ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

Efficient Revocation on Identity Based Encryption with Public Key Infrastructure in Cloud Computing

N S Sale, N R Talhar

ME Students, Department of Computer Engineering, All India Shri Shivaji Memorial Society's College of Engineering, Pune, Savitribai Phule Pune University Pune India.

Professor, Department of Computer Engineering, All India Shri Shivaji Memorial Society's College of Engineering, Pune, Savitribai Phule Pune University Pune India.

ABSTRACT: Distributed computing gives an adaptable and convenient route for information sharing, which brings different advantages for both the general public and people. In any case, there exists a characteristic resistance for clients to specifically outsource the shared information to the cloud server since the information frequently contains significant data. In this manner, it is important to put cryptographically upgraded get to control on the common information. Identity based encryption is a promising crypto graphical primitive to build a practical information sharing framework. However, access control is not static. That is, the point at which some client's approval is expired; there should be an instrument that can remove him/her from the framework. Thus, the revoked client can't access to both the previously and therefore shared information. To this end, we propose an idea called revocable-storage identity based encryption (RS-IBE), which can give the forward/backward security of cipher content by presenting the functionalities of client revocation and cipher content upgrade at the same time. Moreover, we display a solid development of RS-IBE, and demonstrate its security in the characterized security show. The execution correlations show 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.

KEYWORDS; Cloud Computing, Data Sharing, Revocation, Identity-Based Encryption, Cipher Text Update, Decryption Key Exposure.

I. INTRODUCTION

Cloud computing is a worldview that gives massive computation limit and huge memory space at a low cost. It empowers clients to get proposed benefits independent of time and location across multiple platforms (e.g., cell phones, PCs), and in this manner conveys extraordinary accommodation to cloud clients. Among various administrations gave by distributed computing, distributed storage administration, for example, Apple's iCloud , Microsoft's Azure and Amazon's S3 , can offer a more adaptable and simple approach to share information over the Internet, which gives different advantages to our general public . In any case, it additionally experiences a few security threats, which are the primary concerns of cloud clients. Firstly, outsourcing information to cloud server suggests that information is out control of clients. This may bring about clients' hesitation since the outsourced information normally contain important and sensitive data. Secondly, information sharing is frequently actualized in an open and hostile environment, and cloud server would become a target of attacks. Surprisingly more terrible, cloud server itself may uncover clients' information for unlawful benefit. Thirdly, information sharing is not static. That is, the point at which a client's approval gets expired, he/she should no longer possess the privilege of accessing the previously and subsequently shared data. Therefore, while outsourcing information to cloud server, clients additionally need to control access to these information such that only those currently authorized users can share the outsourced data.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

II. RELATED WORK

1. An efficiently outsourcing Attribute Based Encryption using SPs

Refer Points-

The reducer executes reduce function on the set of intermediate pairs (k', v') with the same key and outputs the final result.

2.Certicate Revocation using Fine Grained Certicate Space Partitioning

Refer Points-
The result displays that right balance between CA to directory communication costs and query costs by carefully selecting the number of partitions.

3.Fast Digital Identify Revocation

Refer Points-

The results were displayed that the proof from user to vendor of the validity of user's ID remains very small as per the micali method.

4.Privacy-Assured Outsourcing of Image Reconstruction Service in Cloud

Refer Points-

. The System effectiveness and efficiency and speedup of OIRS through hardware built-in system design.

5. Two Protocols for Delegation of Computation

Refer Points-

As extension of this protocol that somewhat reduces the workload of the client at the price of a comparable increase in the number of rounds.

6.Quasimodo: Efficient Certificate Validation and Revocation

Refer Points-

A result displayed that the direct improvement in both the overall verification complexity, as well as the communication complexity, over previous Tree-based schemes.

III. EXISTING SYSTEM APPROACH

1. Boneh and Franklin initially proposed a characteristic revocation way for IBE. They affixed the present era to the cipher text, and non-revoked users periodically received private keys for each time period from the key authority.
2. 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.
3. Subsequently, by using the aforementioned revocation technique, Libert and Vergnaud proposed an adaptively secure RIBE scheme based on a variant ofWater's IBE scheme.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

4. Chen et al. constructed a RIBE scheme from lattices.

Disadvantages of Existing System:

1. 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.
2. However, existing scheme only achieves selective security.
3. 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.
4. Furthermore, to update the cipher text, 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.

