International Journal of Engineering Research and General Science Volume 3, Issue 2, March-April, 2015
ISSN 2091-2730

Privacy-Preserving Public Auditing for Secure Cloud Storage

Prof. N.L. Chourasiya, Dayanand Lature, Arun Kumavat, Vipul Kalaskar, Sanket Thaware.

kptarun74@gmail.com
Contact no: 9970131164

Abstract— The cloud storage has a lot of problems about the security and data Integrity. So we need to prevent the all problems. In cloud storage users can remotely store their data and enjoy the on-demand high quality applications and services from shared resources, without the burden of local data storage and maintenance. Users are not able to check his data again and again from the cloud storage it is secure or not. 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, 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.

Keywords— Privacy-preserving, auditability, Cryptographic protocols, cloud computing, data compression, Data integrity, Third Party Auditor (TPA).

1. INTRODUCTION

The cloud services mainly include sharing, online storage, Web-based email and database processing. By adapting the Cloud computing, it becomes easy to share the virtualized resources. Here Users do not need any background knowledge of the services and it's very easy to maintain when compared to any traditional technologies. Cloud computing is of three types named Infrastructure as a Service, Platform as a Service, and Software as a service .By these three; it is possible to make complex things very easy. Infrastructure as a Service delivers basic storage and computing capabilities as standardized services over the network.

Third Party Auditor is kind of inspector. There are two categories: private auditability and public auditability. Although private auditability can achieve higher scheme efficiency, public auditability allows anyone, not just the client, to challenge the cloud server for the correctness of data storage while keeping no private information. To let off the burden of management of data of the data owner, TPA will audit the data of client. It eliminates the involvement of the client by auditing that whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for Cloud Computing. The released audit report would help owners to evaluate the risk of their subscribed cloud data services, and it will also be beneficial to the cloud service provider to improve their cloud based service platform. Hence TPA will help data owner to make sure that his .data are safe in the cloud and management of data will be easy and less burdening to data owner.

2. OBJECTIVE

1. Storing of user data in the cloud despite its advantages has many interesting Security concerns which needs to be extensively investigated for making it reliable solution to the problems in local storage of data.

2. The main problem with cloud storage is securities of information as the cloud server we use are the third party. So we need to use the encryption algorithm which will give security to our data. We also need to keep some auditor who will take care of data integrity by monitoring the data.

3. We are compressing the data using algorithm for Data optimization. Algorithm works by manipulate bits of data to reduce the size and optimize input. Algorithm is to split the input data into two data where the first data will contain original nonzero byte and the

second data will contain bit value explaining position of nonzero and zero bytes. Data then can be compress with data compression algorithm to achieve maximum compression ratio.

3. RELATED WORK

The public auditability in their defined "provable data possession" model for ensuring possession of data files on untrusted storages. Their scheme utilizes the RSA based homomorphic non-linear authenticators for auditing outsourced data and suggests randomly sampling a few blocks of the file.

However, the public auditability in their scheme demands the linear combination of sampled blocks exposed to external auditor. When used directly, their protocol is not provably privacy preserving, and thus may leak user data information to the auditor. Jules etal describe a "proof of irretrievability" model, where spot-checking and error-correcting codes are used to ensure both "possession" and "irretrievability" of data files on remote archive service systems. However, the number of audit challenges a user can perform is fixed a priori, and public auditability is not supported in their main scheme. Although they describe a straightforward Merkle-tree construction for public PoRs, this approach only works with encrypted data. Dodis et al.give a study on different variants of PoR with private auditability. Shacham et al.design an improved PoR scheme built with full proofs of security in the security model defined. Similar to the construction, they use publicly verifiable homomorphic non-linear authenticators that are built from provably secure BLS signatures. construction, a compact and public verifiable scheme is obtained. Again, their approach does not support privacy preserving auditing for the same reason. The propose allowing a TPA to keep online storage honest by first encrypting the data then sending a number of pre-computed symmetric-keyed hashes over the encrypted data to the auditor. The auditor verifies both the integrity of the data file and the server's possession of a previously committed decryption key. This scheme only works for encrypted files, and it suffers from the auditor state fullness and bounded usage, which may potentially bring in online burden to users when the keyed hashes are used up.

The dynamic version of the prior PDP scheme, using only symmetric key cryptography but with a bounded number of audits. Consider a similar support for partial dynamic data storage in a distributed scenario with additional feature of data error localization. In a subsequent work, Wang et al. propose public auditability and full data dynamics. Almost simultaneously developed a skip lists based scheme to enable provable data possession with full dynamics support. However, the verification in these two protocols requires the linear combination of sampled blocks and thus does not support privacy preserving auditing. While all the above schemes provide methods for efficient auditing and provable assurance on the correctness of remotely stored data, none of them meet all the requirements for privacy preserving public auditing in cloud computing. More importantly, none of these schemes consider batch auditing, which can greatly reduce the computation cost on the TPA when coping with a large number of audit delegations.

