Privacy Preserving using Data Partitioning Technique for Secure Cloud Storage

Yogesh Shinde
Department of Computer Engineering
Dr. D. Y. Patil SOET
Lohgaon,Pune

Alka Vishwa
Department of Computer Engineering,
Dr. D. Y. Patil School of Engineering & Technology
Pune, India

ABSTRACT
Cloud Computing is a utility computing such asPay-as-you-go computing, Illusion of Infinite Resources, No UpfrontCost, Fine grained billing. User's store their large amountof data on a cloud severs at remote place without worryingabout Storage Correctness as well as information Integrity. Sothat users can option to a Third Party Auditor (TPA) to testthe data integrity and be worry-free because user does not physical present at all time. The Third Party Auditor(TPA) performs audits for multiple cloud users simultaneouslyand efficiently.In this paper, proposed scheme contain data files dividedinto small block technique. which ensure cloud storage security, integrity. To increase the user level security we proposed One Time Password (OTP) at the time of file uploading. Partitioning process implemented at TPA side. TPA performs operation like data files divided into small part of block, take hash of each block, each block Encrypt using cryptographic algorithm.

Keywords
cloud computing, Third Party Auditing, Data storage, Integrity, Batch Verification, One Time Password engines.

1. INTRODUCTION
Cloud Computing is an rising style of Information Technology(IT) delivery in which Applications , Data Files ,andVarious IT resources are quickly provisioned and provided asconsistent offering to users over the web in flexible pricingmodel. The Essential characteristics of Cloud computing isOn-demand service, Location Independent, wide network access,Measured services, Rapid elasticity and Pay as use. Itprovides service models such as Platform as a Service (PaaS),Infrastructure as a Service (IaaS), and Software as a Service(SaaS) [2].cloud computing provides various advantages butalso increased security risk towards the user outsourced data.Cloud Service Providers (CSP) is separate external entity. Theyare still facing the wide range of both inside and outsidethreats for data integrity. Internal Threats such as CSP is self-interested, modify user data, some employee at CSP or leaksdata to other party. External Threats such as external attacker'shack the user data's might be behave unfaithfully for moneyreason; CSP might delete a data file that's rarely accessed; CSPmight hide data files loss to protect their reputation. Clouduser stored data on remote location without worrying aboutcorrectness and integrity of data files how user will get theproof about data stored on cloud whether modify or delete. Asusers no more physically possess the storage of their data. Files, traditional cryptographic primitives for the purpose ofdata security protection cannot be directly adopted [5]. Thus,how to efficiently verify the correctness of outsourced clouddata files without the local copy of data files becomes a bigchallenge for data storage security in Cloud Computing. If userdownloads all the data files for checking its integrity then thereis communication and network overhead. To guarantee the datafiles integrity and save the cloud user's computation resourcesas well as online burden, it is of critical importance to allowpublic auditing service for secure cloud data storage, so thatclient may resort to an self-governing third-party auditor (TPA)to audit the outsourced data when needed. Another outsideaudit party is called TPA. TPA helps the client to review theclient information files. To permit TPA safely.

1. Without asking the copy of files from cloud, TPA should audit the data files.
2. TPA should not create new vulnerability to user dataprivacy.
3. At times check the integrity of outsourced data files.

The TPA is an expertise in knowledge as well as has capabilitiesthat users do not. TPA does not need to maintain andupdate state between audits process, which is an attractiveproperty especially in the public auditing system. As theindividual auditing of these growing tasks can be tediousand burdensome, but the TPA to efficiently perform multipleauditing tasks in a batch manner, i.e. at the same time as. TPAis also help to Cloud Service Provider to get better cloud-basedservice platform.

