International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 03 | Mar 2019 www.irjet.net p-ISSN: 2395-0072

SECURITY ENHANCE USING HASH AND CHAOSTIC ALGORITHM IN CLOUD

Asst. Prof. Naziya Pathan, Sneha Chouriya,Arti Choure,Priyanka Chikhle,Shraddha Ninave

[1]Asst.Prof. Naziya Pathan C.E.Department Nuva College of Engineering & Technology, Nagpur
[2]Sneha Chouriya ,Arti Choure,Priyanka Chikhle,Shraddha Ninave,student C.E. Dept. NCET, Nagpur

---

Abstract *- Most of the security solutions use routers, firewalls, and intrusion detection systems implemented to tightly control, access to networks from outside authors. Cloud computing breaks these organizational bounds. When the data is present in the cloud, it resides outside the organizational bounds. Hence, a user loses control over their data. Another problem is most of the time users are anxious about uploading private and confidential files for online backup due to concern that the service provider might use it inappropriately. So, providing security at the required level is a major concern. This existing system presents a data-centric access control solution with enriched role-based expressiveness in which security is focused on protecting user data regardless the Cloud service provider that holds it.*

1. INTRODUCTION

Cloud computing could be a revolutionary mechanism that ever-changing way to enterprise hardware and software system style and procurements. The cloud computing provides made advantages to the cloud clients like complimentary services, elasticity of resources, easy accessibility through net, etc. From little to massive enterprises poignant towards cloud computing to extend their business and tie-ups with different enterprises [1]. Although cloud computing has huge advantages, cloud user are unwilling to place their confidential or sensitive information, it includes personal health records, emails and government sensitive files. Suppose once information is placed in cloud information center; the cloud consumer lost their direct control over their data sources. The Cloud Service supplier (CSPs) has promise to confirm the information. Security over hold on information of cloud shoppers by using strategies like firewalls and virtualization. These mechanisms wouldn't offer the entire information protection due to its vulnerabilities' over the network and CSPs have full command on cloud applications, hardware and client's information. Encrypting sensitive information before hosting will be information privacy and confidentiality against CSP. A typical drawback with encryption scheme is that it's impractical due to large quantity communication overheads over the cloud access patterns. Therefore, cloud desires secure strategies to storage and management to preserve the information confidentiality and privacy [2].Cloud computing security is that the major concern to be addressed these days. If security measures aren't provided properly for information operations and transmissions then information is at high risk [3].

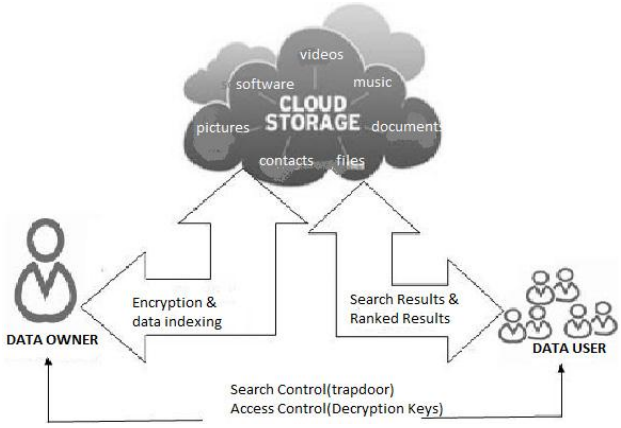

Figure 1.1 Cloud data storage model

2 .LITERATURE SURVEY

A. Proofs of Ownership in Remote Storage Systems Author Shai Halevi Cloud stockpiling frameworks are ending up increasingly famous. A promising innovation that holds their cost down is de duplication, which stores just a solitary duplicate of copying information. Customer side de duplication endeavors to recognize de duplication openings as of now at the customer side and spare the data transmission of transferring duplicates of existing records to the server. In this work we distinguish assaults that endeavor customer side de duplication, allowing an aggressor to access selfassertive size records of different clients in light of a little hash mark of these documents. All the more particularly, an aggressor who knows the hash mark of a record can guarantee the capacitybenefit that it possesses that document; subsequently the server gives the assailant a chance to download the whole record [2].