3. EXISTING SYSTEM

Cloud improves due to centralization of data, increased security-focused resources, etc., but concerns can persist about loss of control over certain sensitive data, and the lack of security for stored kernels. Security is often as good as or better than other traditional systems, in part because providers re able to devote resources to solving security issues that many customers cannot afford.

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) he third party auditing process should bring in no new vulnerabilities towards user data privacy.

Drawbacks of existing system:

•Cloud Storage system provides the user for safe and consistent place to save valuable data and documents. However, user's files are not encrypted on some open source cloud storage systems. I.e. TPA demands retrieval of user data, here privacy is not preserved.

•The storage service provider can easily access the user's files. This brings a big concern about user's privacy. The user has no supreme control over the software applications including secret data. User has to depend on the provider's action, maintenance and admin it.

4. PROPOSED SYSTEM

In this paper, the TPA will be fully automated and will be able to properly monitor confidentiality and integrity of the data and uniquely integrate it with random mask technique to achieve a privacy-preserving public auditing system for cloud data storage security while keeping all above requirements in mind. Extensive security and performance analysis shows the proposed schemes are provably secure and highly efficient. We are encrypt the data using RSA algorithm cloud computing can be applied to the data transmission security. Transmission of data will be encrypted, even if the data is stolen, there is no corresponding key that cannot be restored. Only the user knows the key, the clouds do not know the key. Also, because the properties of encryption, the cloud can operate on cipher text, thus avoiding the encrypted data to the traditional efficiency of operation. User's privacy is protected because user's files are encrypted in cloud storage.

The main issue with the cloud is data integrity, in this paper we are going to use MD5 algorithm for maintain the integrity of data. This MD5 algorithm has more expensive and more secure than other algorithms. MD5 Message Digest is a widely used hash technique, such that it will produce 128-bit hash value we need to convert the input data into bytes in order to convert it to hash value. This is useful in many security applications and it ensures data integrity. Sender creates input message (M) and computes its message digest. Then he uses his private key and encrypts message digest. Encrypted message digest is attached to the input message and the whole message is sent to receiver. Receiver gets the message and extracts the encrypted message digest. Then he computes his own message digest of the received message. He also decodes received message digest with sender's public key and gets decoded message digest. Then he compares both message digests. When both message digests are equal, the message was not modified during the data transmission.

Advantages:

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.

