High Data Availability with Effective Data Integrity and User Revocation Using Abe Scheme for Cloud Storage

Prashant mininath mane, C. M. Sheela rani

Abstract*: With Cloud Storage, organizational members can outsource their sensitive information on cloud; utilize the on demand quality applications and services of cloud, with less control over stored data. With this, there is important concern issue with security over sensitive data, which can be fixing with data encryption techniques. In this, owner of the data encrypt their sensitive information before storing on cloud systems. Attribute based Encryption (AttBE) system is one of the asymmetric key based cryptosystem, used for secure control to access the stored data of cloud. Unfortunately, AttBE provides fine grained control to access the data but suffers from a drawback of data integrity. As Sensitive information is stored on the cloud, there is no guarantee of integrity of data because of data may loss or stolen by cloud itself or any hacker. Proposed system handles this problem by introducing the third party authority. TPA stores the data on cloud in the form of blocks and then he checks each and every block by regular integrity check. Proposed system also address the issue of revocation in case of user leaving the group or organization; once a user is removed from the group, the keys are updated and these new keys are distributed among the existing users. Experimental results show the performance of projected system is better than the current implemented systems in terms of time consumption and memory utilization.

***Index Terms*: Searchable Encryption, Data Availability, Cloud Computing, Revocation of Attributes, User Revocation.**

I. INTRODUCTION

Cloud systems are also known as 'on-demand computing'. Data is stored centrally and by third-party user data get processed also solutions for storage issues given to user's cloud computing accepts and enterprises with various capabilities. With minimum efforts from management available resources are cater and freed very often. Due to points such as, highest computing power, minimum cost of applications and services, high scalability, accessibility and availability cloud computing is very largely demanded service over the globe.

While operating depository storage demands the guarantees related with the authenticity of information on storage, particularly that storage servers data. Very small part of information is fetched whereas the depository servers store a large amount of data. While storing the data for long period of time there might be high risk for data by the means of machine or human errors. Solutions made previously are not up to the mark for securing data by human or machine errors in the matter of information possession. By extending storage complexity some of systems give a weaker guarantee. Also in all systems available till now are depending on server for fetching the total file, which is not doable when the working with the large amount of information. To maintain the status or economic explanations the service provider of cloud break trust, for hiding the information loss or corruption. So that for the clients it is nice to have a protocol for checking the information they stored on the cloud to make sure that cloud is always maintaining their information. Form past few years' regeneration codes are on boom due to their minimized restore bandwidth whilst provides fault tolerance.

Because of high availability as well as reliability at the time of launching low storage overhead in storage framework the regeneration coding in used widely. It is nothing but a process of data security which saves information from getting damaged into fragments, improved, encoded and also precludes duplicate data portions and stored across distinct areas or storage media. To regenerate corrupted information by using data which is stored in some other place as the array in the disk storage approach is the main purpose of erasure coding. This can be turned out to be major measurement of information and any function or system. The system must go through some issues like disk array methods, data grids, disbursed storage purpose, object retailers also archival storage. Presently object-headquartered cloud repository is using of erasure coding.

TPA -Third Party Auditor which acts as a public entity who checks the integrity of data uploaded by Data Owner(DO)with most protected and resourceful approach saving computation load in downloading of complete data on client side.TPA stores the file in Cloud in the form of fragments. He gets the fragments from the cloud and check its Hash value with the stored hash value. If there is any change in hash value, then the file considered as tempered. The group owner will readily broadcast clients private keys to the individuals who have been renounced in case of user revocation from group. We are focusing on security integrity with fine-grained access control so that proposed scheme withstand against chosen-keyword attack.

In proposed framework of ABE, Sensitive data get stored on the cloud by encrypting with the set of attributes and Key generated by both Cloud Authority and TPA. So access control is achieved through such type of encryption. User can download or access the data only if he have set of attributes and the key generated by Cloud and TP

Revised Manuscript Received on March 02, 2019.

Mr. Prashant Mininath Mane, *Ph. D. Research Scholar, CSE Department, K.L.E.F.University, Vijaywada ,India*

Dr. C. M. Sheela Rani, *Professor, CSE Department, K.L.E.F.University, Vijaywada ,India*

A. *Motivations*

Huge amount of sensitive information is stored on the cloud servers which enables to data owners to share their data but it also required the security and privacy of sensitive information. The big issue regarding the storage of data on cloud is Confidentiality of Sensitive information. Another big issue to provide the Effective Access control. Motivation behind this research to provide the confidentiality of data and effective control to access the data stored in cloud.

