Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 6, June 2016, pg.545 – 551

Privacy Preserving in TPA Using Secured Encryption Technique for Secure Cloud

Jyotshana, Vinod Saroha
vermajyoti13993@gmail.com
Department of Computer Science and Engineering BPSMV Khanpur Kalan, Sonepat Haryana 131001

Abstract: - Cloud Computing is the new buzz word in today's computing world. Although there is huge buzz, many people are confused as to exactly what cloud computing is, especially as the term can be used to mean almost anything. Cloud Computing has been envisioned as the next generation architecture of IT Enterprise. It moves the application software and databases to the centralized large datacenters, where the management of the data and services may not be fully trustworthy. This unique paradigm brings about many new security challenges, which have not been well understood. This work studies the problem of ensuring the integrity of data storage in Cloud Computing. In particular, we consider the task of allowing a third party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. To securely introduce an effective third party auditor (TPA), the following two fundamental requirements have to be met: 1) TPA should be able to efficiently audit the cloud data storage without demanding the local copy of data, and introduce no additional on-line burden to the cloud user; 2) he third party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper, we utilize and uniquely combine the Blowfish Algorithm to encryption and safeguarding of data with Feistel Networks to achieve the privacy-preserving public cloud data auditing system, which meets all above requirements.

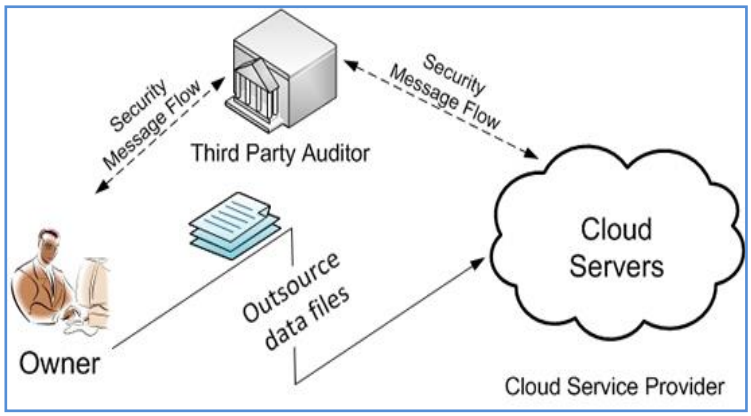
I. Introduction

Cloud computing is an innovative technology that is revolutionizing the way we do computing. The key concept of cloud computing is that you don't buy the hardware, or even the software, you need anymore, rather you rent some computational power, storage, databases, and any other resource you need by a provider according to a pay-as-you-go model, making your investment smaller and oriented to operations rather than to assets acquisition. But there is much more than that, of course, and there are many different ways how this approach can be put 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). Mainly users can depart the maintenance of IT services to cloud service provider who 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 on protecting the integrity and privacy of users' data in the cloud. To address these problems, our work utilizes the technique of secret key based symmetric key cryptography which enables TPA to perform the auditing without demanding the local copy of user's stored data and thus severely deduces the transmission and computation overhead as compared to the straightforward data auditing approaches. Thereby integrating the encryption with hashing, our protocol guarantees that the TPA could not learn any knowledge about the data content stored in the cloud server during the efficient auditing process. Cloud Computing, which provides Internet based service and use of computer technology. This is cheaper and more strong processors, together with the software as a service (SaaS) computing architecture, are transforming data into data centers on huge scale. The increasing network and flexible network connections make it even possible that users can now use high quality services from data and provides remote on data centers. Storing data into the cloud offers great help to users since they don't have to care about the problems of hardware problems. While these internet-based online services do provide huge amounts of storage space and customizable computing resources, this computing platform shift, however, is avoids the responsibility of local machines for data maintenance at the same 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; although the cloud services are much more powerful and reliable than personal computing devices and broad range of both internal and external threats for data integrity still exist. Examples of outages and data loss incidents of noteworthy cloud storage services appear from time to time. On the other hand, since users may not keep a local copy of outsourced data, there exist various incentives for cloud service providers (CSP) to behave unfaithfully towards the cloud users regarding the status of their outsourced data. Our 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 investigation from a single party audit the outsource data to ensure data security and save the user's computation and data storage. It is very important to provide public auditing service for cloud data storage, so that the user trusts an independent third party auditor (TPA). TPA checks the integrity of data on cloud on the behalf of users, and it provides the reasonable way for users to check the validity of data in cloud. Public auditing in addition to user provides the external party to verify the correctness of stored data against external attacks it's hard to find. However these schemes, as in don't involve the privacy protection of the data. It is a main disadvantage which affect the security of the protocols in cloud computing. So users who depend on only TPA for their security storage want their data to be protected from external auditors. I.e. Cloud service provider has significant storage space and computation resource to maintain the users' data. It also has expertise in building and managing distributed cloud storage servers and ability to own and operate live cloud computing systems. Users who put their large data files into cloud storage servers can relieve burden of storage and computation. At the same time, it is important for users to ensure that their data are being stored correctly and security check. Users should be equipped with certain security means so that they can make sure their data is safe. Cloud service provider always online & assumed to have abundant storage capacity and computation power. The third party auditor is invariably online, too. It makes every data access be in control.



