Secure Privacy Preserving in TPA Using Encryption Technique for Cloud

Reshu Tomar , Raj Kumar Singh Rathore
Dept. of computer science,
Galgotia College of engineering and technology, GreaterNoida

Abstract - Cloud Computing is the new fizz word in today's computing world. Although there is huge buzz, many people are confused on exactly what cloud computing is, particularly as the term can be used to mean almost anything. Cloud Computing has been anticipated as the next generation architecture of IT Enterprise. It moves the application software and databases to the centralized massive datacenters, wherever the management of the data and services may not be absolutely trustworthy. This unique paradigm brings about several new security challenges, that haven't been well understood. This work studies the problem of assuring the integrity of data storage in Cloud Computing. Specifically, we consider the task of authorizing a third party auditor (TPA), In place of the cloud client, to verify the integrity of the dynamic data stored within the cloud. To securely introduce an effective third party auditor (TPA), the subsequent two fundamental requisites have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the native copy of data, and bring up no additional on-line burden to the cloud user. 2) The third party auditing method should bring in no new vulnerabilities in relation to user data privacy. In this paper, we tend to utilize and uniquely combine the public key based homomorphic authenticator with random masking to achieve the privacy-preserving public cloud data auditing system, which fits all above requirements.

Keywords: Key data storage, privacy preserving, public audit ability, cloud computing, delegation, batch verification.

I. INTRODUCTION

Cloud computing is an innovative technology that's revolutionizing the manner we tend to do computing. The key concept of cloud computing is that you simply do not buy the hardware, or even the software, you need anymore, rather you rent some computational power, storage, databases, and any other resource you wish by a provider according to a pay-as-you-go design, making your contribution smaller and oriented to operations rather than to assets acquisition. However there's rather more than that, of course, and there are many various ways in which however this approach is place in action. Cloud computing is a model for enabling everywhere, well-located, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, applications, and services). Principally users will depart the upkeep of IT services to cloud service provider who is skilled in providing knowledge and also maintains the vast amount of IT resources. A bit like a double-bladed weapon, cloud computing additionally brings in several new security challenges on protecting the integrity and privacy of users' data within the cloud. to handle these issues, our work utilizes the technique of secret key primarily based symmetrical key cryptography that enables TPA to perform the auditing while not demanding the native copy of user's stored data and thus severely deduces the transmission and computation overhead as compared to the simple data auditing approaches. Thereby integrating the encryption with hashing, our protocol guarantees that the TPA couldn't learn any information concerning the information content hold on within the cloud server throughout the efficient auditing process. Cloud Computing, which provides internet primarily based service and use of computer technology.

This can be cheaper and a lot of strong processors, along with the software as a service (SaaS) computing architecture, are transforming data into data centers on big scale. The increasing network and versatile network connections make it even possible that users will now use high quality services from data and provides remote on data centers. Storing data into the cloud offers great benefit to users since they don't have to care concerning the issues of hardware problems. Whereas these internet-based on-line services do provide large amounts of storage space and customizable computing resources, this computing platform shift, however, is constraints the responsibility of native machines for data maintenance at a similar time. As a result, users are at the interest of their cloud service providers for the availability and integrity of their data the one hand; though the cloud services are far more all powerful and reliable than personal computing devices and broad vary of both internal and external threats for data integrity still exist. Examples of

outages and data loss events of remarkable cloud storage services seem from time to time. On the opposite hand, since users might not keep a local copy of outsourced data, there exist varied incentives for cloud service providers (CSP) to behave unreliably towards the cloud users concerning the status of their outsourced data. Our work is among the primary few ones during this field to consider distributed data storage security in Cloud Computing.

