International Journal of Future Innovative Science and Engineering Research (IJFISER)
Volume - 2, Issue - II ISSN (Online): 2454- 1966

Research Manuscript Title

User Data Integrity Checking and Dynamic Reallocation of Data for Security on Multi cloud

P.S.Thumilvannan,M.E., B.kalpana,M.E.,
Assistant Professor, P.G Scholar,
Computer Science and Engineering,
Arulmigu Meenakshi Amman College of Engineering, Vadamavandal, Kanchipuram.Tamilnadu, India.
E-Mail: stvvannan@gmail.com, bkalpana993@gmail.com.

JUNE – 2016

www.istpublications.com

User Data Integrity Checking and Dynamic Reallocation of Data for Security on Multi cloud

Mr.P.S.Thumilvannan,M.E., B.kalpana,M.E.,
Assistant Professor, P.G Scholar,
Computer Science and Engineering,
Arulmigu Meenakshi Amman College of Engineering, Vadamavandal, Kanchipuram.Tamilnadu, India.
E-Mail: stvvannan@gmail.com, bkalpana993@gmail.com.

ABSTRACT

The cloud computing is an important theme in the computer field. It lies in the outsourcing of computing tasks to the third party. In cloud computing, contains the security risks in terms of confidentiality, integrity, availability of data and service. Nowadays, cloud service provides low cost, scalable, position-independent platform for clients data. The main issue is to convince the cloud clients data are kept intact especially vital. Since the clients do not store their data locally. Remote data integrity checking is a primitive to address this issue. When the client stores his data on multicloud servers, the distributed storage and integrity checking are indispensable. However a multicloud allows user to easily access his/her resources remotely through interfaces such as web services like Amazon EC2, Google, IBM, etc. The data integrity checking protocol must be efficient in order to make it suitable for capacity-limited end devices. If the data gets corrupted in multicloud, the continuous auditing process helps the verifier (Third party) to perform Block level and File level checking for remote data integrity checking. Cloud provides random blocks to verifier (Third party) for integrity checking which is to protect user privacy from verifier (Third party). Data integrity checking is to ensure user uploaded data in multicloud maintain security and privacy on cloud data and provide access confidentiality through dynamic reallocation of data at every user access.

Keywords: Multicloud, Scalable, Outsourcing, Random Blocks, Data Integrity, Third party.

1 Introduction

Cloud computing is a kind of internet-based computing.It has Progressed by addressing the QoS (quality of service) and reliability problems .cloud computing provides tools and technologies to build data/compute intensive parallel applications with much more low prices compared to traditional parallel computing techniques. Cloud computing is the result of the evolution and idea of current technologies and paradigms compared to traditional parallel computing techniques. Nowadays, cloud storage service has become a rapid growth by providing a comparably low-cost, scalable, position-independent platform for user data. Since cloud computing environment is constructed based on open architectures and interfaces, it has the capability to integrate multiple internal and/or external cloud services together to provide high interoperability. Such a distributed cloud environment as a multi-Cloud (or hybrid cloud), a multi-cloud allows clients to easily access his/her resources remotely through interfaces such as Web services provided by Amazon EC2. However, if such an important platform is vulnerable to security attacks, it would bring irreversible losses to the clients. For example, the confidential data in an business or company may be illegally accessed through a remote interface provided by a multi-cloud, or relevant data and archives may be lost or altered with when they are stored into an uncertain storage pool outside the business or company.

Verifying the authenticity of data has emerged as a critical issue in storing data on untrusted servers. However, archival storage requires guarantees about the authenticity of data on storage, namely that storage servers possess data. It is insufficient to detect that data have been modified or deleted when accessing the data, because it may be too late to recover lost or damaged data. Archival storage servers retain tremendous amounts of data, little of which are accessed. They also hold data for long periods of time during which there may be the file across a network. Furthermore, I/O become liable to establish data possession interferes with on-demand bandwidth to store and

retrieve data. We conclude that clients need to be able to verify that a server has retained file data without retrieving the data from the server and without having the server access the entire file.

1.1 Motivation

The previous section defined cloud computing, Different cloud service providers have different reputation and charging standard. Of course, these cloud service providers need different charges according to the different security levels. Usually, more secure and more expensive. For the private data, data will store them on the private cloud server. For the public advertisement data, data will store them on the cheap public cloud server. In multicloud environment, distributed provable data possession is an important element to secure the remote data. Thus, the distributed cloud storage is indispensable.

In PKI (public key infrastructure), provable data possession protocol needs public key certificate distribution and management. It will become liable to considerable overheads since the verifier will check the certificate when it checks the remote data integrity. In addition to the heavy certificate verification, the system also suffers from the other complicated certificates management such as certificates generation, delivery, retraction, renewals, etc. In cloud computing, most verifiers only have low computation capacity.

