrypt the ciphertext only under the condition that he/she is not revoked at that time period.
- A RIBE-based data sharing system works as follows:
- Step 1: The data provider (e.g., David) first decides the users (e.g., Alice and Bob) who can share the data. Then, David encrypts the data under the identities Alice and Bob, and uploads the ciphertext of the shared data to the cloud server.
- Step 2: When either Alice or Bob wants to get the shared data, she or he can download and decrypt the corresponding ciphertext. However, for an unauthorized user and the cloud server, the plaintext of the shared data is not available.
- Step 3: In some cases, e.g., Alice's authorization gets expired, David can download the ciphertext of the shared data, and then decrypt-then-re-encrypt the shared data such that Alice is prevented from accessing the plaintext of the shared data, and then upload the re-encrypted data to the cloud server again.

ADVANTAGES OF PROPOSED SYSTEM:

- 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
- The procedure of ciphertext update only needs *public information*. Note that no previous identity-based encryption schemes in the literature can provide this feature;
- The additional computation and storage complexity, which are brought in by the forward secrecy, is all upper bounded by O(log(T)2), where T is the total number of time periods.

4. System Architecture

We present a specific architecture of RS-IBE. The confidentiality of the valuable information and backward/forward secrecy are implemented simultaneously by this proposal. By the presumption of the decisional ℓ-Bilinear Diffie-Hellman Exponent (ℓ-BDHE), the secrecy of the proposed system in the defined model. Additionally, the proposed model can endure decryption key exposure. This not only achieves the integrity of the data but also the confidentiality. Revocable-storage identity-based encryption (RS-IBE), which can provide the forward/backward security of cipher text by introducing the functionalities of user revocation and cipher text update simultaneously. Furthermore, we present a concrete construction of RS-IBE, and prove its security in the defined security model. The performance comparisons indicate that the proposed RS-IBE scheme has advantages in terms of functionality and efficiency, and thus is feasible for a practical and cost-effective data-sharing system.

