

An Innovative Method for 3rd Party Auditing With Improved User Data Privacy Protection in the Cloud

K Ravi Kiran

B.Tech,

Department of CSE,

TKR College of Engineering
& Technology.

B Sushanthi Reddy

B.Tech,

Department of CSE,

TKR College of Engineering
& Technology.

V Archana Reddy, M.Tech

Asst Professor,

Department of CSE,

TKR College of Engineering
& Technology.

Abstract:

Cloud computing is computing in which large groups of remote servers are networked to allow centralized data storage and online access to computer services or resources. Cloud computing relies on sharing of resources to achieve coherence and economies of scale, similar to a utility (like the electricity grid) over a network. The cloud must have to ensure data integrity and security of data of user. 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.

Keywords:

Privacy Preserving, Public Auditing, Watermarking, TPA, Securit, Cloud Computing

Introduction:

Cloud computing security or, more simply, cloud security is an evolving sub-domain of computer security, network security, and, more broadly, information security. It refers to a broad set of policies, technologies, and controls deployed to protect data, applications, and the associated infrastructure of cloud computing.

Security issues associated with the cloud:

Organizations use the Cloud in a variety of different service models (SaaS, PaaS, and IaaS) and deployment models (Private, Public, Hybrid, and Community). There are a number of security issues/concerns associated with cloud computing but these issues fall into two broad categories: security issues faced by cloud providers (organizations providing software-, platform-, or infrastructure-as-a-service via the cloud) and security issues faced by their customers (companies or organizations who host applications or store data on the on the cloud). The responsibility goes both ways, however: the provider must ensure that their infrastructure is secure and that their clients' data and applications are protected while the user must take measures to fortify their application and use strong passwords and authentication measures.

When an organization elects to store data or host applications on the public cloud, it loses its ability to have physical access to the servers hosting its information. As a result, potentially business sensitive and confidential data is at risk from insider attacks. According to a recent Cloud Security Alliance Report, insider attacks are the third biggest threat in cloud computing. Therefore, Cloud Service providers must ensure that thorough background checks are conducted for employees who have physical access to the servers in the data center. Additionally, data centers must be frequently monitored for suspicious activity. In order to conserve resources, cut costs, and maintain efficiency, Cloud Service Providers often store more than one customer's data on the same server. As a result there is a chance that one user's private data can be viewed by other users (possibly even competitors). To handle such sensitive situations, cloud service providers should ensure proper data isolation and logical storage segregation.

The extensive use of virtualization in implementing cloud infrastructure brings unique security concerns for customers or tenants of a public cloud service. Virtualization alters the relationship between the OS and underlying hardware - be it computing, storage or even networking. This introduces an additional layer - virtualization - that itself must be properly configured, managed and secured. Specific concerns include the potential to compromise the virtualization software, or "hypervisor". While these concerns are largely theoretical, they do exist. For example, a breach in the administrator workstation with the management software of the virtualization software can cause the whole datacenter to go down or be reconfigured to an attacker's liking.

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 be accessed by only authorized user or owner. So all the contents are accessible by only authorized user.
- 6) No Data Loss: Provider may hide data loss on a cloud for the user to maintain their reputation

Compliance & Audits in Cloud:

Numerous laws and regulations pertain to the storage and use of data. In the US these include privacy or data protection laws, Payment Card Industry - Data Security Standard (PCI DSS), the Health Insurance Portability and Accountability Act (HIPAA), the Sarbanes-Oxley

Act, the Federal Information Security Management Act of 2002 (FISMA), and Children's Online Privacy Protection Act of 1998, among others. Similar laws may apply in different legal jurisdictions and may differ quite markedly from those enforced in the US. Cloud service users may often need to be aware of the legal and regulatory differences between the jurisdictions. For example data stored by a Cloud Service Provider may be located in, say, Singapore and mirrored in the US.

Many of these regulations mandate particular controls (such as strong access controls and audit trails) and require regular reporting. Cloud customers must ensure that their cloud providers adequately fulfil such requirements as appropriate, enabling them to comply with their obligations since, to a large extent, they remain accountable.

Business continuity and data recovery:

Cloud providers have business continuity and data recovery plans in place to ensure that service can be maintained in case of a disaster or an emergency and that any data loss will be recovered. These plans may be shared with and reviewed by their customers, ideally dovetailing with the customers' own continuity arrangements. Joint continuity exercises may be appropriate, simulating a major Internet or electricity supply failure for instance.