IV. PROPOSED SYSTEM ARCHITECTURE

1. It appears that the idea of revocable Identity based encryption (RIBE) may be a promising methodology that satisfies the previously mentioned security prerequisites for information sharing. RIBE features a mechanism that enables a sender to append the current time period to the cipher text such that the receiver can decrypt the cipher text only under the condition that he/she is not revoked at that time period.
2. A RIBE-based data sharing system works as follows:
3. 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 cipher text of the shared data to the cloud server.
4. Step 2: 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.
5. Step 3: In some cases, e.g., Alice's authorization gets expired, David can download the cipher text 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:

1. We provide formal definitions for RS-IBE and its corresponding security model;
2. We present a concrete construction of RS-IBE.
3. The proposed scheme can provide confidentialityand backward/forward secrecy simultaneously.
4. 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.
5. The procedure of cipher text update only needs public information. Note that no previous identity-based encryption schemes in the literature can provide this feature;
6. 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.

Equations are created using the traditional equation environment: To revoke ID at time period update the revocation list by

$$RL \leftarrow RL \cup \{(ID, t)\}$$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

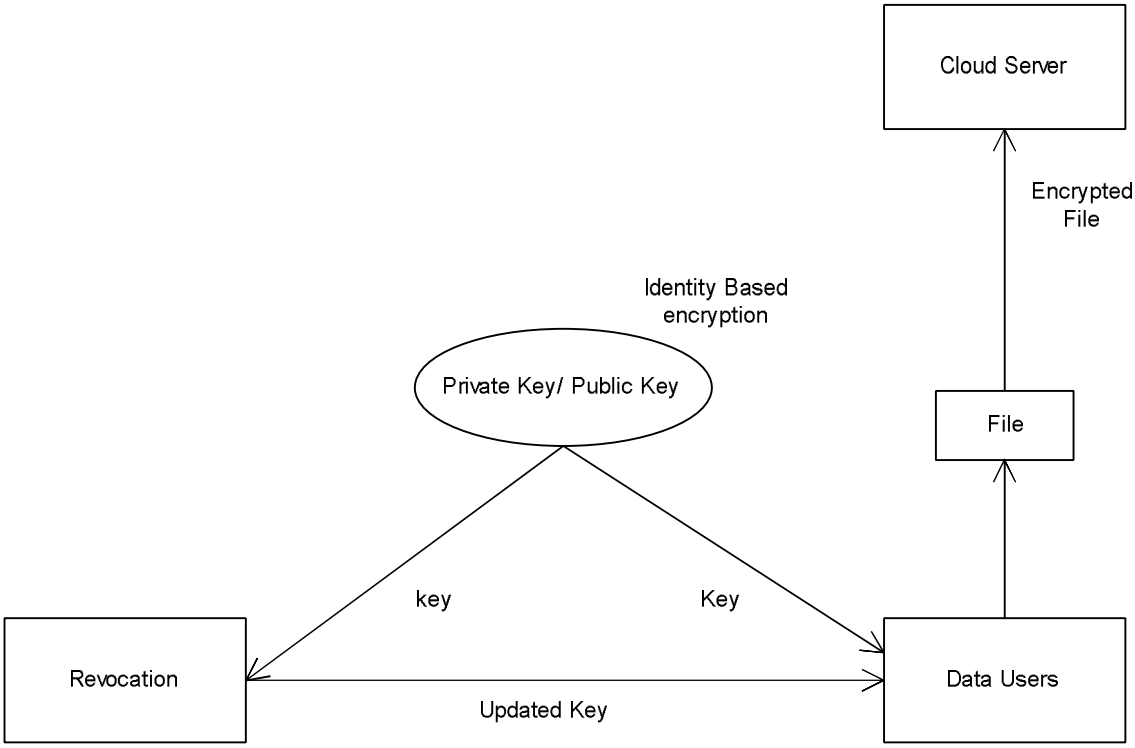


Fig 1.Proposed System Architecture

V. SOFTWARE REQUIREMENT SPECIFICATION

This software requirement specification (SRS) expresses complete description about Revocation on Identity Based Encryption with Public Key Infrastructure in Cloud Computing. This document includes all the functions and specifications with their explanations to solve related problems.
In proposed work is designed to implement above software requirement. To implement this design following software requirements are used.

