Privacy Preserving in TPA using Secured Encryption Technique for Secure Cloud

Reshu Tomar
Dept. of computer science,
Galgotia College of engineering and technology,
GreaterNoida

Rajkumar Singh Rathore
Assistant Professor
Dept. of computer science and information technology,
Galgotia College of engineering and technology,
Greater Noida

ABSTRACT
Cloud computing is a model for enabling everywhere, well-located, on-demand network access to a shared pool of compo sable computing resources (e.g., servers, networks, applications, and services). Mainly users can digress the support and maintenance of IT services to cloud service providers which is expert in providing knowledge and also maintains the vast amount of IT resources. Just like a double-bladed sword, cloud computing also brings in many new security challenges to ensure the protection of confidentiality and to preserve the integrity of users data in the cloud. To resolve these problems, this work uses the technique of secret key based symmetric key cryptography which enables TPA to perform the auditing task without demanding the local copy of user's stored data and thus severely reduces the computation and transmission overhead as compare to simple, straightforward data auditing approaches. Thereby integrating the encryption with hashing, this work guarantees that the TPA could not learn any knowledge about the data content that is store in the cloud server during the auditing process.

Keywords
Cloud computing, Cloud ,TPA ,Cryptography

1. INTRODUCTION
In recent times, the Cloud Computing is gaining much more courtesy, from both industrial and academic community. Cloud Computing, that provides Internet based service and use of computer technology. This is cheaper and more stronger processors, along with the software as a service (SaaS) computing architecture, are transforming data into data centers on large scale. The continuously increasing network and flexible network connections make it even possible that users now a days can use high quality services from data and provides remote on data centers. Storing data into the cloud offers great advantage to users since they don't have to worry about the hardware problems. While these internet-based online services provides users huge amounts of storage space and customizable computing resources, this computing platform shift, however, avoids the task of local machines for data maintenance at the same time. It is routine for users to leverage cloud storage services to share data with others in a group, as data sharing becomes a standard feature in most cloud storage offerings, including Dropbox, iCloud and Google Drive [2].

As a result, users are at the concern of their cloud service providers for the availability, confidentiality and integrity of their data the one hand; although the cloud services are much more reliable and powerful than personal computing devices and broad range of both internal and external threats for data integrity, privacy still exist. Examples of disruption and data loss incidents of noteworthy cloud storage services appear many times. On the other hand, since users may not keep a local copy of outsourced data, there exist various inducement for cloud service providers (CSP) to behave unfaithfully towards the cloud users concerning the status of their outsourced data. This work is among the first few ones in this field to consider distributed data storage security in Cloud Computing.

Third Party Auditor (TPA)

For well organization it is very essential that cloud that allows inquiry from a single party audit the outsource data to ensure data security and save the user's computation and data storage. It is very essential to provide public auditing service for cloud data storage, so that the user trusts an independent third party auditor (TPA)[11],[12]. Recently, many mechanisms [7]-[12], have been proposed to permit not solely a data owner itself but also a public verifier to efficiently perform integrity checking without downloading the entire data from the cloud, which is referred to as public auditing [5]. TPA checks the integrity of data on cloud on the part of users, and it provides the reasonable way for users to check the validity of data in cloud. Public auditing simultaneously to user provides the external party to verify the correctness of stored data against external attacks it's hard to seek out. However these schemes, as in [1] don't involve the privacy protection of the data. It is a main drawback which affect the security of the protocols in cloud computing. So users who rely on only TPA for their secure storage want their data to be protected from external auditors. I.e. Cloud service provider has considerable storage space and computation resource to maintain the users data. It also has expertise in building distributed cloud storage servers and ability to manage, own and operate live cloud computing systems. Users who send their large data files into cloud storage servers can relieve burden of storage and computation. At the same time, it is necessary for users to confirm that their data are being stored correctly and security check. Users should be equipped with some security means so that they can make sure their data is safe. Cloud service provider always online and presupposed to have abundant storage capacity and computation power. The third party auditor is always online, too. It makes every data access be in control.