In cloud computing, remote data integrity checking is an important security problem. The clients' huge data is outside his control. The malicious cloud server may corrupt the clients' data in order to gain more benefits.

1.2 Related Work

In cloud computing, remote data integrity checking is an important security problem. The clients' massive data is outside his control. The malicious cloud server may corrupt the clients' data in order to gain more benefits. Many researchers proposed the corresponding system model and security model. In 2007, provable data possession (PDP) paradigm was proposed by Ateniese et al. [11]. In the PDP model, the verifier can check remote data integrity with a high probability. Based on the RSA, they designed two provably secure PDP schemes. After that, Ateniese et al. proposed dynamic PDP model and concrete scheme [2] although it does not support insert operation. In order to support the insert operation, in 2009, Erway et al. proposed a full-dynamic PDP scheme based on the authenticated flip table [1]. The similar work has also been done by F. Sebe´ et al. [3]. One of benefits of cloud storage is to enable universal data access with independent geographical locations. This implies that the end devices may be mobile and limited in computation and storage. Efficient integrity checking algorithm are more suitable for cloud clients equipped with mobile end devices.

2 System Model

Data integrity checking is an efficient way to secure user data on mutlicloud. In this algorithm some entites are following:

User : an entity, which has huge data to be stored on the multicloud for maintenance and computation, can be either individual user or corporation.

Cloud Server : an entity, which is managed by cloud service provider, has important storage space and computation resource to maintain the user data.

Verifier (third party) : User will upload file to Cloud. This file is split into blocks using Dynamic Block generation Algorithm and stored in a MultiCloud environment. Cloud provides random blocks to Verifier for Integrity Checking which is to protect user privacy from Verifier (Third Party).

3 The Proposed Model

In multicloud environment, remote data integrity checking is required to secure user's data. User will upload file to cloud. This file is split into blocks using Dynamic Block generation Algorithm and stored in a multicloud environment. File Allocation Table (FAT) File System has proper Indexing and Metadata's for the different chunks of the cloud storage. If attacker corrupts data in multicloud, the continuous auditing process helps the verifier to perform Block level and File level checking for remote data Integrity checking using verifiable data

integrity checking Algorithm. Cloud provides random blocks to verifier for integrity checking which is to protect user privacy from Verifier (Third Party). File recovery is done by the verifier automatically if the data gets corrupted during checking. User can complaint cloud for File Recovery.

At every access of the file by the user, blocks of the data will be dynamically reallocated between the cloud servers. This achieves access confidentiality in cloud computing. To recover the corrupted user uploaded data, the verifier using data integrity checking and also reallocating data dynamically to provide access confidentiality.

3.1 FAT(File Allocation Table) :

FAT FS is a technique which has a proper indexing for different blocks of data that is being uploaded by user. FAT tables must be stored in a fixed location so that the files needed to start the system can be correctly located**.**

FAT is a table which contains user ID, name date, File ID Filename, File size, File status etc. Free areas are nor currently in use by the file data and so available for storing new files**.**

3.2 MD5 based :

This method is based on MD5 function. In this method first file is read and compressed. This compressed content is input to the MD5 function which generates the message digest . This Message digest is encrypted and appended with the original file content within pre defined tag. For verification, file is read back. File is compressed and MD5 is used to generate hash value. This hash value is encrypted and compared with appended one in original file. If both matches then file is intact otherwise it is tampered.

4 Data Integrity Checking and Automatic on Demand File Recovery

4.1 Data Integiry Checking :

Data should be in a self-motivated computing infrastructure. The main concept in this dynamic environment is that all standardized and scalable infrastructure should have dynamic operation such as modification, append, and delete. The cloud platform which has virtualized conditions also should have some specific independent environment.

To reduce the work load of the user, Verifier (third party) has the delegation for the data checking with a few limitation so that he can‘t modify content of the data in his auditing. And Verifier (third party) pays due care on storage correctness verification. Verifier (third party) auditing is in the manner of privacy preserving concept so that verification can be done in separate manner alone from any interaction by others. In the existing system, distributing protocol is used for this purpose. Here Verifier (third party) has does not have special authority for data integrity checking. However don‘t give more importance to Verifier (third party) to such a great degree but a small bit only since our proposed system pays more concentration on client‘s access for full security.CSP allotted space is a major concern for our data maintenance in all manner for dynamic operations. All outsourced data and data entering into the cloud . So in order to keep integrity of overall data, to use ―data integrity checking its well as cloud storage level before and after the data adding into the cloud server area‘ and another ―multi-server data comparison algorithm for every data upload for the purpose of data recovery management‖ for proposed achievement. When server failure occurs in cloud entire data may be affected so that user can‘t foresee data‘s trustworthiness in its whole atmosphere depending on variety of situation or CSP‘s process to hide the loss of data. And user can know if there has been done any change, remove, and attach operations that can occur for data from its storage level with the help of proposed scheme that never has been told. It can be effectively administered by clients from appropriate efficient data integrity checking from cloud server position.

