International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 05 Issue: 07 | July 2018 www.irjet.net p-ISSN: 2395-0072

Identity Based Encryption with Use of Fragments in Revocable Storage for Secure Data Sharing

Rutambh Alkeshbhai Trivedi[1], Shyamsuder P. Kosbatwar[2]

[1]*Student.Dept.Computer Engineering,Sinhgad Institute's Smt.Kashibai Navale College Of Engineering, Pune, India*
[2]*Professor, Dept.Computer Engineering, Sinhgad Institute's Smt.Kashibai Navale College Of Engineering,Pune,India*

Abstract – *The major benefit of cloud computing over others is that the cloud computing gives the flexible and Convenient way to share the data. But the main problem that exists and faced by every user is that the data outsourcing. That is one of the biggest threats in the cloud computing because sometimes it also contains the valuable information for the user and if it can't be secured that what is the point of using the cloud computing. That's why that is necessary that to place a tool that should control the accessing file users. We developed the cryptographically supported access control on the shared data. Our Encryption method is a cryptographical approach to build the sharing system that is practical for all the applications. When some user's authorization is expired, there should be a module that can remove the user from the system. The user which is no longer in the system or revoked user can't access both the previously shared data and subsequently shared data, And for the security issues, our system is based on the Fragment Storage too. In the end, we providing implementation results of the Given scheme to show its practical Performance.*

Key Words: Revocation based storage, Cloud computing, Ciphertext, Identity Based, Security Sharing, Data Sharing, Fragment Storage

1. INTRODUCTION

In this modern day's Cloud computing is the easy and feasible way to give the reasonable solution to taking control of our data without question of time and location. There are numerous services provide by cloud computing, for example, cloud storage services, such as Amazon's S3, Microsoft's Azure and, Apple's iCloud which offer a more easy and flexible way to share data over the Internet, which will give many benefits to us and our society. There are many clouds available nowadays but the in them all security concern common to all is security issues. Furthermore, There is one disadvantage of that is it also suffers from several security issues, which are the primary points and issues for cloud users too.

When a user uploads the data to the cloud which chosen by the user, it will be no longer in under users control and that is one of the big and main reasons why that is not secured and the further risk is that the cloud is open to the attacks will be big that can highly damage. Outsourcing data to cloud server means that Uploaded data by users is out control of users who Uploaded it. And that is the reason why cause users' hesitation because the data which is the outsourced data many times contain a valuable and sensitive information from the user side. Second of all, data sharing is done in an open and vulnerable environment, and cloud server would become an easy target for the attacks. Not only that but worse, cloud server itself may show the users' data to the attackers for illegal profit. And third, data sharing is not that static. So That is why, when a user's authorization is no longer works or we can say that gets expired, that user should no longer get the benefit of accessing the subsequently and Data that is previously shared.

We are providing the major benefit over other system is that we are using the Fragment storage which is better providing the security compared to the other systems. While outsourcing data to cloud server, users also want to control access to these data such that only those currently have the authorization only that users can share that data. A natural solution to conquer the shown problem is to use our system access control. Furthermore, to overcome the above security problems, such kind of access control placed on the shared data should meet the following security goals.

1.1 Security Goals

These three are security goals that are introduced in this paper.

Data confidentiality

Those Users who have not authorization they will be prevented from the access the data. Cloud server will have also a Plain-text of the shared data. It is necessary to have the mechanism that prevents revoked users to access the data.

Backward secrecy

When Authorization of the particular user expired, or a user's secret key is attacked, a user should be prevented from accessing the plain-text of the data that is subsequently encrypted under its identity.

Forward secrecy

When Authorization of the particular user expired, or a user's secret key is attacked, the user should be prevented

from accessing the plain-text of the data that is previously encrypted under its identity.

1.2 Motivation

The Concept of this paper is Give the access control to the user for their Uploaded data and it can solve the issues regarding the currently existing systems, and our system also gives a facility to revoke the user from the system that has no authorization, the big advantage of that will be the user can't access the data which is encrypted even if that data is encrypted under user's identity.

2.REVIEW OF LITERATURE

1. A. Shamir, "Identity-based cryptosystems and signature schemes [5]"

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).

2. D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing [6]"

There should 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 by S. Micali, W. Aiello, S. Lodha, and R. Ostrovsky, D. Naor, M. Naor, and J. Lotspiech, C. Gentry, V. Goyal, and several techniques are widely approved, such as certi_cate 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 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.

