Privacy Preserving for Remote Data Based On Identity with High Performance for Cloud Storage

Kaveri Umarani[1], Manju Khanna[2]

[1]Student, Dept. Of CSE, MVJCE, Bangalore, Karnataka, India
[2] Assistant professor, Dept. Of CSE, MVJCE, Bangalore, Karnataka, India

---

Abstract - *Privacy preserving for the user data stored in a storage server like cloud server forms a complex task with performance and the maintenance issue alongside the security overheads. Many remote data integrity checking protocols have been designed till date which may create an issue of generating key to protect the privacy of user data stored in cloud. Making the data available for the user when needed in the high traffic scenario is the much needed job of the data servers. In this paper, we have designed a privacy preserving for the remote data stored by the user, based on the identity by making use of encryption techniques like SHA1 and SHA2 algorithms which increases the security of the user data. We make use of zero knowledge checks against the third party verifiers which in turn increase the privacy of the user data. The performance is hiked in our design by the use of file signature generating servers which act according to traffic over the network and try and access the lower traffic network which has a required data. Our design has proved to be secured over the threats and provides the high security using the identity based user data storage and increases the performance by smartly selecting the server over the traffic in the cloud. Proves to be more relevant with protection and also proves to be secured and practical.*

***Key Words*: Cloud Computing, Privacy preserving, Key homomorphic cryptography, Performance, Security.**

1. INTRODUCTION

Cloud Computing [1] is serving the wide range of computing and research communities in the everyday growing researches. It helps in making the resources available to everyone who virtually increases the storage space, processor speed, memory and the applications stored. Cloud computing provides three kinds of services, most commonly used is software as a service. Cloud computing has a huge number of advantages and benefits: a) reduces the high investment on the hardware's by providing the virtual availability of all the hardware's needed. b) Maintenance of the cloud contents is left to the cloud servers by transferring the overhead to the cloud server's. c) Your data is available whenever you needed to use it, no need to take your computers with you always.

However the most useful cloud computing also has some of the drawbacks which is hard to digest.one of most important problem to worry with cloud servers are the security and the availability of your data. The data stored in cloud are stored in the third party servers where in the access over the data you stored is preserved with cloud servers. Where in the cloud servers can miss use the data you stored. There is no guarantee for the data you stored as the data can be lost or damaged and the cloud servers do not take any responsibility for the data stored. Your data may become temporarily un available in case of cloud failures.in case of data shift to untrusted clouds or the user your personal information leaked to the third party.

Preserving the privacy of the data stored by the user into the public clouds are always need to be secured and made available to the user at all times whenever he needed with zero damage. Remote data integrity protocols helps in maintaining the data security [4] by using key protection and the data labeling based on the keys. The user data should be necessarily made available to the user when he wants to access it. In our design we make use of security and the performance concepts. We allow the user to upload his file to the cloud servers where in the data is stored with the primary level protection with a key generation with a digital signature by using the SHA1 and SHA2 algorithms which is better used than the md5 encryption. The file uploaded by the user can be verified before he download's the file ensuring the data preserved and the data security which we made it possible by the use of zero knowledge check.by making use of the file signature generating servers. We could able to reduce the overheads and the traffic over the networks by selecting the server with the less traffic and making the data available to user as early as he can.

The contribution of this paper is summarized as bellow.

- Identity based keys are generated using the third party auditor where in the remote data integrity checks are used. Based on which the keys are generated for an identity that's the id level.
- We provided the detailed security proofs of the protocols including sounding of privacy with SHA1 and SHA2 with the key level encryption
- File signature generating servers are used along with the cloud servers to controlling the traffic over the network.

2. OBJECTIVES

The main objective of the system is to increase the data integrity of the user data based on the identity which in turn increased the privacy of the stored data in cloud. The data of the user is stored in to the cloud the in the encrypted format using the SHA1 and SHA2 encryption techniques along with the digital signature and the data is secured to the user, the user can verify the data stored in the cloud using the auditor server and the file is verified if the content is not changed. Auditor will check the file contents without having the knowledge of the data stored with the help of a digital signature. And the file signature generating servers are used to decrease the traffic over the cloud the get the faster access to the files stored over the cloud.

3. LITERATURE SURVEY

The importance and popularity of cloud security has led to several previous surveys. A. F. Barsoum and M. A. Hasan [3] discussed "Provable Multicopy dynamic data possession in cloud computing systems," Customers expect their data to be replicated, redundant and available on the multiple data servers to achieve scalability, availability and the durability of the data. This in turn will result into the cost factor and matter as the data storage is increasing. To overcome, the above drawback a map-based provable Multicopy dynamic data possession (MB-PMDDP) scheme has been introduced.

G. Ateniese et al., [2] "Provable data possession at untrusted stores," Has invented the model for the provable data possession which allows a client who has stored his data in an untrusted server and to verify the data which exposing the original data to the third party. The client maintains the limited data to verify the content. The overhead here is to overcome the increase the network communication. PDP supports large datasets in distributed server systems.

J. Liu, K. Huang, H. Rong, H. Wang, and M. Xian, [4] Privacy preserving public auditing for regenerating-code-based cloud storage Outsourced data in cloud storage has to be protected against the outsourced corruptions by adding fault tolerance to cloud storage together which allows the data integrity. Without secrete key file can't be upload and download to cloud storage.

Making the codes fault tolerant is major requirement. Here the public auditing scheme is used to regenerate the code based cloud storage.

4. METHODOLOGY

Data integrity of a remote data checks provides the security for the user data by keeping the separate third party auditor [6] and by then making the system secure. Along with the cloud storage servers the file signature generating servers has to be clubbed ,the third party auditor will be given the access and made the entire content available to him whenever the auditor requests the file which in turn will create the risk of data loss making insecure and resulting in the increase of cost. The system architecture of the proposed system is as shown in the figure 1.