- Operating system : Windows XP/7.
- Coding Language: JAVA/J2EE
- Database : MYSQL
- Tool : Eclipse Luna

VI. MATHEMATICAL MODEL

Revoke(PP, ID, RL, t, st) :-
RL :- Revocation List
t :- Time Period

$$\epsilon : -Denotebyrootnodeofthebinarytree BT$$

Path(n) :- Set of node on the path from ϵ to the leaf node n. for a non leaf node θ
To revoke ID at time period update the revocation list by

$$RL \leftarrow RL \cup \{(ID, t)\}$$

And return the updated RL.
Firstly , given a node

$$\theta \epsilon \, KUNodes(BT, RL, t) \cap Path(n) \ ,$$

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

we have that ,

$$DK_{t,\theta} = (SK_{\theta,0}.KU_{\theta,0}.F_u(ID)^{r_0}.Fh(t)^{r_1}, SK_{\theta,0}.g^{r_0}, KU_{\theta,1}.g^{r_1})$$
$$= (g_2^{\alpha}F_u(ID)^{r_{\theta,0}+r_0}Fh(t)^{r_{\theta,1}+r_1}, g^{r_{\theta,0}+r_0}, g^{r_{\theta,1}+r_1}).$$

Then, For a cipher text ,

$$CT_{ID,t} = (ID, t, C_0, C_1, C_2, \{C_u\}u\epsilon T_t),$$

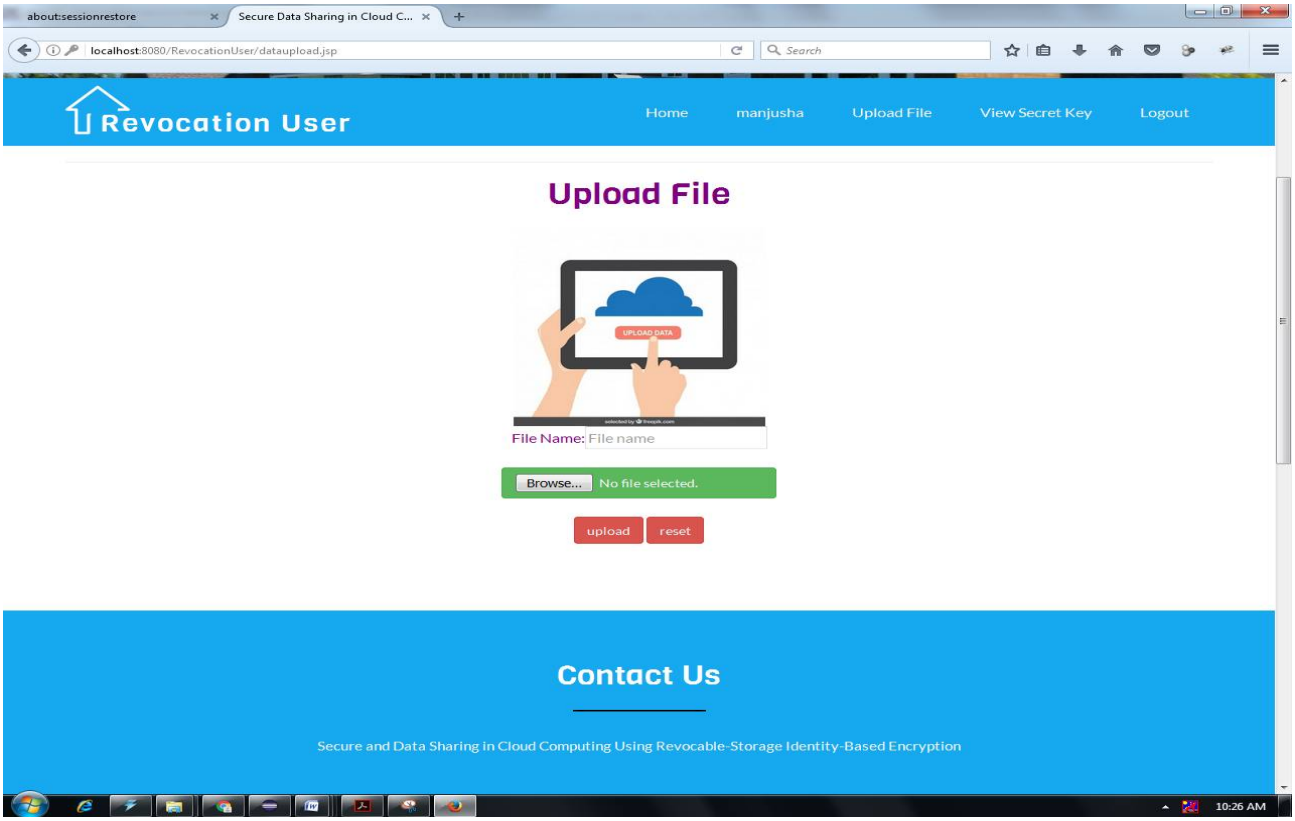
$$C_{u_{t,0}} = Fh(t)^{st}.$$

VII. IMPLEMENTATION STATUS

Proposed System divided into 4 modules:

1) **Data owner**
2) **Authority**
3) **User**
4) **Server**

First module data owner uploads the file in encrypted format to the server.



ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

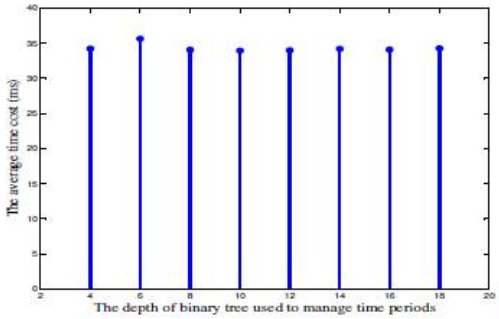
Vol. 5, Issue 2, February 2017

VIII. PERFORMANCE MEASURES

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, which are summarized in Table:

Schemes	Encryption	Decryption	STUpdate
Libert&Vergnaud	O(1)e+O(1)p	O(1)p	0
Seo&Emura	O(1)e+O(1)p	O(1)p	0
Liang et al.	O(1)e+O(1)p	O(1)p	(O(N))e+O(1)p
Our Scheme	O(logT)e+O(1)p	O(1)p	$O(\log(T)^2)$+O(1)p

IX. EFFICIENCY CALCULATION



(a) PKGen

X. EFFICIENT COMPARISONS FOR STAGES IN REVOCABLE IBE

	Our Scheme	IBE without Revocation
Setup	83.764ms	80.233ms
Key-Issuing	40.369ms	20.121ms
Encryption	39.840ms	24.595ms
Decryption	21.278ms	10.285ms

XI. CONCLUSION