Phishing, a serious security threats to Internet users an e-mail fraud. One of the ways to prevent the password theft is to avoid using passwords and to authenticate a user without a text password. User will obtain the One Time Password (OTP) at the time of file uploading on cloud. This is send to user valid mail id. One time password to achieve high level of security in authenticating the user over the internet. An OTP is a set of characters that can act as a form identity for one time only. Here we are using dynamic password instead of static password. Once the password is used, it is no longer used for any further authentication. Even if the attacker gets the password, it is most likely that it was already used once, as it was being transmitted, thus useless to the attacker [6]. Cloud storage integrity checked by comparing Hash of data. Hash of data extracted before sending data to sever these hash stored at TPA, at time of data retrieval again hash of data extracted and compares with hash stored at TPA. If both are same then integrity of data not violated. Specifically, our contribution can be summarized as the following three aspects;

1. To protect the Integrity of outsourced data using Third Party Auditing mechanism.
2. To enable Privacy Preserving Public Auditing using TPA for Secure Cloud Storage.
3. To increase user level security by using One Time Password (OTP) at the time of uploads the file.

The proposed scheme utilizes the technique of public key-based homomorphic linear authenticator (HLA) integrating with random masking, the framework assurance that the TPA could not gain knowledge regarding content of data files stored in the cloud server (CS) during the proficient auditing process [4].

2. ISSUES IN CLOUD

A. Security Issues

Security issues are considered as most key essential issues in cloud computing. Because client store its data files on cloud. Following are some major security issues-

1. Access Control: Unauthorized access may be occurs when security mechanism is not provided by CSP at some level.
2. Authentication and Identification: Number of clients Serve by cloud at same time there is a problem of authentication and identification.
3. Availability: Cloud Service is not available all the time then the availability issues will be occurs.
4. Control Policy: It is most important issues in cloud Because multiple cloud server providers have different protection mechanisms. There is possibility that CSP may be self-interested in client's data files without his permission.

B. Privacy Issues

Privacy is another main issues in cloud computing. Following are a few privacy issues:

1. Unauthorized usage: Unauthorized data usage can become serious problem in cloud. CSP is self-interest or leak user's data files without user permission.

2. Lack of user control: User stored data files at remote

Location on cloud. That's means users have no control on his data files. So there is need of protection mechanism.

3. Unclear responsibility: Unclear responsibility is one

Problem related to the privacy. At which Cloud Service

Provider (CSP) is dependable for privacy protection, detecting who alter the client data.

3. RELATED WORK

In this section describe Survey related to Privacy preserving and Data security using TPA for Secure cloud storage and also some relative mechanisms and the previous methods which are working earlier to achieve a security and privacy are discussed. According to the survey of the earlier mechanism, it finds that the current system implemented has more advantages.

Qian Wang[3] describe the Scheme Allows third partyauditor (TPA), on behalf of the cloud client, Merkle HashTree (MHT) is used for the construction of block tag authentication.but it has some drawback like Third party can beuntrustworthy or not be able to commit necessary working outresources performing constant verifications.

Cong Wang,Qian Wang,KuiRen, [5] has describe a method Distributed storage integrity auditing mechanism. It has some advantages such as Dynamic data verification and Resilient against Byzantine failure and malicious data modification attack. But disadvantages of that method are multiple copies are present which requires a high memory and Data Integrity is not achieved.

Himika Parmar, Nancy Nainan [6] describe a authentication service method such as Image based and One Time Password after Image based Authentication (IBA) .which provide high level security mechanism.

Huaqun Wang [7] focuses on Proxy provable data possession method. It has some advantages such as efficient user controlled data management. Disadvantages like Public verifiability may cause intruders collision on data files.

The dynamic data storage with token pre-computation and AES algorithm how it is stored in cloud is analysed [8] Integrity checking concepts is also used to detect and avoid misbehaving server considering data correction and error localization.

C. Wang, Q. Wang [9] focus on file distribution and token pre computation model. But it does not provide the files block insertion operation. it requires lots of shifting of block when insert blocks

4. PROPOSED SYSTEM

In this section describe about System Design of publicauditing scheme which provides a complete outsourcing solutionof data files and also integrity checking. After introducingProblem definition, system begin from a summary of our publicauditing system for secure cloud storage. .

4.1 Problem Statement

To develop system which Protect the user data Integrity at Remote place using Third Party Auditor for Secure Cloud Storage.

4.2 Proposed Architecture

In this section describe about System model of Privacy Maintaining using public auditing scheme which provides a complete solution of data files and also integrity checking. The cloud data storage service consists of following different Entities

1. Client (User): Who have to stores large amount files on Cloud server.
2. Cloud Service Provider (CSP): It is separate entity that provides major storage space, resources, and maintenance for user data files.
3. Third Party Auditor (TPA): TPA is another network entity that has knowledge capability that client does not have. This is checking the user outsourced data files without copy of those files.

