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

IJCSMC, Vol. 4, Issue. 1, January 2015, pg.168 – 174

SURVEY ARTICLE

A Survey on Privacy-Preserving Public Auditing for Secure Cloud Storage Using Third Party Auditor

Mayuri V. Badhe[1], Prof. Prabhakar L. Ramteke[2]

[1]PG Student, Department of Computer Science & Information Technology
H.V.P.M.C.O.E.T. Amravati, India
[2]Professor, Department of Information Technology
H.V.P.M.C.O.E.T. Amravati, India
[1] MayuriBadhe93@Gmail.com; [2] pl_ramteke@rediffmail.com

Abstract— The Cloud computing is a latest technology which provides 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 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.

Keywords— Privacy Preserving, Public Auditing, Cloud Storage, 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 usage basis. Hardware and software resources are easily available without location independent. The major disadvantages of cloud computing is security.

A. Security Issues

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 in the cloud.

2) Correctness of data: This is the way through which user will get the confirmation that the data stored in the cloud is secure.

3) Availability: The cloud data should be easily available and 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: User doesn'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 can accessed 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 cloud for the user to maintain their reputation. In cloud computing, cloud data storage contains two entities as cloud user and cloud service provider cloud server.

Cloud user is a person who stores large amount of data on cloud server which is managed by the cloud service provider. User can upload their data on cloud without worrying about storage and maintenance. A cloud service provider will provide services to cloud user. The major issue in cloud data storage is to obtain correctness and integrity of data stored on the cloud. Cloud Service Provider (CSP) has to provide some form of mechanism through which user will get the confirmation that cloud data is secure or is stored as it is. No data loss or modification is done.

The correctness of data can be violated due to a broad range of both internal and external threats and CSP may hide data loss or damage from users to maintain a reputation. Major security issues associated with cloud user and CSP are as follows:

1) Cloud Service Provider (CSP): Organization or enterprises 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 being stored 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 like username and password [9]. Key management is major issue in encryption techniques. Data dynamic issues need to be considered by CSP. Cloud Computing Threads [9] are as follows:

- Spoofing Identity Theft
- Data Tempering Threat
- Repudiation Attack
- Information Disclosure on up/download Intra-Cloud
- Denial of Service Attack
- Log In

To achieve security, we can handover our data to a third outsource party who will specify the correctness and integrity of the cloud data. Hence, new concept arrives as Third party auditor (TPA) who will audit the user data stored on the cloud, based on the user's request. In this case, the Cloud service provider doesn't have to worry about the correctness and integrity of the data. In this technique, TPA will audit the cloud data to check the integrity or correctness in two ways as:

1) Download all files and data from the cloud for auditing. This may include I/O and network transmission cost.
2) Apply auditing process only for accessing the data but again in this case, data loss or data damage cannot be defined for unaccessed data. Public audit ability allows user to check integrity of outsource data under different

system & security models. We cannot achieve privacy as TPA can see the actual content stored on a cloud during the auditing phase. TPA itself may leak the information stored in the cloud which violate data security. To avoid this, Encryption technique is used where data is encrypted before storing it on the cloud.

II. RELATED WORK

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.

- *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 the user to setup the scheme.
2) Singen: It is used by the user to generate verification metadata which may include digital signature.
3) GenProof: It is used by CS to generate a proof of data storage 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 are initialized by using keygen and data files f are pre-processes by using singen to generate verification metadata at CS & delete its local copy. In pre-processing user can alter data files F.
2) Audit Phase: TPA issues an audit message to CS. The CS will derive a response message by executing Genproof. TPA verifies the response using F and its verification metadata. TPA is stateless i.e. no need to maintain or update the state information of audit phase. Public key based homomorphic linear authentication with random masking technique is used to achieve privacy preserving public auditing. TPA checks the integrity of the outsourced data stored on a cloud without accessing actual contents. Existing research work of proof of retrievability (PoR) or Proofs of Data Possession (PDP) technique doesn't consider data privacy problem. PDP scheme first proposed by Ateniese et al. used to detect large amount corruption in outsourced data. It uses RSA based Homomorphic authentication for auditing the cloud data and randomly sampling a few blocks of files. A Second technique proposed by Juels as Proofs of retrievability (PoR) allows user to retrieve files without any data loss or corruptions. It uses spot checking & error correcting codes are used to ensure both "Possession" and "Retrievability". To achieve Zero knowledge privacy, researcher [3] proposed Aggregatable Signature Based Broadcast (ASBB). It provides completeness, privacy and soundness. It uses 3 algorithms as Keygen, Gentag and Audit.

C. Using Virtual Machine

Abhishek Mohta 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.