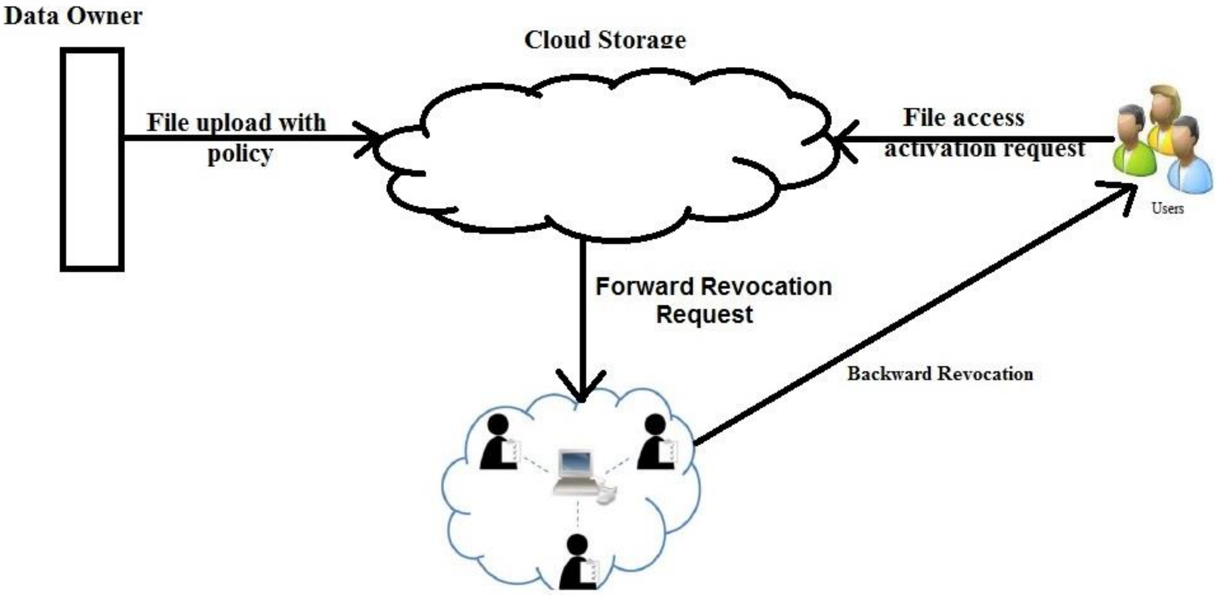

Fig:- Architecture

5. Modules Description

System Construction Module: In the first module, we develop the proposed system with the required entities for the evaluation of the proposed model. The data provider (e.g., David) first decides the users (e.g., Alice and Bob) who can share the data. Then, David encrypts the data under the identities Alice and Bob, and uploads the cipher text of the shared data to the cloud server. When either Alice or Bob wants to get the shared data, she or he can download and decrypt the corresponding cipher text. However, for an unauthorized user and the cloud server, the plaintext of the shared data is not available.

Data Provider: In this module, we develop the Data Provider module. The data provider module is developed such that the new users will Signup initially and then Login for authentication. The data provider module provides the option of uploading the file to the Cloud Server. The process of File Uploading to the cloud Server is undergone with Identity-based encryption format. Data Provider will check the progress status of the file upload by him/her. Data Provider provided with the features of Revocation and Cipher text update the file. Once after completion of the process, the Data Provider logouts the session.

Cloud User:-In this module, we develop the Cloud User module. The Cloud user module is developed such that the new users will Signup initially and then Login for authentication. The Cloud user is provided with the option of file search. Then cloud user feature is added up for send the Request to Auditor for the File access. After getting decrypt key from the Auditor, he/she can access to the File. The cloud user is also enabled to download the File. After completion of the process, the user logout the session.

Key Authority (Auditor):-Auditor Will Login on the Auditor's page. He/she will check the pending requests of any of the above person. After accepting the request from the above person, he/she will generate master key for encrypt and Secret key for decrypt. After the complete process, the Auditor logout the session.

6. Algorithm

Algorithm 1 KUNodes(BT , RL, t) :

```
$X, Y \leftarrow - \emptyset$
for all $(\eta i, ti) \in RL$ do
    if $ti \leq t$ then
        Add Path($\eta i$) to X
    end if
end for
for all $\theta \in X$ do
    if $\theta l \in/ X$ then
        Add $\theta l$ to Y
    end if
    if $\theta r \in/ X$ then
        Add $\theta r$ to Y
    end if
end for
if $Y = \emptyset$ then
```

```
Add the root node $\varepsilon$ to $Y$
end if
return $Y$
```

Our RS-IBE scheme uses the same binary tree structure introduced by Boldyreva, Goyal and Kumar [20] 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 rightchild, 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 KUNodes(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 2:- Revocable-Storage Identity-Based Encryption

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:

• **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 MSK, associated with the initial revocation list RL = ∅ and state st.

• **PKGen(P P, MSK, ID):** The private key generation algorithm takes as input P P, MSK and an identity ID ∈ I, and it generates a private key SKID for ID and an updated state st.

• **KeyUpdate(P P, MSK, RL, t, st):** The key update algorithm takes as input P P, MSK, the current revocation list RL, the key update time $t \leq T$ and the state st, it outputs the key update KUt.

• **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.

• **Encrypt(P P, ID, t, M):** The encryption algorithm takes as input P P, an identity ID, a time period $t \leq T$, and a message M ∈ M to be encrypted, and outputs a ciphertext CTID,t.

• **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 ciphertext CTID,t′ .

• **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.

• **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 $t \leq T$, and it updates RL to a new one.

7. 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.