Logs and audit trails:

In addition to producing logs and audit trails, cloud providers work with their customers to ensure that these logs and audit trails are properly secured, maintained for as long as the customer requires, and are accessible for the purposes of forensic investigation (e.g., eDiscovery).

Unique compliance requirements:

In addition to the requirements to which customers are subject, the data centers used by cloud providers may also be subject to compliance requirements. Using a cloud service provider (CSP) can lead to additional security concerns around data jurisdiction since customer or tenant data may not remain on the same system, or in the same data center or even within the same provider's cloud.

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.

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, TPA can audit the data and cloud data privacy is maintained. 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 preprocessed by using $sigen$ 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. 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 proposed Aggregatable Signature Based Broadcast (ASBB). It provides completeness, privacy and soundness. It uses 3 algorithms as Keygen, GenTag and Audit.

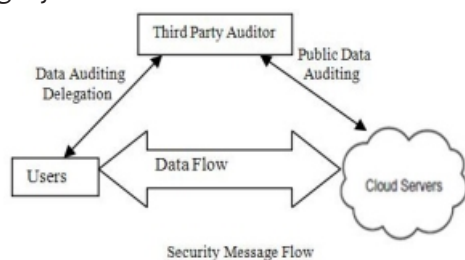
Using Virtual Machine:

Abhishek Mohta proposed Virtual machines which uses RSA algorithm, for client data/file encryption and decryptions. 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.

EXISTING SYSTEM:

Since cloud service providers (CSP) are separate administrative entities, data outsourcing is actually

relinquishing user's ultimate control over the fate of their data. As a result, the correctness of the data in the cloud is being put at risk due to the following reasons. First of all, although the infrastructures under the cloud are much more powerful and reliable than personal computing devices, they are still facing the broad range of both internal and external threats for data integrity.



Architecture of Cloud Data storage service

DISADVANTAGES OF EXISTING SYSTEM:

Although outsourcing data to the cloud is economically attractive for long-term large-scale storage, it does not immediately offer any guarantee on data integrity and availability. This problem, if not properly addressed, may impede the success of cloud architecture. As users no longer physically possess the storage of their data, traditional cryptographic primitives for the purpose of data security protection cannot be directly adopted. In particular, simply downloading all the data for its integrity verification is not a practical solution due to the expensiveness in I/O and transmission cost across the network. Besides, it is often insufficient to detect the data corruption only when accessing the data, as it does not give users correctness assurance for those unaccessed data and might be too late to recover the data loss or damage.

PROPOSED SYSTEM:

To fully ensure the data integrity and save the cloud users' computation resources as well as online burden, it is of critical importance to enable public auditing service for cloud data storage, so that users may resort to an independent third party auditor (TPA) to 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, and even serve for independent arbitration purposes. In a word, enabling public auditing services will play an important role for this nascent cloud economy to become fully established, where users will need ways to assess risk and gain trust in the cloud.

ADVANTAGES OF PROPOSED SYSTEM:

- 1) We motivate the public auditing system of data storage security in Cloud Computing and provide a privacy-preserving auditing protocol. Our scheme enables an external auditor to audit user's cloud data without learning the data content.
- 2) To the best of our knowledge, our scheme is the first to support scalable and efficient privacy preserving public storage auditing in Cloud. Specifically, our scheme achieves batch auditing where multiple delegated auditing tasks from different users can be performed simultaneously by the TPA in a privacy-preserving manner.
- 3) We prove the security and justify the performance of our proposed schemes through concrete experiments and comparisons with the state-of-the-art.

OTHER ADVANTAGES:

- Public auditability
- Storage correctness
- Privacy-preserving
- Batch auditing
- Lightweight

ALGORITHM:

A public auditing scheme consists of four algorithms (KeyGen, SigGen, GenProof, VerifyProof).