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.

3. A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with e_cient revocation "[7][8]

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.

4. B. Libert and D. Vergnaud, "Adaptive-id secure revocable identity-based encryption "[9]

The author proposed an adaptively secure RIBE scheme based on a variant of Water's IBE scheme, Chen et al. constructed an RIBE scheme from lattices.

5. J. H. Seo and K. Emura, "Revocable identity-based encryption revisited: Security model and construction"[10]

Recently, Seo and Emura proposed an efficient RIBE scheme resistant to a realistic threat called decryption key exposure, which means that the disclosure of decryption key for current time period has no effect on the security of decryption keys for other time periods.

6. 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" [11]

Inspired by the work Liang introduced a cloud-based revocable identity-based proxy re-encryption that supports user revocation and ciphertext update. To reduce the complexity of revocation, they utilized a broadcast encryption scheme to encrypt the ciphertext of the update key, which is independent of users, such that only non-revoked users can decrypt the update key. However, 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.

7. M. Bellare and S. K. Miner, "A forward-secure digital signature scheme " [13]

They provided formal definitions of forward-secure signature and presented practical solutions.

Since then, a large number of forward-secure signature schemes M. Abdalla and L. Reyzin, A new forward-secure digital signature scheme, A. Kozlov and L. Reyzin, Forward-secure signatures with the fast key update, X. Boyen, H. Shacham, E. Shen, and B. Waters Forward-secure signatures with the untrusted update, J. Yu, R. Hao, F. Kong, X. Cheng, J. Fan, and Y. Chen Forward secure identity-based signature: security notions and construction, has been proposed.

8. R. Canetti, S. Halevi, and J. Katz, "A forward-secure public key encryption scheme"[14]

The author proposed the first forward-secure public-key encryption scheme. Specifically, they firstly constructed a binary tree encryption and then transformed it into a

forward-secure encryption with provable security in the random oracle model.

9. D. Yao, N. Fazio, Y. Dodis, and A. Lysyanskaya, "Id-based encryption for complex hierarchies with applications to forward security and broadcast encryption "[15]

They proposed a forward-secure hierarchical IBE by employing two hierarchical IBE schemes, and Nieto et al. designed a forward-secure hierarchical predicate encryption. Particularly, by combining Boldyreva et al. s revocation technique and the aforementioned idea of forward security, in CRYPTO 2012 Sahai, Seyalioglu and Waters Revocable storage attribute-based encryption

10. A. Sahai, H. Seyalioglu, and B. Waters, "Dynamic credentials and ciphertext delegation for attribute-based encryption "[16][17]

They proposed a generic construction of so-called revocable storage attribute-based encryption, which supports user revocation and ciphertext update simultaneously. In other words, their construction provides both forward and backward secrecy. What must be pointed out is that the process of ciphertext update of this construction only needs public information. However, their construction cannot be resistant to decryption key exposure, since the decryption is a matching result of private key and update key.

11. Jianghong Wei, Wenfen Liu, Xuexian Hu, "Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encrypt" [18]

They proposed the time period for revoking the user, When Sender will upload the file he can also set the timing for that _le, so in that current time Ciphertext can be decrypted. They didn't t implement the idea of revocation in their system. The author proposed the way to efficiently upload the data and Download the data with the help of identity-based encryption. That is remarkable that they also gave the revocation mechanism with that. But the main issue is that their scheme is taking more time in Encryption and Decryption. The base on the revocation should be done is not mentioned in their scheme. And the also didn't mention about they require the secure channel or not. The security on their scheme is less.

2.1 Our Contributions

In this paper, we introduce a notion called revocable storage identity-based encryption (RS-IBE). The main benefit of this system will build a cost-saving data sharing system that fulfills our three security goals.

• We provide the basic structure and the definitions for RS-IBE, We also provided the security model that perfectly balanced with this scheme.

• We also presented the concrete construction of RS-IBE.

The main advantage of this scheme over other existing scheme is that our proposed scheme can provide confidentiality, backward secrecy, and forward secrecy simultaneously;

• Our proposed scheme can withstand decryption key exposure;

We also added the Fragment Storage system

Our main secured part is Dynamic auditing, By that way if the part of the File is modified by an attacker than it Will Show the user that it is modified and User can know that.

The user won't revoke the client but User can Block the specific file from sharing. The user doesn't have to delete the file from the server.

The user can block the certain users from getting the files too.