III.EXISTING SYSTEM

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. Cloud server is a place where we are storing cloud data and that data will be managed by the cloud service provider. Third party auditors will do the auditing on users request for storage correctness and integrity of data. 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.

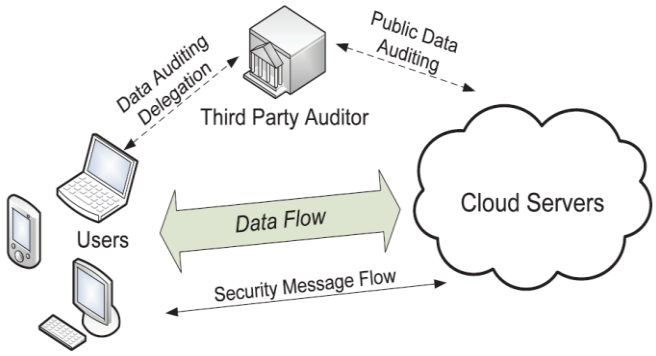


Fig.1 The Architecture of cloud data storage service.

Hence, TPA is used to check the integrity of data. It supports privacy preserving public auditing. 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. 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. TPA checks the integrity of the data stored on a cloud but if the TPA itself leaks the user's data. Hence the new concept comes as auditing with zero knowledge privacy where TPA will audit the users' data without seeing the contents. It uses public key based homomorphic linear authentication (HLA) [1], [2] which allows TPA to perform auditing without requesting for user data. It reduces communication & computation overhead. In this, HLA with random masking protocol is used which does not allow TPA to learn data content.

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 to check 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' data during the auditing phase.
4) Batch Auditing: Multiple users auditing request is handled simultaneously.
5) Light Weight: Less communication and computation overhead 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. Through this scheme, we can identify invalid response. It uses bilinear signature (BLS proposed by Boneh, Lynn and Shacham) to achieve batch auditing. System performance will be faster.

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 audability and data dynamics. It uses Merkle Hash Tree (MHT) which works only on encrypted data. It [11] uses MHT for block tag authentication.

IV. PROPOSED SYSTEM

I am proposing a "Privacy-Preserving Public Auditing System for Data Storage Security" in cloud computing. I will utilize the Homomorphic Random Authenticator (HRA) by using ElGamal Public Key Encryption Algorithm and random masking to guarantee that the, TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the users' fear of their outsourced data leakage. Considering TPA may concurrently handle multiple audit sessions from different users for their outsourced data files, they further extend our privacy-preserving public auditing protocol into a multiuser setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency. Extensive analysis shows that their schemes are provably secure and highly efficient. With random masking, the TPA no longer has all the necessary information to build up a correct group of linear equations and therefore cannot derive the user's data content.

- *The Third-Party Auditor:*

TPA check the integrity of outsourced data and be worry free. TPA to perform audits for multiple users simultaneously and efficiently. TPA audit the outsourced data when needed. The TPA, who has expertise and capabilities that users do not, can periodically check the integrity of all the data stored in the cloud on behalf of the users, which provides a much more easier and affordable way for the users to ensure their storage correctness in the cloud. Moreover, in addition to help users to evaluate the risk of their subscribed cloud data services, the audit result from TPA would also be beneficial for the cloud service providers to improve their cloud-based service platform.

- *The ElGamal Public Key Encryption Algorithm:*

The security of ElGamal is based on the discrete logarithm problem. To encrypt and respectively decrypt a message, a discrete power is executed. This operation is e_cient to compute. An attacker that seeks to decrypt an intercepted message may try to recover the private key. To this end a logarithm needs to be computed. No actual method exists for this, given certain requirements on the initial group are met. Under these circumstances, the encryption is secure. Today the ElGamal algorithm is used in many cryptographic products. The open-source software GnuPG uses ElGamal as standard for signatures. On behalf of this software and its problems with ElGamal [10] discovered in late 2003 we will show the importance of correct implementation of cryptographic algorithms.

Thus ElGamal simplified the Difie-Hellman key exchange algorithm by introducing a random exponent k. This exponent is an replacement for the private exponent of the receiving entity. Due to this simplification the algorithm can be used to encrypt in one direction, without the necessity of the second party to take actively part. The key advance here is that the algorithm can be used for encryption of electronic messages, which are transmitted by the means of public store-and-forward services.

The ElGamal Algorithm provides an alternative to the RSA for public key encryption.

