ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Vol. 4, Issue 1, January 2016

A Review on Privacy Preserving Public Auditing for Data Storage Security

Akhil D More[1], Shailesh Nelwade[2], Avinash Chhabra[3], Nachiket Bhosale[4], Abha Pathak5

Student, Dept. of Computer Engineering ,Dr.D.Y.Patil Institute of Engineering & Technology, Pimpri, Pune, Savitribai Phule Pune University, Pune, India[1,2,3,4]

Dept. of Computer Engineering, Dr.D.Y.Patil Institute of Engineering & Technology Pimpri Pune, Savitribai Phule Pune University, Pune, India[5]

ABSTRACT: The Cloud computing is a latest technology whichprovides various services through internet. The Cloud server allows user to store their data on a cloud without worrying about correctness & integrity of data. Cloud data storage has many advantages over local data storage. User can upload their data on cloud and can access those data anytime anywhere without any additional burden. The User doesn't have to worry about storage and maintenance of cloud data. But as data is stored at the remote place how users will get the confirmation about stored data. Hence Cloud data storage should have some mechanism which will specify storage correctness and integrity of data stored on a cloud. The major problem of cloud data storage is security. Many researchers have proposed their work or new algorithms to achieve security or to resolve this security problem. In this paper, we propose a new innovative idea for Privacy Preserving Public Auditing with watermarking for data Storage security in cloud computing. It supports data dynamics where the user can perform various operations on data like insert, update and delete as well as batch auditing where multiple user requests for storage correctness will be handled simultaneously which reduce communication and computing cost.

KEYWORDS: Privacy Preserving, Public Auditing,Watermarking, TPA, Security

I. INTRODUCTION

Cloud Computing is using hardware and software as computing resources to provide service through internet. Cloud computing provides various service models as platform as a service (PaaS), software as a service (SaaS), Infrastructure as a service (Iaas), storage as a service (STaaS), security as a service (SECaaS), Data as a service (DaaS) & many more. Out of this Paas, SaaS and IaaS are most popular.Cloud computing has four models as Public cloud: though which the service is available to all public use. Private cloud: Through which service is available to private enterprise or organization. Community Cloud: It allows us to share infrastructure among various organizations through which we can achieve security, compliance and jurisdiction. This can be managed internally or by a third-party and hosted internally or externally. Hybrid cloud: it is a combination of public and private cloud. Cloud computing has many advantages as: we can easily upload and download the data stored in the cloud without worrying about security. We can access the data from anywhere, any time on demand. Cost is low or pay per usagebasis. Hardware and software resources are easily available without location independent. The major disadvantages of cloud computing is security.

The security is a major issue in cloud computing. It is a sub domain of computer security, network security or else data security. The cloud computing security refers to a broad set of policies, technology & controls deployed to protect data, application & the associated infrastructure of cloud computing. Some security and privacy issues that need to be considered are as follows

1) *Authentication:* Only authorized user can access data inthe cloud
2) *Correctness of data:* This is the way through whichuser will get the confirmation that the data stored in the cloud is secure

DOI: 10.15680/IJIRCCE.2016. 0401138

3) *Availability:* The cloud data should be easily availableand accessible without any burden. The user should access the cloud data as if he is accessing local data
4) *No storage Overhead and easy maintenance*:Userdoesn't have to worry about the storage requirement & maintenance of the data on a cloud

5) *No data Leakage:* The user data stored on a cloud canaccessed by only authorize the user or owner. So all the contents are accessible by only authorize the user.
6) *No Data Loss:* Provider may hide data loss on a cloudfor the user to maintain their reputation.

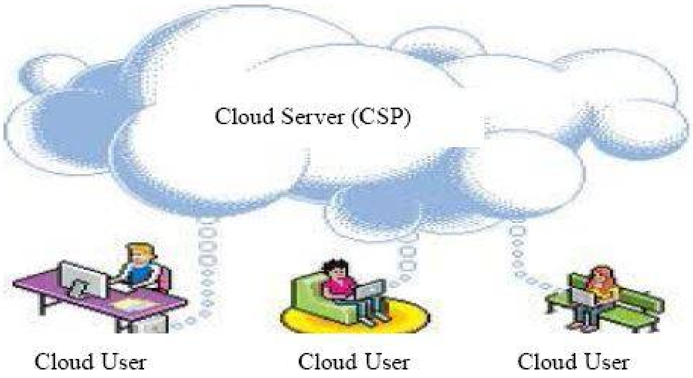

Fig 1: Cloud Architecture

It provides data confidentiality in two stages as 1) Data at rest 2) Data in transmission.

