A Review on Fragmentation and Replication Related Security in Cloud

[1]Sharayu V. Powar, [2]Prof.K.T.Mane
[1]Student, [2]Assistant Professor
[1]Department of Computer Science and Engineering
[1]D. Y. Patil College of Engineering &Technology, Kasaba Bawada, Kolhapur, Maharashtra, India.

Abstract: ***Cloud computing is a rising term that offers number of essential focal points. One of the key preferences of Cloud computing is pay according to utilize, and clients will pay by their use of the storage space. Concept of Third Party Service Provider and Auditing are widely used for providing different techniques like data storage, encryption. Data replication is face by clients whenever he is provided with backup management for storing data hence to overcome this problem of redundancy mapping hash key is used as a key factor which is further discussed in paper. How to provide security in the form of integrity, correctness and confidentiality is focused in this paper.***

Index Terms - Cloud storage, Backup/recovery, Centrality, cloud security, fragmentation, replication, performance, Advanced Encryption Standard Algorithm (AES), BLS (Boneh–Lynn–Shacham).

I. INTRODUCTION

The Cloud Computing is a latest technology which provides many services through internet and use anytime, anywhere. Cloud computing means keep information on a remote server (i.e. cloud), instead of keeping data on your own hard drive or disk. Users can access your data from a Smartphone, tablet, laptop, or a desktop—wherever you have an Internet connection. Storing and accessing data and programs over the Internet. The Cloud Server allows user to store their data on a cloud without worrying about correctness of data. The cloud has unlimited storage. One of the example is Amazon Web Services S3 storage can be set up with policies to control and automate access and archiving. No matter how large your local storage is, this isn't a surprise as we are storing more multimedia data in the different forms like video, image and audio files. From a business point of view, storing many documents in the cloud removes the need for each user to hold a personal copy of documents, saving disk space. Storing our data in the cloud introduces a number of set of risks, but we can avoid those using different techniques like data encryption, automation and password devices on your smart phone. Data security is protecting our data from corruption and inappropriate access.

One of the problems arrives in data replication. In data replication no of copies presents in same data. So storage problem is facing. To solve those problems, different solutions presents. To increase the overall performance of the system and increase the efficiency one of the technique is used this is called as fragmentation. In fragmentation whole data can divide into multiple fragments (Fixed or variable size) and these fragments can be individually uploaded to the server. For data security and integrity purpose then use cryptographic techniques to the individual fragments. Time evaluation is also an important aspect which should be calculated as a sum of time required to generate the fragments, encrypt these fragments and finally uploading or transferring these fragments to the main and replica server.

II. ADVANCED ENCRYPTION STANDARD (AES) ALGORITHM

Now a days the more popular and widely used symmetric encryption algorithm is the Advanced Encryption Standard (AES). It is minimum six times faster than triple DES algorithm. In DES its key size was too small, so to overcome this problem AES is used. The characteristics of AES are as follows: Key type Symmetric, 128,192,256 -bit data, bit keys 128,192,256, faster and stronger than triple-DES cryptography technique, in C and Java language software is easy to implement.

2.1 An Optimization and Security of Data Replication In Cloud Using Advanced Encryption Algorithm

Cloud computing is a expanded term that describes many services like storage, communication, database. In previous system, exchanging data, files downloading, uploading etc. operations are not secure in a cloud due to the increasing hacking and cracking process. In this paper focuses information related to data replication in cloud computing. To minimize privacy and security related issues used AES (Advanced Encryption Standard Algorithm) Encryption Algorithm. With the help of AES algorithm data stored in the encrypted format and stored onto cloud. Files or data divided into fragments and stored that fragments on nodes. Fragments are stored in distributed format so in cloud no node catch more than one fragments. So no any leaks of data possible in successful attack. In this paper generating fragments are uniform in between 10kb to 60 kb size i.e. Limited size only used for this process. The nodes randomly selected for replication algorithms. In this paper limited size is used for distributing fragment purpose.