Blowfish

Blowfish is a symmetric block cipher that can be effectively used for encryption and safeguarding of data. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for securing data. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Blowfish is unpatented and license-free, and is available free for all uses. Blowfish Algorithm is a Feistel Network, iterating a simple encryption function 16 times. The block size is 64 bits, and the key can be any length up to 448 bits. Although there is a complex initialization phase required before any encryption can take place, the actual encryption of data is very efficient on large microprocessors. Blowfish is a variable-length key block cipher. It is suitable for applications where the key does not change often, like a communications link or an automatic file encryptor. It is significantly faster than most encryption algorithms when implemented on 32-bit microprocessors with large data caches.

Feistel Networks

A Feistel network is a general method of transforming any function (usually called an F function) into a permutation. It was invented by Horst Feistel and has been used in many block cipher designs. The working of a Feistal Network is given below:

- Split each block into halves
- Right half becomes new left half
- New right half is the final result when the left half is XOR'd with the result of applying f to the right half and the key.
- Note that previous rounds can be derived even if the function f is not invertible.

II. RELATED WORK

Privacy-Preserving Public Auditing for Secure Cloud Storage, In this paper they explain, Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third party auditor

(TPA) to check the integrity of outsourced data and be worry-free. To securely introduce an effective TPA, the auditing process should bring in no new Vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy-preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient.

Privacy-Preserving Public Auditing & Data Intrgrity for Secure Cloud Storage, In this paper they explain, Using Cloud Storage, users can remotely store their data and enjoy the on-demand high quality applications and Services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. However, the fact that users no longer have physical possession of the outsourced data makes the data integrity protection in Cloud Computing a formidable task, especially for users with constrained computing resources. Moreover, users should be able to just use the cloud storage as if it is local, without worrying about the need to verify its integrity. Thus, enabling public auditability for cloud storage is of critical importance so that users can resort to a third party auditor (TPA) to check the integrity of outsourced data and be worry-free. To securely introduce an effective TPA, the auditing process should bring in no new vulnerabilities towards user data privacy, and introduce no additional online burden to user. In this paper, we propose a secure cloud storage system supporting privacy preserving public auditing. We further extend our result to enable the TPA to perform audits for multiple users simultaneously and efficiently. Extensive security and performance analysis show the proposed schemes are provably secure and highly efficient. Our preliminary experiment conducted on Amazon EC2 instance further demonstrates the fast performance of the design.

Privacy-Preserving Public Auditing using TPA for Secure Cloud Storage, In this paper they explain, By using Cloud storage, users can access applications, services, software whenever they requires over the internet. Users can put their data remotely to cloud storage and get benefit of on-demand services and application from the resources. The cloud must have to ensure data integrity and security of data of user. The issue about cloud storage is integrity and privacy of data of user can arise. To maintain to overkill this issue here, we are giving public auditing process for cloud storage that users can make use of a third-party auditor (TPA) to check the integrity of data. Not only verification of data integrity, the proposed system also supports data dynamics. The work that has been done in this line lacks data dynamics and true public auditability. The auditing task monitors data modifications, insertions and deletions. The proposed system is capable of supporting public auditability, data dynamics and Multiple TPA are used for the auditing process. We also extend our concept to ring signatures in which HARS scheme is used. Merkle Hash Tree is used to improve block level authentication. Further we extend our result to enable the TPA to perform audits for multiple users simultaneously through Batch auditing.

Secure Privacy Preserving Public Auditing for Cloud storage, In this paper they explain, Cloud storage provides users to easily store their data and enjoy the good quality cloud applications need not install in local hardware and software system. So benefits are clear, such a service is also gives users' physical control of their outsourced data, which provides control over security problems towards the correctness of the storage data in the cloud. In order to do this new problem and further achieve secure and dependable cloud storage services. The main goal of cloud computing concept is to secure, protect the data and the processes which come under the property of users. The security of cloud computing environment is an exclusive research area which requires further development from both the academic and research communities

III. PROPSED METHODLOLGY

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.

