Secure Privacy Preserving Using Multilevel Trust For Cloud Storage

Anju Panicker[1], Ankita Bhavsar[2], Monika Mandge[3], Pooja Bothara[4]

[1]*Anju Panicker, Dept. of Information Technology, NDMVP's KBTCOE, Nasik*
[2]*Ankita Bhavsar, Dept. of Information Technology, NDMVP's KBTCOE, Nasik*
[3]Monika Mandge, *Dept. of Information Technology, NDMVP's KBTCOE, Nasik*
[4]*Pooja Bothara, Dept. of Information Technology, NDMVP's KBTCOE, Nasik*

---***---

Abstract - *Cloud computing known to be the latest development in data center technology. User use to store their confidential data on cloud, so security and data integrity is main concern while using cloud services. 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, but while using TPA, there is chances of data leakage from TPA, so we are handling data leakage from TPA. Along with that in our system extensive security and performance analysis is handled by encryption algorithms like AES , RSA.*

Key Words: Privacy preserving, Public auditability, Random masking, Encryption algorithms, Batch auditing.

1. INTRODUCTION

The recently emerged cloud computing, known to be the latest development in data center technology. Users can remotely store their data and enjoy the on-demand high-quality applications and services from a shared pool of configurable computing resources, without the burden of local data storage and maintenance. From user's perspective, including both individuals and IT enterprises, storing data remotely to the cloud in a flexible on-demand manner brings appealing benefits relief of the burden for storage management,universal data access with location independence. While cloud computing makes these advantages more appealing than ever, it also brings new and challenging security threats toward user' s outsourced data. As users no longer physically possess the storage of their data, To fully ensure the data integrity and save the cloud user' s 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. In these paper we are also focusing on encryption algorithms for data security and data integrity. For extensive security and integrity we are using encryption algorithm. In symmetric algorithm, both parties share the secret key for both encryption/decryption, and from privacy perceptive it is important that this key is not compromised, because cascading data will then be compromised. On the other hand in asymmetric algorithm uses Pairs of keys, of which one key is used for encryption while other key is used for decryption. In this paper to check the performance analysis one of symmetric algorithm and one of the asymmetric algorithm is used i.e. AES and RSA. Multilevel trust has been identified as vital component for establishing and maintaining successful relational exchanges between e-commerce trading partners in cloud environment.

2. LITERATURE SURVEY

[1] G. Ateniese, R. Burns, R. Curtmola , J. Herring, L. Kissner, Z.Peterson, and D. Song, "Provable Data Possession at Untrusted Stores," In this paper public auditability is defined as "provable data possession" model for ensuring possession of files on untrusted storages. In their scheme, they utilize RSA-based homomorphic tags for auditing outsourced data, thus public auditability is achieved. However, they do not consider the case of dynamic data storage, and the direct extension of their scheme from static data storage to dynamic case may suffer design and security problems.

[2] Chang Liu*, Rajiv Ranjan+, Xuyun Zhang*, Chi Yang*, Dimitrios Georgakopoulos+, Jinjun Chen, "Public Auditing for Big Data Storage in Cloud Computing -- A Survey", In this paper we provide an analysis on authenticator-based efficient data integrity verification. In their scheme, they introduce two standard signature schemes (RSA and BLS) and one authenticated data structure (MHT). For Dynamic data possession they utilized another authenticated data structure rank-based skip list mainly for verification of updates. They also proposed a new scheme that can support both dynamic data and public verifiability at the same time. Although the current formalizations and security model seemed very rigorous and potent, new exploits can always exist, especially with dynamic data streams and varying user groups. Finding the security holes and fixing them can be a long-lasting game.

[3] Prof. D. N. Rewadkar, Suchita Y. Ghatage, Cloud Storage System Enabling Secure Privacy Preserving Third Party

Audit. This article studies the problems of ensuring data storage correctness and proposes an efficient and secure method to address these issues. A homomorphic encryption scheme is used to encrypt the data which will be shared with the TPA. In this they analyzed two basic schemes MAC based solution and HLA based solution. HLA allows efficient data auditing and consumes only constant bandwidth. However HLA technique may reveal user data information to TPA as he can simply solve a system of linear equations used in the HLA technique. So it violates the privacy preserving guarantee.

3. PROPOSED MODEL

In this paper, we utilize the public key based homomorphic authenticator and uniquely integrate it with random mask technique to achieve a privacy-preserving public auditing system for cloud data storage security. 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. TPA to support batch auditing. In previous papers several schemes are proposed for data security and data integrity but new exploits can always exist in system so to handle the security issue we are using two different encryption algorithms like AES and RSA . In order to find out which is more efficient we are comparing them.