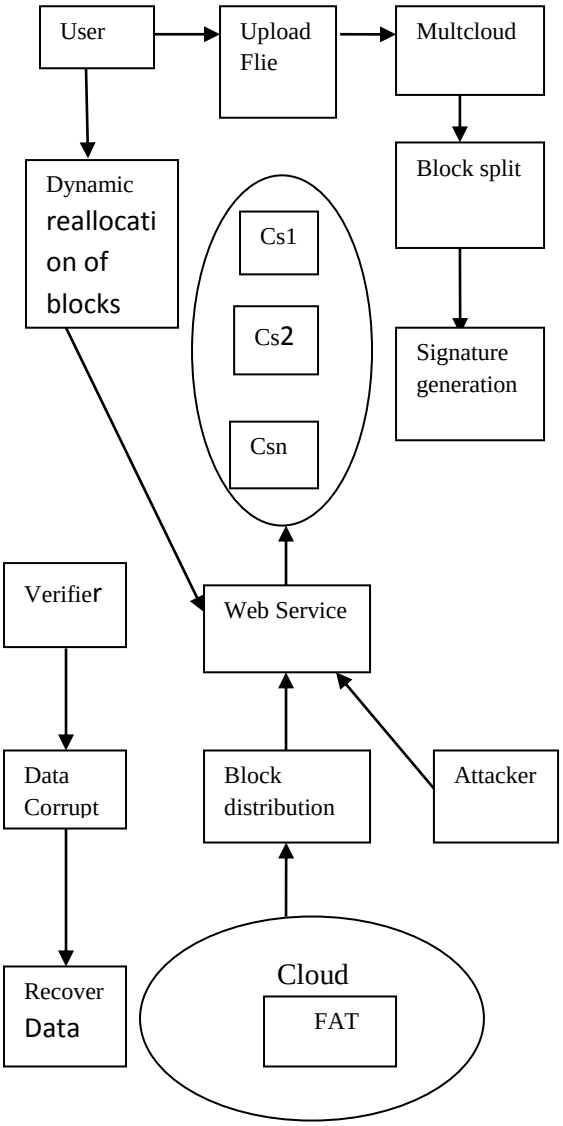

Fig. 1 Data integrity checking

4.2Verifiable data Integrity Checking :

Verifiable Data Integrity Checking Algorithm is done in two steps: Block Checking and File Checking. In Block Checking step: Three signatures are generated for Block level Checking.

1. A signature of a block retrieved from a FATFS

2. A new signature is generated for block to be checked

3. A Signature is retrieved from the block appended with the signature which is stored in the Cloud

The above three signatures are cross checked for Block level Integrity Checking. And the block contents are appended to verify with File level Integrity Checking.

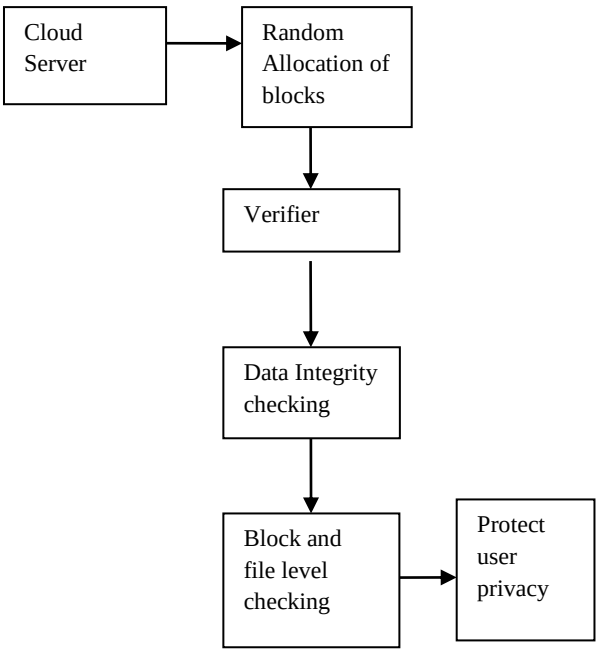

Fig . 2 Verifier Data integrity checking.

4.3 Automatic and On Demand File Recovery :

Attacker can corrupt data in any one of the cloud servers. On Data Integrity Checking done by the Verifier, Verifier informs Corrupted blocks to the Cloud. Recovery Process will be done by the verifier automatically when data gets corrupted.