III. THIRD PARTY PUBLIC AUDITING SCHEME

Cloud storage is the service provided by Cloud computing. In cloud storage data is managed, maintained, and backed up remotely available to users over a network (typically the Internet). The user is worried about the integrity of data Therefore, a new term called data auditing is introduced. In data auditing checks the integrity of data with the help of an entity called Third Party Auditor (TPA). The purpose of auditing scheme is public auditing, privacy preserving, maintaining the data integrity along with confidentiality. The new auditing scheme is invented it consists of three entities: data owner, TPA and cloud server. The data owner performs operations like dividing the file into blocks, encrypting, generating a hash value for each block etc. The TPA performs important role that is data integrity check (includes activities like generating hash value for encrypted blocks received from cloud server, concatenating). The cloud server is used to save the storage.

3.1 Fine Grained Updation of Data on Cloud

In different organizations already follow data integrity. Provide maintenance ,assurance of the privacy accuracy and consistency of data over cloud or network is called ad data integrity. For verifying data over a trusted third party (auditor) is called data auditing. In existing work BLS (Boneh–Lynn–Shacham) signature process is used updates over data blocks in fixed size over dynamic data. BLS signature only supports coarse-grained updates. Coarse-grained updates are also called as fixed size blocks. There are three participants are used these are Client, CSS (Cloud Storage Server) and TPA (Third Party Auditor).

In existing public auditing processes can already Follows full data dynamics. In full data dynamics only discussed deletions, insertions, modifications on fixed-sized blocks. In BLS-signature-based schemes each block is fragmented 160 bit, 160 bit is a fixed number block. Support for fixed size can provide an integrity verification scheme. Integrity verification scheme is used for data updating, scalability and more operations. In this scheme more number of updating the wasting amount of storage will be increased. For example, size for a data block is 16k is wasted. Block is reused until the deleted that block permanently. These problems can be solved if fine-grained data updates are supported to that reused blocks. According to this observation, supporting of grained updates can give improved efficiency bytes. One problem facing that is very small update will leads to recomputation and updating of the authenticator for an whole file block, which leads to higher storage and communication overheads.

3.2 Cloud storage with improved access control and Assured deletion

One of the important problem of cloud computing is to provide security and efficient access to large data. One of the major challenge is to provide balminess of assured deletion .i.e. data files are permanently inaccessible or unreachable in the requests of deletion. It is not possible to keep backups of data permanently. Assured deletion is to provide cloud users or clients an option of reliably deleting their data backups upon clients or users requests.

Assured deletion can be implemented by multiple ways these are: first is securing overwriting [6].In secure overwriting data is overwritten by new file to make original data files unrecoverable. Second is disk scrubbing [7].In disk scrubbing deleted data on disk by overwriting data in number of times. There is no assurance that all backup copies of data files will be simultaneously destroyed or deleted. Third is Self-destruct [8]. Self-Destruct is a related to email systems. In this copy of email at the user or client side will be assuredly deleted after completing reading email. In this paper FADE concept is used. A FADE[10] is a secure cloud storage system that achieves policy-based access control, fine-grained, file assured deletion. Key derivation is used for providing access control. Attribute-Based Encryption (ABE) [9].In this ABE approach, each client first obtains an -based private access key from the key issuing authority of the ABE system that corresponds to a set of attributes the client satisfies. This can be done by having the client present authentication credentials to the key issuing authority. The problem is arrived i.e. cloud providers creates multiple copies of data over the cloud or internet. Clients have no idea that how many number of copies data replicate over the cloud. Second, it is not clear whether cloud providers can permanently remove all replicated copies when cloud clients sends requests of deletion for their data.

3.3 Utilizing Third Party Auditing to Manage Trust in the Cloud

In this paper, focuses on security auditing framework related information. The user trust by (a) allowing the cloud service users (CSUs) to provide their security preferences with the desired cloud services, controls and internal security policies of cloud service providers (CSPs) published in the CSA's (Cloud Security Alliance) Security Trust and Assurance Registry (STAR) database, maintaining a database of CSPs along with their responses. In this paper framework facilitates the how CSP and CSUs relates each other with security and services point of view. Terms of cloud computing, used as CSU, CSP and a TPA are in the concerns to establish a trust model. To enter the cloud computing infrastructure sends request to CSP. CSP provides related information to TPA. This information would include basic material of services that the CSP can offer the CSUs. Not all of the services required by the CSU may be available from a given CSP [12]. Author in [13] identified an analysis of problems that may arise for CSU using a CSP. The first problem faced was the provides protection of data integrity. The solution for data integrity is implementing provable data possession (PDP). Support for access control is the second problem faced .The third problem [13] is to minimize the cost of auditing. Solution to this drawback of cloud computing is not found.