Cloud computing brings extraordinary convenience for people. Especially, it perfectly coordinates the expanded need of sharing information over the Internet. In this paper, to assemble a cost effective and secure information sharing framework in cloud computing, we proposed a thought called RS-IBE, which supports identity revocation and cipher content upgrade simultaneously such that a revoked user is kept from getting previously shared information, and also therefore shared information. Besides, a concrete construction of RS-IBE is introduced. The proposed RS-IBE plan is demonstrated adaptive secure in the standard model, under the decisional ℓ-DBHE presumption. The correlation result shows that our in term of efficiency and functionality and in this way is more achievable for useful applications.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Website: www.ijircce.com

Vol. 5, Issue 2, February 2017

REFERENCES

[1] Jianghong Wei, Wenfen Liu, Xuexian Hu , "Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption", Journal Of Latex Class Files, Vol. 14, No. 8, August 2015.
[2] 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.
[3] G. Anthes, "Security in the cloud," Communications of the ACM, vol. 53, no. 11, pp. 16–18, 2010.
[4] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," Parallel and DistributedSystems, IEEE Transactions on, vol. 24, no. 9, pp. 1717–1726, 2013.
[5]W. Aiello, S. Oldham, and R. Ostrovsky, "Fast digital identity revocation, "in Advances in Cryptology (CRYPTO'98). New York, NY, USA: Springer, 1998, pp. 137–152.
[6] 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.
[7] B. Libert and J.-J. Quisquater, "Efficient revocation and threshold pairing based cryptosystems," in Proc. 22nd Annu. Symp.Principles Distrib.Comput., 2003, pp. 163–171.
[8] 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.
[9] A. Shamir, "Identity-based cryptosystems and signature schemes," in Advances in cryptology. Springer, 1985, pp. 47–53.
[10] D. Boneh and M. Franklin, "Identity-based encryption from the weil pairing," SIAM Journal on Computing, vol. 32, no. 3, pp. 586– 615, 2003.
[11] S. Micali, "Efficient certificate revocation," Tech. Rep., 1996.