Block of data files performed at User level. Block module accept user input file. When user Browse fileit divided into smaller parts. It helps to store the data effectively in quick manner enhancing easy access to data also when there is need. The original data is complex and there is difficulty in storing it in cloud, so blocking function is used to make the storage easy in cloud. The block of files are encrypted, that is encoded with the public key and stored in cloud.

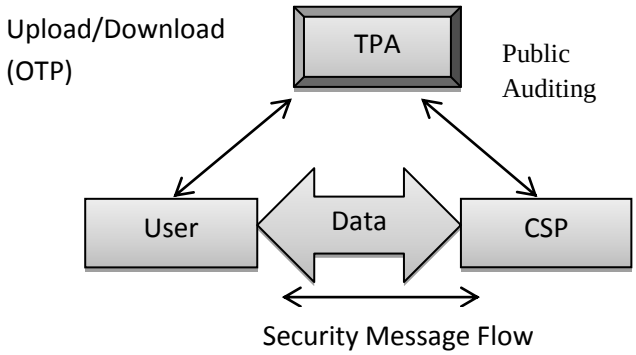

Fig.1: System Architecture

In our proposed system user will first encrypt data and then Encrypted file divided into block that encrypted block will store on cloud. For encrypting data we are using AES Algorithm and for generation of Hash using MD5 algorithm.

4.3 System Phases

The A Public Auditing Scheme Consists Two Phases:

1. SETUP PHASE: Setup phase contain following Algorithms

    1. Key generation Algorithm: This algorithm used for generation of Public and Private Key. Here we are using RSA algorithm for generating both key.

    2. Signature generation: This is used for generation of hash, metadata and digital signature.

2. VERIFICATION PHASE: Audit phase contain following Algorithms:

    1. Generation of Proof: when user send request for checking integrity of file. Each server computes a response as Integrity proof.

    2. Verify Proof: This is run by Third Party Auditor for verify integrity of files which is stored onremote place.

4.4 Mathematical Model

System S= {U, F, B, Cs ,TPA,H }

Where, U is Set of User (u_1, u_2, …u_n Є U)

1. F is Set of Files (f_1, f_2, ….f_n Є F)
2. B is Block of files (b_1,b_2,…,b_n Є B)
3. CS is Cloud data storage server.
4. TPA is Third Party Auditor.
5. H is hash of file.(h_1,h_2…h_n)

Table 1. Activities Table

Activity	Relation	Description
Activity 1:	U →F	Every User has No. of Data files
Activity 2:	B→TPA	Block of file send to Third Party Auditor
Activity 3:	TPA → H	TPA generates Hash of Each Block. Store along with.
Activity 4:	TPA → CS	TPA sends File To CS for Storing purpose.
Activity 5:	CS→TPA	CS sends newly Hash To TPA. Compare both hashes for Integrity Checking.
Activity 6:	TPA→U	Acknowledgement to User

4.5 Algorithm

Third Party Auditor performed file partition. File is divided into small chunks. Chunks size is calculated using no. of lines divide 4. Chunks module accept user input file. The original files are composite and there is Trouble in storing it in cloud, so partitioning function is used to make the storage easy in cloud. The partitioned files are encrypted, that is encoded with the public key and stored in cloud. Partitioning takes place automatically when the data is fed for storing in cloud. Original file is also reconstructed when there is need to access the same.

Partitioning Algorithm

1. Browse the File for Upload
2. Calculate size of input file.
3. Chunk Size=numbers of lines/4
4. Encrypt each block using AES algorithm
5. Generate hash of particular block using MD5 Algorithm
6. Store files id, hash of block, key at TPA.
7. Forward each encrypted blocks to cloud server for storing purpose
8. If user want to check Integrity of particular block he send request to Third Party Auditor (TPA).
9. CSP send newly generated hash to TPA and TPA compare

Both hash.

10. If new hash equals to store hash at TPA.Acknowledgement will be that stored data is as it is. Otherwise data is corrupted or modified.
11. Decrypt the combined file using Private Key.