II. SYSTEM MODEL

Third Party Auditor (TPA)

For well organization it's very essential that cloud that enables investigation from one party audit the outsource data to assure data security and saves the user's computation and data storage[6],[7]. It's vital to provide public auditing service for cloud data storage, so the user have faith in an independent third party auditor (TPA)[8]. TPA checks the integrity of data on cloud on the behalf of users, and it provides the reasonable means for users to ascertain the validity of data in cloud[9]. Public auditing in addition to user provides the external party to verify the correctness of stored data towards external attacks it's hard to find. However these schemes, as in don't involve the privacy protection of the data. It's a main disadvantage that affect the security of the protocols in cloud computing. So users who depend on solely TPA for their security storage need their data to be protected from external auditors. I.e. Cloud service provider has vital space for storing and computation resource to maintain the users' data. It additionally has expertise in building and maintaining distributed cloud storage servers and ability to own and operate live cloud computing systems. Users who put their massive data files into cloud storage servers will relieve burden of storage and computation.

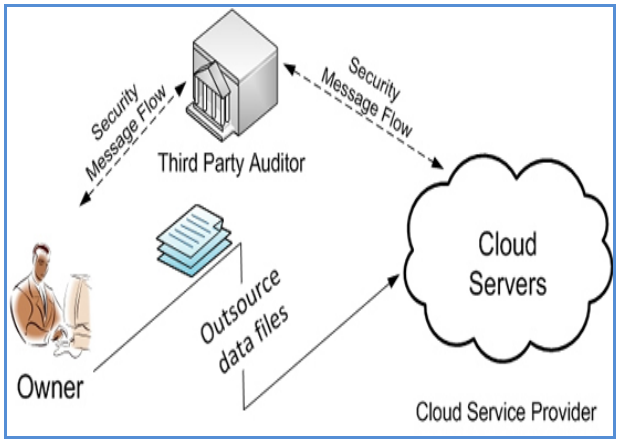

Fig. 2.1 Third Party Auditor

At the same time, it's necessary for users to ensure that their data are being stored correctly and security check. Users should be assembled with certain security means so they will make sure their data is safe. Cloud service provider always online assumed to have ample storage capability and computation power. The third party auditor is invariably on-line, too. It makes each data access be in control.

Blowfish

Blowfish is a symmetric block cipher which will be effectively used for encryption and safeguarding of data. It takes a variable-length key, from thirty two bits to 448 bits, creating it ideal for securing data. Blowfish was designed in 1993 by Bruce Schneier as a quick, free substitute to existing encryption algorithms. Blowfish is nonproprietary and license-free, and is offered free for all uses. Blowfish algorithmic rule is a Feistel Network, iterating a straightforward encryption operate sixteen times. The block size is sixty four bits, and therefore the key may be any length up to 448 bits. Though there's complicated initialize section needed before any encryption can occur, the particular encryption of data is extremely efficient on massive microprocessors. Blowfish is a variable-length key block cipher. It's appropriate for applications wherever the key doesn't modify often, sort of a communications link or an automatic file encryptor. It's considerably quicker than most encryption algorithms once enforced on 32-bit microprocessors with giant data caches.

Feistel Networks

A Feistel network is a general methodology of transforming any function (usually referred to as an F function) into a permutation. It absolutely was fabricated by crust Feistel and has been employed in several block cipher technique.

The functioning of a Feistal Network is given below:

- Split every block into halves
- Right half becomes new left half
- New right half is that the end result when the left half is XOR'd with the results of applying f to the right half and also the key.
- Note that previous rounds are often derived even though the function f isn't invertible.

III. PREVIOUS WORK

Privacy-Preserving Public Auditing for Secure Cloud Storage[1], in this paper they justify, using Cloud Storage, users can remotely store their data and use the on-demand top quality applications and services from a shared pool of configurable computing resources, without the burden of native data storage and maintenance. However, the actual fact that users now not have physical propriety of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, particularly for users with constrained computing resources. Moreover, users ought to be ready to simply use the cloud storage as if it's native, without fear of concerning the requirement to verify its integrity. Thus, enabling public auditability for cloud storage is of quite significant so users will resort to a third party auditor (TPA) to examine the integrity of outsourced data and be worry-free. To firmly introduce an efficient TPA, the auditing method should bring in no new Vulnerabilities towards user data privacy, and introduce no further on-line burden to user. in this paper, we tend to propose a secure cloud storage system supporting privacy-preserving public auditing. we tend to additional extend our result to enable the TPA to perform audits for multiple users at the same time and with efficiency. in depth security and performance analysis show the proposed schemes are demonstrably secure and extremely efficient.