If the fragment of the file is missing, deleted or because of attack, it modified than we also added the Module that it can be Regenerated.

No existing scheme gives the All security goals Completed, and the Storage of that is really vulnerable for the Outside attacks where in our scheme it's really secured.

3. Proposed System

Step 1

First of all, we are taking the data provider who will decide that which users can share their data. Then the data provider will encrypt the data on the based on their identities and also uploads the data ciphertext on the cloud. Here the encryption will be based on the identities of the users

Step 2

If both the users want to share the data, then, first of all, they have to download and decrypt the ciphertext first. if there is the third user and that user also wants to see the data or share the data it has to get the authorization or that user cant gets the data. The user won't authorized.

Step 3

For instance when some user's Authorization is expired then the data provider will download the ciphertext of the data and will decrypt first then again data provider will re-encrypt it so that the second user which has still an authorization won't access that data. Its necessary that Both the users have the authorization And after the re-encryption of the data, the data provider will again upload that data to the cloud so that it can be secured.

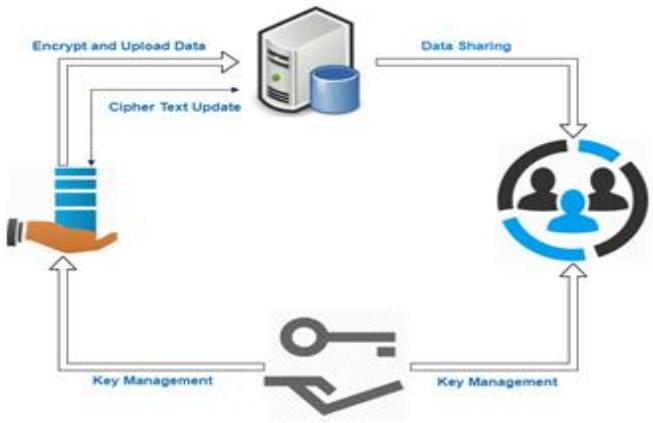

Fig-1: Proposed System

4. ALGORITHM

In our Revocable storage Identity-based encryption we are using the Binary tree structure, Which was also introduced by Boldyreva, Goyal, and Kumar to achieve efficient and Fast revocation. For Show the Revocation mechanism, First of all, we had to present the several notations. The Root node of the binary tree BT denotes by ε the, and Path(η) which is the set of nodes on the path from ε to the leaf node η (including ε and η). For a node which not currently in the leaf or we can say non-leaf node θ, we let θl and θr as for its left and right child. we took the revocations list as RL, which is comprised of the tuples (ηi, ti) which are stands for the node ηi was revoked at time period ti, the algorithm KUNodes(BT, RL, t) outputs the smallest subset Y of nodes of BT because Y contains an ancestor for each node which is not revoked.

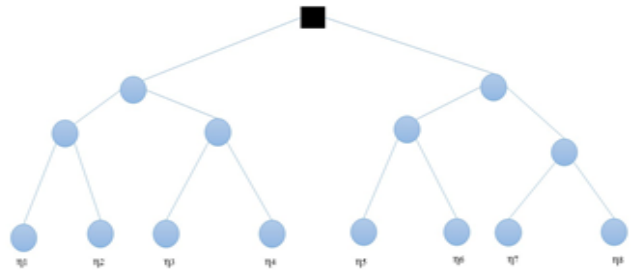

Fig -2: When No Nodes are Revoked

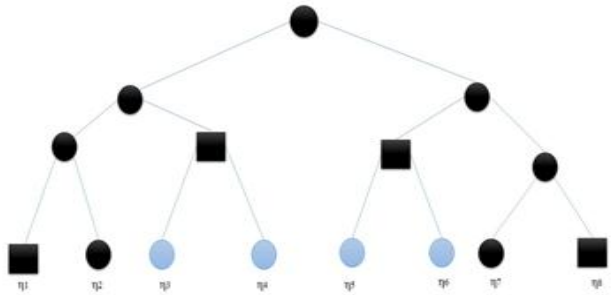

Fig-3: When Specific Nodes are Revoked

Informally, to identify the set Y, First, the algorithm will do is marks all the ancestors of revoked nodes as revoked, the second it only outputs all the non-revoked children of revoked nodes, not the Ancestors. As an example, we present two instances of the algorithm KUNodes in The formal description is given below.