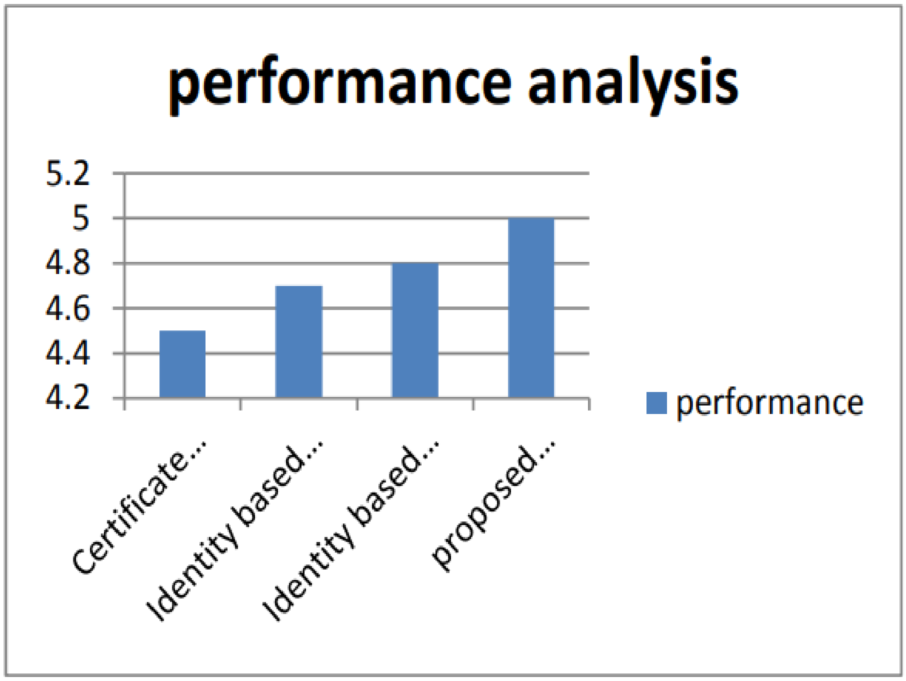

Fig:- Performance Analysis

8. 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 ciphertext 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.

REFERENCES

[1] L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud definition," ACM SIGCOMM Computer Communication Review, vol. 39, no. 1, pp. 50–55, 2008.

[2] iCloud. (2014) Apple storage service. [Online]. Available: https://www.icloud.com/

[3] Azure. (2014) Azure storage service. [Online]. Available: http://www.windowsazure.com/

[4] Amazon. (2014) Amazon simple storage service (amazon s3).[Online]. Available: http://aws.amazon.com/s3/

[5] K. Chard, K. Bubendorfer, S. Caton, and O. F. Rana, "Social cloud computing: A vision for socially motivated resource sharing," Services Computing, IEEE Transactions on, vol. 5, no. 4, pp. 551–563, 2012.

[6] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy preserving public auditing for secure cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013.

[7] G. Anthes, "Security in the cloud," Communications of the ACM, vol. 53, no. 11, pp. 16–18, 2010.

[8] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 9, pp. 1717–1726, 2013.

[9] B. Wang, B. Li, and H. Li, "Public auditing for shared data with efficient user revocation in the cloud," in INFOCOM, 2013 Proceedings IEEE. IEEE, 2013, pp. 2904–2912.

[10] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 384–394, 2014.

[11] 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," Computers, IEEE Transactions on, 2014, doi: 10.1109/TC.2014.2315619.

[12] C.-K. Chu, S. S. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 468–477, 2014.

[13] A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in cryptology. Springer, 1985, pp. 47–53.

[14] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586– 615, 2003.

[15] S. Micali, "Efficient certificate revocation," Tech. Rep., 1996.

[16] W. Aiello, S. Lodha, and R. Ostrovsky, "Fast digital identity revocation," in Advances in Cryptology–CRYPTO 1998. Springer, 1998, pp. 137–152.

[17] D. Naor, M. Naor, and J. Lotspiech, "Revocation and tracing schemes for stateless receivers," in Advances in Cryptology– CRYPTO 2001. Springer, 2001, pp. 41–62.