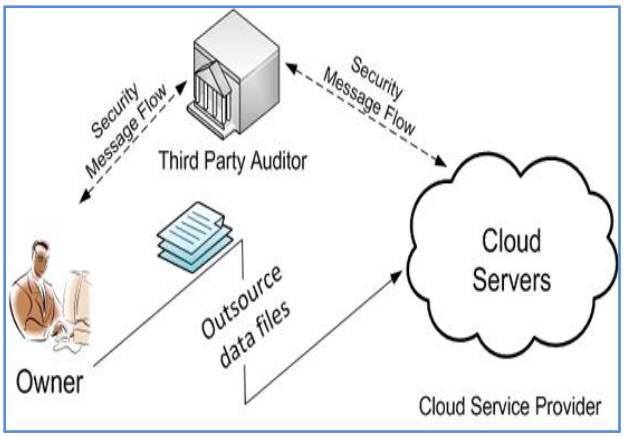

Figure1: Third Party Auditor

2. PROBLEM DEFINITION

2.1 The System and Threat Model

Security in cloud has become the foremost on demand issue to be addressed in cloud computing atmosphere.

Because of cloud, user become free from totally different data management task, as this data management is done by the third party ingenious auditor (TPA). However still there are certain security issues of this third party auditor as throughout this audit TPA can get access to the data within the cloud.

Cloud services is additionally provides users physical management of their outsourced data, that provides control over security issues towards the correctness of the storage data within the cloud

The integrity of data in cloud storage, however, is subject to skepticism and scrutiny, as data stored within the cloud can easily be lost or corrupted because of the inevitable hardware/software failures and human errors [3], [4].

To make this matter even worse, cloud service providers is also reluctant to tell users regarding these data errors so as to maintain the name of their services and avoid losing profits [5]. Therefore, the integrity of cloud data ought to be verified before any data utilization, like search or computation over cloud data [6]. Since users might not keep a local copy of outsourced data, there exist numerous incentives for cloud service providers (CSP) to behave unreliably towards the cloud users regarding the stature of their outsourced data[10].

3. PROPOSED WORK TECHNOLGY

To achieve privacy preserving public auditing we proposed a standard solution for TPA by three way handshaking by Extensible Authentication Protocol (EAP) with advanced encryption .The proposed system provide more secure Architecture by using light weighted APCC(Authentication protocol for cloud computing).In precedent system SSL is employed 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 VerifyProof 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.

Step1: When Client request for any service to Cloud, SPA send a CHAP message to client

Step2: Client sends CHAP response to SPA and calculates its weight

Step3: Now SPA check the response value with its own calculated value .If both value are matched then SPA sends CHAP success message to the client .Implementation if these algorithm provide effective authentication to client in cloud.

Step4: For public auditing we will use four algorithm (KeyGen,SignGen,GenProof, VerifyProof)

- KeyGen: Key generation algorithm run by the user
- SignGen: used by user to generate verification
- GenProof: Run by the cloud Server to generate a proof of data storage correctness
- VerifyProof : Third party auditor runs Algorithm to audit the proof from the cloud server

Step5: Encryption of data is done by using blowfish Encryption and send or receive on cloud.

