ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 8, August 2019

A Novel Enhanced Protected Cloud Storage Scheme

Koppu Eswar Prasanth Kumar[1], Prof. Kunjam Nageswara Rao[2],Sitaratnam Gokuruboyina[3],
Prof.K Raja Kumar[4]

M.Tech Student, Department of Computer Science and System Engineering, Andhra University College of Engineering, Visakhapatnam, India[1]

Professor, Department of Computer Science and System Engineering, Andhra University College of Engineering, Visakhapatnam, India[2]

Associate professor, Department of Computer Science and Engineering, Lendi Institute of Engineering and Technology, Vizainagaram, India[3]

Professor, Department of Computer Science and System Engineering, Andhra University College of Engineering, Visakhapatnam, India[4]

ABSTRACT: From the past few years the cloud computing technology is growing rapidly. Withthe heavy growthofdata, cloud storage technology is mainly used.However, the present storage schema, user's data is totally stored in cloud servers.It means that users lose their right of control on their data and face privacy leakage risk. Encryption alone doesn't guarantee protection,thesekindsofmethodscannot efficiently resistattackfromthe inside of cloud server. In order to solve this problem, the proposed algorithm split the user's data into three parts and store the data in three different nodes in the cloud. Hash-Solomoncode algorithm is used to divide data into different parts. It ensure that the original data cannot be retrieved from the partial data. By reasonable allocation of the original data,our scheme can really help in protecting the cloud data. A strong authentication procedure is also used in this paper for better security. In order to reduce the redundant data to store in the cloud, the algorithm restrict the duplicate files to be stored in cloud. Using the safety analysis and experimental evaluation, the feasibility of our scheme is validated, which is truly a better method to existing cloud storage scheme.

KEYWORDS: Cloud Storage, Encryption, Hash-Solomon algorithm.

I. INTRODUCTION

Due to the rapid growthof network bandwidth, the number ofuser'sdataisrising exponentially.User's requirement cannot be fulfilled by the local machine any more. Therefore, people try to find new methods to store their data.Searching for more powerful storage capacity, more number of users select cloud storage. Storing data on a public cloud server is common in the future and the cloud storage technology willbecome popular inafewyears.Cloudstorageisacloud computingsystemwhichprovidesdatastorageand management service.With a cluster of applications, network technology and distributed file system technology, cloud storage makes a large number of different storage devices work together co-ordinately. Nowadays there are a lot of companies providing a variety of cloud storage services, such as Dropbox, Google Drive, iCloud, Baidu Cloud, etc.These companies provide large capacity of storage. However, in cloud storage service still exists a lot of security problems. The privacy problem is mainly important among those security issues. In history, there were a many cloud storage privacy leakage issues. For

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 8, August 2019

example,ApplesiCloudleakageeventin2014,numerousHollywood actresses private photos stored in the clouds were stolen. This event caused an outrage, which in turn causes users' anxiety about the privacy of their data stored in cloud server. As shown in Figure 1, user uploads data to the cloud server directly. Also the Cloud Server Provider (CSP) manage the user's data.

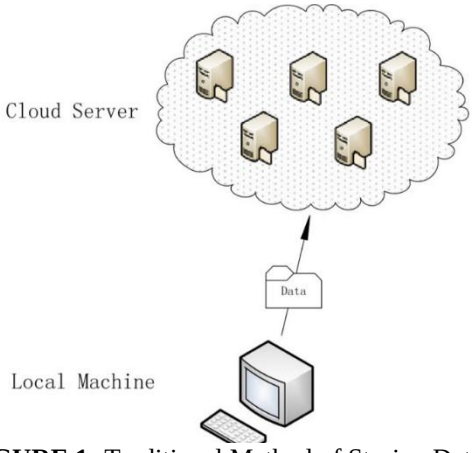


FIGURE 1: Traditional Method of Storing Data in Cloud

In addition,one can say the user loses control over his data, which results in the division of ownership of data. The CSP can freely access and search the data stored in the cloud. Meanwhile the attackers can also attack the CSP server to obtain the user's data. The above two cases both make users fell into the danger of information leakage and data loss. Existing secure cloud storage solutions for the above problems are mainly focused on access restrictions or data encryption. These methods can actually solve most part of these problem.However, any ofthesesolutionscannotsolvethe internal attack well, how the algorithm improves.Therefore we propose a new scheme to efficiently solve the cloud service provider attack.