Privacy-Preserving Public Auditing and data Integrity for Secure Cloud Storage[2], during this paper they justify, victimization Cloud Storage, users will remotely store their data and can use the on-demand prime quality applications and Services from a shared pool of configurable computing resources, while not the burden of native data storage and maintenance. However, the actual factor that users not have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, particularly for users with constrained computing resources. Moreover, users ought to be able to simply use the cloud storage as if it's native, without fear concerning the necessity to verify its integrity. Thus, sanctionative public auditability for cloud storage is of crucial importance so users will resort to a third party auditor (TPA) to envision the integrity of outsourced data and be worry-free. To firmly introduce an efficient TPA, the auditing method should bring in no new vulnerabilities towards user data privacy, and introduce no extra on-line burden to user. During this paper, we tend to propose a secure cloud storage system supporting privacy conserving public auditing. We tend to more extend our result to modify the TPA to perform audits for multiple users at the same time and expeditiously. in depth security and performance analysis show the planned schemes area unit incontrovertibly secure and extremely economical. Our preliminary experiment conducted on Amazon EC2 instance more demonstrates the quick performance of the planning.

Privacy-Preserving Public Auditing using TPA for Secure Cloud Storage [3][4], during this paper they justify, By victimization Cloud storage, users will access applications, services, software system whenever they needs over the net. Users will place their information remotely to cloud storage and acquire advantage of on-demand services and application from the resources. The cloud should got to guarantee information integrity and security of knowledge of user. The problem concerning cloud storage is integrity and privacy of knowledge of user will arise. to keep up to overkill this issue here, we tend to area unit giving public auditing method for cloud storage that users will create use of a third-party auditor (TPA) to examine the integrity of knowledge. Not solely verification of knowledge integrity, the planned system additionally supports information dynamics. The work that has been drained this line lacks information dynamics and true public auditability. The auditing task monitors information modifications, insertions and deletions. The planned system is capable of supporting public auditability, information dynamics and Multiple TPA area unit used for the auditing method. We tend to additionally extend our concept to ring signatures within which HARS scheme is employed. Merkle Hash Tree is used to enhance block level authentication. Additionally we tend to extend our result to enable the TPA to perform audits for multiple users at the same time through Batch auditing.

Secure Privacy conserving Public Auditing for Cloud storage [5], in this paper they justify, Cloud storage provides users to simply store their data and enjoy the great quality cloud applications needn't install in native hardware and software system. Thus advantages are clear, such a service is additionally provides users physical management of their outsourced data, that provides management over security issues towards the correctness of the storage data within the cloud. So as to try and do this new drawback and further attain secure and dependable cloud storage services. The main goal of cloud computing concept is to secure, shield the data and also the processes that come beneath the property of users. The security of cloud computing environment is an exclusive research area which needs more development from each the academic and research communities. In cloud environment the computing resources are beneath the control of service provider, the third party auditor ensures the data

integrity over out sourced data. During this paper we tend to project encryption and Proxy encryption algorithm to safeguard the privacy and integrity of outsourced data in cloud Environments.

IV. PROPOSED METHODOLOGY

To achieve privacy preserving public auditing we proposed a solution for TPA by three way handshaking by Extensible Authentication Protocol (EAP) with advanced encryption standard .The proposed system provide more secure Architecture by using light weighted APCC(Authentication protocol for cloud computing).In previous system SSL is used for this purpose. Than challenge handshake authentication protocol is used for authentication. Challenge Handshake authentication protocol is used for authentication when client request for any data or service on the cloud .We will use Verify Proof run by TPA to audit the proof from the cloud. First request sends for identity of client by Service provider authenticator. For sending or receiving data over cloud we will use blowfish for security purpose.