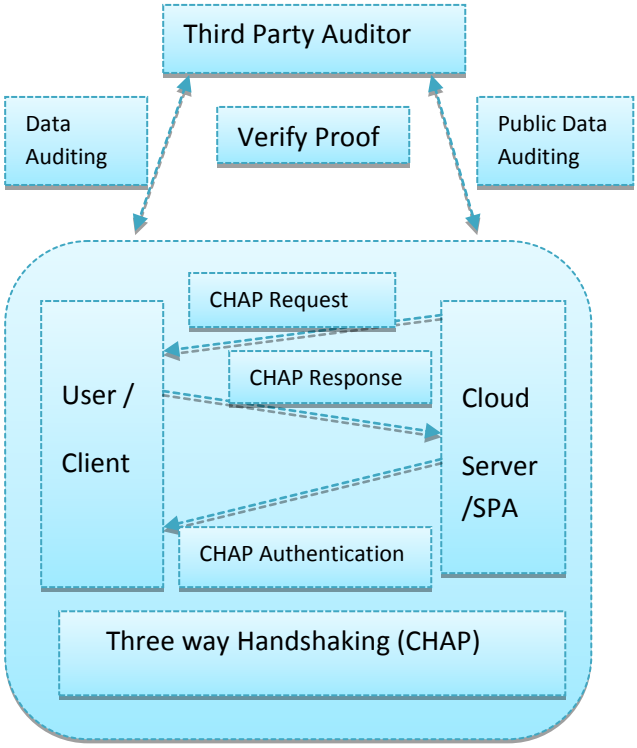

Figure2: Proposed System Architecture

3.1 Blowfish

Blowfish is a bilaterally symmetric block cipher that may be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, creating it ideal for securing knowledge. Blowfish was designed in 1993 by Bruce Schneier as a quick, free alternative to existing cryptography algorithms. Blowfish is generic and license-free, and is obtainable free for all uses. Blowfish algorithm is a Feistel Network, iterating an easy encryption operate sixteen times. The block size is sixty four bits, and also the key is any length up to 448 bits. though there's a complex initialisation part needed before any encoding will occur, the particular encryption of information is extremely efficient on massive microprocessors. Blowfish is a variable-length key block cipher. It's appropriate for applications wherever the key does

not modification usually, sort of a communications link or an automatic file encryptor. It is considerably quicker than most encryption algorithms. once enforced on 32-bit microprocessors with massive data caches.

Table 1:Comparison of various Encryption Algorithms

Algorithm	Block Size (Bits)	Key Size (Bits)	Speed	Security
DES	64	56	LOW	LESS
3 DES	128	112, 168	LOW	LESS
RC2	64	8-128	FAST	HIGH
RC6	128	128-192	FAST	SECURE
AES	64	128,192, 256	FAST	MORE SECURE
BLOWFISH	64	32-448	FAST	MORE SECURE

3.2 Description Of The Algorithm

Blowfish is a variable-length key, sixty four bit block cipher. The algorithmic rule consists of 2 half: a key-expansion half and a data- encryption half. Key expansion converts a key of at the most 448 bits into many sub key arrays totaling 4168 bytes. Encoding happens via a sixteen rounds of Feistel network. Every round consists of a key dependent permutation, and also a key- and data-dependent substitution. All operations are XOR and addition operations on 32-bit words. The only extra operations are 4 indexed array information lookups per round.

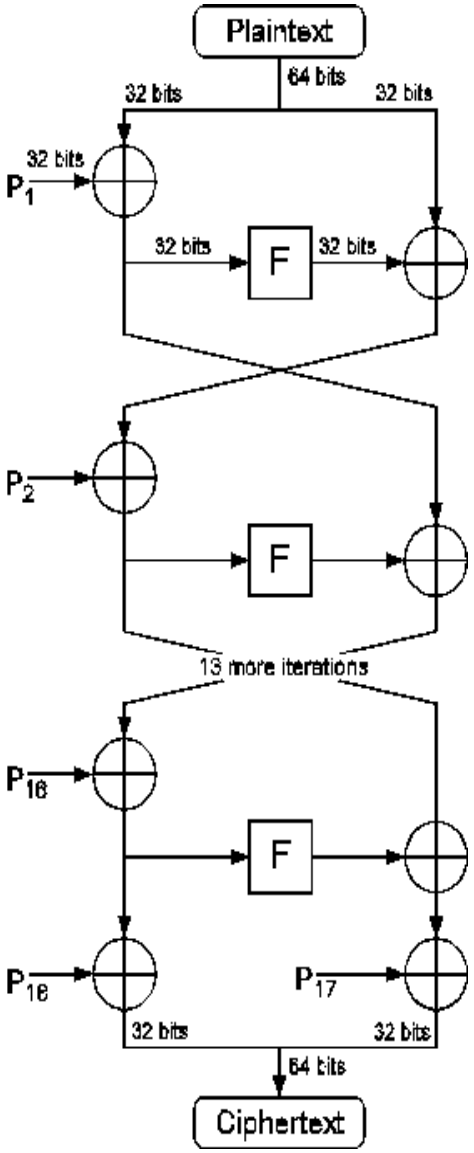

Figure 3: Description of Algorithm

3.3 Feistel Networks

A Feistel network is a traditional method of translating any function (usually called an Ffunction) into a permutation. This was invented by Horst Feistel and it have been used in many block cipher designs. The working of a Feistal Network is explained below:

- First of all, split each block into halves
- Now, right half becomes new left half
- New right half is the final result as the left half is XOR'd with the result of applying f to the right half and the key.
- Also note that previous rounds can be derived even if the function f is not invariable.

