ISSN 2395-1621

Privacy Preserving Public Auditing and Data Integrity Using TPA for Secure Cloud Storage

[#1]Mr. Yogesh N. Shinde, [#2]Mr. Vaibhav N. Patil, [#3]Mr. Harshal A. Karande, [#4]Dr. Ashokkumar S. Karande

[1]yogeshshindeit@gmail.com
[2]vaibhavpatil521@gmail.com
[3]harshalkarande89@gmail.com
[4]ashokkarande9@gmail.com

[#1]Assistant Professor, Department of Computer Science Engineering
Yashoda Shikshan Prasarak Mandal's Yashoda Technical Campus, Wadhe, Satara.

[#2]Assistant Professor, Department of Computer Science and Engineering,
Arvind Gavali College of Engineering, Panmalewadi,Varye, Satara-415015, Maharashtra, India.

[#3]Assistant Professor, Department of Computer Science and Engineering,
Arvind Gavali College of Engineering, Panmalewadi,Varye, Satara-415015, Maharashtra, India

[#4]Associate Professor, Department of Business Economics, Mahila Mahavidyalaya, Karad.
Karad-415110, Maharashtra, India.

ABSTRACT

Cloud computing is a utility computing such as pay as you go computing, the illusion of infinite resources, no upfront cost, fine-grained billing. User's store their large amount of data on a cloud severs at the remote place without worrying about storage correctness and integrity of data. Personal Information is stored at another place how users will get the confirmation about data stored on the cloud. So that, cloud data storage have unique method which will specify storage Accuracy and integrity of data stored on a cloud. Permitting public auditability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the ethics of outsourced data and be worry-free because user does not physical present at all time. The framework consists of the secure cloud storage system supporting privacy-preserving public auditing. The proposed method have also assures recovery of data files, in case of data loss or corruption. System supports data dynamics where user can perform different operations on files like as insert, delete and update as well as batch auditing, where multiple cloud client requests for storage correctness will be handled simultaneously which decrease communication and also computing cost. To use and expand the user level safety, proposed procedure supplied a click on point based graphical password scheme and One Time Password (OTP) on the time of uploading the file.

Keywords: Cloud Storage, Data Availability, data storage auditing, Privacy and Security.

ARTICLE INFO

Article History

Received: 25th March 2017

Received in revised form :

25th March 2017

Accepted: 25th March 2017

Published online :

4th May 2017

I. INTRODUCTION

Cloud Computing uses hardware and software as computing resources to provide service through the internet. Cloud computing provides various service models such as Platform as a service (PaaS), Infrastructure as a Service (Iaas), Software as a Service (SaaS), Storage as a Service (STaaS), Security as a Service (SECaaS), Data as a Service (DaaS) etc. Cloud storage becomes a growing attraction in cloud computing model, which allows client to store their data on cloud and access them anywhere without any risk. The advantages can be listed as on demand self-service, worldwide network access, location independent resource pooling, faster resource elasticity. Cloud data storage

permits client to collection their files at remote place and reduce local storage maintenance and management. However, the benefits are clear, such a service is also relinquishing users physical possession of their utsourced data, which inevitably poses new security risks towards the correctness of the data in cloud [1-4]. The users require that their data remain secure over the CSP and they need to have a strong assurance from the cloud servers that CSP store their data correctly without tampering or partially deleting because the internal operation details of service providers may not be known to the cloud users. Thus, an efficient and secure scheme for cloud data storage has to be in a position to ensure the data integrity and confidentiality. Encrypting the data before keeping in cloud can deal with the confidentiality issue. However, verifying integrity of data is a difficult task without having a local copy of data or retrieving it from the server. Due to this reason the straightforward cryptographic primitives cannot be applied directly for protecting outsourced data. Besides a naive way to check the data integrity of data storage is to download the stored data in order to validate its integrity, which is impractical for excessive I/O cost, high com-munication overhead across the network and limited computing capability. Therefore, efficient and effective mechanisms are needed to protect the confidentiality and integrity of users data with minimum computation, communication and storage overhead.

