Attribute Based Dual Encryption Scheme Secure P2P Storage Cloud Storage User Revocation

Varsha S. Bandagar[1] Hema V. Kumbhar[2]
[1]PG Student [2]Associate Professor
[1,2]Department of Computer Engineering
[1,2]P.V.P.I.T. College, Bavdhan, Pune, Maharashtra, India

Abstract— In attributed based encryption we design a secure data sharing scheme, for dynamic group in untrusted cloud. By combining group signature with the dynamic broadcast encryption technique. User to able share data with the other group without interleaving identity privacy to the cloud. Additional it support efficient user revocation can be achieved through the public revocation without updating private key of the reaming user. And new user can be directly decrypt file stored in the cloud before their participation moreover the storage overhead encryption computation cost is the constant. Extensive analysis shows that our proposed scheme satisfies the desired security requirement and guarantees efficiency as well.

Key words: Secure P2P Storage Cloud Storage, Attribute Based Dual Encryption

I. INTRODUCTION

Cloud computing and peer to peer with storage is similar distributed application. Cloud computing and Peer-to-Peer (P2P) computing there are two of the node of internet the last decade, both of which a form of are large-scale distributed systems and have gained popularity in both research and industrial communities. Cloud computing is historically storage data computing paradigm in which resources in the computing infrastructure are provided as services over the Internet by cloud service providers. The multiple resources could be software, hardware, data storage, access with broadband internet access, users are able to acquire these services for application. Huge of data center's consisting thousands of server application cloud computing processing and resources are centralized in data-center's. P2P computing is a highly does not centralized decentralized computing paradigm application. that resources of large number participating users to support large-scale decentralized applications effectively.

This applications include backup and storage systems content distribution music or video streaming and online gaming In recent years, there are several actually, this times using pair connected computer in cloud system. Companies such as security issues have been the top concerns in cloud computing. When users store important data in the cloud, maintaining confidentiality and privacy of the data to create one challenge. Furthermore, users (i.e. data owners) publish data in the cloud and need terms of which users (i.e. data consumers) have the access privilege to which types of data. To achieve secure and flexible data sharing among a large number of users in P2P storage cloud, the security requirements are usually more complex.

II. PROPOSED SYSTEM

In attribute based encryption p2p storage on cloud which part done of particular user attribute (e.g. He/She living in country) identical information .We consider in group manager and group member registration with particular user. And the access the key generation in a cloud server the encryption stage1 with help of Advanced encryption algorithm(AES) the group manager was share some files with group member sharing that files with is group member download with help of message digest algorithms. The actual part in dual encryption user revocation concept this leaves one user authentication. The data store garbage collection gives to ownership the message was display who access by as well as who was owner.

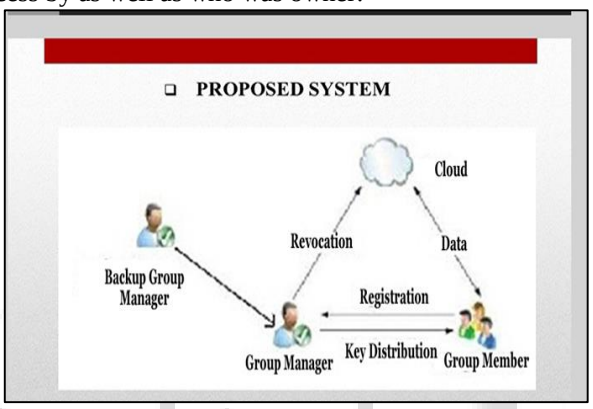

Fig. 1: Proposed System

III. MATHEMATICAL MODEL

A. Shared Key generation (Data Owner)

1) Randomly choose SR 2 U

Where U is set of big integer

2) Randomly select key attributes SAT1, SAT2, SAT3 2 ATA

KAT = SAT1, SAT2, SAT3

Where SAT1, SAT2, SAT3 Data Owner attribute values and ATT Data Owner credentials stored in cloud DB

3) Shared Key set as Shk =fr, KAT g

Generate Shared Key as

$$ShK = \text{å}SR\ KAT \quad (1)$$

4) Compute base64 form of SHK

$$FShK = bytes[ShK]!chars[4ShK/3] \quad (2)$$

B. Private Key Generation (Data Consumer)

1) Randomly Choose PR 2 U

Where U is set of big integer

2) Randomly select key attributes PAT1, PAT2, PAT3 2 ATA

KAT = PAT1, PAT2, PAT3

Where AT1, AT2, AT3 Data Consumer attribute values and ATT Data Owner credentials stored in cloud DB

3) Private Key set as Phk =r, KAT

Generate Private Key as

$$Phk = \text{å}\ Pr\ Kk \quad (3)$$

4) Compute base64 form of SHK

$$FPhk = bytes[Phk]!chars[4Phk/3] \quad (4)$$

IV. ALGORITHM

A. AES Algorithm

In cryptography, the Advanced Encryption Standard (AES) is asymmetric-key encryption standard. Each of these ciphers has a 128-bit block size, with key sizes of 128, 192 and 256 bits, respectively. AES algorithm ensures that the hash code is encrypted in a highly secure manner. AES has a fixed block size of 128 bits and uses a key size of 128 in this paper.