1) *Data at rest:* Symmetric key encryption technique(i.e. AES, TDES, and DES) are recommended which are secure but more time consuming.

2) *Data in transmission:* Secure Socket Layer (SSL)protocol is used for integrity verification. It uses a two different hash function such as Secure Hash Algorithm (SHA1) for digital signature and Message Digest (MD5) is a cryptographic hash function which is used to check the data integrity.

1) Cloud Service Provider (CSP): Organization orenterprises provide various services to cloud users. Confidentiality and integrity of cloud data should be maintained by CSP. The Provider should ensure that user's data and application are secured on a cloud. CSP may not leak the information or else cannot modify or access user's content. The attacker can log into network communication [9].

2) Cloud Server (CS): The cloud server where data beingstored and accessed by cloud data owner or users. Data should not be accessed by unauthorized users, no data modification or no loss of data.

3) Cloud User: Attackers can access basic information likeusername and password [9]. Key management is mojor issue in encryption techniques. Data dynamic issues need to be considered by CSP.

II. EXSISTING MECHANISM

The cloud data storage service contains 3 different entities as cloud user, Third party auditor & cloud server / cloud service provider. Cloud user is a person who stores large amount of data or files on a cloud server. [2] Cloud server is a place where we are storing cloud data and that data will be managed by the cloud service provider. [7]Third party auditors will do the auditing on users request for storage correctness and integrity of data. [9]

The proposed system specifies that user can access the data on a cloud as if the local one without worrying about the integrity of the data. Hence, TPA is used to check the integrity of data. It supports privacy preserving public auditing.[5] It checks the integrity of the data, storage correctness. It also supports data dynamics & batch auditing. The major benefits of storing data on a cloud is the relief of burden for storage management, universal data access with location independent & avoidance of capital expenditure on hardware, software & personal maintenance. [10]

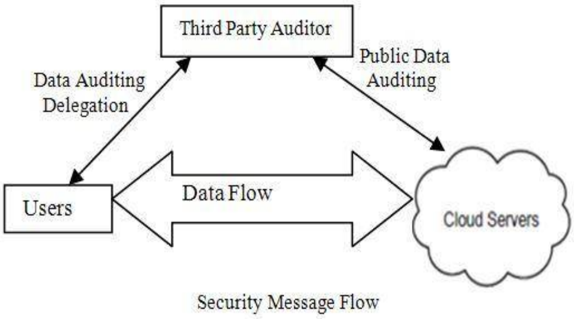

Fig 2: Architecture of Cloud Data storage service

In cloud, data is stored in a centralized form and managing this data and providing security is a difficult task. TPA can read the contents of data owner hence can modify. The reliability is increased as data is handled by TPA but data integrity is not achieved. It uses encryption technique to encrypt the contents of the file.

A. Goals

It allows TPA to audit users' data without knowing data content
It supports batch auditing where multiple user requests for data auditing will be handled simultaneously.
It provides security and increases performance through this system.

B. Design Goals

1) *Public audit ability:* Allows third party auditor tocheck data correctness without accessing local data.
2) *Storage Correctness:* The data stored on a cloud is as it.No data modification is done.
3) *Privacy preserving:* TPA can't read the users' datadıring the auditing phase.
4) *Batch Auditing:* Multiple users auditing request ishandled simultaneously.

5) *Light Weight:* Less communication and computationoverhead during the auditing phase.

C. Batch Auditing

It also supports batch auditing through which efficiency is *improved.* It allows TPA to perform multiple auditing task simultaneously and it reduces communication and computation cost.

D. Data Dynamics

It also supports data dynamics where user can frequently update the data stored on a cloud. It supports block level operation of insertion, deletion and modification. Author of [6] proposed scheme which support simultaneous public audibility and data dynamics. It uses Merkle Hash Tree (MHT) which works only on encrypted data. It [11] uses MHT for block tag authentication.