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: endif

6: end for

7: for all θ ∈ X do

8: if θl /∈ X then

9: Add θl to Y

10: endif

11: if θr /∈ X then

12: Add θr to Y

13: endif

14: end for

15: if Y = ∅ then

16: Add the root node ε to Y

17: endif

18: return Y

5. SECURITY MODEL

Syntax of RS-IBE

Definition (Revocable-Storage Identity-Based Encryption).

A revocable-storage identity-based encryption scheme with message space M, identity space I and the 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 PP and the master secret key MSK, associated with the initial revocation list RL = ∅ and state st.

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

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

• DKGen(PP, SKID, KUt): The decryption key generation algorithm takes as input PP, 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(PP, ID, t, M): The encryption algorithm takes as input PP, an identity ID, a time period t ≤ T, and a message M ∈ M to be encrypted, and outputs a ciphertext CTID,t.

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

• Decrypt(PP,CTID,t,DKID,t′): The decryption algorithm takes as input PP, CTID,t, DKID,t′ , and it recovers the encrypted message M or a distinguished

symbol ⊥ indicating that CTID,t is an invalid ciphertext.

• Revoke(PP, ID, RL, t, st): The revocation algorithm takes as input PP, 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.

Security Model

Setup

The setup takes as input the security parameter, the time-bound T, and the maximum number of system users N, and it outputs the public parameter PP and the master secret key M SK, associated with the initial revocation list RL = and state st.

C performs Setup(1, T,N) (PP,MSK) and sends PP to A;

Phase 1

The following queries in an adaptive way: a. OSK(ID): C performs PKGen(PP,MSK, ID) (SKID, st) and returns SKID to A;

OKU(t): C runs KeyUpdate(PP,MSK,RL, t, st) KUt and returns KUt;

ODK(ID, t): C runs PKGen(PP,MSK, ID) (SKID, st) and DKGen(PP, SKID,KUt) DKID,t, then forwards DKID,t to A;

ORV (ID, t): C updates the current revocation list RL by running Revoke(PP, ID,RL, t, st) RL and returns the updated RL to A;

6. SECURTIY ANALYSIS

All are the adaptive-secure model. PKU is Private key updation. PCU is Private Ciphertext Updation. DBDH is Decisional Bilinear Diffie-Hellman assumption, and - dBDHE is decisional - Bilinear Diffie-Hellman Exponent assumption. CA is collusion attack. DKE is decryption key exposure. FS and BS indicate forward and backward secrecy, respectively.

In this table, these four schemes are all secure insecurity models, and can also capable to provide the backward secrecy because all other schemes are using the identity revocation. But the security assumptions are different in ours than others.

First two schemes will update the user's secret keys in a public way so Update key will available for all the users. And in the third scheme, it involves the broad encryption to update the secret key so that only non-revoked user can have update key. In their scheme, they can not resist the attack of revoked and non-revoked users attacks simultaneously. In the comparison of the above three schemes and our scheme, Our scheme gives the forward secrecy too and additionally introduces the ciphertext update. In the third scheme, The procedure for update the ciphertext is private and interact way because it requires the periodically re-encryption keys to update them in the cloud.

Table -1: Comparison of Secure Revocation Schemes

Schemes	PKU	PCU	CA	DKE	FS	BS
Libert and Vergnaud	YES	NO	YES	NO	YES	NO
Seo and Emura	YES	NO	YES	YES	YES	NO
Liang et al.	NO	NO	NO	YES	YES	YES
Jianghong Wei, Wenfen Liu, and Xuexian Hu	YES	YES	NO	YES	YES	YES
Our scheme	YES	YES	YES	YES	YES	YES

7. PERFORMANCE ANALYSIS

Presenting the Results of the System done on various Modules.