The confidentiality and integrity of the outsourced data in clouds are of paramount importance for their functionality. The reasons are listed as follows [5],

• The CSP, whose purpose is mainly to make a profit and maintains a reputation, has intentionally hide data loss an incident which is rarely accessed by the user's

• The malicious CSP might delete some of data or is able to easily obtain all the information and sell it to the biggest rival of Company.

• An attacker who intercepts and captures the communications is able to know the user's sensitive information as well as some important business secrets.

• Cloud infrastructures are subject to wide range of internal and external threats Remote data integrity checking is a protocol that focuses on how frequently and efficiently we verify whether cloud server can faithfully store the users data without retrieving it. In this protocol, the user generates some hash. Earlier, The user send request to server for checking the integrity of file blocks through challenge response protocol. Then the cloud server generates responses and sent to third party or verifier. As of late, a few analysts have proposed distinctive varieties of remote data checking under different cryptography schemes [6].

In order to resolve the issue of data integrity checking, many techniques are proposed under various systems and security models. In all these works, much more efforts are made to design solutions that meet different requirements such as high methodology efficiency, stateless verification, unbounded use of queries and retrievability of data etc.

II. MOTIVATIONS

The Cloud computing is a leading technology which provides various services to users such as allows users to store their data on a cloud without worrying about correctness and integrity of data, use on-demand high-quality applications and services. Data is stored at the remote place how users will get the confirmation about data stored in the cloud. Accuracy and security of data are fundamental concerns. Security in the cloud network is achieved by the sign the data block before sending the data to the cyber network.

In proposed system, The cloud server is considered as untrusted thing. After a check is performed, a notification is sent to the client about the status of his data. Showing whether the data is in its actual form or if its integrity is lost. A large amount of data is generated due to applications. This data need to be stored which requires a large amount of storage space. Data generation is currently outpacing storage availability, hence, there will be more and more need to outsource data. The cloud service provider may hide the data corruptions to maintain the reputation. To avoid this problem, the system introduce an effective third party auditor (TPA) to audit the users outsourced data when needed verification of data integrity is the at most important for a user. Who has outsourced data to the cloud . To make the integrity check, a public auditing must be made possible.

III. LITERATURE SURVEY

Cloud computing providing big infrastructure to store and execute client data. There is not need of to make own the infrastructure. The main benefits are to reduce capital expenditure. Benefits are minimized capital expenditure, location, device independence, utilization and proficiency improvement.

The author proposes a approach which consist on RSA based hash function for integrity verification of the stored data at remote server. Using this scheme, it is possible for the client to perform multiple challenges using the same metadata. But the limitation of this scheme lies in the computational complexity at the server which must exponentiate all the blocks in the file [6] .

Miller and Schwarz [8] proposed a technique in which the data stored remotely across Multiple sites can be ensured. The scheme makes use of an algebraic signature. In this, a function is used to fingerprint the file block and then verifies if the signature of the parity block is same as the signature of the block. The main disadvantage of this scheme is that the computation complexity at the client side and server side takes place at the cost of the linear combination of file blocks. Also, the security of this scheme remains unclear.

Q. Wang et al.[9] achieved the difficulties and potential security problems of direct extensions with fully dynamic data updates from prior works and then show how to construct an elegant verification scheme for the seamless integration of these two important features in their protocol design. To assist efficient handling of multiple auditing tasks, they further explored the technique of bilinear aggregate signature to extend their main result into a multi-user setting As storage outsourcing services and resource sharing networks have become popular, the problem of efficiently proving the integrity of data stored at untrusted servers has received increased attention. The Provable Data Possession [PDP]

model for remote data checking supports large data sets in widely distributed storage systems. It is the provably-secure scheme for remote data checking. The main disadvantage of this scheme is that an overhead of generating metadata is imposed on the client. No support provided for dynamic auditing[10].

The first proof of retrievability mechanisms with full proofs of security against arbitrary adversaries in the strongest model, that of Juels and Kaliski. Their first scheme was built from BLS signatures and secure in the random oracle model. Their second scheme was building on Pseudo-Random Functions (PRFs) and they stated that this scheme is secure in the standard model which allows only private verification [11].