- KeyGen: key generation algorithm that is run by the user to setup the scheme

- SigGen: used by the user to generate verification metadata, which may consist of MAC, signatures or other information used for auditing

- GenProof: run by the cloud server to generate a proof of data storage correctness

- VerifyProof: run by the TPA to audit the proof from the cloud server

Encryption Algorithm:

Step 1: Generate the ASCII value of the letter

Step 2: Generate the corresponding binary value of it. [Binary value should be 8 digits (no matter how much the length of it, we should represent it in 8 digits. $2^8=256$). e.g. for decimal 32 binary number should be 00100000 (underlined zeros are required)]

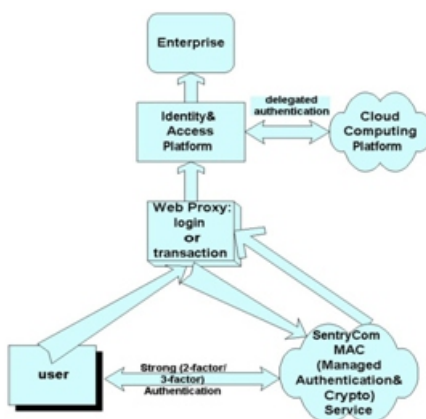
Step 3: Reverse the 8 digit's binary number

Step 4: Take a 4 digits divisor (≥ 1000) as the Key

Step 5: Divide the reversed number with the divisor

Step 6: Store the remainder in first 3 digits & quotient in next 5 digits (remainder and quotient wouldn't be more than 3 digits and 5 digits long respectively. If any of these are less than 3 and 5 digits respectively we need to add required number of 0s (zeros) in the left hand side. So, this would be the ciphertext i.e. encrypted text

FLOWCHART:



MODULES:

Privacy-Preserving Public Auditing Module:

Homomorphic authenticators are unforgeable verification metadata generated from individual data blocks, which can be securely aggregated in such a way to assure an auditor that a linear combination of data blocks is correctly computed by verifying only the aggregated authenticator. Overview to achieve privacy-preserving public auditing, we propose to uniquely integrate the homomorphic authenticator with random mask technique. In our protocol, the linear combination of sampled blocks in the server's response is masked with randomness generated by a pseudo random function (PRF).

The proposed scheme is as follows:

- Setup Phase
- Audit Phase

Batch Auditing Module:

With the establishment of privacy-preserving public auditing in Cloud Computing, TPA may concurrently handle multiple auditing delegations upon different users' requests. The individual auditing of these tasks for TPA can be tedious and very inefficient. Batch auditing not only allows TPA to perform the multiple auditing tasks simultaneously, but also greatly reduces the computation cost on the TPA side.

Data Dynamics Module:

Supporting data dynamics for privacy-preserving public risk auditing is also of paramount importance. Now we show how our main scheme can be adapted to build upon the existing work to support data dynamics, including block level operations of modification, deletion and insertion. We can adopt this technique in our design to achieve privacy-preserving public risk auditing with support of data dynamics.

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. It also supports data dynamics. It uses Merkle Hash Tree (MHT) for it. We are introducing Privacy Preserving Public Auditing with watermark process for secure cloud Storage.

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 cryptologyeprint-archieve: 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: 6602 3127, 2011
- [12] C. Wang, Q. Wang and K. Ren, "Ensuring Data Storage security in Cloud Computing", IEEE Conference Publication, 17th International Workshop on Quality of Service (IWQoS), 2009
- [13]Balkrishnan.S,Saranya.G,Shobana.SandKarthikeyan. S, "Introducing Effective Third Party Auditing (TPA) for Data Storage Security in Cloud", International Journal of computer science and Technology, vol. 2, no. 2, ISSN 2229-4333 (Print) | ISSN: 0976-8491(Online), June 2012
- [14] K. Kiran Kumar, K. Padmaja, P. Radha Krishna, "Automatic Protocol Blocker for Privacy-Preserving Public Auditing in Cloud Computing", International Journal of Computer science and Technology, vol. 3 pp, ISSN. 0976-8491(Online), pp. 936-940, ISSN: 2229-4333 (Print), March 2012
- [15] Lingaraj Dhabale, Priti Pavale, "Providing Secured Data Storage by Privacy and Third Party Auditing In Cloud", International Conference on Computing and Control Engineering, ISBN 978-1-2248-9, 12 & 13 April, 2012 .
- [16] Jachak K. B., Korde S. K., Ghorpade P. P. and Gaware G. J. , "Homomorphic Authentication with Random Masking Technique Ensuring Privacy & Security in Cloud Computing", Bioinfo Security Informatics, vol. 2, no. 2, pp. 49-52, ISSN. 2249-9423, 12 April 2012