3.1 Algorithm used

1. Advanced Encryption Standard (AES)
Advanced Encryption Standard is a symmetric key cryptographic algorithm which means same key is used to both encrypt and decrypt data. Also cipher text produced by AES algorithm is the same size as the plain text data.

2. Ron Rivest, Adi Shamir, Leonard Aldmen (RSA)
Rivest, Shamir, Aldmen is asymmetric key cryptographic algorithm which means two different keys are used during encryption and decryption process .It is block cipher which converts plain text into cipher text at sender side and vice versa at receiver side.

3.2 System Architecture

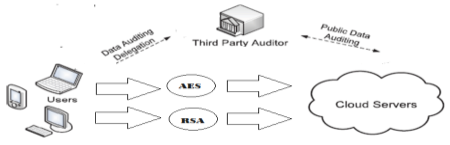

Fig -1: System Diagram

The cloud user, who has large amount of data files to be stored in the cloud. The cloud server, which is managed by the cloud service provider to provide data storage service and has storage space and computation resources. The third-party auditor, who has expertise and capabilities that cloud users do not have and is trusted to assess the cloud storage service reliability on behalf of the user upon request. Users rely on the CS for cloud data storage and maintenance. In this system two algorithms AES and RSA are compared in terms of time and security. TPA to audit user's data which is stored on cloud and also data leakage from TPA is handled.

4. OBJECTIVES

Following are the objectives of the system:-

1. We encourage the public auditing system of data storage security in cloud computing and provide a privacy preserving auditing record. Our scheme enables an Third Party Auditor (TPA) to audit user's cloud data without learning the data content.

2. This scheme achieves batch auditing where multiple authorized auditing tasks from different users can be performed simultaneously by the TPA in a privacy-preserving manner.

3. Privacy is main concern in the cloud storage In order to preserve privacy many algorithms are been adapted but in this paper we are mainly focusing on AES and RSA.

5. CONCLUSIONS

In these system we propose a privacy- preserving public auditing system for data storage security in cloud computing. To achieve privacy-preserving public auditing, we propose to uniquely integrate the homomorphic linear authenticator with random masking technique. Third party auditor to audit users data on cloud to maintain integrity. TPA would not learn any knowledge about the data content stored on the cloud server during the data auditing process. These system also used to prevent data leakage.

ACKNOWLEDGEMENT

With all respect and gratitude, we would like to thank all the people who have helped us directly or indirectly for the completion of the project "Secure Privacy Preserving Using Multilevel Trust For Cloud Storage". We express our heartily gratitude towards Prof. S.P.Jadhav for guiding us to understand the work conceptually and also for his constant encouragement to complete the project. Our association with his as a student has been extremely inspiring. We would like to give our sincere thanks to Prof. V. S. Patil, Head of the Department of Information Technology for his technical support and constant encouragement. We would also like to extend our sincere thanks to our Principal Dr. K. S. Holkar for his help and support in all respects. We would also like to thank all our staff members and collogues who helped us directly or indirectly throughout our dissertation work.

REFERENCES

[1] 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.

[2] Cong Wang, Member, IEEE, Sherman S.M. Chow, Qian Wang, Member,IEEE, KuiRen, Senior Member, IEEE, and Wenjing Lou, Senior Member, IEEE, ”Privacy-Preserving Public Auditing for Secure Cloud Storage*” IEEE Transactions on Computers, vol. 62, no. 2, February 2013.*

[3] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z.Peterson, and D. Song, “Provable Data Possession at UntrustedStores,” Proc. 14th ACM Conf. Computer and Comm. Security(CCS ’07), pp. 598-609, 2007.

[4] Prof. D. N. Rewadkar, Suchita Y. Ghatage, **“**Cloud Storage System Enabling Secure Privacy Preserving Third Party Audit**”** *2014 International Conference on Control,* Instrumentation, Communication and Computational Technologies (ICCICCT).

[5] Chang Liu*, Rajiv Ranjan+, Xuyun Zhang*, Chi Yang*, Dimitrios Georgakopoulos+, Jinjun Chen, “Public Auditing for Big Data Storage in Cloud Computing -- A Survey”2013 IEEE 16th International Conference on Computational Science and Engineering.

[6] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing," *IEEE Transactions on Parallel and Distributed Systems,* vol. 22, pp. 847 - 859, 2011.

[7] Cloud Security Alliance, “Top Threats to Cloud Computing,”http://www.cloudsecurityalliance.org, 2010.