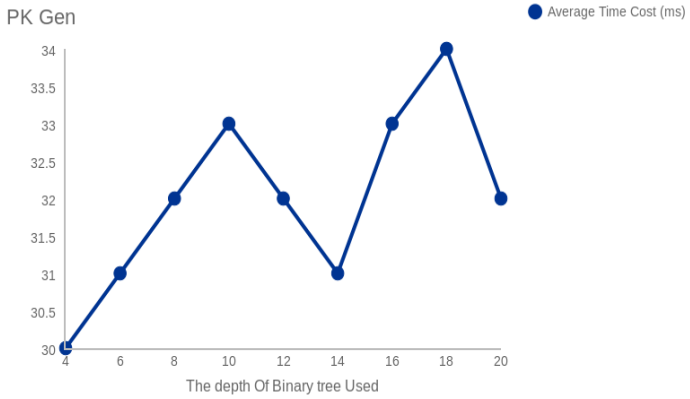

Chart -1: PKGEN

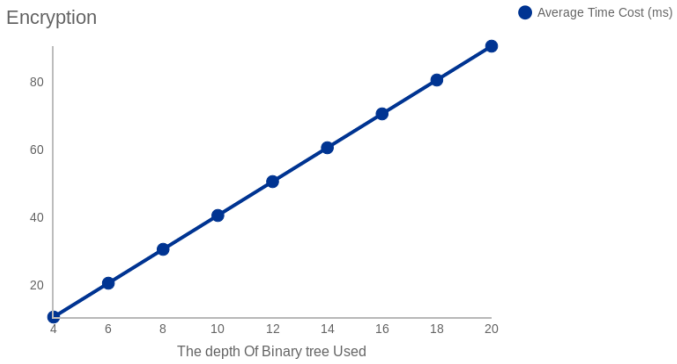

Chart -2 :Encryption

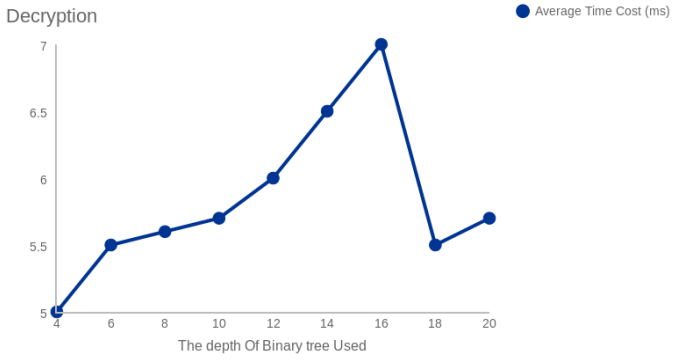

Chart -3: Decryption

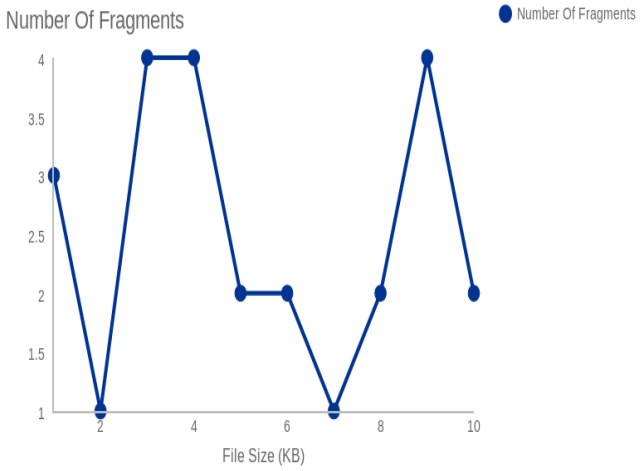

Chart -4: Number of Fragments Generated

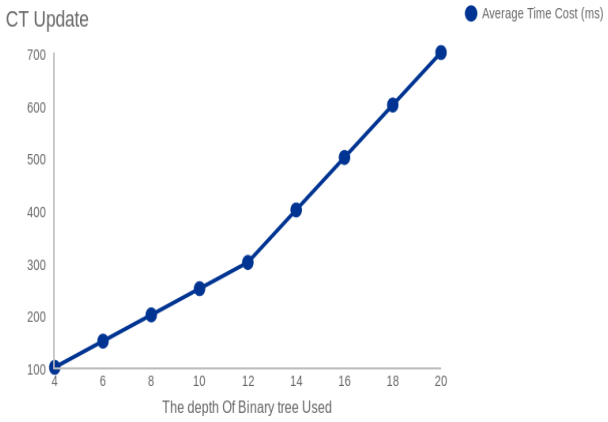

Chart-5 : CT Update

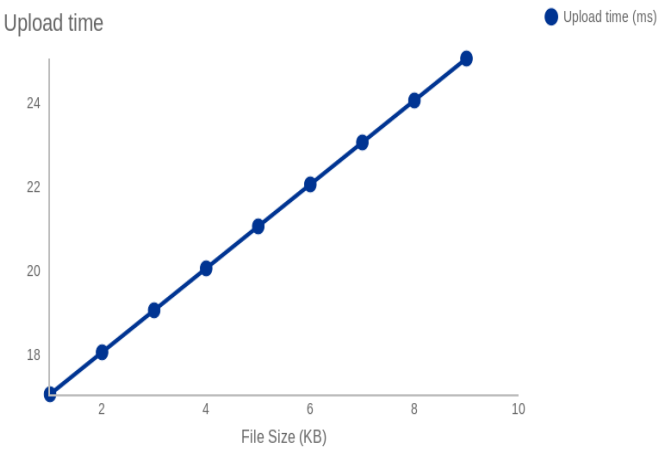

Chart-6: Upload time in CSP

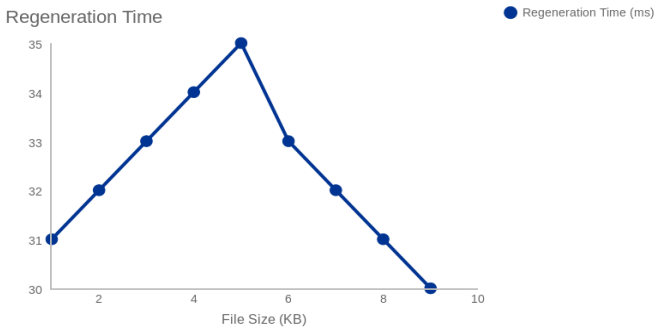

Chart-7: Regeneration Time Taken

This performance analysis shows that our scheme is better than all existing schemes, Also our scheme is in better in the way of Efficiency and Flexibility.

8. CONCLUSION

With The Cloud Computing, we can access our data anytime anywhere. In this paper, we are implementing a tool which will be of no high cost but It we will give better security, Its called Revocable storage identity based encryption, which will do both the things simultaneously which are identity revocation and ciphertext update, which will prevent user from accessing the shared data which is previously shared, as well as subsequently shared data.RS-IBE is better than others in the security in terms of efficiency and functionality, and RSIBE is more reliable. We also added the Fragment storage for this system. We can also save the Each Fragment on different Servers but that will be included in Future Scope.

REFERENCES

1. L. M. Vaquero, L. Rodero-Merino, J. Caceres, and M. Lindner, "A break in the clouds: towards a cloud de_nition" ACM SIGCOMM Computer Communication Review, vol. 39,

no. 1, pp. 50 55, 2008.

2. 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.

3. 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.

4. G. Anthes, Security in the cloud, Communications of the ACM, vol. 53, no. 11, pp. 16 18, 2010.

