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: 6.017

IJCSMC, Vol. 6, Issue. 10, October 2017, pg.83 – 89

A Review on Privacy Preserving in TPA Using Secured Encryption Technique for Secure Cloud

Sneha Khemani, Payal Awwal

Govt. Women's Engineering College, Ajmer
Email: - sneha199060@gmail.com, payalawwal@gweca.ac.in

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 data canters, 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) the third party auditing process should bring in no new vulnerabilities towards user data privacy. In this paper, we use and interestingly join the Blowfish Algorithm to encryption and shielding of information to accomplish the privacy preserving open cloud information reviewing framework, which meets every single above necessity.

Keywords: Cloud Computing, Public Auditing, Privacy Preserving, data storage, TPA, Security.

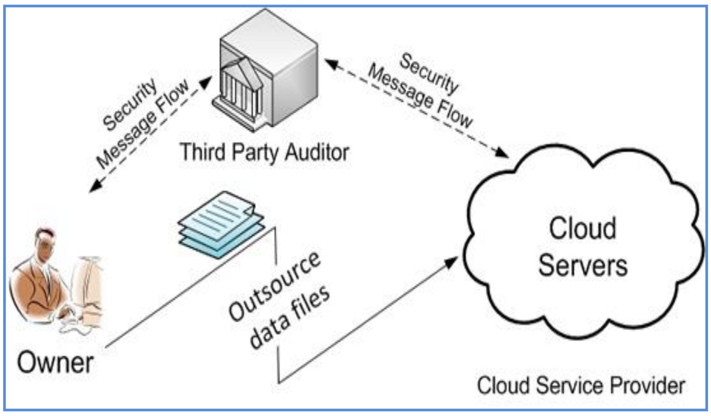
INTRODUCTION

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. In this manner coordinating the encryption with hashing, our convention ensures that the TPA couldn't take in any learning about the information content put away in the cloud server amid the productive reviewing process. Distributed computing, which gives Internet based administration and utilization of PC innovation. 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. While these internet-based online services do provide huge amounts of storage space and customizable computing resources, this computing platform shift, however 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 clients who rely upon TPA for their security stockpiling need their information to be shielded from outside evaluators. Cloud specialist organization has huge storage room and calculation asset to keep up the clients' information. It likewise has aptitude in building and overseeing disseminated distributed storage servers and capacity to possess and work live distributed computing frameworks. Clients who put their substantial information documents into distributed storage servers can assuage weight of capacity and calculation. In the meantime, it is critical for clients to guarantee that their information are being put away effectively and security check.

Clients ought to be outfitted with certain security implies so they can ensure their information is sheltered. Cloud service provider is 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.



RELATED WORK

Privacy-Preserving Public Auditing for Secure Cloud Storage [01], 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, they propose a secure cloud storage system supporting privacy-preserving public auditing. They 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.

The framework for privacy-preserving public auditing system maintains the data integrity. Public auditing schemes consist of four algorithms. KeyGen, SigGen, GenProof, VerifyProof. In KeyGen the Key is generated called as Key generation algorithm, which is run by the user to set up scheme. In SigGen verification metadata is generated by the user which consists of digital signature. GenProof is run by the cloud server to generate a proof of data storage. VerifyProof algorithm is run by TPA to audit and verify the proof.

Privacy-Preserving Public Auditing using TPA for Secure Cloud Storage [02], 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, they 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. They also extend our concept to ring signatures in which HARS scheme is used. Merkle Hash Tree is used to improve block level authentication. Further they extend our result to enable the TPA to perform audits for multiple users simultaneously through Batch auditing.

This paper used HARS contains three algorithms: KeyGen, RingSign and RingVerify. In KeyGen, each user in the group generates her public key and private key. In RingSign, a user in the group is able to sign a block with her private key and all the group members' public keys. A verifier is allowed to check whether a given block is signed by a group member in RingVerify.

Secure Privacy Preserving Public Auditing for Cloud storage [03], 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. In cloud environment the computing resources are under the control of service provider, the third party auditor ensures the data integrity over out sourced data. In this paper they proposed Encryption and Proxy encryption algorithm to protect the privacy and integrity of outsourced data in cloud Environments.

Balkrishnan. S, Saranya. G, Shobana. S and Karthikeyan. S [4] enhanced the scheme with explicit and efficient dynamic data operations for data storage security in Cloud Computing. Therefore, it is crucial to consider the dynamic case, where a user may wish to perform various block-level operations of update, delete and append to modify the data file while maintaining the storage correctness assurance. The straightforward and trivial way to support these operations is for user to download all the data from the cloud servers and re-compute the whole parity blocks as well as verification tokens.