II. RELATED WORK

The importance of security in cloud storage has attracted a lot of attention no matter in academe or industry. There are a lot of researches about secure cloud storage architectures in recent years. In order to solve the privacy issue in cloud computing, a privacy-preserving and copy-deterrence CBIR scheme using encryption and watermarking techniques. This scheme can protect the image content and image features well from the semi-honest cloud server, and deter the image user from illegally distributing the retrieved images[1].The cloud is semi-trusted and propose a framework for urban data sharing by exploiting the attribute-based cryptography.The scheme they proposed is secure and can resist possible attacks[2].A content-aware search scheme, which can make semantic search smarter. The experiments results show that their scheme is efficient[3]. They consider that in traditional situation, user's data is stored through CSP, even if CSP is trustworthy, attackers can still get user's data if they control the cloud storage management node. To avoid this problem, they propose an encrypted index structure based on an asymmetric challenge-response authentication mechanism. When user requests data from cloud server, the user sends a password to the server for identification. Taking it into consideration that the password may be intercepted, the structure uses asymmetric response mode[4]. The secure core of cloud storage is security and privacy in distributed system. So they propose a secure virtual protection scheme based on SSL and Daoli in paper.By transferring data over SSL and deploying Daoli on the cloud server, the system encrypts data before it is written into the hard disk[5][6]. One can say that the service provider is not complete trusted, so they design a virtual private storage service based on recent developed cryptographic techniques. Such a service achieves the best of both worlds by providing the security of a private cloud and the functionality and cost saving of a public cloud [7].Most of the previous works on the cloud security focus on the storage security rather than taking the computation security into consideration together. Thus they propose a privacy cheating discouragement and secure computation auditing protocol, also named SecCloud which is a first

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 8, August 2019

protocol bridging secure storage and secure computation auditing in cloud and achieves privacy cheating discouragement by designated verifier signature, batch verification and probabilistic sampling techniques[8].

III. METHODOLODY

Firstly user must register with the cloud in order to upload any data into the cloud, the cloud admin has to authenticate the user. A strong authentication procedure is used in the paper. After the registration process is done, the cloud admin has to authenticate the user and the user gets his secret key to his registered mail. Using this secret key only the user can login to his account and can upload any data into the cloud.Even if an attacker tries to login into a user account to download any data he may crack the user's password but he may not knew about the secret key sent to user's mail id.This paper collectively approach the issue of security and performance as a secure Cloud data problem. This paper presents a system that judicially fragments user files into pieces and replicates them at strategic locations within the cloud. The division of a file into fragments is performed using the given user data such that the individual fragments do not contain any meaningful information. Each of the cloud nodes contains a distinct fragment to increase the data security.The proposed scheme fragments and replicates the data file over cloud nodesas shown in figure 2.