B. *Contributions*

In this system, we are proposed the ABE framework to provide excellent access control, excellence data integrity check and effective user revocation scheme. Excellent access control achieved through encryption of data by set attribute and secrete key generated by both TPA and Cloud entity. Excellence Data integrity is achieved through TPA. It divides the file in fragments, store hash value of each fragment on TPA and then stores each fragment of that file on cloud. During integrity check, TPA matches the hash value of file fragments stored on cloud and hash values of that file he stored on TPA. if hash values are not matched, then there is a loss of data or corruption of data. if any user leaves the group, all existing keys are updated and distribute to all the existing users. In this way the system provides the effective User Revocation.

C. *Organization* of *paper*:

Remaining paper is divided as: Part 2 Contains literature survey, Part 3 contains proposed system architecture, Part 4 contains Results and Discussion, Part 5 contains conclusion.

II. LITERATURE REVIEW

Amit Sahai and Brent Waters[2005][1], firstly introduces secure and fault tolerant system using Fuzzy IBE. In this system data is encrypted using biometric and set of attributes. But this scheme faces the problem of encrypt the data using attributes from multiple agencies.

Hur[2013]9 presents CPABE scheme to solve the key-escrow problem using generation of secrete key by two authorities. Also presents the effective user revocation using proxy encryption scheme. But this scheme is also work for single attribute authority environment.

Yu S, Wnag C[2010]5 proposed KPABE Scheme combined with proxy reencryprion and Lazy Reencryption to achieve the effective access control and integrity of data. Confidentiality of data access policies and accountability of user private keys is achieved in this scheme. Is also achieve scalability of the data. This scheme is not much more useful because of it generates multiple ciphertext replica of same data.

Kan Yang[2013]10 presents CPABE scheme of multi authority cloud system, where attributes are selected for encryption from multiple authority centers. It also provides revocation of attribute method to achieve forward as well as backward security. In user revocation technique non revoked user cannot disclose the received key updates to the user who is revoked from the group.

Lija Mohan[2014]12 presents a scheme to achieve the effective access control using basic cryptographic techniques combined with bivariate scheme and symmetric polynomials. this framework provided the capability of access revocation. In this framework the new polynomial is generated and distributed to all non revoked users.

Nikita Gorasia[2016]13 proposed the multiple authority ABE using fast Encryption. This scheme uses and, threshold and OR to acheiev the fast encryption as well as effective access control.

Robert H.[2013]11 presents ABE scheme which is designed on the basis outsourcing the encryption task. The scheme provides new technique which is verifiable and more secure and it does not depend on random predictions. In their work, they developed a different view for ABE that, all things considered, wipes out the overhead for clients. However, their construction does not consider overhead computation at the attribute authority involved in the key-issuing process.

B. Waters[2006]2 consider the problems of user revocation which involves re-encrypting e information that is accessible to the client leaving the system and updating the private keys of users remaining in the system. They have proposed a scheme that enables the owner of the data to outsource the task of re-encryption and private key updates to a third party without revealing the content and the user information. They have very well attained the finely grained and scalable access in cloud computing. However, the complexity in client revocation increases with the addition in the number of clients which makes the system more difficult. And that does not support user accountability.

Chase M.[2007]3 proposed the scheme in which any polynomial integer number of individual authorities to observe attributes and issue the private key. An owner encrypt the data with a number d[k] and attribute set. The user can decrypt the data if he have atleast d[k] attributes. This scheme also contributes to provide multiple authority ABE to provide excellence control to data access. One of the requirement of this scheme is attribute set of each Authority be disjoint.

Chase M.[2009]4 proposed the scheme attribute dependant encryption technique without reliable central authority. it introduces the anonymous key issuing technique to provide effective access control.

Yang K, Jia X.[2012]7 proposes multiple authority ABE technique without any global authority and use LSSS data access technique. Also work on effective revocation of attributes from any attribute authority.

Wan Z, Liu J, Deng R-H. [2012]8 proposed the system which is the combination of Hierarchical ABE and Ciphertext ABE to provide effective access control. It provides not only effective access control but also complete delegation and excellence performance. Also provide the scalable revocation technique by using proxy RE and Lazy RE for revoking the access rights from revoked user.