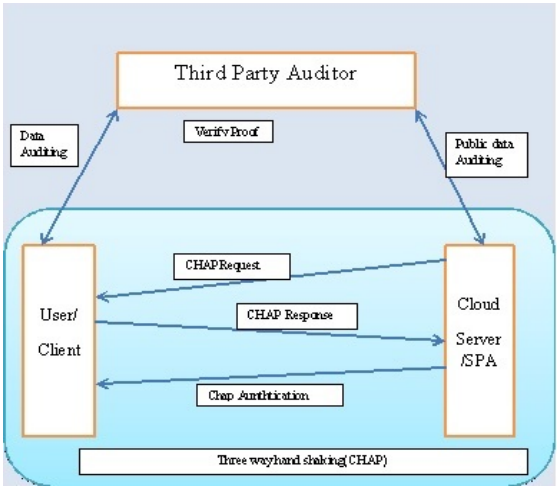

Fig. 4.1 Proposed System Model

V. IMPLEMENTATION DETAILS

File Upload:
The owner is facilitated here to securely store the data it wants to distribute for public access. The key associated with the data is then distributed across users for accessing the data

Generation of public and private keys:
This module involves the generation of security keys required to access the data. These keys after generation are distributed using a specific mechanism wherein the private key is stored at cloud server and the hash of public key stored for the TPA.

View Verification Status:
The admin is facilitated here to continuously analyze the audits performed by the TPA and get a better understanding of the security status of the documents.

TPA: The third party auditor (TPA), who has competence and capabilities that cloud users do not have and is trusted to assess the cloud storage service security on account of the user upon request. Users depends on the CS for cloud data storage and maintenance. They may also dynamically interact with the CS to access and update their stored data for various application purposes. The users may resort to TPA for assuring the storage security of their outsourced data, while hoping to keep their data private from TPA.
TPA do following:
1. View the Files
2. Verify the Files

Download File:
This module facilitates the user to get a view of all data on the server verified by the TPA and thus, facilitates User access to the cloud data.