[18] C. Gentry, "Certificate-based encryption and the certificate revocation problem," in Advances in Cryptology–EUROCRYPT 2003. Springer, 2003, pp. 272–293.

[19] V. Goyal, “Certificate revocation using fine grained certificate space partitioning,” in Financial Cryptography and Data Security. Springer, 2007, pp. 247–259.
[20] A. Boldyreva, 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.
[21] B. Libert and D. Vergnaud, “Adaptive-id secure revocable identity based encryption,” in Topics in Cryptology–CT-RSA 2009. Springer, 2009, pp. 1–15.
[22] ——, “Towards black-box accountable authority ibe with short ciphertexts and private keys,” in Public Key Cryptography–PKC 2009. Springer, 2009, pp. 235–255.
[23] J. Chen, H. W. Lim, S. Ling, H. Wang, and K. Nguyen, “Revocable identity-based encryption from lattices,” in Information Security and Privacy. Springer, 2012, pp. 390–403.
[24] J. H. Seo and K. Emura, “Revocable identity-based encryption revisited: Security model and construction,” in Public-Key Cryptography–PKC 2013. Springer, 2013, pp. 216–234.
[25] ——, “Efficient delegation of key generation and revocation functionalities in identity-based encryption,” in Topics in Cryptology– CT-RSA 2013. Springer, 2013, pp. 343–358.
[26] 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,” in Computer Security-ESORICS 2014. Springer, 2014, pp. 257–272.
[27] D.-H. Phan, D. Pointcheval, S. F. Shahandashti, and M. Strefler, “Adaptive cca broadcast encryption with constant-size secret keys and ciphertexts,” International journal of information security, vol. 12, no. 4, pp. 251–265, 2013.
[28] R. Anderson, “Two remarks on public-key cryptology (invited lecture),” 1997.
[29] M. Bellare and S. K. Miner, “A forward-secure digital signature scheme,” in Advances in Cryptology–CRYPTO 1999. Springer, 1999, pp. 431–448.
[30] M. Abdalla and L. Reyzin, “A new forward-secure digital signature scheme,” in Advances in Cryptology–ASIACRYPT 2000. Springer, 2000, pp. 116–129.
[31] A. Kozlov and L. Reyzin, “Forward-secure signatures with fast key update,” in Security in communication Networks. Springer, 2003, pp. 241–256.
[32] X. Boyen, H. Shacham, E. Shen, and B. Waters, “Forward-secure signatures with untrusted update,” in Proceedings of the 13th ACM conference on Computer and communications security. ACM, 2006, pp. 191–200.
[33] J. Yu, R. Hao, F. Kong, X. Cheng, J. Fan, and Y. Chen, “Forward secure identity-based signature: security notions and construction,” Information Sciences, vol. 181, no. 3, pp. 648–660, 2011.
[34] R. Canetti, S. Halevi, and J. Katz, “A forward-secure public-key encryption scheme,” in Advances in Cryptology–Eurocrypt 2003. Springer, 2003, pp. 255–271.

[35] D. Yao, 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.

[36] J. M. G. Nieto, M. Manulis, and D. Sun, “Forward-secure hierarchical predicate encryption,” in Pairing-Based Cryptography–Pairing 2012. Springer, 2013, pp. 83–101.

[37] A. Sahai, H. Seyalioglu, and B. Waters, “Dynamic credentials and ciphertext delegation for attribute-based encryption,” in Advances in Cryptology–CRYPTO 2012. Springer, 2012, pp. 199–217.

[38] B. Waters, “Efficient identity-based encryption without random oracles,” in Advances in Cryptology–EUROCRYPT 2005. Springer, 2005, pp. 114–127.

[39] B. Lynn. (2014) Pbc library: The pairing-based cryptography library. [Online]. Available: http://crypto.stanford.edu/pbc/