International Journal of Engineering Research and General Science Volume 3, Issue 1, January-February, 2015
ISSN 2091-2730

Review on: Privacy Preserving and Verification of Integrity Threat by TPA of Shared Data in Cloud

Yogesh Lubal,[1] Megha Borole[2]

P.G Scholar, Computer Engineering Department, JSPMNTC RSSOER,Savitribai Phule Pune University [1].

Assistant Professor, Computer Engineering Department,JSPMNTC RSSOER,Savitribai Phule Pune University [2]

yogeshlubal@gmail.com[1]
megha.borole@gmail.com[2]

Abstract: The Cloud computing is a recent technology which provides various services through internet. The Cloud server allows user to store their data remotely on a cloud storage and enjoy on-demand services and application from the configurable resources.without worrying about correctness & integrity of data From anywhere at any time. In cloud computing, data owners host their data on cloud servers and users access that data from cloud server. Due to outsourcing of data on cloud many security challenges occurs. The auditing protocol must be required to check the data integrity in the cloud. Cloud also provides efficient solution for sharing resources among the group. In a group, every member is able to host their data and access data stored by another group member. Owner of data is able to add new users in the group. Identity of user preserved from third party auditor. There are many internal and external threats, which affect on cloud data storage. Every time it is not possible for a user to download all data and verify integrity, so in this paper we proposed system named Privacy Preserving And Verification Of Integrity Threat By Tpa Of Shared Data In Cloud.

Keywords— Cloud Computing, Cloud Data Storage, Public Auditability, Data Auditing, Dynamic Data, Batch Auditing.

I-Introduction

The construction of cloud and storing data on it has a remarkable benefits. It facilitates the authenticated and authorized cloud users to access huge resources that are outsourced and shared on the cloud. Whenever required, the user can request and gain the access (only, if the users' credentials are validated [4]) to the resources in an easy way and at low cost, irrespective of the user locality. Also, cloud computing takes away the expenses that are spent on installing all hardware and software.Cloud computing paradigm allows users to rent the resources based on their needs and pay them as per the use. Despite of all these benefits, cloud computing still a faces broad range of challenges which forbid the successful implementation of the cloud. These include both the traditional as well as cloud security challenges . Specific to cloud computing, the issues are many, of which some are: identity management of cloud users, multi-tenancy support, securing the security of applications, preserving privacy of the users, attaining control over the life cycle of outsourced data, etc. Among which, the issues related to privacy preserving are alone looked at in this survey.

Privacy preserving is used to provide an trusted service sends does not reveal the key and the data that an trusted customer sends in response to an auditor that follows the protocol (honest, but curious) does not reveal the key. Security in cloud computing can be achieved in several ways as authentication, integrity, confidentiality. Data integrity or data correctness is another security drawback that needs to be considered. Preserving the privacy of user, his identity and data in the cloud is very mandatory. With the rise in growth of cloud computing, the concerns about privacy preserving are also getting increased [3]. Several methods have been put forward to tackle this issue of privacy preserving. This work studies few of those approaches and provides a brief overview. It is important that the privacy of the user data has to be preserved anytime and anywhere. So, the work takes us in both tracks: preserving the privacy of the data as well as preserving the integrity of data. While we prefer some third party auditing to assure the data correctness.But reaching the

peak in providing and assuring privacy-preserved data access in cloud is yet in progress and still needs much attention to attain the goal.

A. **Challenges in the cloud data storage security are:**

• Snooping: Snooping is to steal a look into others private data. The efficient way to send and retrieve the data over a secure communication line.

• Cloud Authentication: The clients can acquire's others authorization and may try to delete the data. So it is necessary to guard one's unique authorization. The unauthorized clients must not be log in to others account and delete the data.

• Key Management: The cryptographic keys has to be managed in the cloud environment but this key management must be user friendly.

• Data Leakage: Data leakage takes place when data is transmitted between the user and the cloud server. The best way to protect is to encrypt the data from owner's side.

• Performance: An resilient security approach is necessary for encrypting as well as decrypting the data to and from the cloud but it should keep the user's performance integral.

B. major goals of proposed schemes are.

- 1 The User needs to use best encryption method.
- 2 Secure key management.
- 3 Supple access right managements.
- 4 Light weight integrity verification process for verifying the unauthorized change in the original data without need of local copy data [2].

