Scientific Journal Impact Factor (SJIF): 1.711

e-ISSN: 2349-9745
p-ISSN: 2393-8161

International Journal of Modern Trends in Engineering and Research
www.ijmter.com

Enhanced Data Partitioning Technique for Improving Cloud Data Storage Security

Sangram Rananavare[1], Prof. Anjali More[2], Pritam Vanne[3], Sneha Nanaware[4]

[1]*Department of Computer Engineering, S.B. Patil COE, Indapur*
[2]*Asst.Prof. Department of Computer Engineering, S.B. Patil COE, Indapur*
[3,4] *Department of Computer Engineering, S.B. Patil COE, Indapur*

Abstract— Cloud computing is a model for enabling for on demand network access to shared configurable computing resources (e.g. networks, servers, storage, applications, and services).It is based on virtualization and distributed computing technologies. Cloud Data storage systems enable user to store data efficiently on server without any trouble of data resources. User can easily store and retrieve their data remotely. The two biggest concerns about cloud data storage are reliability and security. Clients aren't like to entrust their data to another third party or companies without a guarantee that they will be able to access therein formations whenever they want. In the existing system, the data are stored in the cloud using dynamic data operation with computation which makes the user need to make a copy for further updating and verification of the data loss. Different distributed storing auditing techniques are used for overcoming the problem of data loss. Recent work of this paper has show that data partitioning technique used for data storage by providing Digital signature to every partitioning data and user .this technique allow user to upload or retrieve the data with matching the digital signatures provided to them. This method ensures high cloud storage integrity, enhanced error localization and easy identification of misbehaving server and unauthorized access to the cloud server. Hence this work aims to store the data securely in reduced space with less time and computational cost.

Keywords—Cloud Storage, Data Security, Cloud Partitioning, Digital Signature Extraction, Error Identification, Integrity Checking, Encryption, Decryption.

I. INTRODUCTION

Cloud computing is becoming increasingly important for provision of services and storage of data in the Internet. However there are several significant challenges in securing cloud infrastructures from different types of attacks. Client privacy is a most tentative issue in cloud as all clients don't have the same demand regarding with privacy. Some clients are satisfied with the current security aspects while others are concerned about their privacy. The proposed system is designed for the clients who belonging to the second category for whom privacy is a great concern. The client may not afford the luxury of maintaining private data storage, while they are interested in spending a little more money on maintaining their privacy and availability. Especially companies dealing with financial, educational, health, legal, banking are hit listed targets and leaking information of such companies can do significant harm to customer's stored data.

Cloud is work on different security aspects of the different cloud service security layers.

In which cloud providers and customers must share the responsibility for security and privacy in cloud computing environments, but sharing levels will differ for different delivery models, which in turn affect.

A**. Cloud Extensibility:**

SaaS: It is a provider which typically enables services with a large number of integrated features, resulting in less extensibility for customers. Providers are more responsible for the security and privacy of application services, more so in public than private clouds where the client organization might have stringent security requirements and provide the needed enforcement services. Private clouds could also demand more extensibility to accommodate customized requirements.

PaaS: In this the goal is to enable developers to build their own applications on top of the platforms provided. Thus, customers are primarily responsible for protecting the applications they build and run on the platforms. Providers are then responsible for isolating the customers' applications and workspaces from one another.

IaaS: It is the most extensible delivery model and provides few, if any, application-like features. It's expected that the consumers secure the operating systems, applications, and content. The cloud provider still must provide some basic, low-level data protection capabilities.

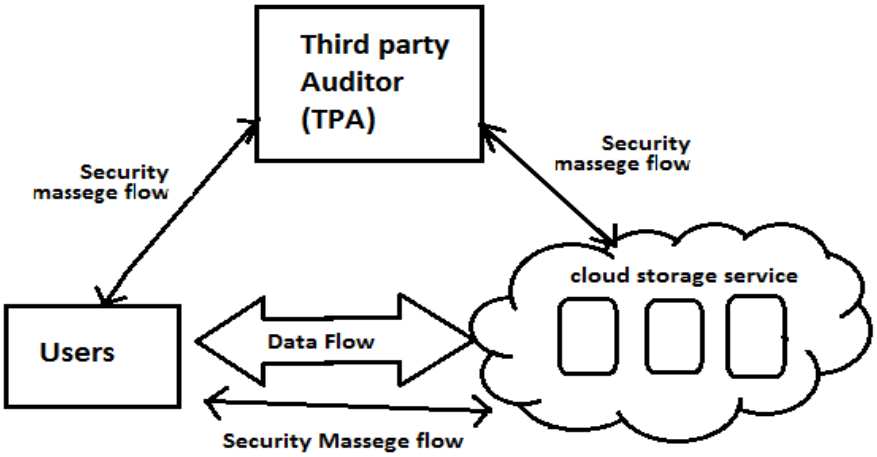

Figure 1 : The Architecture of Cloud Data Storage

The proposed approach will provide the cloud computing users with a decision model that supply better security by providing digital signature on partitioning data over cloud database, in such a way that none of the cloud service providers can successfully retrieve and upload meaningful information by using through significant manner data signatures allocated to their servers. Also, it provides the user with better assurance of availability of data by maintaining redundancy in distribution of data. Partitioning happens in vertical and horizontal directions where the data being used is controlled. The security mechanism is also used to prevent unrecoverable data loss.