4. Interoperability

Access information from anywhere

Can be accessed using different devices

4. A fragment technique is introduced in this paper to improve performance and reduce extra storage.

5. The data integrity will be safer.

Architecture of Cloud Data Storege Service

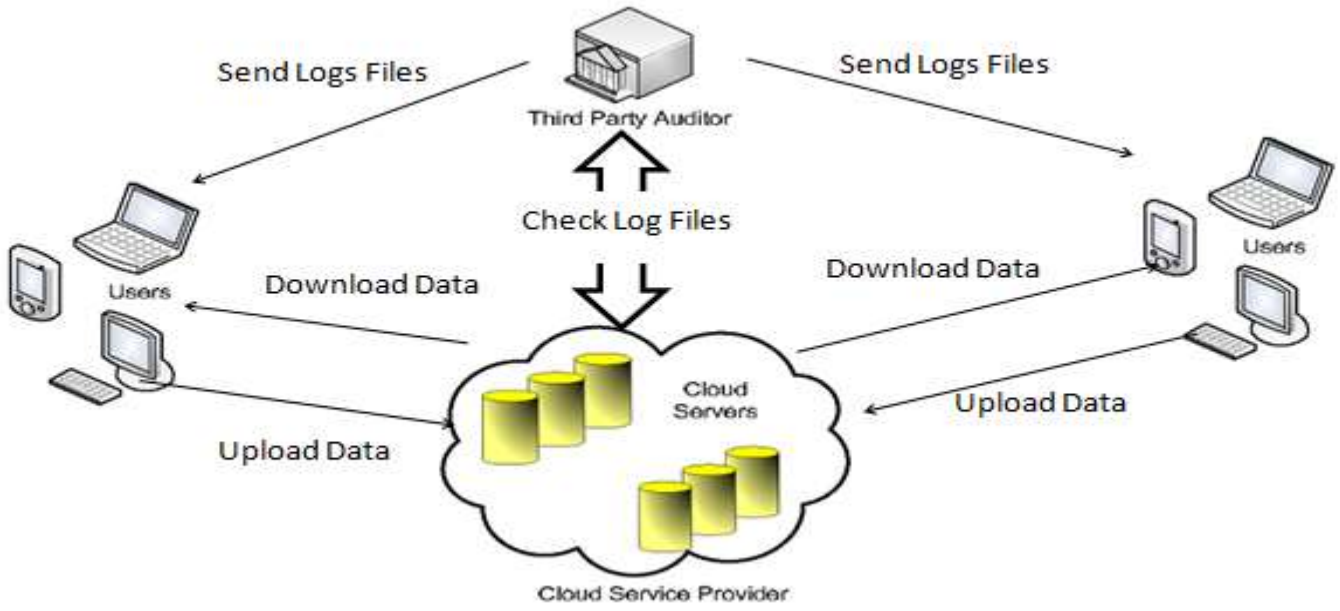

Fig -Architecture of Cloud Data Storege Service

In the above figure there three main parts i.e Users,Cloud service provider and Third Party Auditor(TPA).The user uploads the data on to the clouds and downloads from the cloud using cloud service provider.then user needs a integrity to his data that integrity maintain using TPA.It maintain the all logs file and check simulteneously the data on to the cloud.The main purpuse of the TPA is to maintain and check the integrity of data.If small changes occurs into the data then TPA send that report to the user.The integrity of the data can be maintain using the MD5 algorithm.The MD5 algorithm is intended for digital signature applications, where a large file must be "compressed" in a secure manner before being encrypted with a private (secret) key under a public-key cryptosystem such as RSA."

For the compression of data we are using huffman code algorithm in which tree generated from the exat frequence of text.this algorithm is an optimal compression algorithm when only the frequency of individual letters are used to compress the data. The technique works by creating a binary tree of nodes. These can be stored in a regular array, the size of which depends on the number of symbols, n. A node can be either a leaf node or an internal node. Initially, all nodes are leaf nodes, which contain the symbol itself, the weight (frequency of appearance) of the symbol and optionally, a link to a parent node which makes it easy to read the code (in reverse) starting from a leaf node. Internal nodes contain symbol weight, links to two child nodes and the optional link to a parent node. the process of decompression is simply a matter of translating the stream of prefix codes to individual byte values, usually by traversing the Huffman tree node by node as each bit is read from the input stream

APPLICATION

This system will be used to store the data on cloud server with safety and the data integrity of data can be maintain automatically using the third party authenticator.

ACKNOWLEDGMENT

My deepest thanks to Prof.N.L Chourasiya, the guide of the project for guiding and correcting various documents of ours with attention and care. She has taken a pain to go through the project and make the necessary correction as and when needed.

We would also thank my Institution and my Faculty members without whom this project would have being a distant reality. We are grateful for their constant help and support.

CONCLUSION

In this paper, we propose a privacy-preserving public auditing system for data storage security in Cloud Computing. We utilize the homomorphic linear authenticator 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, we further extend our privacy-preserving public auditing protocol into a multi-user setting, where the TPA can perform multiple auditing tasks in a batch manner for better efficiency. Extensive analysis shows that our schemes are provably secure and highly efficient.

REFERENCES:

[1] CongWang; Chow, S.S.M.; QianWang ; KuiRen ;WenjingLou "Privacy_preserving Public Auditing for Secure CloudStorage", IEEE Transactions on Computers Volume: 62 , Issue: 2 2013 ,PP no : 362 – 375.
[2] C.Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Storage Security in Cloud Computing," Proc. IEEE INFOCOM '10, Mar. 2010.
[3] P. Mell and T. Grance, "Draft NIST Working Definition of Cloud Computing," http://csrc.nist.gov/groups/SNS/cloudcomputing/
[4] index.html, June 2009.
[5] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz,A. Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, "Above the Clouds: A Berkeley View of Cloud Computing," Technical Report UCB-EECS-2009-28, Univ. of California, Berkeley, Feb. 2009.
[6] M. Arrington, "Gmail Disaster: Reports of Mass Email Deletions," http://www.techcrunch.com 006/12/28/gmaildisasterreportsof-mass-email-deletions/, 2006.
[7] J. Kincaid, "MediaMax/TheLinkup Closes Its Doors," http://
[8] www.techcrunch.com /2008/07/10/mediamaxthelinkupclosesits-
[9] doors/, July 2008.
[10] Amazon.com, "Amazon s3 Availability Event: July 20,
[11] 2008," http://status.aws.amazon.com/s3-20080720.html,
[12] July 2008.L. Hubert and P. Arabie, "Comparing Partitions," J. Classification, vol. 2, no. 4, pp. 193-218, Apr. 1985. (Journal or magazine citation)
[13] R.J. Vidmar, "On the Use of Atmospheric Plasmas as Electromagnetic Reflectors," IEEE Trans. Plasma Science, vol. 21, no. 3, pp. 876-880, available at http://www.halcyon.com/pub/journals/21ps03-vidmar, Aug. 1992. (URL for Transaction, journal, or magzine)
[14] J.M.P. Martinez, R.B. Llavori, M.J.A. Cabo, and T.B. Pedersen, "Integrating Data Warehouses with Web Data: A Survey," IEEE Trans. Knowledge and Data Eng., preprint, 21 Dec. 2007, doi:10.1109/TKDE.2007.190746.(PrePrint)