Lewko A,Waters B.[2011]6 presents the system to achieve the goal of self-directed key generation and prevent collision attacks between user and different authorities.

III. PROPOSED APPROACH

A. Objectives:

To design an significant and Efficient data access control technique for multiple authority cloud systems.

To provide effective security to the data stored on cloud using data fragmentation.

To provide integrity checking against the service attacks and threats.

B. Problem Statement

Implementation of multiple authority attribute based access control system to provide the fine grained access control with proper integrity checking against lost or tampered of data by attacker using third party auditor.

C. Proposed System Overview

Proposed system contains the four entities:

1. User: this entity wants to download the files stores on the cloud.

2. Owner: this entity stores the sensitive information files on the cloud. Owner encrypts the data before storing on cloud using different attributes and key generated by TPA and cloud authority.

3. TPA: this entity provides addition or deletion of attribute set. Also it generates the key with the help of cloud authority.

4. Cloud System: All the sensitive information is get stored on cloud.

Propose system contains the four modules to provide the effective access control and data integrity.

1. Admin Head(Owner) : first, owner stores their sensitive information on cloud after encryption. The data is encrypted by attribute set atrk from multiple authorities and the combined key Ck generated by TPA and Cloud authority. The admin send the encrypted data to TPA.7

$$CipherText \rightarrow File + C_k + atr_k$$

2. TPA: TPA & cloud authority generates the key Ck for the encryption of data. That key is send to owner after he receives the request for key to upload the data. When owner get the key Ck, then he upload the sensitive information to TPA. Then TPA divides the file into fragments and stores its hash value. Then he uploads the file fragments on different blocks of cloud. TPA scan the stored file by the request of owner for loss or stolen of data stored on the cloud. Then TPA, on request from owner check the hash values of the files stored on cloud and the hash value he have on TPA. If hash values matches then there is no tempering of data.

$$TPA \rightarrow S_{k1}$$
$$CSS \rightarrow S_{k2}$$
$$C_k \rightarrow S_{k1} + S_{k2}$$

TPA also works on User or Attribute Revocation. When any attribute or user revoked, then he updates the all key values and distributes it to all the non revoked users.

Key updating is done by gid, original key Ck, Revocation list Rl. it generates the new key Ck1 by

$$C_{k1} \rightarrow gid + C_k + R_l$$

The newly generated C_{k1} is distributed to all non revoked users.

3. User: when user want to download any file from cloud then he need to decrypt that file. The file is decrypted only when he has the attribute set and Ck. then he send the request for downloading the file to TPA.

$$File \rightarrow CipherText + C_k + atr_k$$

4. Cloud: All the files are stored on the cloud. it view all files present on the cloud. Also it views all the users registered for using cloud system

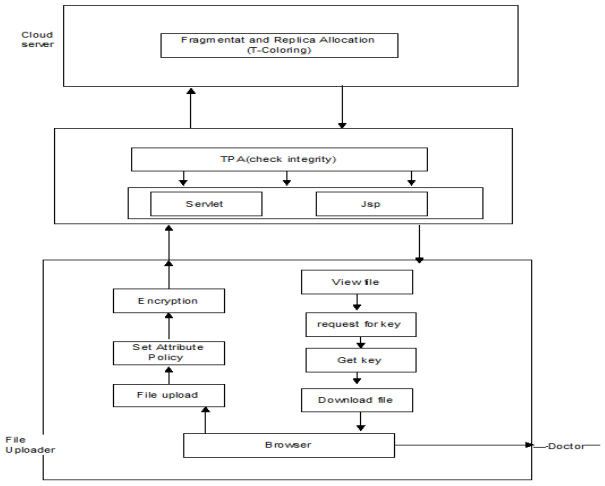

Fig 1: Time Comparison Graph

IV. RESULTS AND DISCUSSIONS

A. Experimental Setup

All the experimental cases are implemented in Java with Netbeans tools and MySql as backend, algorithms and strategies, and the competing rule generation approach along with various encryption technique, and run in distributed environment with Master System having configuration of Intel Core i5-6200U, 2.30 GHz Windows 10 (64 bit) machine with 8GB of RAM and Slave System with configuration of Intel Core i5-2430M, 2.40 GHz Windows 7 (64 bit) machine with 4GB of RAM.

B. Dataset Description

The Input for Project is real time dataset such as news dataset or email dataset from the Machine Learning UCI Repository, News Dataset is a text data set which contains sports and political related data.