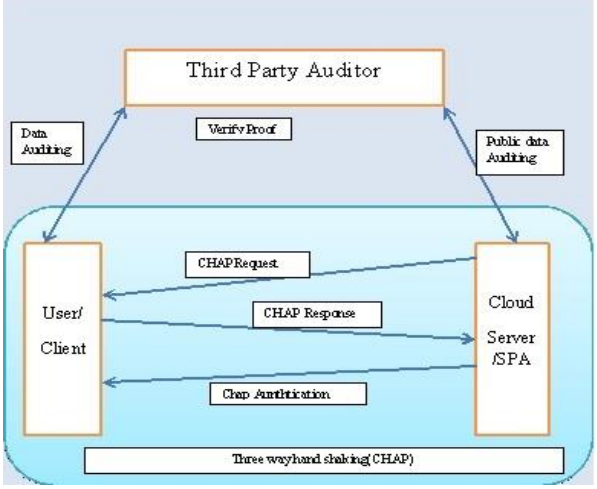


Figure: Proposed System Architecture

IV. 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 expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service security on behalf of the user upon request. Users rely 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 ensuring 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.

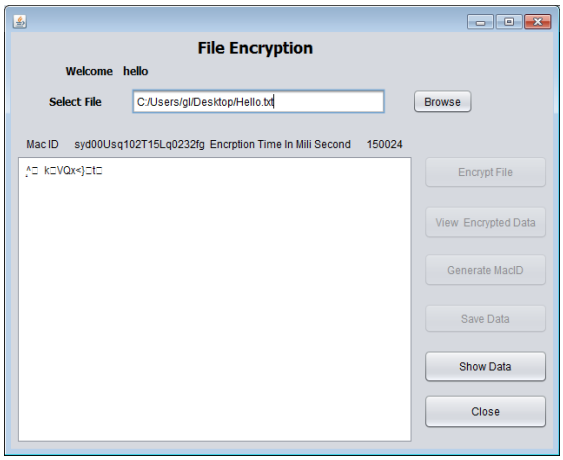


Fig 1: Data Encrypt

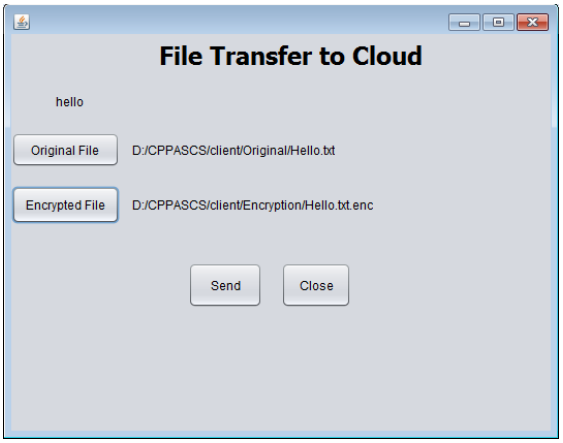


Fig 2: Data Transfer

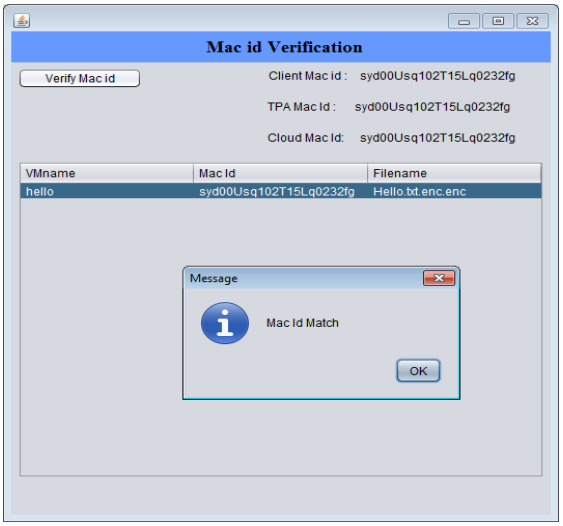


Fig 3: Checking MAC Id

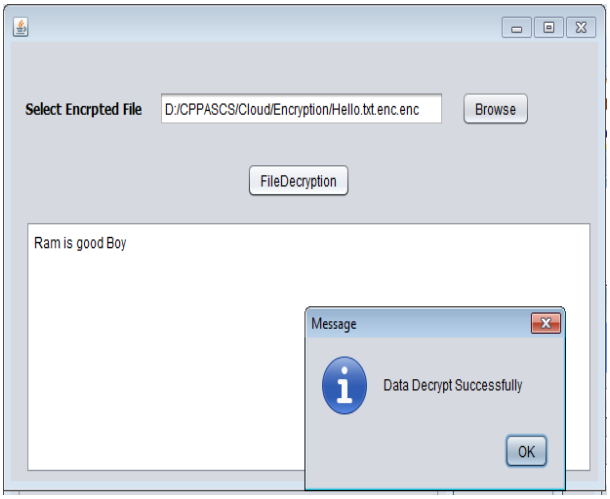


Fig 4: Data Decrypt

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.