III. LITERATURE SURVEY

A. MAC Based Solution

It is used to authenticate the data. In this, user upload data blocks and MAC to CS provide its secret key SK to TPA. The TPA will randomly retrieve data blocks & Mac uses secret key to check correctness of stored data on the cloud. Problems with this system are listed below as

It introduces additional online burden to users due to limited use (i.e. Bounded usage) and stateful verification. Communication & computation complexity TPA requires knowledge of data blocks for verification Limitation on data files to be audited as secret keys are fixed After usages of all possible secret keys, the user has to download all the data to recomputed MAC & republish it on CS. TPA should maintain & update states for TPA which is very difficult. It supports only for static data not for dynamic data

B. HLA Based Solution

It supports efficient public auditing without retrieving data block. It is aggregated and required constant bandwidth. It is possible to compute an aggregate HLA which authenticates a linear combination of the individual data blocks.

C. Privacy Preserving Public Auditing Proposed by Cong Wang

Public auditing allows TPA along with user to check the integrity of the outsourced data stored on a cloud & Privacy Preserving allows TPA to do auditing without requesting for local copy of the data. Through this scheme [1], TPA can audit the data and cloud data privacy is maintained. It contains 4 algorithms as

1) ***Keygen:***It is a key generation algorithm used by theuser to setup the scheme.
2) ***Singen:***It is used by the user to generate verificationmetadata which may include digital signature.
3) ***GenProof:***It is used by CS to generate a proof of datastorage correctness.
4) ***Verifyproof:***Used by TPA to audit the proofs

It is divided into two parts as setup phase and audit phase.

1) ***Setup Phase:***Public and secret parameters areinitialized by using keygen and data files f are preprocesses by using singen to generate verification metadata at CS & delete its local copy. In preprocessing user can alter data files F.

2) ***Audit Phase:***TPA issues an audit message to CS. TheCS will derive a response message by executing Genproof. TPA verifies the response using F and its verification metadata.

D. Using Virtual Machine

AbhishekMohta proposed Virtual machines which uses RSA algorithm, for client data/file encryption and decryptions [5]. It also uses SHA 512 algorithm which makes message digest and check the data integrity. The Digital signature is used as an identity measure for client or data owner. It solves the problem of integrity, unauthorized access, privacy and consistency.

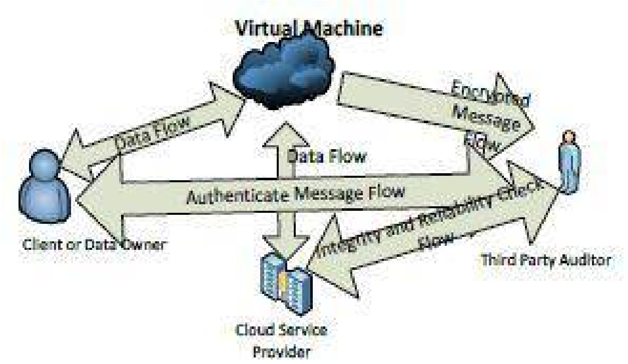

Fig 3: Architecture of Cloud server with CU and TPA

E. Non Linear Authentication

D. Shrinivas suggested Homomorphic non linear authenticator with random masking techniques to achieve cloud security [7]. K. Gonvinda proposed digital signature method to protect the privacy and integrity of data [8]. It uses RSA algorithm for encryption and decryption which follows the process of digital signatures for message authentication.

F. Using EAP

S. Marium proposed use of Extensible authentication protocol (EAP) through three ways hand shake with RSA. They proposed identity based signature for hierarchical architecture. They provide an authentication protocol for cloud computing (APCC) [9]. APCC is more lightweight and efficient as compared to SSL authentication protocol. In this, Challenge –handshake authentication protocol (CHAP) is used for authentication. When make request for any data or any service on the cloud.

G. Using Automatic Protocol Blocker

Dr. P.K. Deshmukh uses the new password at each instance which will be transferred to the mail server for each request to obtain data security and data integrity of cloud computing [17]. This protocol is secure against an untrusted server as well as third party auditor. Client as well as trusted third party verifier should be able to detect the changes done by the third party auditor.