II. CURRENT METHODOLOGY

Third Party Auditor (TPA) is middleware and checker between the user machine and cloud data storage server. TPA work on the basis of two auditability categories which are Private and Public auditability. Private auditability which provides higher efficiency to the authorize client, where public auditability permits anyone, not only authorize client but also give the ultimatum to cloud

server while keeping no private information for the purpose of correctness of storage data. TPA will audit the data of client to decrease the difficulty of data management of the client. For achieving economies of scale for Cloud Computing, it terminates the association of the client by auditing that whether his data stored in the cloud are actually together. The produced audit report which can be help client to calculate the risk of their cloud data services, and it will also be helpful to the cloud service provider to improve their cloud service platform. Hence TPA will give conformation to client to make sure that his data is safe in the cloud server and management of data will be easy and less difficult to client [1]. Data can be physically located anywhere in the world as Clouds have no limitations. So this aspect increases different issues related to user authentication and data confidentiality [5].

A privacy-preserving public auditing system for data storage security in Cloud Computing, where without asking the local copy of data TPA can able to perform the storage auditing[2]. It uses the homomorphism authenticator and random mask technique to guarantee the user that TPA would not aware about the data content stored on the cloud server during the auditing process, which not only removes the burden of cloud user from the complicated and expensive auditing task, but also relieves the user from the fear of data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, we further extend our privacy-preserving public auditing protocol into a multi-user setting, where TPA can perform the multiple auditing tasks in a batch manner, i.e., simultaneously. Extensive security and performance analysis shows that the proposed schemes are provably secure and highly efficient. [3]The public key, hash, and private key ciphers that are proposed between cloud service provider, data owner, and user ensure an isolated and secure execution environment at the cloud. We believe all these advantages of the proposed schemes will shed light on economies of scale for Cloud Computing.

[4] A cloud-based capacity plot that permits the information holder to profit from the offices offered by the CSP and empowers roundabout shared trust between them. The proposed plan has four essential peculiarities: (i) it permits the holder to outsource delicate information to a CSP, and perform full square level element operations on the outsourced information, i.e., piece alteration, insertion, erasure, and affix, (ii) it guarantees that approved clients get the most recent rendition of the outsourced information, (iii) it empowers backhanded common trust between the manager and the CSP, and (iv) it permits the manager to concede or repudiate access to the outsourced information. We talk about the security issues of the proposed plan.

In the overview led the examinations are connected existing framework, which guarantees to have information duplicate in the neighborhood framework. This restriction is overcome with the proposed methodology. This instrument gives information stockpiling security. The confinement with existing system is, it takes additional time and expense to perform the element transforming of information encryption and unscrambling procedures to store information in cloud with security. Proposed technique overcomes such restrictions with superior, lessened cost and restricted information storage room in cloud.

A. Review Table:

Techniques	Advantages	Disadvantages
Authentication and Identity	Authentication of users takes place in various ways like in the form of passwords that is known individually, in the form of a security token, or in the form a measurable quantity like fingerprint	Disadvantages of traditional identity approaches in a cloud environment is faced when the enterprise uses multiple cloud service providers (CSPs)

Data Encryption	If you are planning to store sensitive information on a large data store then you need to use data encryption techniques	When data is encrypted it is in a form that cannot be read without an Encryption key.
Captcha	It use for Authentication purpose	It not provide so much security for data storage

Table 1: Review of Current Technologies.

III. PROPOSED METHODOLOGY

In cloud system client upload his data on cloud servers and which is maintained locally. Data partitioning provides security to data and by using which user avoid local copy of data or multiple copies of data.

In architecture of network for cloud data storage there are three different network entities can be present as follows:

• User: It is an entity or person who has data to be store, upload and retrieve from the data cloud storage and relies on the cloud for data storage and computation; they can be either enterprise or individual clients

• Cloud Server (CS): It is an entity, which is managed by cloud service provider (CSP) to provide data storage service and has significant storage space and computation resources

• Third Party Auditor (TPA): It is a TPA, who has expert and capabilities and responsibilities that users may not have, is trusted to expose risk of cloud data storage services on behalf of the users upon request.