A scheme called, "Proofs of Retrievability (POR), proposed by Juels and Kalisiki focuses on static archival of large files. To ensure data possession and retrievability, it makes use of spot checking and error correcting codes. POR scheme cannot be used for public databases. It is suitable only for confidential data. The disadvantages of this scheme are that the number of queries clients used is fixed priority. Preprocessing of each file is needed prior to storage at the server. The scheme cannot be used for public databases and can only be used for confidential data. POR does not support Public Auditability, i.e. it supports only two party auditing, which is not efficient because neither the client nor the cloud service provider can give assurance to provide balance auditing[12]. The main approach based on public auditability for checking the integrity of confidential data. This auditability can be done by Third Party Auditor (TPA) on behalf of the cloud client to analyze the integrity of the dynamically stored cloud data. This removes the interference of users to check their intactness which could be important in achieving economies of scale for Cloud Computing[13].

S. Marium [14] is containing to highlight security and privacy problems in a cloud. Their research was mainly focused on service providers side security. The author purposed the implementation of Extensible Authentication Protocol through three-way handshake with RSA to ensure the security of client data in the cloud. I-Hsun Chuang, Syuan-Hao Li[15] describe the encryption algorithm for security purpose, but it has some drawbacks. It does not describe the dynamic data operations and server misbehavior. The auditing result not only ensures strong cloud storage correctness guarantee but also simultaneously achieves fast data error localization, i.e. the identification of misbehaving server. The main system is highly efficient and resilient against Byzantine failure, malicious data modification attack, and even server colluding attacks. It has some disadvantage like high redundant copies are present which may cause high memory occupation and data Integrity is not achieved [16]

IV. SYSTEM OVERVIEW

Problem Statement

The issue of the framework integrates with past system benefits and covers to find the unap proved client, to check the unauthorized data usage and access maintaining data privacy. The framework displays the user requests according the client specified attributes such that user name , password , click point password and it checks the arguments for the original(new)and current(existing) users. If the user attributes matches with cloud provider , it gives authority to access data otherwise auditing system block that user. To develop system which improve the user level security using graphical click point passwords and protect the integrity of data at remote place using Third Party Auditor(TPA) for secure cloud storage. When download any files from cloud, there should not be any loss of data.

Goals and Objectives

The design goals of the proposed system are,

1. The main objective of cloud storage is guaranteeing control and the necessary integrity and confidentiality of all stored data.

2. To increase the user level security using knowledge based authentication mechanisms such as "Click Point Image Based Authentication".

3. To improve the high level of security in authenticating, one time password is used by the user over the internet and to recover data in case of data loss or corruption

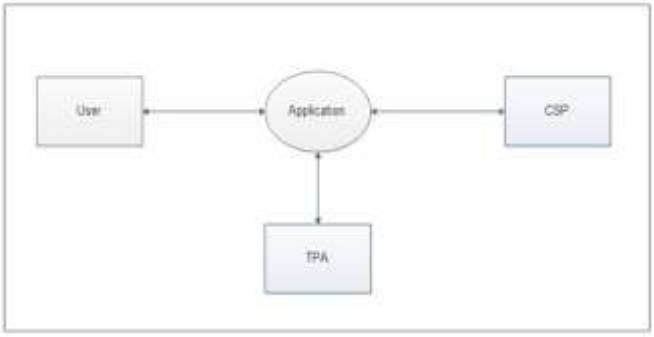

Figure 1: Product overview diagram of the system .

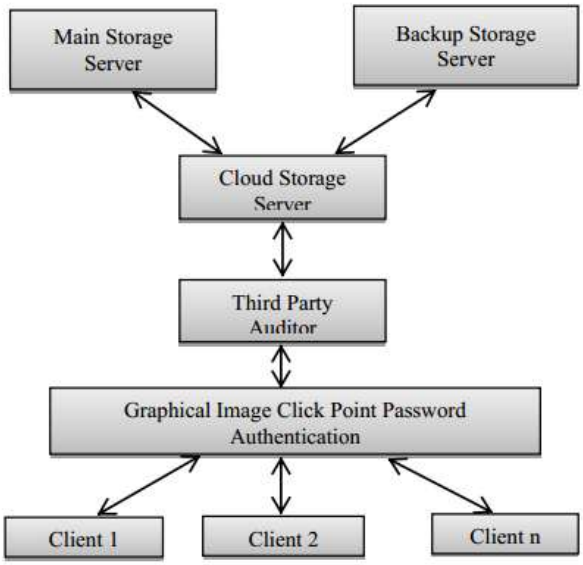

Figure 2: Architectural diagram of proposed system.