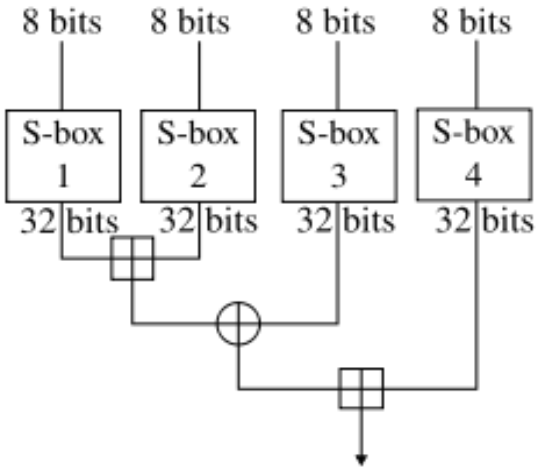

Figure 4: The Feistel structure of Blowfish

4. CONCLUSION

In this paper, we introduce a privacy-preserving public auditing system for data storage security in Cloud Computing, wherever TPA will perform the storage auditing without demanding the local copy of data .we tend to utilize the homomorphic linear authenticator and also random masking to ensure that the TPA wouldn't learn any knowledge regarding the data content keep on the cloud server throughout the efficient auditing method, that not solely eliminates the burden of cloud user from the tedious and probably expensive auditing task ,but additionally alleviates the users' concern of their outsourced data leakage. Cloud data security is a very important facet for the client while using cloud services. Third Party Auditor are often accustomed make sure the security and integrity of data. Third party auditor are often a trustworthy third party to resolve the conflicts between the cloud service provider and also the client. Numerous schemes are proposed by authors over the years to provide a trustworthy atmosphere for cloud services. Encryption and decryption algorithms are used to offer the protection to user via using third party auditor. This paper provides an encryption algorithm named Blowfish for cloud data security using third party auditor. Most of the authors have projected schemes that rely on encrypting the data using some encryption algorithmic rule and create third party auditor store a message digest or encrypted copy of a similar data that's keep with the service provider. The third party is employed to resolve any kind of conflicts between service provider and client. Wide range security and performance analysis shows that the projected schemes are demonstrably secure and extremely efficient. we believe that advantages of the proposed schemes can shed light on economies of scale for Cloud Computing.

5. REFERENCES

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

[2] Boyang Wang,"Oruta: Privacy-Preserving Public Auditing for Shared Data in the Cloud" IEEE Transactions on Cloud Computing, Vol. 2, no. 1, Jan-March 2014.

[3] K. Ren, C. Wang, and Q. Wang, "Security Challenges for the Public Cloud," IEEE Internet Computing, vol. 16, no.1 pp. 69-73, 2012.

[4] D. Song, E. Shi, I. Fischer, and U. Shankar, "Cloud Data Protection for the Masses," Computer, vol. 45, no. 1, pp. 39-45, 2012.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Data Storage Security in Cloud Computing," Proc. IEEE INFOCOM, pp. 525-533, 2010.

[6] B. Wang, M. Li, S.S. Chow, and H. Li, "Computing Encrypted Cloud Data Efficiently under Multiple Keys," Proc. IEEE Conf.Comm. and Network Security (CNS'13), pp. 90-99, 2013.

[7] 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 Comm.Security (CCS '07), pp. 598-610, 2007.

[8] H. Shacham and B. Waters, "Compact Proofs of Retrievability,"Proc. 14th Int'l Conf. Theory and Application of Cryptology and Information Security: Advances in Cryptology (ASIACRYPT '08), pp. 90-107, 2008.

[9] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," Proc. 16th ACM Conf. Computer and Comm. Security (CCS'09), pp. 213-222, 2009.

[10] 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.

[11] 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.

[12] 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.