The proposed scheme uses symmetric encryption which provides confidentiality, integrity, verification with low cost. It also provides enquiry for data owner and access control through which only authorized user can access the data. CSP may hide data loss or damage from users to maintain a reputation. To achieve security, we can handover our data to a third outsource party who will be assigned a task of identify the correctness and integrity of the cloud data. Hence Third party auditor (TPA) will check the data stored on the cloud based on the user's request.

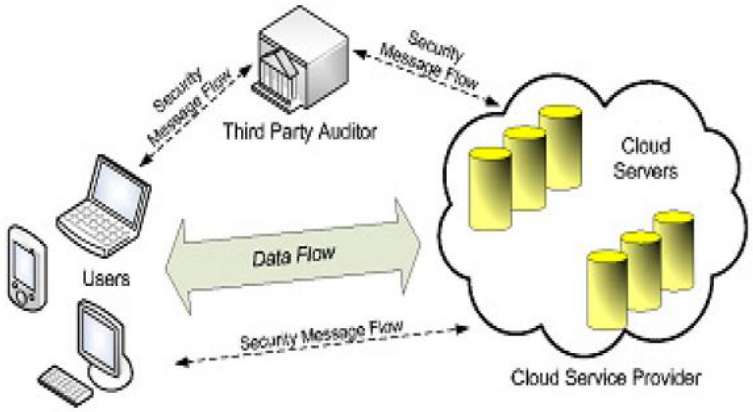

Fig.1: The framework of cloud data storage [1].

Fig.1.show the architecture of cloud storage where the cloud user (U), who has huge amount of data files to be stored on the cloud; the cloud server (CS), which is handled by cloud service provider (CSP) to provide data storage service and has considerable storage space and computation resources the third party auditor (TPA), who has expertise and capabilities

that cloud users do not have and is authorized to assess the cloud storage service security on behalf of the user upon request [1] [10].

We cannot achieve privacy; TPA can see the actual content stored on a cloud during the verifying phase. TPA itself may distribute the information stored in the cloud which violate security concept. To avoid the violation of security, Encryption technique is used where data is encrypted before storing it on the cloud. Hence using auditing with zero knowledge privacy technique where TPA will audit users data without seeing the contents. It uses existing public key based homomorphic linear authentication (HLA) [5] that allows TPA to perform auditing without requesting for user data. It reduces communication and computation overhead.

II. LITERATURE SURVEY

A. MAC Based Solution

It is used to verify the data. In this, user uploads the data blocks along with their MAC to CS and provides its secret key SK to TPA. Afterward the TPA will randomly retrieve data blocks & Mac uses secret key to check correctness of stored data on the cloud. Various issues with this system are listed below as [11]

☐ It introduce an additional online burden to users due to limited use (i.e. Bounded usage) and stateful verification.

☐ Communication & computation complexity

☐ TPA requires familiarity of data blocks for verification

☐ restriction on data files to be audited as secret keys sk are limited

☐ After usages of all possible secret keys, the user has to download all the data again and recomputed MACfor each data block & republish it on CS.

☐ TPA should preserve & update states for TPA which is very difficult

☐ It does not work with dynamic data ie it works only for static data.

B. HLA Based Solution

It supports efficient public auditing without retrieve data block. It is aggregated and required stable bandwidth. It is possible to calculate an aggregate HLA which authenticates a linear combination of the individual data blocks [11].

C. Provable Data Possession

G. Ateniese et al., used a provable data possession with homomorphic verifiable tags [6]. It allows the verification of data without retrieving it from the original source. The model generates probabilistic proofs of possession by sampling random set of blocks of data from the server, which reduce the cost.

The homomorphic verifiable tags computes multiple file blocks which can be combined to form a single file. The client pre-computes the tags and the tags are stored in the Third Party Auditor for verification. The modified file is stored in the server storage. The verification process is done in the requested style generated by the client.

It performs well and supports blockless verification. Its client/server computation is in O (1). Verification and communication takes time. It does not consider the privacy protection of the user's data against the external auditors

D. Dynamic Provable Data Possession

C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia,Dynamic Provable Data Possession (DPDP) [7]. PDP is mostly applicable for static files. The DPDP is an updated version of the PDP where it supports the updates while storing the data. It can append, modify, or delete the existing blocks of files. This scheme uses rank information to organize the dictionary entities. It supports the verification of files for different users and does not need to download the whole file for verification. It also explains the security and blockless verification of DPDP. Its hashing schemes use ranks based RSA trees. The experimental results show that the block size minimizes the communication and computational overhead.

