www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 12 December 2014, Page No. 9552-9554

Data Integrity Proofs in Document Management System under Cloud with Multiple Storage

Ms. Payal P. Kilor[1], Prof. Vijay B. Gadicha[2]

[1]M.E Second Year CSE, P.R.Patil COET
Amravati, Maharashtra, INDIA
[1]payalpatil20@gmail.com

[2] HOD,CSE Dept, P. R. Patil COET
Amravati, Maharashtra, INDIA
[2]v_gadicha@rediffmail.com

Abstract

Cloud computing is a web based computing which presents different customers an opportunity to store their data in the cloud. For cloud storage, privacy and security are the burning issues. Storing our data in cloud may not be fully trustworthy. When users store their data on the cloud then there may be a risk of losing the data, or sometimes data may be modified or updated. Cloud storage moves the user's data to large data centers, which are remotely located, on which user does not have any control. One of the important concerns that need to be addressed is to assure the customer of the integrity i.e. correctness of his data in the cloud. As the data is physically not accessible to the user the cloud should provide a way for the user to check if the integrity of his data is maintained or is compromised. The aim of this paper is to ensure the integrity of the data and provides the proof that data is in secured manner and provide a Cryptographic key to secure the data in the cloud

.

Keywords: cloud computing, data integrity, privacy, Cryptography, cloud storage.

1. Introduction

Cloud computing is a new paradigm and dimension of the information and technology, which aims to provide reliable, customized and guaranteed computing dynamic environment on "Pay-per-use" or "Pay-as-you-go" basis for the end users. "Clouds are a large pool of easily available, usable and accessible virtualized resources (such as hardware, development platform and/or services). These resources can dynamically reconfigured to adjust to a variable load (scale), allowing also for an optimum resource utilization" [1]. Cloud computing provides you a service through which you can use all the computer hardware and software sitting on your desktop, or somewhere inside your company's network but they are not actually installed on your computer, it is provided for you as a service by another company and accessed over the internet. End users can access these services available in the internet without knowing how these
resources are managed and where. This is transparent to end users [2] .
It is highly mobile and available across platforms. Cloud reduced the cost of deployment. Cloud increased computing power with rapid scalability as and when needed. It reduced
risk of data loss. Cloud improves compatibility between operating system [3],[4].

Still, in cloud computing, there is unresolved, security and privacy issues. Data integrity is very important among the other cloud storage issues. data integrity ensured that data is of high quality, correct, consistent and accessible. After moving the data to the cloud, owner hopes that their data and applications are secured manner. But that hope may fail sometimes the owner's data may be altered or deleted. In that scenario it is important to verify if one's data has been tampered with or deleted. From the data owners' perspective, storing data remotely in a cloud in a flexible on-demand manner brings appealing benefits: relief of the burden of storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, software, personnel maintenance, and so on. While cloud computing makes these advantages more appealing than ever, it also brings new and challenging security threats to the outsourced data.

2. 2. Literature Review:

In Cloud computing the issue of data security is still carried on, many researchers are still working with many different solutions. In Cloud Computing, one of the major threats is data privacy and data integrity in cloud storages. There is lot of research going on in this field to ensure and provide data integrity in cloud storages. Calce says about cloud computing putting everything into single box will only make it easier for hackers [5]. Priya Metri and Geeta Sarote introduce threat

model to treat privacy problems in the cloud [6]. One of the service is third party auditing because it notify threats in cloud computing is tampering the data in cloud that interfere with unauthorized modification for data, which lead to an effectiveness processors, data storage and data fow.

Dalia Attas, Omar Batrafi implemented a mechanism in which integrity is checked at 2 sides- by cloud server (for inside attack) and by TPA (for outside attack) using digital signature with MD5 [7]. But we analyze that as cloud server is not trustworthy so data should not be exposed to the cloud. Instead user can rely on TPA who has expertise in verification process and moreover user can authenticate TPA to check for its credibility. Juels and Kaliski proposed a model Proofs of Retrievability(POR) was one of the first most important attempts to formulize the notion "guaranteed remotely and reliable integrity of the data without retrieving of data file"[8]. Shacham and Waters gave a new model for POR enabling verifiability of unlimited number of queries by user with reduced overhead [9].

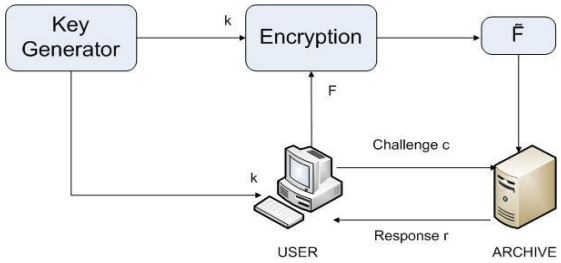

Figure 1: Schematic view of a Proof of Retrievability

K.Govinda, E.Sathiyamoorth proposed auditing scheme in which TPA checks the integrity of data outsourced by user in the cloud [10]. For monitoring integrity auditor takes cipher text from the cloud and generates original data from it using XOR. TPA calculates the hash value using SHA-1 algorithm and compares it with the hash value taken from user. If the value matches it is ensured that data is safe, otherwise tampered. Song et al proposes data protection as services, which offer data security and privacy on cloud Platform. These services can be provided using full disk encryption technique but it slow down data access time [11].

Some scheme provides a weaker guarantee by ensuring storage complexity. Earlier scheme has to access entire file from the server to check data integrity and which is not feasible in case of small computational devices.

3. Proposed Work:

The proposed work aims at developing a private cloud for storing files of the registered users. The paper implements the concept of the cloud as "Storage as a Service". Even after storing the files into the cloud, in their private space, the users usually are worried about the security of the files.The proposed work focuses on maintaining integrity of the data on the cloud by various techniques like generating encrypted keys for each file uploaded on the cloud, encrypting the metadata of the file, building a distributed database to store the information of the files, maintaining system logs and user notifications for the activities performed on any file. The mirror database would be developed as an exact replica of the main database which would be created to safeguard the system from any unwanted event that may occur. The idea of relying on third party auditors for monitoring integrity of the data stored in cloud does not eliminate the "trust problem." In order to avoid third party auditors in this chain, we propose that the integrity check of data stored in cloud can be checked at customer's side.

.

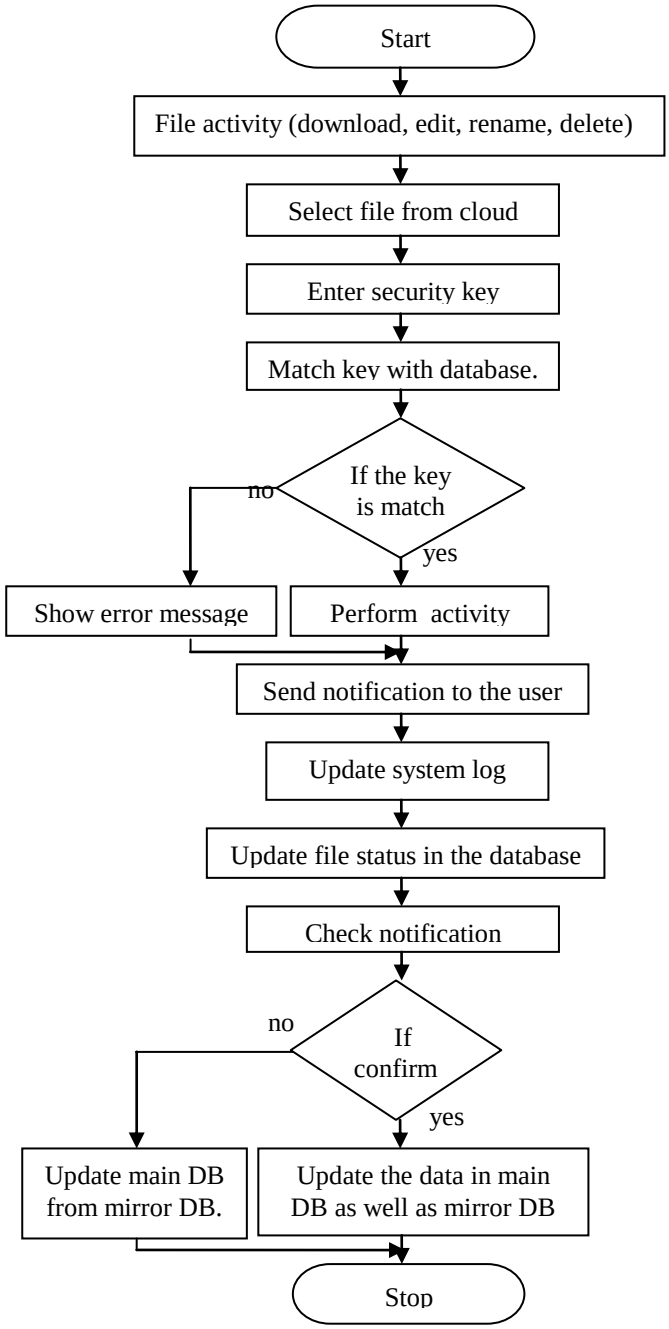

Figure 2: DFD for maintaining integrity of data

After successfully uploading the files, the activities like viewing the contents of file, rename the file, delete, download or edit the files can be performed. Hence the user will select the file from the cloud and will enter the security key for performing the activity. Then the key will get matched with the key in the database. If the key is matched with key stored into the database then the user will perform the activity otherwise it will throw the error message. But in both the cases the

notification will be get send to the user and the system log that is maintained on the cloud will get update. Then the user will check the notification if he will confirm it then both the mirror database and main database will get update but if he will not confirm it then main database will get update from mirror database. In this way the integrity of the file on the cloud will be checked.

4. Conclusion:

Privacy and security are the burning issues of any technology. As cloud is mainly used for the storage of the data, data integrity is the main issue of the client. So monitoring integrity of cloud data storage is of critical importance. There are so many techniques discussed in the literature which facilitate the client in getting a proof of integrity of the data which She wishes to store in the cloud storage servers with bare minimum costs and efforts. In this paper, we study the integrity and security of cloud storage data in order to give efficient proficiency to user for trustworthiness in each attempt in the data block when user is doing some updates such as append, deletion, and modification in his own will.

Reference:

1] J. Ruiter and M. Warnier, Privacy regulation for cloud computing, compliance and implementation in theory and practice, article.

2] P. Metri and G. Sarote, Privacy Issues and Challenges in Cloud Computing, International journal of Advanced Engineering Sciences and Technologies, Vol. No. 5, Issue No. 1,001-006

3] A white paper on , Cloud Computing : What How and Why.

4] R. Pandya, K. Sutaria, "An analysis of privacy techniques for data integrity in the cloud environment", International Journal of Computer and Electronics Engineering,(Dec 2012) ISSN: 0975-4202

5]Paul Zimski, "Cloud Computing faces security storms" in 2009.

6]Jia xu and Ee chien-chang, "towards efficient proof of retrievability in cloud storage".

7] Dalia Attas and Omar Batrafi "Efficient integrity checking technique for securing client data in cloud computing" in IJECS-IJENS, 2011

8] A. Juels and B.S. Kaliski, Jr., "Pors: proofs of retrievability for large files," in CCS˝07: Proceedings of the 14th ACM conference on Computer and communications security.

9] H. Shacham and B. Waters, "Compact Proofs of Retrievability," In Proceedings.of Asiacrypt ˝08, Dec. 2008.

10] K.Govinda, E.Sathiyamoorthy, "Data Auditing in Cloud Environment using Message Authentication Code", International Conference on Emerging Trends on Advanced Engineering Research(ICETT), 2012

11] Song.D, Shi.E, Fischer.I, Shankar.U,"Cloud Data protection for the masses", IEEE computer Society, Vol: 45, issue. pg.: 39-45, ISSN: 0018-9162