3.4 Addressing cloud computing security issues

The fast growth of cloud computing services has pulled up new problems for information systems, communication and security. Numbers of risks and challenges have been occurring in the cloud. In this paper firstly focused is cloud security. In cloud security identifying unique security requirements and then finding a solution that eliminates these security concerns. In this paper Trusted Third Party also used to provide security to the cloud. PKI (Public Key Infrastructure) along with SSO (Single-Sign-On) and LDAP (lightweight directory access protocol) is used to provide the authentication, integrity and confidentiality of involved data and communications.

This paper proposes a security solution that leverages from the safety load, by trusting a third party. The task for Third Party is reassuring security features among a distributed information system, whereas realizing a trust mesh between concerned entities, forming of clouds. In this paper try to eliminate the different security challenges that is introduced in a cloud environment. Overcome these problems to a security perspective. Trust and security is out and specific security requirements for different documented. The analysis methodology introducing towards the goal, that is predicated on software package engineering and information systems approaches.

IV. CONCLUSION

In this paper, we discussed fragmentation and replication related approaches and cloud computing security issues. We also concerns about how this can be achieved within a cloud infrastructure. Implements different algorithms to provide the security and confidentiality to a data. Analyze the files in the form of fragments, upload it onto server that has been evaluated and considered as a part of estimation.

REFERENCES

[1] Mazhar Ali, Student Member, IEEE, Kashif Bilal, Student Member, IEEE,et.al, "DROPS: Division and Replication of Data in Cloud for Optimal Performance and Security", IEEE TRANSACTIONS ON CLOUD COMPUTING, DOI 10.1109/TCC.2015.2400460.

[2] S.Suganya, R.Kalaiselvan, "An Optimization And Security Of Data Replication In Cloud Using Advanced Encryption Algorithm", International Journal Of Engineering And Computer Science ISSN: 2319-7242 Volume 5 Issues 6 June 2016, Page No. 16836-16841.

[3] Mrs.K.Valarmathi "Fine Grained Updation Of Data on Cloud", International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)ISSN: 0976-1353 Volume 13 Issue 4 –MARCH 2015.

[4] Ranjana Badre, "Cloud storage with improved access control and assured deletion", International Journal of Innovations in Engineering and Technology (IJIET)Volume 3, Issue 3 February 2014, ISSN: 2319 – 1058.
[5] Dimitrios Zissis and Dimitrios Lekkas, "Addressing cloud computing security issues", Future Generation Computer Systems 28 (2012) 583–592.
[6] P. Gutmann 8ecure deletion of data from magnetic and solid state memory. *In Proc. of USENIX Security Symposium*, 1996
[7] Lingfang Zeng, Shibin Chen, Qingsong Wei and Dan Feng, SeDas: A self-destructing data system based on active storage framework. *In APMRC, 2012, Digest*.
[8] Junping Liu, Ke Zhou, Liping Pang, Zhilun Wang, Yuhui Deng and Den Feng , A novel cost effective scrubbing scheme. *In fifth International joint conferenceon INC, ISM and ISC 2009*.
[9] J. Bethencourt, A. Sahai, and B. Waters, Ciphertext-Policy Attribute-Based Encryption, *Proc. IEEE Symp. Security and Privacy, May 2006*.
[10] Yang Tang, Patrick P. C. John C. S. Lui and Radia Perlman . Secure Overlay Cloud Storage with Access Control and Assured Deletion. *In IEEE transactions on dependable and secure computing Vol. No. 6, December 2012*.
[11] Syed Rizvi*, Kelsey Karpinski et.al "Utilizing Third Party Auditing to Manage Trust in the Cloud", Department of Imformation Sciences and Technology, Penn State University, Altoona PA, 16601, USA.
[12] S. Rizvi, J. Ryoo, Y. Liu, D. Zazworsky, ,and A. Cappeta., "A centralized trust model approach for cloud computing," in proceedings of 2014 23rd Wireless and Optical Communication Conference, Newark, NJ, 2014, pp. 1-6.
[13] L. Li, L. Xu, J. Li, and C. Zhang, "Study on the third-party audit in cloud storage", *Department of Computer Engineering, A.C.Patil College of Engineering, Kharghar, Navi Mumbai 410210, India*.