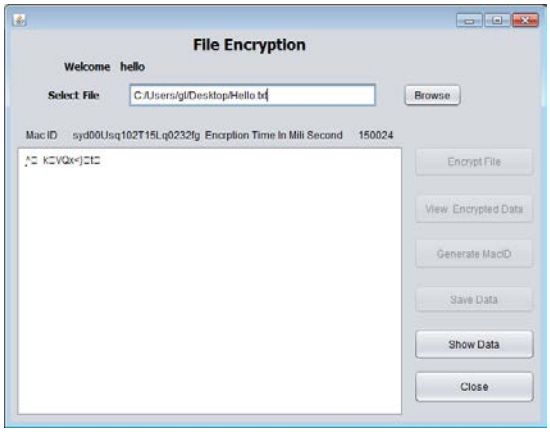

Fig. 5.1 Data Encrypt

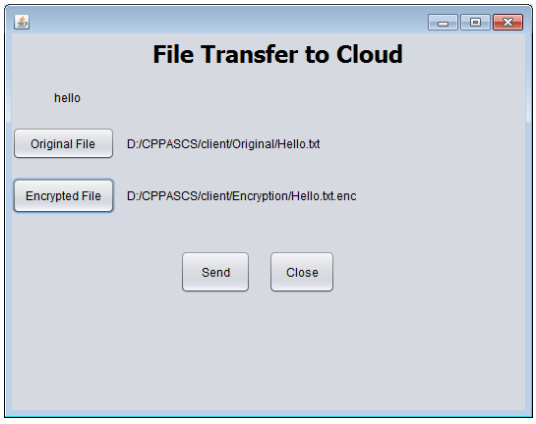

Fig. 5.2 Data Transfer

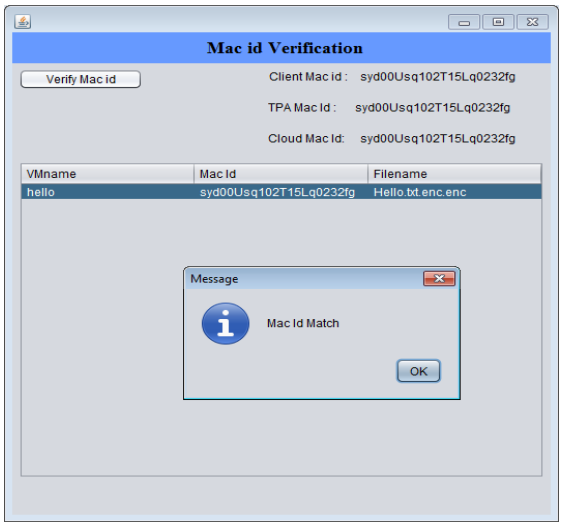

Fig. 5.3 Checking Mac Id

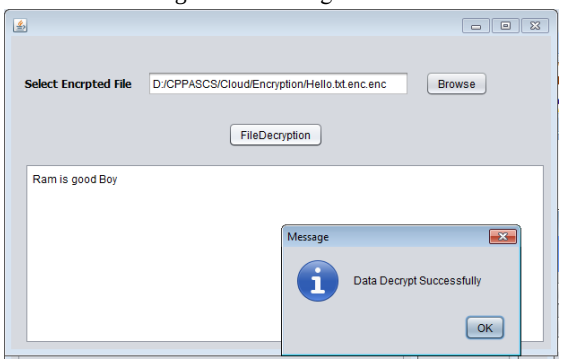

Fig. 5.4 Data Decrypt

V. CONCLUSION

In this paper, we have analyzed data storage correctness issue in reference of cloud computing. We have provided the mechanism for trusted and secure data storage model with new scheme with integrity verification. The features of algorithm are useful to reduce computational cost for the client who may not have much security processing power. Using TPA we can audit the data on the server, and can preserve the privacy in data communication. The data owners have an assurity of validity of data due to the implementation of the Audit Mechanism. Thus we can secure our data on the cloud servers using this Mechanism.

REFERENCES

[1] Bilal Ahmed, Pushpalatha M.N, "A Novel Privacy Preserving Public Auditing For Secure Cloud Storage", 10th IRF International Conference, 04th October-2014, Bengaluru, India, ISBN: 978-93-84209-56-8.

[2] Imran Ahmad, Prof.Hitesh Gupta, "Privacy-Preserving Public Auditing & Data Intrgrity for Secure Cloud Storage", International Conference on Cloud, Big Data and Trust 2013, Nov 13-15,

[3] Jyoti R Bolannavar, "Privacy-Preserving Public Auditing using TPA for Secure Cloud Storage", International Journal of Scientific Engineering and Research (IJSER) ISSN (Online): 2347-3878 Volume 2 Issue 6, June 2014.

[4]. Salve Bhagyashri, Prof. Y.B.Gurav, "Privacy-Preserving Public Auditing For Secure Cloud Storage", IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 16, Issue 4, Ver. III (Jul – Aug. 2014), PP 33-38

[5] Sathiskumar R, Dr.Jeberson Retnaraj, "Secure Privacy Preserving Public Auditing for Cloud storage", International Journal of Innovative Research in Science, Engineering and Technology, Volume 3, 1st January 2014, International Conference on Engineering Technology and Science-(ICETS'14) On 10th & 11th February.

[6] 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, 2009.

[7] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote Data Checking for Network Coding-Based Distributed Storage Systems," Proc. ACM Workshop Cloud Computing Security Workshop(CCSW'10), pp. 31-42, 2010.

[8] Q. Wang, C. Wang, J. Li, K. Ren, and W. Lou, "Enabling Public Verifiability and Data Dynamic for Storage Security in Cloud Computing," Proc. 14th European Conf. Research in Computer Security(ESORICS'09), pp. 355-370, 2009.

[9] Farzad Sabahi,"Cloud Computing Security Threats and Responses" ,IEEE confer. 2011, 978-1-61284-486-2/111