In cloud data storage, a user stores his data through a CSP into a set of cloud servers. The user interacts with the cloud servers via CSP to access or retrieve his data.

TPA (Third Party Auditor) perform partitioning of the data which uploaded by the user. Data partitioning method takes user input file. Data partitioning method has an important role. This method divide i.e. break up the large file into smaller modules or pieces. Data dividing into partitions helps to store data quick and effectively. It also improves easy access to data whenever data is needed. User's original data is complex and it faces difficulty in storing as it is into the cloud, that's why the data partitioning method is used which makes data storage easy in cloud. The partitioned data are then encrypted i.e. by applying public key they are encoded. The data partitioning is performed automatically when the data is get for storing in cloud. Whenever the user needs or request for its original file then it is reconstructed.

A. Algorithm: Partitioning and merging files

1. Get the Input file.
2. Calculate file size.
3. Data Partitioning file: If size<=min size or size>=max size Show error message.
   Else Divide file as per the number of servers with index value and extension.
4. Generate private key for each partition.
5. Encrypt respective partition using respective private keys.

6. Assign Digital Signature for each encrypted partition
7. Save partition sequence, digital signature, keys and file attribute at TPA.
8. Send each partition at respective storage server.
9. Merging file: TPA request for file partitions from storage servers.
10. Extract new digital signature of each partition and compare it with stored digital signature at TPA. If new digital signature equals to stored digital signature at TPA Merge file otherwise data is corrupted.
11. Decrypt the merged file with key.

B. Encryption: Encryption is used to encrypt the partitions of user's files for security. By use of encrypting the file, cipher text will be generated. By apply this approach of encryption of data it will randomly generate shared key algorithm and public key. Here we can store data in cloud by encrypting the files by using public and private RSA key. The length of generated private RSA key is 2048 bits. It uses symmetric encryption for secret key.

C. Decryption: Decryption is a technique which is used to decrypt the data partitions of files store on cloud which is access by generating the private key. A unique private key is generated for each end user for securely access the data from any location. For decrypt files it used non shared private key. The private key is use asymmetric technique. Private Key is generated while decrypting file for accessing file access control.