5. EXPECTED RESULTS

Following figure shows that performance analysis of partitioning techniques. In which storage size of chunks file vs. Storage size of original file. It will be see that data partitioning techniques more powerful and increase performance over existing System. It allows the user to outsourced personal data to a CSP, and performs block-level dynamic operations on the data, i.e., block modification, insertion, deletion, and append,

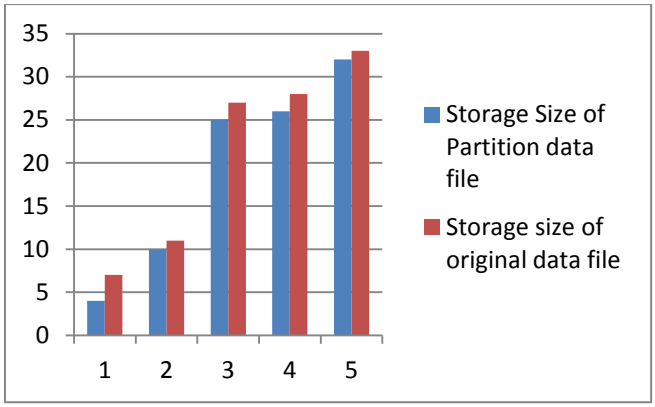

Figure 2: Minimize Storage Size in Partition Data files

6. CONCLUSION

In this paper we proposed Privacy Preserving public auditing using TPA for security to data files stored on cloud. Our proposed scheme support data partitioning technique for data storage security in cloud service. Third party does not contain any state at the time of auditing. One time password (OTP) achieves great level of security in authenticating the user over network. Many company such as Google, Hot mail, RBI use OTP for high security to User. The block of data enables storing of the data in easy and effective manner. Partitions are again divided into chunks for send at servers this helps to quick retrieval and store.

Future work is planned to provide higher level of security using Image based Authentication and searching mechanisms over encrypted data for outsourced computations in cloud services

7. ACKNOWLEDGMENTS

I express my sincere gratitude to Dr. U. B. Kalwane, Principal for providing me an opportunity to undergo this work. I am thankful to Prof. Alka Vishwa, Asst. Professor of Computer Engineering for her support, co-operation, and motivation provided to us during the work for constant inspiration, presence and blessings. I take this opportunity to express my profound gratitude and deep regard Prof.Arti Mohanpurkar, HOD and Asst. Professor Department of Computer Engineering for her exemplary guidance, monitoring and constant encouragement throughout the course of this work.

8. REFERENCES

[1] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage", IEEE Transactions on computers, vol. 62, no. 2, february 2013

[2] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing",http://csrc.nist.gov/groups/SNS/cloud-omputing/index.html, June 2009.

[3] 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 and Distributed Systems, vol. 22, no. 5, pp. 847-859, May 2011

[4] A. Juels and J. Burton, S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. ACM Conf. Computer and Comm. Security (CCS '07), pp. 584-597, Oct. 2007.

[5] C. Wang, K. Ren, W. Lou, and J. Li, "Towards Publicly Auditable Secure Cloud Data Storage Services," IEEE Network Magazine, vol. 24, no. 4, pp. 19-24, July/Aug. 2010..

[6] Himika Parmar, Nancy Nainan and Sumaiya Thaseen, "Generation of secure one-time password based on image Authentication", Computer Science & Information Technology, pp. 195–206, 2012.

[7] Huaqun Wang, "Proxy Provable Data Possession in Public Clouds", IEEE Transactions On Services Computing, Vol. 6, No. 4, October-December 2013, ISSN: 1939-1374

[8] Santosh Jogade, Ravi Sharma, Prof. Rajani Kadam, "Partitioning Data and Domain Integrity Checking for Storage - Improving Cloud Storage Security Using Data Partitioning Technique", International Journal of Emerging Research in Management &Technology, ISSN: 2278-9359 (Volume-3, Issue-3)

[9] C. Wang, Q. Wang, K. Ren, and W. Lou, "Ensuring Data Storage Security in Cloud Computing," Proc. 17th Int'l Workshop Quality of Service (IWQoS '09), pp. 1-9, July 2009