Cloud data storage service involving five different entities ,

1. **User -** Clients rely on the cloud for data computation. They include individual consumers and organization.

2. **Cloud Service Provider (CSP) -** Cloud server maintained by Cloud Service Provider (CSP), has consequential storage space and estimation resources to maintain the clients remote data.
3. **Third Party Auditor (TPA) -** The third party auditor or verifier, who has proficiency , capabilities to audit data any time and verifies the integrity of outsourced data in cloud on behalf of users.
4. **Main Storage Server-** Storage in main server is also called as primary storage . It is area in a computer device in which files are stored and access by processor very efficient manner.
5. Backup Storage Server- A backup, or the process of backing up, refers to the copying and archiving of computer data so it may be used to restore the original after a data loss event.

The public auditing process, it consists of two phases as explain below,

• Setup Phase

In this phase, the user pre-processes the file before storing in cloud. The Setup phase consists of three algorithms, those are: KeyGen, Encryption, HashGen. The file F= $\{p_1; p_2; \ldots . . ; p_n\}$ is generated by the client, which is a finite collection on n blocks. Using the key generation algorithm, the secret key is generated. In the first step, a signature is generated for each file block using the secret key and MD5 hash algorithm

• Audit or Verifier Phase

Once data has stored in cloud, in order to ensure the integrity of data, our scheme entirely relies on verification phase. Client sending a request to TPA for auditing the desired file or data. This is done by sending some metadata such as id of file and user id. The TPA send request to the cloud provider and in response, the server generates a proof for the corresponding challenge. The proof contains the hash for the respective file. If newly send hash by csp matches with hash stored during file upload, the output is given as file will safe. If the hash does not match, it means that some changes are made to the file and the file has lost its integrity. In both the cases, a acknowledgement is sent to the user. In case of data loss or if the file is corrupted, the client can recover the file from the recovery system if he has previously taken a backup of the file**.**

V. PERFORMANCE ANALYSIS

Data security in cloud is one of the serious issues with cloud storage facility. Client store their data at the cloud, delete the local copy of that data and rely completely on the cloud server for data safety and maintenance. For this, auditing of the data is necessary to assure client safety of his data. To overcome this problem of data security, we introduce an AES based storage integrated. Following table shows comparison between different systems. Table 1 shows comparison between different systems.

Table 1: Comparison between different systems.

Attributes	C.Wang et al[9]	G. Ateniese[10]	A.Juels[12]	Proposed system
Privacy preserving	NO	NO	YES	YES
Unbound no. of queries	YES	YES	NO	YES
Public verifiability	YES	YES	NO	YES
Use of TPA	YES	NO	NO	YES
Recoverability	NO	NO	YES	YES
One Time Password (OTP)	NO	NO	NO	YES
Graphical password scheme	NO	NO	NO	YES

Encryption and Decryption Time

In most of the previously proposed schemes, RSA algorithm was used for storage security. AES being faster in encryption decryption and the buffer-space requirement being less as compared to RSA. we try to improve the performance by making use of AES algorithm. Figures shows graphically represent the time required for encryption and decryption respectively on different file sizes.

Table 2: Time required for encryption and decryption of different file size

File Size	Encryption time(ms)	Decryption time(ms)
5	297	**305**
10	405	389
15	512	521
20	529	558

Figure 3 : Encryption of different file size.

Figure 4: Decryption of different file size.

VI. CONCLUSION

It is clear that although the use of cloud computing has rapidly increased, cloud computing security is still considered the major issue in the cloud computing environment. Customers do not want to lose their private information as a result of malicious insiders in the cloud. In addition, the loss of service availability has caused many problems for a large number of customers recently. We have seen how the security service which is provided by trusted third party helps in securing data, it provides the facility of data verification and allows data to be shared between designated group of people. The system propose a privacy preserving public auditing system for data storage security in cloud computing. Graphical image click point password and One Time Password (OTP) achieves high level of security in authenticating the user over internet .
Many company such as Google, Hot mail, RBI use OTP for high security. Considering TPA may simultaneously handle multiple audit sessions from different users for their outsourced data files, This is further elaborate our privacy-preserving public auditing protocol into a multi user setting, where the TPA can accomplish multiple auditing tasks in a batch manner for better efficiency..