Its algorithm is as follows:

1) Key Expansion
2) Initial Round
3) Add Round Key
4) Rounds
5) Sub Bytes-a non-linear substitution step where each byte is replaced with another according to a lookup table.
6) Shift Rows-a transposition step where each row of the state is shifted cyclically a certain number of steps.
7) Mix Columns-a mixing operation which operates on the columns of the state, combining the four bytes in each column
8) Add Round Key-each byte of the state is combined with the round key; each round key is derived from the cipher key using a key schedule.
9) Final Round (no Mix Columns)
10) Sub Bytes
11) Shift Rows
12) Add Round Key Encryption- converts data to an unintelligible form called cipher text; decrypting the cipher text converts the data back into its original form, called plain text.

B. MD5

Message digest algorithm 5. The used algorithm function of hash it can creates hash table the hash value that variable length constant range output of 128 bits. The input message is wake up into different part of 512-bit blocks. The message spate two parts with find length attribute.

- Step1. Append padding bits: The gives input message extends hence require length equals to 448 mod 512. Combined message is always performed, this length message have before declared 448 mod 552.
- Step2. Append length: A 64-bit representation of the length the shows the message was combined to show answer in giving stage first far then 264, only the low-order 64 bits will be used.
- Step3. Initial that MD attribute the shows the article in word from (A,B,C,D)message digest. Each of A, B, C, D is a 32-bit register.
- Step4. The message should be creates 16 word block require the needed four function will be function creates that input 32 bit words as represented words and produces a 32-bit word output. At the end of this process, a sum of 128 bit message digest is been generated from all the four functions.

The data consumer when retrieving the cloud data from the Cloud Service Provider, then data requested by data consumer again encrypted by using MD5.

V. RESULT

A. Experimental Setup and Results

1) Dataset

As over public cloud user upload its personal data in the form of files and these file having different formats like txt, doc, pdf or it may contains images, audio or video. Before data load to cloud storage it encrypted using AES. Data processes by system are a user input files and user key used in security algorithm also encrypted by MD5.

2) Security Performance Analysis

The following table 1 shows the security algorithms performance analysis on the basis of time required for the key generation file encryption for the given file and file upload time.

File Size (KB)	Key Generation (second)	AES Encryption (second)	File Upload Time (second)
150	0.26	0.954	1.056
510	0.52	1.236	1.230
1024	0.95	1.726	1.756
2048	1.42	2.064	2.157

Table 1: Security performance analysis

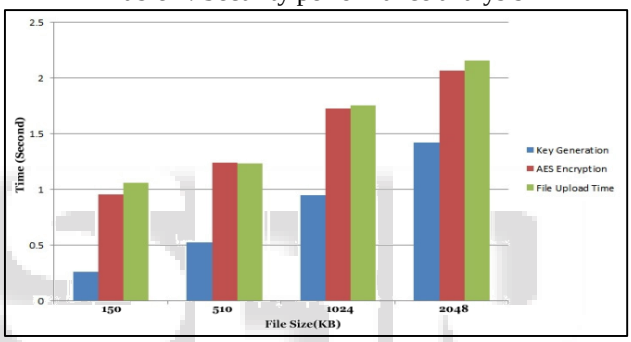

Fig. 2: Security Algorithm Performance

3) Auditing Analysis

The following table 2 shows the difference between the individual and batch auditing performance.

Verified Blocks (Byte)	Individual Auditing Time (milliseconds)	Batch Auditing Time (milliseconds)
3072	1014	921
3891	1154	999
4096	1155	1014
4505	1532	1045

Table 2: Auditing Performance Analysis

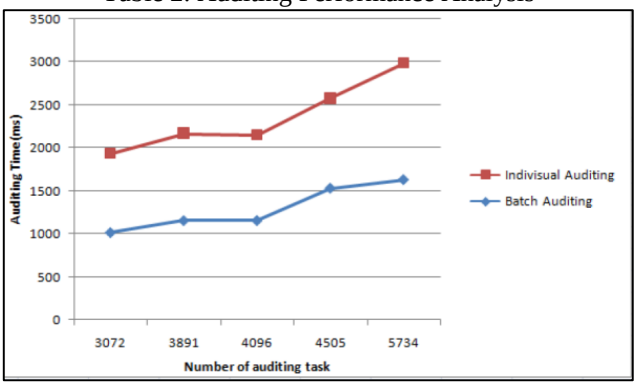

Fig. 3: Comparison on auditing time between batch and individual auditing: Per task auditing time denotes the total auditing time divided by the number of tasks the graph shows the results for the auditing task.