C. Result

Here, the performance between existing and proposed system is compare. The following graph shows the time requires generating encryption key over the number of attributes. In Figure 2, X-axis shows number of attributes used while Y-axis shows required time to run the key generation algorithm in seconds. Table 1 shows the reading from which the below graph is generated.

Table 1: Key Generation Time Comparison

Number of Attributes	Existing CPABE System (Time in ms)	Proposed CPABE System (Time in ms)
5	26	21
10	55	45
15	78	71

Fig. 2 illustrates the graph of time (in second) required for uploading the file on cloud system using both existing CPABE and Proposed CPABE.

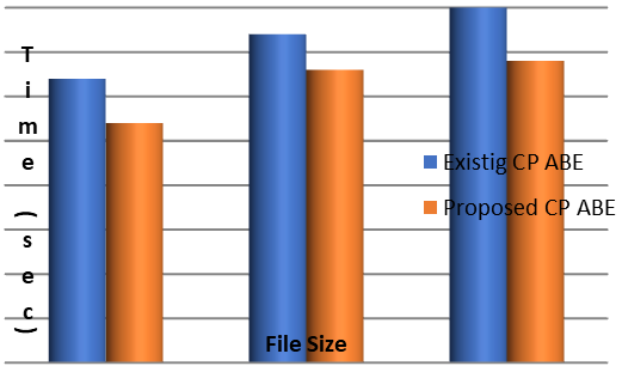

Fig 2: File Uploading Time

Fig. 3 illustrates the graph of time (in second) required for downloading the file on cloud system using both existing CPABE and Proposed CPABE.

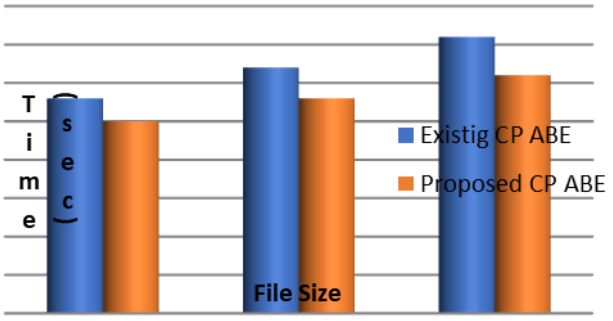

Fig 3: File Downloading Time

Fig. 4 shows the graph of time required for integrity checking of the file on cloud system Proposed CPABE.

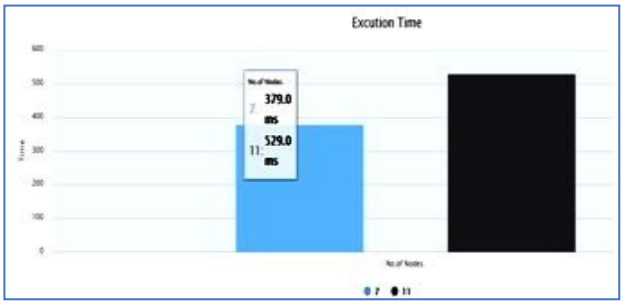

Fig 4: Data Integrity check Time

Table 2 illustrates the parameters comparison between proposed CPABE and existing CPABE system.

Table 2: Result Comparison with Similar System

Parameters	Proposed System CP-ABE	CP-ABE
Access Control	✓	✓
Revocation	Attribute and User Revocation	User Revocation
Data Integrity	Yes by introducing TPA	No

V. CONCLUSION

The major fact which must be taken in account in storing information is the security mechanisms associated with it. The proposed system gives a modified revocable and searchable ABE technique that is much more effective than the previous systems. It provides security for the stored data, by encrypting it using secrete key generated by attribute set and both TPA and Cloud. So it provides effective access control and solves the key escrow problem. The system provides excellence data integrity by introducing third party authority. it check the tempering of data on cloud using hash values. Also, system provides user revocation effectively.

Results show that our system is proficient as well as practical.