In future, this application must be simulated with real cloud and check whether it works exactly in the same way and helps the group access of data for user become secured. Third Party Auditor (TPA) notification regarding data within specific time. TPA included within the cloud with less overhead.

REFERENCES

[1] Cong Wang ,Sherman S.M. Chow ,Qian Wang ,Kui Ren and Wenjing Lou ,"Privacy Preserving Public Auditing for Secure Cloud Storage",IEEE Transactions on Computers, Vol. 62, No. 2, Feb. 2013.

[2] Yogesh Shinde ,Omprakash Tembhurne ,"A Review of Protect The Integrity of Outsourced Data using Third Party Auditing for Secure Cloud Storage ", International Journal of Science and Research (IJSR),ISSN(Online):2319-7064,Vol-3, Issue 10 , Oct.2014.

[3] Yogesh Shinde ,Alka Vishwa,"Privacy Preserving using Data Partitioning Technique for Secure Cloud Storage",International Journal of Computer Applications (0975 8887), Vol. 116 ,No. 16, Apr.2015.

[4] Yogesh Shinde , Alka Vishwa,"Public Auditing Security Scheme To Preserving Privacy For Secure Cloud Storage", Fourth Post Graduate Conference for Computer Engineering students (cPGCON) , Mar.2015.

[5] H. Takabi, J.B.D. Joshi, and G. Ahn, "Security and Privacy Challenges in Cloud Comput ing Environments ", Article in IEEE Security and Privacy, Vol. 8, No.6, Nov-Dec. 2010, pp. 24-31.

[6] Y. Deswarte, J.-J. Quisquater, and A. Saidane ,"Remote integrity checking ", In Proc. Of Conference on Integrity and Internal Control in Information Systems (IICIS),Vol. 3 , Nov. 2003.

[7] Farnaz Towhidi, Maslin Masrom ,"A Survey on Recognition-Based Graphical User Authentication Algorithms ",International Journal of Computer Science and Information Security, Vol.6, No.2, Nov. 2009.

[8] T.Schwarz and E.L. Miller, "Store, forget, and check: Using algebraic signatures to check remotely administered storage,In Proceedings of ICDCS . IEEE Computer Society, 2006.

[9] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing",IEEE Transaction Parallel and Distributed Systems, Vol. 22,No. 5, PP. 847-859, May 2011.

[10] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z.Peterson, and D. Song,"Provable Data Possession at Untrusted Stores",Proc. 14th ACM Conf. Computer and Communication Security(CCS 07), PP. 598-609, 2007.

[11] H. Shacham and B. Waters, "Compact Proofs of Retrievability",Proc. Intl Conf. Theory and Application of Cryptology and information Security: Advances in Cryptology (Asiacrypt), Vol. 5350, PP. 90-107, Dec. 2008.

[12] 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.

[13] B. Dhiyanesh "A Novel Third Party Auditability and Dynamic Based Security in Cloud Computing",International Journal of Advanced Research in Technology, Vol. 1,No. 1, PP. 29-33, ISSN: 6602 3127,2011

[14] S. Marium, Q. Nazir, A. Ahmed, S. Ahthasham and Aamir M. Mirza, "Implementation of EAP with RSA for Enhancing The Security of Cloud Computing",International Journal of Basic and Applied Science, Vol 1, No. 3, PP. 177- 183, 2012

[15] I-Hsun Chuang, Syuan-Hao Li, Kuan-Chieh Huang, Yau-Hwang Kuo, "An Effective Privacy Protection Scheme for Cloud Computing",ICACT-2011, Pages 260-265

[16] Cong Wang,Qian Wang,Kui Ren, Ning Cao , and Wenjing Lou "Toward Secure and Dependable Storage Services in Cloud Computing",IEEE Transaction On Service Computing ,Vol. 5,No.2,Apr-Jun. 2012.