B. DupLESS: Server-Aided Encryption for De copied Storage Author: MihirBellare and Sriram Keelveedhi.de duplication to spare space by just putting away one duplicate of each record transferred. Should customers oftentimes encode their documents, in any case, reserve funds are lost. Message-bolted encryption (the most exceptional appearance of which is focalized encryption) settles this strain. Notwithstanding it is characteristically powerless against savage - compel assaults that can recoup documents falling into a known set. We propose a design that gives secure de copied capacity contradicting beast drive assaults, and acknowledge it in a framework called DupLESS. In DupLESS, clients scramble the under message-based keys got from a key-server by methods for a truant PRF tradition.It empowers customers to store encoded information with a present administration, have the administration perform de duplication for their benefit, but then accomplishes solid secrecy ensures. We demonstrate that encryption for de copied capacity can accomplish execution and space funds close to that of utilizing the capacity benefit with plaintext data [3].

C. Provable Data Possession at Untrusted Stores Authors: Giuseppe Ateniese We present a model for provable information ownership (PDP) that permits a customer that has put away information at an untrusted server to confirm that the server has the first information without recovering it. The model creates probabilistic confirmations of ownership by examining irregular arrangements of squares from the server, which radically lessens I/O costs. The client keeps up an unfaltering measure of metadata to check the confirmation. The test/response tradition transmits an s strip mall, consistent measure of data, which limits sort out correspondence. In this way, the PDP exhibit for remote data checking supports extensive educational accumulations in comprehensively - dispersed limit structures [4].

D. Remote Data Checking Using Provable Data Possession Authors: Giuseppe Ateniese We proposes a model for provable information ownership (PDP) that can be utilized for remote information checking: A customer that has put away information at an untrusted server can confirm that the server has the first information without recovering it. The model creates probabilistic confirmations of ownership by examining irregular

arrangements of pieces from the server, which radically decreases I/O costs. The customer keeps up a steady measure of metadata to check the verification. The test/reaction convention transmits a little, steady measure of information, which limits organize correspondence. In this way, the PDP show for remote information checking is lightweight and backings vast informational indexes in circulated capacity frameworks. The model is likewise hearty in that it fuses systems for alleviating discretionary measures of information de basement [5]

3. PROPOSED PLAN OF WORK

To solve the problem on exiting system we propose two secure systems Sec Cloud and Sec Cloud + while generated better and efficient system for accessing massive data on cloud. In this, firstly encrypted the plain data file and perform integrity auditing on that encrypted file. Sec Cloud system has achieved both integrity auditing and file de duplication in this process Server doesn't known the contain in file. In other word the functionalities of integrity auditing and secure de duplication are only imposed on plain text.SecCloud + managing de duplication on encrypted files. On other word operation perform on secure file.

Module:

Module 1:- User / End User: - user responsible to upload the Data in cloud and that file send to Auditor.

Module 2: -Auditor: - Auditor check the file of user and check file copy is already present or not and Encryption at file level.

Module 3:- Cloud Server Provider: - CSP check the user details and Encrypted at second level and generated the key.

REQUIREMENTS –

Technology Used –

Language – MATLAB

Front end – MATLAB

Backend – MATLAB Version (13R)

Database – MySQL Version (5.5.16)

System Requirement –

Minimum RAM –60 MB

Hard Disk –2 GB

Processor –I3 Processor

Operating System – Windows XP Service Pack

4. METHODOLOGY

In the proposed scheme, an image owner having a low computational power (e.g., mobile devices) connects to the cloud. The user desires to use the storage capacity and cloud computational power. He/She stores the images securely and wants to retrieve or access them afterwards. The image owner has a collection of his sensitive images. However, the image owner wants that his collection must be secure enough before outsourcing to the cloud for further processing. Figure 3.1 shows the System framework of proposed algorithm. In this figure only encryption algorithm has been explored. User authentication using image captcha is explored in section while reusing the system framework of Figure 3.1. The security enhancing process which performs in image owner's machine uses images obtained from social media sites such as flicker to create masks for the original image with a lightweight encryption algorithm to further enhance the security of the image. The identity of the masks