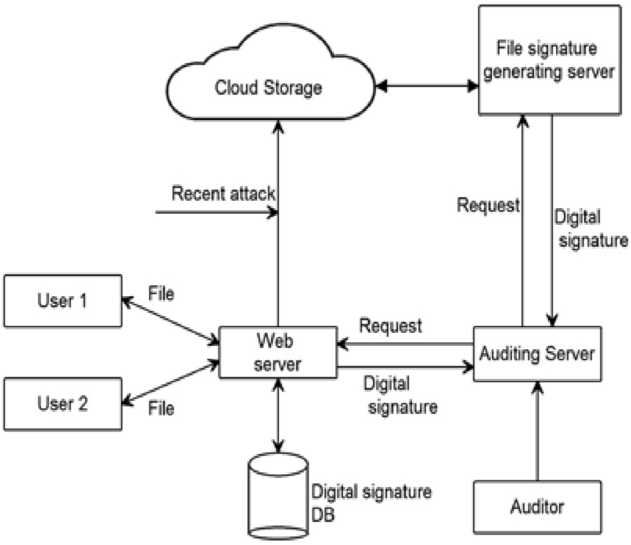

Figure 1: System Architecture

And to get rid of all this above mentioned drawbacks we are introducing the file signature server which in turn will get the file content before passing it to the auditor and tagging the digital signature to the file requested. And by using the digital signature the content exposed to the auditor is limited and the cost can be considerably reduced.

5. IMPLEMENTATION

In this section we determine the implementation of privacy preserving for cloud security.

a) User Secrete Key Generation

When New User is registering to OPOR Application, each new user will get the secrete key for his privacy to upload and download the files.

b) Hashing processing

When user is uploading the File to cloud, first the File will be read in byte stream for generating the SHA1 key using Hashing Technique. The SHA1 Key will be contains 16 bit and SHA1 key will be generating based on the content of the uploading File. This SHA1 key will be stored in users database Server.

c) File Upload Process with Encryption

User has to login to upload the File, when user wants to upload data file to the cloud storage he has to select the file from his storage. When file is uploading to the cloud, we are generating the digital signature of the file and keep a copy of the digital signature in the users database storage .The File content will be encrypted with users secrete key using the AES Algorithm. The Encrypted file will be send to the cloud storage by connecting through the file transfer protocol (ftp).once the connection is establish with the cloud storage, encrypted file will be transferred to cloud storage .

d) Integrity Checking Process

When Users wants to verify the files from the auditor, Auditor going to check the integrity checking process .While auditor checking the integrity check for the file verification process he has to request for web server storage to get the digital signature of the uploaded file instead of file which is present in the cloud storage and has to get the original digital signature .finally web server storage will compare the both digital signatures for integrity checking process. If both are identical then his file is not modified or else appropriate message will be display.

e) File Download Process with Decryption

User wants to download the file from the cloud storage his has to select the particular file .while downloading first web application has to connect with cloud storage .The Cloud connection is establishes using FTP protocol .select the particular file in cloud and using AES algorithm it will decrypt the file to download the original file.

f) Public auditing process.

Auditor can audit the files without having knowledge of auditing process because while checking file verification web server will check only the digital signature of the file, instead of files. So it is easy to verify the files.

6. CONCLUSION

In this paper we have come up with an new idea of Privacy Preserving for Remote Data Based On Identity with High Performance in Cloud Storage which will provide the perfect data privacy with the low traffic over the network alongside high security for the data stored by the user. And provides the practical was of efficiently demonstrating the privacy and the performance values with the data security.

REFERENCES

[1] P. Mell and T. Grance. (Jun. 3, 2009). Draft NIST Working Definition of Cloud Computing. [Online]. Available: http://csrc.nist.gov/groups/SNC/cloud-computing/index.html

[2] G. Ateniese et al., “Provable data possession at untrusted stores,” in Proc. 14th ACM Conf. Comput. Commun. Security, 2007, pp. 598–609.

[3] A.F. Barsoum and M.A.Hasan, “Provable Multicopy dynamic data possession in cloud computing systems,” IEEE Trans. Inf. Forensics Security, vol. 10, no. 3, pp. 485–497, Mar. 2015.

[4] J. Liu, K. Huang, H. Rong, H. Wang, and M. Xian, “Privacy preserving public auditing for regenerating-code-based cloud storage,” IEEE Trans. Inf. Forensics Security, vol. 10, no. 7, pp. 1513–1528, Jul. 2015.

[5] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-preserving public auditing for data storage security in cloud computing,” in Proc. IEEE INFOCOM, Mar. 2010, pp. 1–9.

[6] C. Wang, K. Ren, W. Lou, and J. Li, “Toward publicly auditable secure cloud data storage services,” IEEE Netw., vol. 24, no. 4, pp. 19–24, Jul./Aug. 2010.

[7] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, “Privacy preserving public auditing for secure cloud storage,” IEEE Trans. Comput., vol. 62, no. 2, pp. 362–375, Feb. 2013.

[8] Y. Yu et al., "Enhanced privacy of a remote data integrity-checking protocol for secure cloud storage," Int. J. Inf. Security, vol. 14, no. 4, pp. 307–318, 2015.

[9] F. Hess, "Efficient identity based signature schemes based on pairings," in Proc. Sel. Areas Cryptography, vol. 2595. 2003, pp. 310–324.

[10] X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, "New publicly verifiable databases with efficient updates," IEEE Trans. Depend. Sec. Comput., vol. 12, no. 5, pp. 546–556, Sep./Oct. 2015.

[11] G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," in Proc. ASIACRYPT, 2009, pp. 319–333.

[12] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 5, pp. 847–859, May 2011.