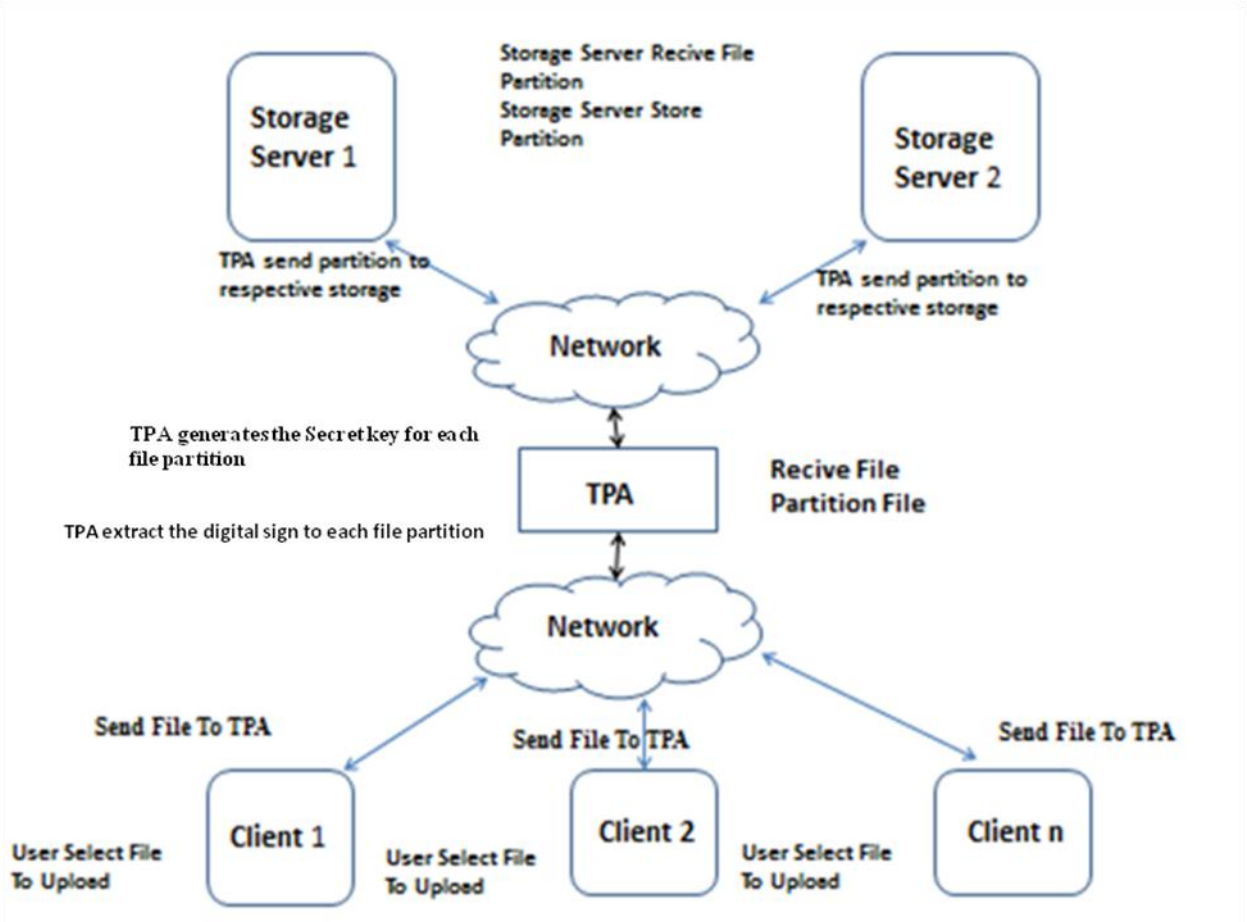

Figure 2: Proposed System Architecture

D. Storage Integrity Checking: Cloud storage integrity checking is accustomed to keeping the information misfortune. It additionally deals with the powerful stockpiling and recovery forms. General society auditability system deals with the lapse distinguishing proof by contrasting digital signature, confirmation, acting up server and blunder recuperation. This guarantees information security from unapproved access. It likewise builds the execution. Adaptable access control is additionally given to authentication in this work and to locate the assaults. Dynamic information operation, in the same way as insertion, deletion, and overhauling is additionally done before partitioning the information.

IV. CONCLUSION

In this paper we proposed data partitioning strategy for information stockpiling security in cloud administration. The partitioning of information empowers putting away of the information in simple and viable way. Segments are again separated into pieces for send at servers this serves to brisk recovery and store. It likewise gives path for adaptable access and there is less cost in information stockpiling. Cloud stockpiling integrity idea used to guarantee integrity of put away information. The space and time is likewise successfully lessened between capacities. Dynamic operation, encoding and translating procedure secures information, when putting away into cloud. Additionally Future work is wanted to give more elevated amount of security and scanning instruments for outsourced processing in cloud administrations.

REFERENCES

[1] Bhavna Makhija,VinitKumar gupta,Indrajit Rajput ,"Enhanced Data Security in Cloud Computing with Third Party Auditor",Hasmukh Goswami College of Engineering,Vahelal,Gujarat, International Journal of Advanced Research in Computer Science and Software Engineering.

[2] Cong Wang, Qian Wang, Kui Ren, and Wenjing Lou,"Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing", IEEE INFOCOM 2010, San Diego, CA, March 2010.

[3] Sunil Sanka, Chittaranjan Hota, Muttukrishnan Rajarajan," Secure Data Access in Cloud Computing", Computer Science and Information Systems Group, Birla Institute of Technology and Science-Pilani.

[4] Ayad F. Barsoum and M. Anwar Hasan," Enabling Data Dynamic and Indirect Mutual Trust for Cloud Computing Storage Systems", University of Waterloo, Ontario, Canada. IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSYEMS VOL: PP NO: 99 YEAR 2013.

[5] Nelson Gonzalez, Charles Miers, Fernando Red, Marcos," A quantitative analysis of current security concerns and solutions for cloud computing", at Journal of Cloud Computing: Advances, Systems and Applications 2012.

[6] M. Sudha, Dr.Bandaru Rama Krishna Rao, M. Monica," A Comprehensive Approach to Ensure Secure Data Communication in Cloud Environment" International Journal of Computer Applications (0975 – 8887) Volume 12– No.8, December 2010.

[7] C. Selvakumar,G. Jeeva Rathanam, M.R. Sumalatha, "Improving Cloud Data Storage Security Using Data Partitioning Technique ", 2013 3rd IEEE International Advance Computing Conference (IACC).

[8] Wang Cong, Wang Qian, Ren Koi, Cao Ning and Lou Wenjing,"Toward Secure and Dependable Storage Services in Cloud Computing," Services Computing,IEEE Transactions on, vol.5, no.2, pp.220-232, April-June 2012.

[9] C. Selvakumar, G. Jeeva Rathanam, M. R. Sumalatha "PDDS - Improving Cloud Data Storage Security Using Data Partitioning Technique " 3rd IEEE International Advance Computing Conference (IACC),2013.

[10] Takabi. H, Joshi.J.B.D and Ahn.G, "Security and Privacy Challenges in Cloud Computing Environments," Security Privacy, IEEE, vol.8, no.6, pp.24-31, Nov.- Dec. 2010.