called flk_ID and the keys which are used for encryption process are kept secret. The image owner creates the key matrix of the keys used for encryption and ID of the masks. Then the key matrix encryption is performed by the image owner. In key encryption λ-values and λ-vector are created with a secret index of the image. More about λ-values and λ-vector is explained in section. Here in this section λ-values and λ-vector are created. After encrypting the image and keys, image owner sends the encrypted image to the cloud for storage with the λ-values and secret index and λ-vectors are sent to the authorized cloud user. When a cloud user wants to retrieve the image, it sends the request to the cloud. For sending the request he/she extracts the keys and creates the index for searching the remotely stored image collection, and then sends the index to the cloud server. The cloud performs the requested computation on the encrypted images and returns the results in the encoded forms to the image owner. The image owner decodes the received resuits to get the image on which the requested computational are done by the cloud.

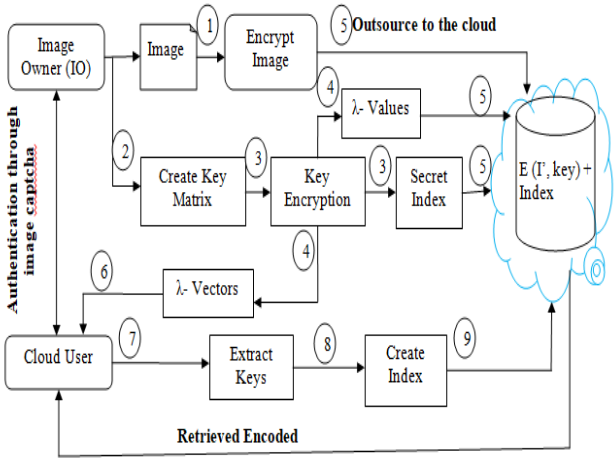

Fig.3.1 .System framework

5.CONCLUSIONS

Aiming at achieving both data integrity and de duplication in cloud. We propose Sec Cloud and Sec Cloud+. Sec Cloud introduces an auditing entity with maintenances of Data Reduce cloud, which helps client generate data tag before uploading as well as audit integrity of data having been stored in cloud. In addition, Sec Cloud (Public Cloud) enables secure de duplication through introducing a Proof of Ownership protocol and preventing the leakage of side channel information in data de duplication. Compared with previous work, the computation by user in Sec Cloud is greatly reduced during the file uploading and auditing phases. File uploading by user then check by auditing phase by auditor. An advanced construction motivated by the fact that customers always want to encrypt their data before uploading, and allows for integrity auditing and secure de duplication directly on encrypted data. This would allow extending the privileges of the authorization model with more actions like modify and delete. Another interesting point is the obfuscation of the authorization model for privacy reasons. Although the usage of pseudonyms is proposed but more advanced obfuscation techniques can be researched to achieve a higher level of privacy.

6. REFERENCES

[1] T.Y. Youn, K.Y. Chang, K. R. Rhee, and S. U. shin, Efficient Client-Side De-duplication of Encrypted Data with Public Auditing in Cloud Storage, IEEE Access, 2018,2169-3536

[2]S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg, —Proofs of ownership in remote storage systems,‖ in Proceedings of the 18th ACM Conference on Computer and Communications Security . ACM, 2011, pp. 491–500.

[3] S. Keelveedhi, M. Bellare, and T. Ristenpart, —Dupless: Serveraided encryption for deduplicated storage,‖ in Proceedings of the 22Nd USENIX Conference on Security, ser. SEC'13. Washington, D.C.: USENIX Association, 2013, pp. 179–194. [Online]. Available:https://www.usenix.org/conference/usenixsecurity13/technicalsessions/presentation/bellare.

[4] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, —Provable data possession at untrusted stores,‖ in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07. New York, NY, USA: ACM, 2007, pp. 598–609.

[5] G. Ateniese, R. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. Peterson, and D. Song, —Remote data checking using provable data possession,‖ ACM Trans. Inf. Syst. Secure., 2011, pp. 12:1–12:34,vol. 14, no. 1.