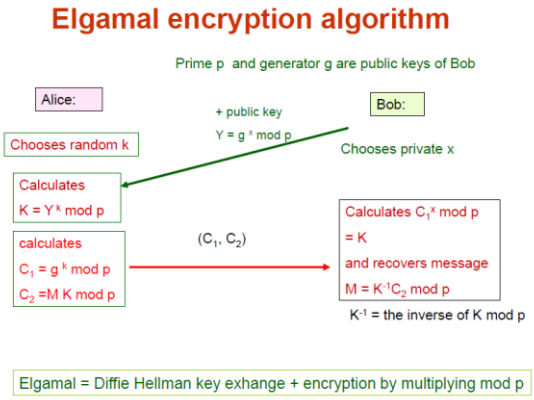
1) Security of the RSA depends on the (presumed) difficulty of factoring large integers.

2) Security of the ElGamal algorithm depends on the (presumed) difficulty of computing discrete logs in a large prime modulus.

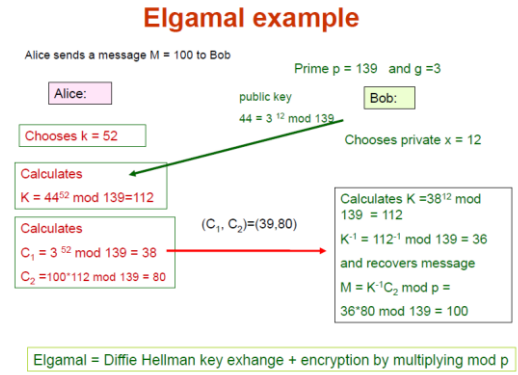
ElGamal has the disadvantage that the ciphertext is twice as long as the plaintext.

It has the advantage the same plaintext gives a different ciphertext (with near certainty) each time it is encrypted.

- *The Structure of ElGamal Public Key Encryption Algorithm:*



- *The Example of ElGamal Public Key Encryption Algorithm:*



- *Proposed System Architecture:*

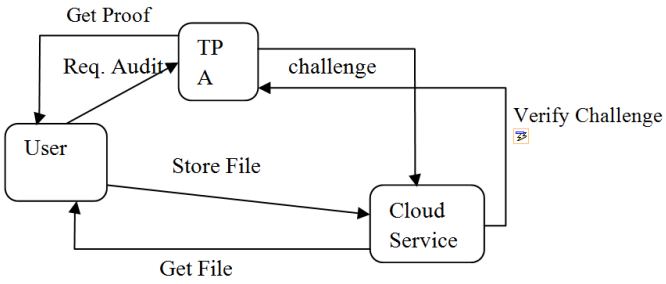


Fig.2 Proposed System Architecture.

User generates Private and public parameters and preprocesses file to create MACs and Store it on cloud Server. He also shares private keys with TPA.

TPA creates a Challenge for Cloud Service. Cloud answers the challenge. TPA verifies the answer.

V. CONCLUSION AND FUTURE WORK

In this way Public Auditing of User Data will be Preserved in cloud computing by utilize the Homomorphic Random Authenticator (HRA) by using ElGamal Public Key Encryption Algorithm and random masking to guarantee that the, TPA would not learn any knowledge about the data content stored on the cloud server during the efficient auditing process, which not only eliminates the burden of cloud user from the tedious and possibly expensive auditing task, but also alleviates the user's fear of their outsourced data leakage. And also considering TPA will concurrently handle multiple audit sessions from different users for their outsourced data files, they further extend our privacy-preserving public auditing protocol into a multiuser setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency.

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] Wang Shao-hu, Chen Dan-we, Wang Zhi-weiP, Chang Su-qin, "Public auditing for ensuring cloud data storage security with zero knowledge Privacy" College of Computer, Nanjing University of Posts and Telecommunications, China, 2009.

[4] KunalSuthar, Parmalik Kumar, Hitesh Gupta, "SMDS: secure Model for Cloud Data Storage", International Journal of Computer applications, vol56, No.3, October 2012.

[5] AbhishekMohta, Lalit Kumar Awasti, "Cloud Data Security while using Third Party Auditor", International Journal 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 "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.

[7] D. Shrinivas, "Privacy-Preserving Public Auditing in Cloud Storage security", International Journal of computer science 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", International Journal 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 for Enhancing The Security of Cloud Computig", International Journal of Basic and Applied Science, vol 1, no. 3, pp. 177- 183, 2012.

[10] XU Chun-xiang, HE Xiao-hu, Daniel Abraha, "Cryptanalysis of Auditing protocol proposed by Wang et al. for data storage security in cloud computing", http://eprint.iacr.org/2012/115.pdf, and cryptologyeprintarchieve: Listing for 2012.

[11] B. Dhiyanesh "A Novel Third Party Auditability and Dynamic Based Security in Cloud Computing" , International Journal of Advanced Research in Technology, vol. 1,no. 1, pp. 29-33, ISSN: 66023127,2011.