H. Random Masking Technique

Jachak K. B. proposed privacy preserving Third party auditing without data encryption. It uses a linear combination of sampled block in the server’s response is masked with randomly generated by a pseudo random function (PRF) [16].

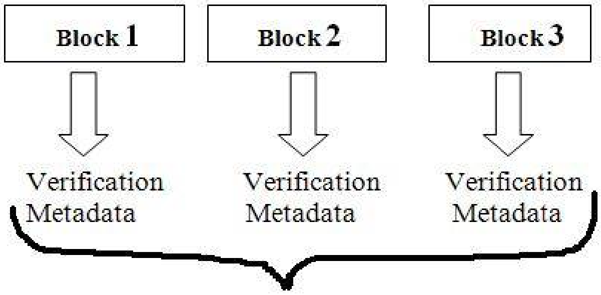

Fig 5: Homomorphic Authenticator

IV. PROPOSED MECHANISM

The data on the cloud has a minimum concern about sensitive information such as social security number, medical records, bank transaction and shipping manifests for hazardous material. We provide additional security such as watermark technique at specific time interval. These techniques enable single sign-on in the cloud and access control for sensitive data in both public and private clouds.In the Proposed system we used water marking process, to store the data or images in the cloud server by assigning the public key, and this key and watermarking images are sent to third party and third party have complete authority to check the key and sent it to the server, and there Third Party Auditor must have a public key whenever the data to be retrieved.

V. CONCLUSIONS

In this paper, we proposed watermarking technique for Privacy Preserving Public Auditing for cloud data storage security. Cloud computing security is a major issue that needs to be considered. Using TPA, We can verify the correctness and integrity of data stored on a cloud. It uses public key based homomorphic linear authentication (HLA) protocol with random masking to achieve privacy preserving data security. We achieved zero knowledge privacy through random masking technique. It supports batch auditing where TPA will handle multiple users request at the same time which reduces communication and computation overhead. It uses bilinear signature to achieve batch auditing.

REFERENCES

1. C wang, Sherman S. M. Chow, Q. Wang, K Ren and W. Lou, *"Privacy-Preserving Public Auditing for SecureCloud Storage",IEEETrasaction on Computers I,* vol. 62,no. 2, pp.362-375 , February 2013.
2. 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. Wang Shao-hu, Chen Dan-we, Wang Zhi-weiP, Chang Su-qin, *"Public auditing for ensuring cloud data storagesecurity with zero knowledge Privacy"* College ofComputer, Nanjing University of Posts and Telecommunications, China, 2009
4. KunalSuthar, Parmalik Kumar, Hitesh Gupta, *"SMDS:secure Model for Cloud Data Storage"*, InternationalJournal of Computer applications, vol56, No.3, October 2012
5. AbhishekMohta, Lalit Kumar Awasti, *"Cloud DataSecurity while using Third Party Auditor"*, InternationalJournal of Scientific & Engineering Research, Volume 3, Issue 6, ISSN 2229-8 June 2012.
6. Q. Wang, C. Wang,K.Ren, W. Lou and Jin Li *"EnablingPublic Audatability and Data Dynamics for Storage Security in Cloud Computing"*, IEEE Transaction onParallel and Distributed System, vol. 22, no. 5, pp. 847 – 859,2011.
7. Shrinivas, *"Privacy-Preserving Public Auditing inCloud Storage security"*, International Journal of computerscience nad Information Technologies, vol 2, no. 6, pp. 2691-2693, ISSN: 0975-9646, 2011
8. K Govinda, V. Gurunathprasad and H. sathishkumar, *"Third Party Auditing for Secure Data Storage in Cloud Through Digital Signature Using RSA"*, InternationalJournal of Advanced science and Technical Research, vol 4,no. 2, ISSN: 2249-9954,4 August 2012
9. S. Marium, Q. Nazir, A. Ahmed, S. Ahthasham and Aamir M. Mirza, *"Implementation of EAP with RSA forEnhancing The Security of Cloud Computig"*, InternationalJournal of Basic and Applied Science, vol 1, no. 3, pp. 177-183, 2012