The number of auditing task and time required for auditing shown in the graph. The performance of the corresponding individual auditing is provided as a baseline for the measurement. Following the same settings for the data blocks of the file; the average per task auditing time, which is computed by dividing total auditing time by the number of tasks, is given for both batch and individual auditing. It can be shown that compared to individual auditing, batch auditing indeed helps reducing the TPAs computation cost, as more than 15 percent of per task auditing time is saved.

4) User Revocation Strategy

The audit task shows the access count of a file with File Id and User Id following tale 3 shows the file access log.

User ID	File ID	File Access Count
1	1	5
2	2	1
3	3	3
4	4	7

Table 3: File Access Log

When user leave or misbehave in group then he/she removed from group; then files uploaded by such user resigned by the key of existing user. The new user for such file is decided by auditing file access log. The user having max access count for such file which gets ownership of file.

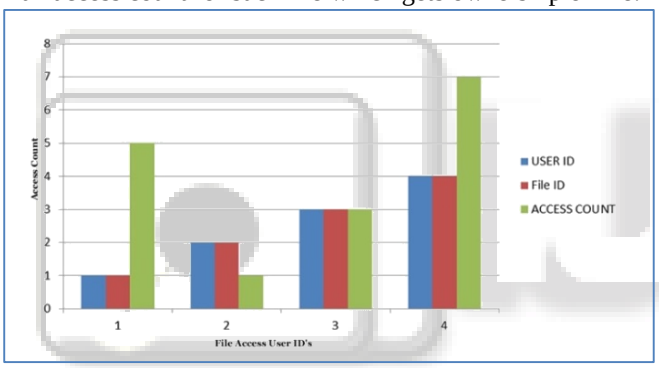

Fig. 4: User Revocation

VI. CONCLUSION

Attribute based dual encryption with secure, efficient access control mechanism In existing approaches attributes depends on time, and contain only fixed values, that can be difficult to maintain for large number of users, each one having a large number of attributes. we using also garbage data when user leaves the group with using garbage data and gives the ownership to easily new concept user revocation this verify peer to peer segments with the help of secret key and the master key.at end part resign key we change key whose access the data group member. In we integrate P2P reputation system and enable the data owner to delegate file re-encryption cloud server using key as secrete change the computation intensive task, to the reputable system peers picked out by P2P reputation system. Moreover is provably secure under the standard security model and can resist the various attack gives protection information effectively.

REFERENCES

[1] Heng He, Ruixuan Li, Xinhua Dong, and Zhao Zhang ”Secure, Efficient and Fine-Grained Data Access Control Mechanism for P2P Storage Cloud” IEEE transactions on cloud computing, vol. 2, no. 4, october-december 2014

[2] P. Mell and T. Grange, ”The NIST definition of cloud computing, NIST Special Publication 800-145, pp. 1-7, Sep. 2011.

[3] Rodrigues and P. Urschel, ”Peer-to-peer systems,” Common ACM, vol. 53, no. 10, pp.72-82, Oct. 2010.

[4] J. Li and Q. Huang, ”Erasure resilient codes in peer-to-peer storage cloud”, in Proc. IEEE Int. Conf. Acoustics, Speech Signalling Process.,2006, pp. 14-19.

[5] H. Kivalina and A. Montresor, ”P2P and cloud: A marriage of convenience for replica management,” in Proc. 6th IFIP TC 6 Int. Conf. Self-Organizing Syst., 2012, pp. 60-71.

[6] R. Ranjan, L. Zhao, Xu, A. Liao. Quiroz, and M. Preacher, ”Peer to-peer cloud provisioning: Service discovery and load-balancing,” in Cloud Compute.: Principles, Systems and Applications, Part 2, N.Antonopoulos,L.Gillam, Ed. London: Springer, pp. 195-217,May 2010.

[7] L. Bremer and K. Graffiti, ”Symbiotic coupling of P2P and cloud systems: The Wikipedia case,” in Proc. IEEE Int. Conf. Communed.,2013, pp. 3444 - 3449.

[8] Z. Yang, B. Zhao, Y. Xing, S. Ding, F. Xiao, and Y. Dai,” Amazing store: Available, low cost online storage service using cloudlets,” in Proc. 9th Int. Workshop Peer-to-Peer

[9] T. Maher, E. Bier sack, and P. Misheard, ”A measurement study of the Wala on-line storage service,” in Proc. 12th IEEE Int. Conf. Peer-to-Peer compute., 2012, pp. 237-248.

[10] A. Montresor and L. Arena, ”Cloudy weather for P2P, with a chance of gossip,” in Proc. 11th IEEE Int. Conf. Peer-to-Peer Compute.,2011, pp. 250-259.

[11] A. H. Payberah, H. Kavalionak, V. Kumaresan, A. Montresor, and S. Haridi, CLive: Cloud-assisted P2P live streaming, in Proc. 12th IEEE Int. Conf. Peer-to-Peer Comput.,2012, pp. 7990.

[12] B. Wang, B. Li, and H. Li, Certificate less Public Auditing for Data Integrity in the Cloud Proc. IEEE Conf. Comm. and Network Security (CNS13), pp. 276-284, 2013.