REFERENCES

1. Waters B., Sahai A, "Fuzzy identity-based encryption", In: Cramer R, editor. Adv. in cryptology EUROCRYPT, Lecture notes in computer sci, Springer Berlin, vol. 3494, 2005.
2. Goyal V, Pandey O, Sahai A,Waters B., "Attribute-based encryption for fine-grained access control of encrypted data". In: Proceedings of the 13th ACM conference on comp. and comm. security, CCS '06. NewYork, NY, USA: ACM; pp. 89–98, 2006.
3. Chase M., "Multi-authority attribute based encryption", In: Vadhan S, editor. Theory of cryptography, vol. 4392. Lecture notes in comp. science. Springer Berlin Heidelberg; pp. 515–34, 2007.
4. Chase M, Chow SS., "Improving privacy and security in multiauthority attribute-based encryption", In: Proceedings of the 16th ACM conference on comp. and comm.. security, CCS '09. NewYork, NY, USA: ACM; pp. 121–30, 2009.
5. Yu S,Wang C, Ren K, Lou W., "Achieving secure, scalable, and fine grained data access control in cloud computing", In: INFOCOM 2010 proceedings IEEE., pp. 1–9. doi:10.1109/ INFCOM.2010.5462174, 2010.
6. Lewko A,Waters B., "Decentralizing attribute-based encryption", In: Paterson K, editor. Advances in cryptology EUROCRYPT 2011, vol. 6632, pp. 568–88, 2011.
7. Yang K, Jia X. "Attributed-based access control for multi-authority systems in cloud storage", In: 2012 IEEE ICDCS, pp:536–45, 2012.
8. Wan Z, Liu J, Deng R-H., "HASBE: a hierarchical attribute-based solution for flexible and scalable access control in cloud computing", IEEE Trans. Inf. Forensics Secu.; pp:743–54, 2012.
9. Junbeom Hur, "Improving Security and Efficiency in Attribute-Based Data Sharing", IEEE Trans. on Knowledge and Data Engg., Vol. 25, No. 10 2013.
10. Yang K, Jia X, Ren K, Zhang B., "DAC-MACS: effective data access control for multi-authority cloud storage systems", In: INFOCOM-2013 proceedings IEEE, pp:2895–903, 2013.
11. J. Lai, R. Deng, C. Guan, and J. Weng, "Attribute-based Encryption with Verifiable Outsourced Decryption", Trans. Inf. Forensics Security, vol. 8, no. 8, pp: 1343-1354,2013.

12. Lija Mohan, Sudheep Elayidom M., "Fine Grained Access Control and Revocation for Secure Cloud Environment - a polynomial based approach", Int. Conf. on Information and Comm. Tech. (ICICT 2014), pp: 719 – 724, 2014.
13. Nikita Gorasia, R.R.Srikanth, Dr. Nishant Doshi, Jay Rupareliya, "Improving Security in Multi Authority Attribute Based Encryption with Fast Decryption", 7th International Conf. on Comm., Computing and Virtualization 2016, pp: 632 – 639, 2016.
14. G. O. Young, "Synthetic structure of industrial plastics (Book style with paper title and editor)," in *Plastics*, 2nd ed. vol. 3, J. Peters, Ed. New York: McGraw-Hill, 1964, pp. 15–64.
15. W.-K. Chen, *Linear Networks and Systems* (Book style).Belmont, CA: Wadsworth, 1993, pp. 123–135.
16. H. Poor, *An Introduction to Signal Detection and Estimation*. New York: Springer-Verlag, 1985, ch. 4.
17. B. Smith, "An approach to graphs of linear forms (Unpublished work style)," unpublished.
18. E. H. Miller, "A note on reflector arrays (Periodical style—Accepted for publication)," *IEEE Trans. Antennas Propagat.*, to be published.
19. J. Wang, "Fundamentals of erbium-doped fiber amplifiers arrays (Periodical style—Submitted for publication)," *IEEE J. Quantum Electron.*, submitted for publication.
20. C. J. Kaufman, Rocky Mountain Research Lab., Boulder, CO, private communication, May 1995.
21. Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interfaces(Translation Journals style)," *IEEE Transl. J. Magn.Jpn.*, vol. 2, Aug. 1987, pp. 740–741 [*Dig. 9th Annu. Conf. Magnetics* Japan, 1982, p. 301].
22. M. Young, *The Techincal Writers Handbook.* Mill Valley, CA: University Science, 1989.
23. (Basic Book/Monograph Online Sources) J. K. Author. (year, month, day). *Title* (edition) [Type of medium]. Volume(issue). Available: http://www.(URL)
24. J. Jones. (1991, May 10). Networks (2nd ed.) [Online]. Available: http://www.atm.com
25. (Journal Online Sources style) K. Author. (year, month). Title. *Journal* [Type of medium]. Volume(issue), paging if given. Available: http://www.(URL)

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication