DATA INTEGRITY PROTECTION IN CLOUD

Indira G[1] Sujitha S[2] Subalakshmi K[3]

[1]Department of Computer Application,Francis Xavier Engineering College,Tamil Nadu, Tirunelveli

[2] AP/Department of Computer Application,Francis Xavier Engineering College,Tamil Nadu, Tirunelveli

[3]Department of Computer Application,Francis Xavier Engineering College,Tamil Nadu, Tirunelveli

ABSTRACT

In cloud computing integrity of data and access control are challenging issues. Protection of outsourced data in cloud storage becomes critical. Codes which are regenerating of data provide fault tolerance. Therefore, remotely checking the integrity of data against corruptions and other issues under a real time cloud storage setting is our problem of study. It practically design and implement Data Integrity Protection (DIP) environment.

KEYWORDS

DBMS,ACID,DIP,RAID,RSA

1. INTRODUCTION

As the data is stored in the remote location the user data falls into threats of the intruders where the confidentiality and integrity of the data is breached. This reduces the trust of the cloud service provider. There are several measures used by the CSP to provide the security of the data, but it never matches to the aspects. More and more owners start to store the data in the cloud. However, this new paradigm of data hosting service also introduces new security challenges. Owners would worry that the data could be lost in the cloud. This is because data loss could happen in any infrastructure, no matter what high degree of reliable measures cloud service providers would take. Sometimes, cloud service providers might be dishonest. It could discard the data which has not been accessed or rarely accessed to save the storage space and claim that the data are still correctly stored in the cloud. Therefore, owners need to be convinced that the data are correctly stored in the cloud.Data integrity is one of the most critical elements in any information system. Generally, data integrity means protecting data from unauthorized deletion, modification, or fabrication. Managing entity's admittance and rights to specific enterprise resources ensures that valuable data and services are not abused, misappropriated, or stolen.Data integrity is easily achieved in a standalone system with a single database. Data integrity in the standalone system is maintained via database constraints and transactions, which is usually finished by a database management system (DBMS). Transactions should follow ACID (atomicity, consistency, isolation, and durability) properties to ensure data integrity. Most databases support ACID transactions and can preserve data integrity.Authorization is used to control the access of data. It is the mechanism by which a system determines what level of access a particular authenticated user should have to secure resources controlled by the system.Data integrity in the cloud system means preserving information integrity.The data should not be lost or modified by unauthorized

D. Angeline, A. Arul et al.(Eds): ICICI-2021
pp. 211-218, 2021. IJCI – 2021 DOI:10.5121/ijci.2021.100223

users. Data integrity is the basis to provide cloud computing service such as SaaS, PaaS, and IaaS. Besides data storage of large-scaled data, cloud computing environment usually provides data processing service. Data integrity can be obtained by techniques such as RAID-like strategies and digital signature.Owing to the large quantity of entities and access points in a cloud environment, authorization is crucial in assuring that only authorized entities can interact with data. By avoiding the unauthorized access, organizations can achieve greater confidence in data integrity. The monitoring mechanisms offer the greater visibility into determining who or what may have altered data or system information, potentially affecting their integrity. Cloud computing providers are trusted to maintain data integrity and accuracy. However, it is necessary to build the third party supervision mechanism besides users and cloud service providers

The impact of algorithms and protocols, used to ensure data integrity and privacy, is studied to test the performance of the proposed model. The prototype system showed that data integrity and privacy are ensured against unauthorized parties. This model reduces the burden of checking the integrity of data stored in cloud storage by utilizing a third party, integrity checking service, and applies security mechanism that ensure privacy and confidentiality of data stored in cloud computing. This paper proposes an architecture based model that provides data integrity verification and privacy preserving in cloud computing.[1]In this paper, we propose the model of distributed virtual machine agent, and the model provides a unique and credible monitoring of virtual machines for each user in the cloud, so that even the sole administrator of the cloud server monitoring mechanism cannot bypass it and obtain protected sensitive data, preventing data from being tampered. In addition, based on virtual machine sagent auditing data, we utilize a data integrity protocol to make sure the users' data availability and integrity. Security analysis proves that the protocol can defend three kinds of attack from cloud service provider in our security model.[2] As many users share their data on a cloud the main question is about security of data present on cloud. In this research paper solution is provided to maintain data security and data integrity. This scheme contains a combination of RSA Partial homomorphic and MD5 hashing algorithm. In this solution data is encrypted by RSA Partial before uploading it on cloud server. After uploading its hash value is calculated by MD5 hashing scheme. All these approaches undergo through the following steps Encryption/Decryption, Data uploading on a cloud, Hashing and Verification.[3] In this paper, a detailed analysis of the cloud security problem is presented. Also the different problem in a cloud computing system and their effect upon the different cloud users are analyzed. It is providing a comparably scalable, position independent. Low cost platform for client's data. Since cloud computing environment is constructed based on open Architecture and interface. Based on this analysis various computing system and their effect upon the system, upon organizations and also upon different cloud users are analyzed. It is providing a comparably scalable, position-independent, low cost platform for client's data. Since cloud computing environment is constructed based on open architecture and interface. Based on this analysis various researches have also presented a view of measures that can be taken to deal with the cloud security problem and prevention that must be taken into account by any organization and cloud users seeking investment in cloud computing. [4]This new paradigm of data storage service also introduces new security challenges, because data owners and data servers have different identities and different business interests. Therefore, an independent auditing service is required to make sure that the data is correctly hosted in the Cloud. This paper surveys protocols that verify remote data possession. These protocols have been proposed as a primitive for ensuring the long-term integrity and availability of data stored at remote untrusted hosts. In this survey, we analyze several of these protocols, compare them with respect to expected security guarantees and discuss their limitations[5]

Architecture Diagram

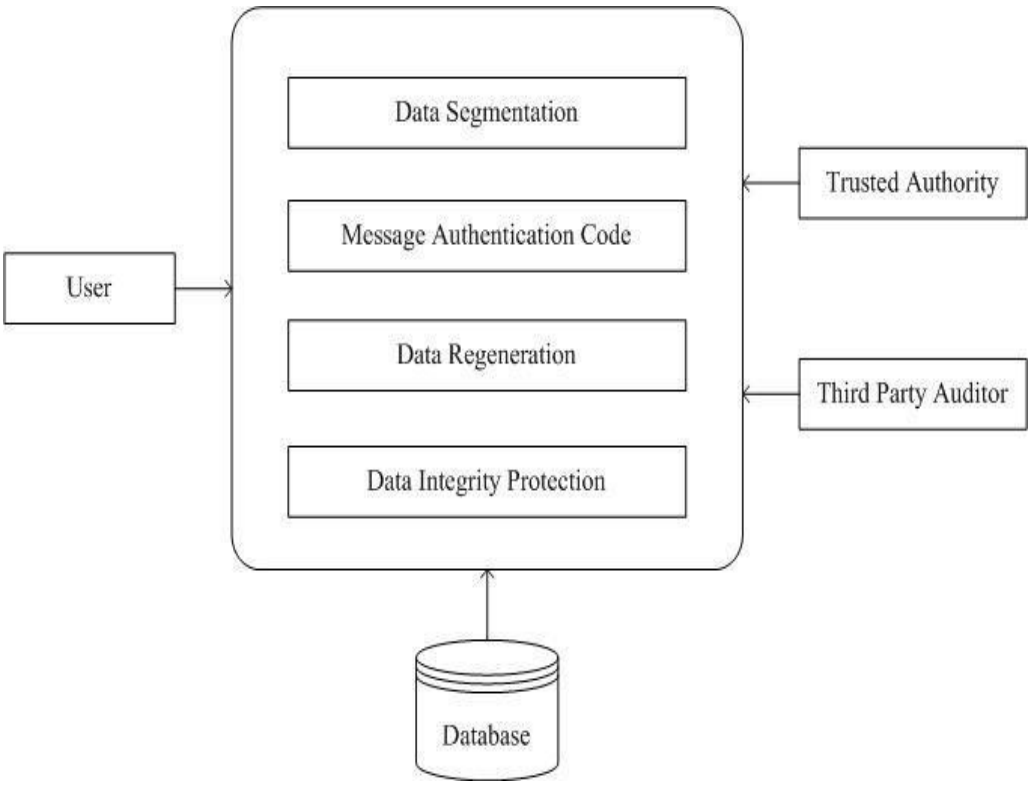

Figure 1 Architecture diagram

2. PROBLEM STATEMENT

Modules

Data Processing

- In this module, apply metadata processing suitable for operating data intensive and computational intensive applications. There is a serious requirement to deal with the data security issues for preserving the data integrity, privacy and trust in the security environment.

- While security concerns are protecting some organizations from adopting cloud computing at all. In this module, data owners first encode the metadata files by using regenerating code, and then store the coded file across multiple cloud servers. The multiple cloud web servers may locate in the same provider or different service providers. Data owners may perform block-level active functions on the outsourced data.

Meta Indexing

- In this module, meta indexing are proposed using data structure to support dynamic data update operations in which the data owner needs to store block index and block logical location for each block of the outsourced file.
- The main advantage of this method is that it is able to efficiently support dynamic update operations efficiently due to the node re-balancing problem.
- Data represent the user's data to be updated
- Index service represent the MAC indexing service
- The data index represent the index of the data on the server Fail Index represent the failed server index
- When any changes occurred then it uploaded

Third Party Auditor

- In this module, for data integrity confirmation use a third get together auditor, specifically a sole third party auditor. TPA helps an end user verify the metadata. TPA can gain access to control should be applied to determine traditional users and minimize the possibility of unauthorized users.
- The communication and computation expense should be reduced. Information integrity with high security may be ensured when blocks of information are distributed between multiple auditors for verification.
- Data represent the user's data to be updated
- Index service represent the MAC indexing service
- The data index represent the index of the data on the server.

3. EXPERIMENT AND RESULTS

Output Screen

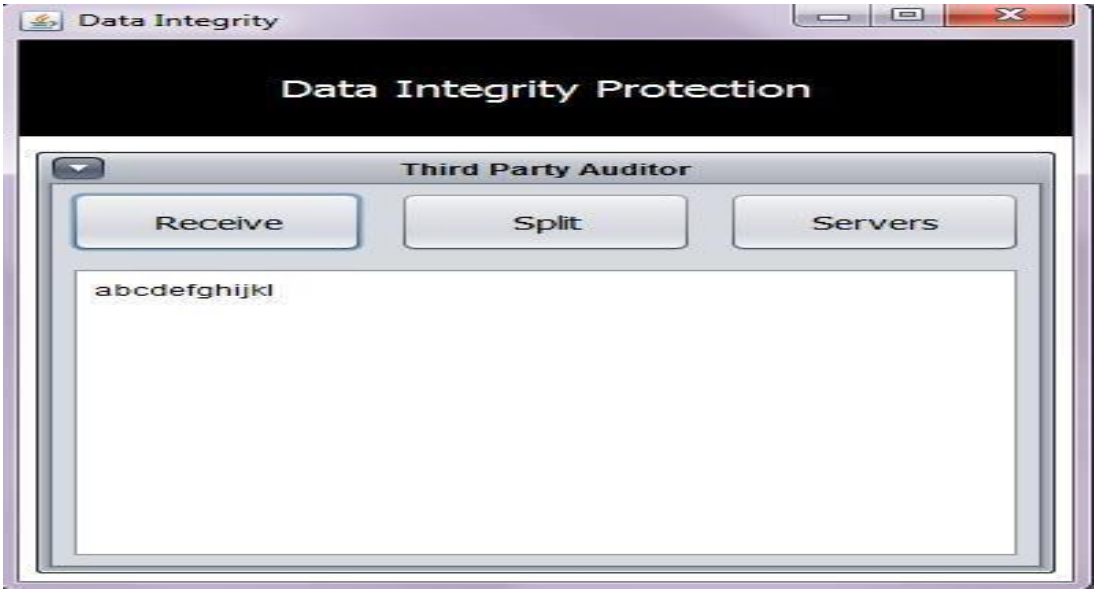

Figure 2 Servers Form

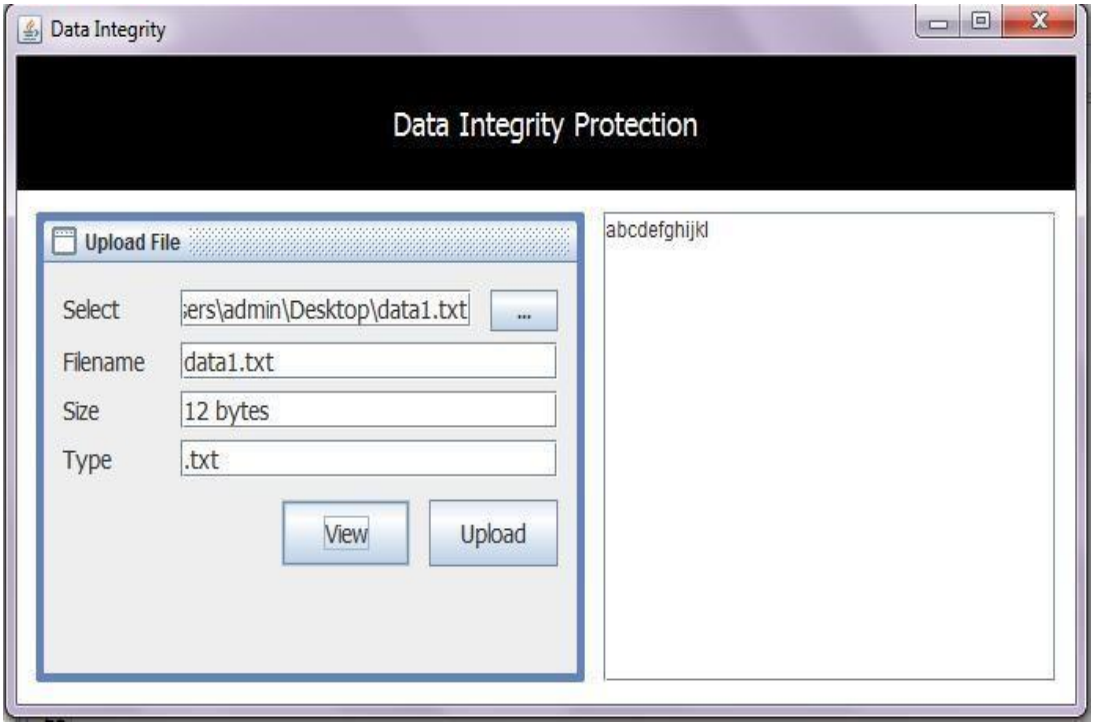

Figure 3. File Upload Form

Figure 4 Split Files

Figure 5 Server Protection

PERFORMANCE ANALYSIS

The exisiting and proposed system are analysed. The problem identified in exsiting The existing system is Storage Based on Erasure Coding that Simplify the content placement and recovery problem at the cost of longer data retrieval. The Rate less property enables its redundancy. Data security requirement of cloud computing and setup a mathematical data model for cloud computing. some of the things that appear on the existing system are given

below. Regenerating codes are implemented to minimize repair traffic in the network. It does not reading and reconstructing the whole file during the repair time. It reads a set of chunks smaller than the original file from the other servers and reconstructs only the lost contents. This assumption has prevented them from automating.Nearly 70% performance has been increased

4. CONCLUSION

In this project, a TPA based Integrity Verification and Data Recovery has been proposed, which helps reducing the computation time delay and traffic mismatch errors. The system mainly depends on Third Party Auditor (TPA) which will verify the status of the servers in regular interval for the lost connection or data. The system will gain more efficient, higher analytical of data records, time consuming. This system provides higher result in time consumption and reduced computation overhead which compared to the previous results. This DIP scheme maintaining the transparency between End user and cloud service provider by performing the tight security manually on the client side so that they can be satisfied on their security of data. So seen the popularity of outsourcing real storage to the respective cloud servers, it is necessary to enable clients to verify the integrity of a data in the cloud. Our DIP scheme preserve a fault tolerance and repair traffic saving.

5. FUTURE ENHANCEMENTS

In the future work, a backup or replication to the TPA can provide higher data retrieval and indexing in very less period. The security can be added to the system will help in protecting the more privacy to the user data and files. An efficient machine learning algorithms like ADABOOST can be implemented in the system which will help the system in time consumption and increase the accuracy of the retrieval.

In future we are going to focus on storage of data and retrieval of data to be done automatically that is auto backup with more tight security of data. It is designed for text file so in future we will further developed for audio and video respectively

REFERENCES

[1].C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-Preserving Public

[2].Auditing tool for cloud Data Storage”, In Proc. of IEEE INFOCOM, 2010.

[3]’Balachandra Reddy Kandukuri, Ramkrishna Paturi V, DR.Atanu Rakshit,

[4].“Cloud Security Issues”, 2009 IEEE International Conference on Services Computing.

[5].Mandeep Kaur and Manish Mahajan, “Implementing Various Encryption Algorithms to Enhance The data Security of Cloud in Cloud Computing”,

[6].2012 VSRD International Journal of Computer Science & Information Technology.

[7].Mehmet Yildiz, Jemal Abawajy, Tuncay Ercan and Andrew Bernoth, “A Layered Security Approach for Cloud Computing infrastructure”, 10th International Symposium on Pervasive Systems, Algorithms, and Networks, 2009 IEEE.

[8].Amazon Elastic Cloud. http://aws.amazon.com/ec2/.

[9]. Amazon Simple Database Service.http://aws.amazon.com/s3/.

[10]. http://ieeeexplore.ieee.org/Cloud Security and Data Integrity Farooq M, Hasan M, Gull F, Mycobial deterioration of stone monuments of Dharmarajika, Taxila, Journal of Microbiology & Experimentation, Vol. 2(1). Pp. 36-412015.

AUTHORS

Indira G doing final year MCA in Francis Xavier Engineering College

Ms. S. Sujitha working as Assistant Professor in the Department of Computer Applications, Francis Xavier Engineering College. Her area of interest is Wireless Sensor networks

Subalakshmi K doing first year MCA in Francis Xavier Engineering College