Analysing Privacy for Remote Data in a Cloud Storage

[1]Madhushree N, [2]Hanuman Kumar
[1]Mtech Student, [2]Sr. Associate Professor
[1]Department of Computer Science and Engineering,
[1]New Horizon College of Engineering, Bangalore, 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 and implemented which may possess an issue of generating key to protect the privacy of user data which is stored in cloud. In this paper, we have designed a privacy preserving for the remote data stored by the user generating servers which act according to traffic over the network and try and access the lower traffic network which has a required data and also verify the data owner data is protected. 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. It proves to be more relevant with protection of user data and also proves to be more secured and practical. 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.

IndexTerms **- Privacy preserving, cloud storage, data integrity, identity based cryptography.**

I. INTRODUCTION

Cloud computing is serving the wide scope of processing and research networks in the ordinary developing investigates. It helps in making the assets accessible to everybody who practically expands the extra room, processor speed, memory and the applications put away. Cloud computing gives three sorts of administrations, most normally utilized is programming as an administration. Distributed computing has a colossal number of preferences and advantages: a) decreases the high speculation on the equipment's by giving the virtual accessibility of all the equipment's required. b) Maintenance of the cloud substance is left to the cloud servers by exchanging the overhead to the cloud server's. c) Your information is accessible at whatever point you expected to utilize it, no compelling reason to take your PCs with you generally.

Anyway the most valuable cloud computing likewise has a portion of the disadvantages which is difficult to digest.one of most significant issue to stress with cloud servers are the security and the accessibility of your information. The information put away in cloud are put away in the outsider servers where in the entrance over the information you put away is saved with cloud servers. Where in the cloud servers can miss utilize the information you put away. There is no assurance for the information you put away as the information can be lost or harmed and the cloud servers don't assume any liability for the information put away. Your information may turn out to be incidentally unaccmation move to untrusted or the client your own.

Protecting the security of the information put away by the client into the open mists are constantly should be verified and made accessible to the client consistently at whatever point he required with zero harm. Remote information trustworthiness conventions helps in keeping up the information security by utilizing key assurance and the information marking dependent on the keys. The client information ought to be essentially made accessible to the client when he needs to get to it. In our plan we utilize security and the execution ideas. We enable the client to transfer his document to the cloud servers where in the information is put away with the essential dimension assurance with a key age with a computerized mark by utilizing the SHA1 and SHA2 calculations which is preferable utilized over the md5 encryption. The document transferred by the client can be confirmed before he download's the record guaranteeing the information protected and the information security which we made it conceivable by the utilization of zero learning check.by utilizing the record signature creating servers. We could ready to lessen the overheads and the traffic over the systems by choosing the server with the less traffic and making the information accessible to client as right on time as possible.

The contribution of this paper is condensed as:

- Identity based keys are produced utilizing the outsider inspector where in the remote information honesty checks are utilized. In view of which the keys are produced for a personality that is the id level.
- We gave the itemized security confirmations of the conventions incorporating sounding of protection with SHA1 and SHA2 with the key dimension encryption.
- File signature producing servers are utilized alongside the cloud servers to controlling the traffic over the system.

II. OBJECTIVES

The main objective of the system is to increase the data integrity of the data provided by the based on the identity which in turn increases the privacy of the stored data in cloud storage. 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.

III. LITERATURE SURVEY

The importance and popularity of cloud security has led to several previous surveys. A. F Barsoum and M. A. Hasan discussed "Provable Multicopy dynamic data possession in cloud computing systems," Clients anticipate that their information should be duplicated, excess and accessible on the different information servers to accomplish versatility, accessibility and the strength of the information. This thusly will result into the cost factor and matter as the information stockpiling is expanding. To survive, the above downside a guide based provable Multicopy dynamic information ownership (MB-PMDDP) conspire has been presented

G.Ateniese et al., "Provable data possession at untrusted stores," Invented the model for the provable information ownership which permits a customer who has put away his information in an untrusted server and to confirm the information which uncovering the first information to the outsider. The customer keeps up the constrained information to confirm the substance. The overhead here is to conquered the expansion the system correspondence. PDP underpins substantial datasets in circulated server frameworks.

J. Liu, K. Huang, H. Rong, H. Wang, and M. Xian, Privacy Preserving for recovering code-based distributed storage Outsourced information in distributed storage must be ensured against the re-appropriated debasements by adding adaptation to internal failure to distributed storage together which permits the information uprightness. Without discharge key record can't be transfer and download to distributed storage. Making the codes fault tolerant is major necessity. Here the open evaluating plan is utilized to recover the code based distributed storage.

IV. METHODOLOGY

Data integrity of a remote information checks gives the security to the client information by keeping the different outsider reviewer and by then making the framework secure. Alongside the distributed storage servers the document signature producing servers must be clubbed ,the outsider inspector will be given the entrance and made the whole substance accessible to him at whatever point the reviewer demands the record which thusly will make the danger of information misfortune making shaky and bringing about the expansion of expense. The framework engineering of the proposed framework is as appeared in the figure 1.

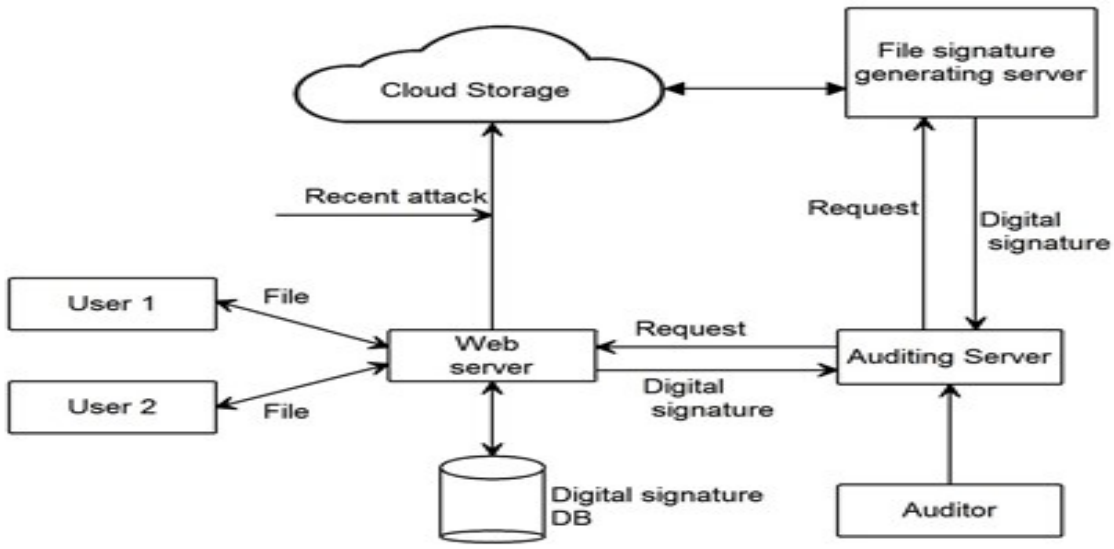

Figure 1: System Architecture

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.

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

4.1 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.

4.2 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.

4.3 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 .

4.4 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.

4.5 File Upload 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.

4.6 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

V. CONCLUSION

In this paper we have come up with an idea of Privacy Preserving for Remote Data Based On Identity based 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 also protect the data user data in a cloud server which in turn provides an efficiently demonstrating the privacy and the performance values with the data security. Thus the implementation result demonstrate the proposed protocol is more secure and praticle in real world application.

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] 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] 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] F. Hess, "Efficient identity based signature schemes based on pairings," in Proc. Sel. Areas Cryptography, vol. 2595.