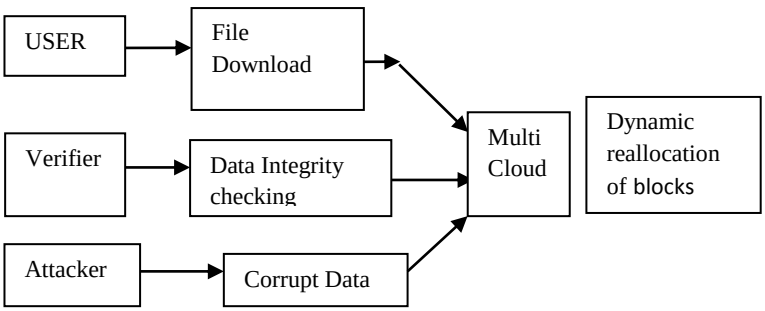

Fig. 3 Automatic and On Demand File Recovery

User can complaint to the Cloud if the user file get corrupted (Verifier doesn't perform checking on this file).Whenever user access file, Blocks will be reallocated dynamically to provide access confidentiality in cloud and FAT File System will get updated.

User has an initial level registration process at the web end. The users provide their own personal information for this process. The server in turn stores the information in its database. After Registration, user can upload files to the server. Uploaded files will be stored in a Server. When the user upload the data to different cloud by the time it is splitted into different blocks using Dynamic block generation algorithm and each block will be appended with signatures before Storing the data in FATFS. Signature generated using MD5 algorithm. Also the data gets encoded using for Base64 algorithm.

5 Conclusion

To summarize, the work described in this paper represents an important step forward towards practical Data integrity checking algorithm.The remote data integrity checking is done by the verifier effectively for maintaining security and privacy in multicloud. Data recovery is done on integrity checking process when data gets corrupted. And also access confidentiality provided by the cloud.

References

[1] C.C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," in *Proc*, CCS, 2009, pp. 213-222.

[2] A.F. Barsoum and M.A. Hasan, "Provable possession and replication of data over cloud servers," Center Appl. Cryptogr. Res., Univ. Waterloo, ON, Canada, 2010/32. [Online]. Available: http://www.cacr.math.uwaterloo.ca/techreports/2010/cacr2010-32.pdf .

[3] F. Sebe´,J. Domingo-Ferrer, A. Martı´nez-Balleste´, Y. Deswarte, and J.Quisquater, ''Efficient Remote Data Integrity Checking in Critical Information Infrastructures,'' IEEE Trans. Knowl. Data Eng., vol. 20, no. 8, pp. 1034-1038, Aug. 2008.

[4] Y. Zhu, H. Hu, G.J. Ahn, andM. Yu, ''Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage,'' IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 12, pp. 2231-2244,Dec. 2012.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, ''Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing,'' in Proc. IEEE INFOCOM, Mar. 2010.

[6] Z. Hao and N. Yu, ''A Multiple-Replica Remote Data Possession Checking Protocol with Public Verifiability,'' in Proc. 2nd Int.Symp. Data, Privacy, E-Comm., 2010.

[7] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, ''Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,'' IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 5, pp. 847-859, May 2011.

[8] C. Wang, Q.Wang, K. Ren, N. Cao, and W. Lou, ''Toward Secure and Dependable Storage Services in Cloud Computing,'' IEEE Trans. Serv. Comput., vol. 5, no. 2, pp. 220-232, Apr./June 2012.

[9] A.F.Barsoum and M.A. Hasan, ''On verifying dynamic multiple data copies over cloud servers,'' Int. Assoc. Cryptol. Res., New York, NY, USA, IACR eprint Rep. 447, 2011. [Online]. Available: http://eprint.iacr.org/2011/447.pdf.

[10] A.F. Barsoum and M.A. Hasan, ''Integrity Verification of Multiple Data Copies over Untrusted Cloud Servers,'' in Proc. 12th IEEE/ACM Int. Symp. CCGRID, 2012, pp. 829-834.

[11] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," in *Proc*. CCS, 2007, pp. 598-609.

[12] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu. Plutus: Scalable secure file sharing on untrusted storage. *FAST*, pages 29–42, 2003.

[13] J. Li, M. Krohn, D. Mazieres, and D. Shasha. Secure Untrusted Data Repository (SUNDR). *OSDI*, pages 121–136, 2004.

[14] M. Naor and K. Nissim. Certificate revocation and certificate update. In *USENIX Security*, pages 17–17, 1998.

[15] A. Oprea, M. Reiter, and K. Yang. Space-Efficient Block Storage Integrity. *NDSS*, 2005

[16] R. Tamassia. Authenticated data structures. In *ESA*, pages 2–5, 2003.