5. A. Shamir, Identity-based cryptosystems, and signature schemes, in Advances in cryptology. Springer, 1985, pp. 47 53.

6. D. Boneh and M. Franklin, Identity-based encryption from the Weil pairing, SIAM Journal on Computing, vol. 32, no. 3, pp. 586 615, 2003.

7. V. Goyal, Certi_cate revocation using _ne grained certi_cate space partitioning, in Financial Cryptography and Data Security. Springer, 2007, pp. 247 259.

8. A. Boldyreva, V. Goyal, and V. Kumar, Identity-based encryption with e_cient Revocation, in Proceedings of the 15th ACM conference on Computer and communications

security. ACM, 2008, pp. 417 426.

9. B. Libert and D. Vergnaud, Adaptive-id secure revocable identity-based encryption, in Topics in Cryptology CT-RSA 2009. Springer, 2009, pp. 1 15.

10. 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.

11. K. Liang, J. K. Liu, D. S. Wong, and W. Susilo, An e_cient cloud-based revocable identity-based proxy re-encryption scheme for public clouds data sharing, in Computer Security-ESORICS 2014. Springer, 2014, pp. 257 272.

12. R. Anderson, Two remarks on public-key cryptology (invited lecture), 1997.

13. M. Bellare and S. K. Miner, A forward-secure digital signature scheme, in Advances in Cryptology CRYPTO 1999. Springer, 1999, pp. 431 448.

14. 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.

15. 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.

16. 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.

17. B. Waters, E_cient identity-based encryption without random oracles, in Advances in Cryptology EUROCRYPT 2005. Springer, 2005, pp. 114 127.

18. Jianghong Wei, Wenfen Liu, Xuexian Hu "Secure Data Sharing in Cloud Computing Using Revocable-Storage Identity-Based Encryption" IEEE Transactions on Cloud Computing,23 March 2016, ISSN: 2168-7161, 10.1109/TCC.2016.2545668