This paper used public key based homomorphic linear authentication (HLA) protocol with random masking to achieve privacy preserving data security.

Sathiskumar R, Dr.Jeberson Retnaraj [5] clarified general society review capacity is a primary downside of distributed computing innovation. In this paper secure open examining plan for distributed storage give greater security thought about past innovation. In this paper open Auditing framework and talk about two direct plans and their bad marks. At that point they exhibit our principle result for protection saving Public examining to accomplish the before said plan Goals. At long last, they demonstrate to degree our fundamental plan to clump examining and encryption calculations. The bunch Auditing used to review the gathering of points of interest. The proposed issue is multi compose and issue of TPA if Third-party-examiner utilizes information as well as change the information than how information proprietor or client will think about this issue.

In this paper a public auditing scheme consists of four algorithms (KeyGen, SigGen, GenProof, VerifyProof) used. KeyGen is a key generation algorithm that is run by the user to setup the scheme. SigGen is used by the user to generate verification signatures. GenProof is run by the cloud server to generate a proof of data storage correctness, while VerifyProof is run by the TPA to audit the proof from the cloud server.

T. Prasanthi, C. Balasubramanian, [6] described to ensure the integrity of dynamic data stored in the cloud, external Third Party Auditor (TPA) is acquainted in a cloud infrastructure. For enabling public auditing in cloud data storage security, users can resort to an external auditor to check integrity of an outsourced data. The third party auditor (TPA) should met the following fundamental requirements: 1) TPA should be able to efficiently audit the cloud data without revealing the original data, and it should not add burden to the cloud user; 2) Auditing process should not bring no new vulnerabilities towards the user data. 3) Integrity of the data is protected against TPA by invoking some cryptographic techniques to ensure the storage correctness in cloud. In particular, this scheme achieves batch auditing where multiple delegated auditing tasks from different users, can be performed by the TPA and further enables TPA to perform data dynamics operations. Thus, the performance analysis depicts that the proposed schemes are more sheltered and highly competent.

This paper used the DES algorithm to encrypt the data to ensure that the file will not be intercepted by an unauthorized person to get the file Content.

Sadia Marium [7] they research on Cloud computing is fast growing technology used by modern world but needs to be covered some open area which is affecting its robust features. In their survey they come to this point that users have very serious concerns about its open nature of privacy and security. As well as they analysis the cloud nature and list out some categories of threats that needs to be address. Security depends upon the way Cloud service provider allows its client to come and get registered with his cloud network. EAP-CHAP and RSA are best solution to provide to any type of Cloud customer. Moreover, they will use low as compared to previous one. Their research is mainly focus on service provider's side security. They must protect their client data by unauthorized access, modification or miss use, denial of services and repudiation. To ensure the security of client data in cloud, they purpose the implementation of Extensible Authentication Protocol through three way hand shake with RSA.

Prakash Kuppuswamy, Saeed Q Y Al-Khalid [8] paper highlighted how important it is to ensure that information within the Cloud environment is to be secure. They have discussed need of securing Cloud storage systems, basic security requirements of a Cloud computing, some of the possible attacks on the Cloud Storage systems and counter measures to deal with these attacks. The future scope of our work is to both protect the active attacks and passive attacks by designing and implementing new strategy plan of cloud architecture. Proposed paper produce many key findings such as cloud infrastructure equipment failure, backup and retention procedures, type of security and monitoring, Service Level Agreements infrastructure and applications, security breach, preventing data, virtualization application etc.

IMPORTANT ALGORITHM

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 Feistel 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.

RESULT ANALYSIS

The computation time of TPA when 100 blocks are checked Times in seconds

File name	size	Number of blocks	Mediator computation time in seconds	TPA computation time in seconds
data.txt	513.4 KB	125	0.32	0.30
1.txt	1.7 MB	415	0.53	0.49
3.txt	4.8 MB	1181	1.05	0.96
5.txt	6.3 MB	1536	1.27	1.15
6.txt	7.1 MB	1725	1.39	1.27

FUTURE SCOPE

Future work is wanted to give more elevated amount of security using different Authentication convention and secure mechanisms over scrambled information for cloud computing in cloud administrations. We additionally expand our security saving open evaluating convention into a multi-client setting, where TPA can play out the different inspecting errands in a bunch way, i.e., at the same time.

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, and ISBN: 978-93-84209-56-8.

[2]. 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.

[3]. 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

[4]. 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 January2014, International Conference on Engineering Technology and Science-(ICETS’14) On 10th & 11th February.