E. Proof-of-Retrievability System

In this paper A.Juels et al., defined the PORs [8] as using an archive or a backup to help the verifier retrieve the file in the target easily. The user can easily retrieve the file from the backup. The POR is viewed as a kind of cryptographic proof of knowledge (POK), which can support large files. POR protocol reduces the communication cost because it doesn't need to access the file from the server, it can easily be accessed from the archive. This PORs is an unusual security formulation.

The main goal of PORs is that they are used to check the file without downloading the files. It also provides quality of service. Here the pre-processing takes time i.e., encoding the file F is required before storing to the prover. At the time of encoding sentinels are randomly added in specific positions, to constitute the contents of a POR. These sentinels can also retrieved by using the PIR, and it can be reused. It does not consider the privacy of the data against the external auditors. It has computational overhead.

F. Compact Proofs of Retrievability System

H. Shacham and B. Waters [9], in a proof-of-retrievability system, a data storage center must prove to a verifier that he is actually storing all of a client's data. The central challenge is to build systems that are both efficient and provably secure — that is, it should be possible to extract the client's data from any prover that passes a verification check. In this paper, we give the first proof-of-retrievability schemes with full proofs of security against arbitrary adversaries in the strongest model, that of Jules and Kaliski. Our first scheme, built from BLS signatures and secure in the random oracle model, features a proof-of-retrievability protocol in which the client's query and server's response are both extremely short. This scheme allows public verifiability: anyone can act as a verifier, not just the file owner. Our second scheme, which builds on pseudorandom functions (PRFs) and is secure in the standard model, allows only private verification. It features a proof-of-retrievability protocol with an even shorter server's.

ACKNOWLEDGMENT

We express our sincere thanks to all the authors, whose papers in the area of cloud computing security and auditability aspect which are published in various conference proceedings and journals.

CONCLUSION

We have proposed a privacy-preserving and Verification Of Integrity Threat by Tpa of Shared Data In Cloud. for securing data storage in cloud computing. Our system is suitable for providing integrity as well as preserving privacy of customers important data from unauthorized access. We supports insertion, modification and deletion of data at the block level, and also supports public verifiability. This scheme is proved to be safe against untrusted server. Privacy of user data is also preserved against third party auditor. This paper focuses on more effective and distributed two level security scheme to address the data storage security issue in cloud computing. As it is based on the symmetric cryptography for protecting user data including encryption prior to storage, user validation procedures prior to storage or retrieval, and building secure channel for data transmission, this method achieves the Reliability, Authenticity and Integrity of the cloud data. This approach of security model is expected to provide more security to user's data in cloud computing during storage and against unauthorized data modification attacks.

REFERENCES:

[1] C wang, Sherman S. M. Chow, Q. Wang, K Ren and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage",IEEE Trasaction on Computers I, vol. 62, no. 2, pp.362-375 , February 2013.

[2] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy- Preserving Public auditing for storage security in cloud computing," in Proc.of IEEE INFOCOM'10, March 2010.

[3] Xiao Z, and Xiao Y. Security and Privacy in Cloud 14. Computing, IEEE Communications Surveys & Tutorials, vol PP(99), 1–17.

[4] Takabi H (2010). Security and Privacy Challenges in Cloud 13. Computing Environments, IEEE Security & Privacy, vol 8(6), 24–31.

[5] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik "Scalable and efficient provable data possession," in Proc. Of SecureComm'08, 2008,

[6] 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), 2007.

[7] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia, "Dynamic Provable Data Possession," Proc. ACM Conf. Computer and Comm. Security (CCS '09), 2009.

[8] A. Juels and J. Burton, S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. ACM Conf. Computer and Comm. Security (CCS '07), Oct. 2007.

[9] H. Shacham and B. Waters, "Compact Proofs of Retrievability," Theory and Application of Cryptology and Information Security: Advances in Cryptology Dec. 2008.

[10] C. Wang, K. Ren, W. Lou, and J. Li, "Towards Publicly Auditable Secure Cloud Data Storage Services," IEEE Network Magazine, vol. 24, no. 4, pp. 19-24, July/Aug. 2010.

[11] Q. Wang, C. Wang,K.Ren, W. Lou and Jin Li "Enabling Public Audatability and Data Dynamics for Storage Security in Cloud Computing", IEEE Transaction on Parallel and Distributed System, vol. 22, no. 5, pp. 847 – 859,2011