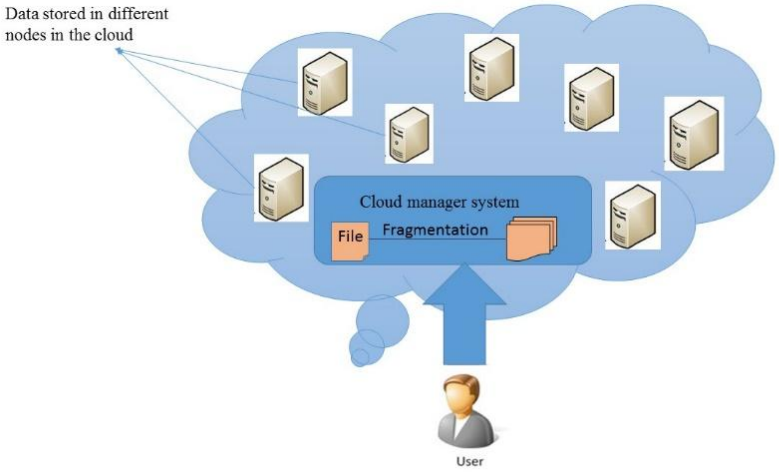


FIGURE 2: User Data Stored In Different Servers in Cloud

Instead of storing the data directly in to the cloud,we divide the data in to three different parts and store them separately in the cloud servers. This scheme is based on the hash-Solomon algorithm, it ensure that the original data cannot be retrieved from the partial data. By reasonable allocation of the original data,our scheme can really help in protecting the cloud data.

For example, after a document is divided, each part of data blocks still contains the information of the document. For some high privacy demanding documents, it is obviously should not available. So we add a hash transform before dividing to disrupt the sequence of original data and save the relevant hash information. As shown in figure 3, the original code (a) divides a sentence into different fragments according to original sequence However, the hash code (b)divides the sentence into different fragments according to random sequence. There by Hash-Solomon code improves the privacy protection and prevents the attacker from getting fragmentary information.

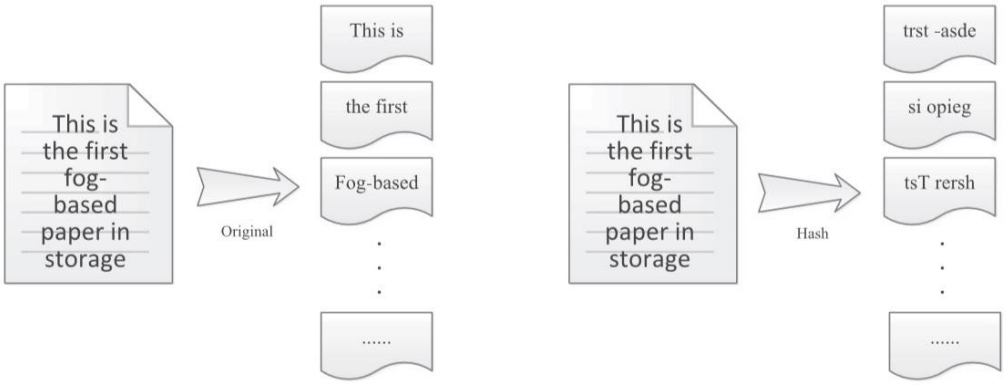
ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 8, August 2019



(a) Original transform(b) Hash transform

FIGURE 3:difference between the Original transform andHash transform

It is impossible to recover the original data with any single server's data. Our proposed frameworkmostly solvestheleakageof user'sprivacy.Furthertakingaworsecase,iftheattackerisbrilliantenough, he steals data blocks from three servers. The attacker might think he can recover original data. But here is the encoding problem. Assuming that the attacker steals enough data, but ifhe doesn't have the information contained in the encoding matrix, he can hardly recover user's original data from the scattered data blocks. If he wants to crack the encoding matrix, the degree of difficulty is shown in the Table 1. If the encoding matrix used in the algorithm is 4x4, it means the number of elements in the Galois filed is 2^4 and we assume the number of data blocks is 6 then the number of attempts required to decode is 256^3, if we use GF (2^8) and number of data blocks as 6 then the number of attempts required to decode is 256^6.

GaloisField	Number of data blocks (k)	Time of exhaustion
GF(2^4)	6	256^3
GF(2^8)	6	256^6
GF(2^16)	6	256^12

TABLE 1: Cracking difficulty degree

A good system with high storage efficiency can save storage capacity as much as possible. We propose a new method to save the storage capacity. Our algorithm detects the duplicate data and notices the user about it. If a user try to upload the same data to the cloud again he is notified with the message "file is already uploaded" thereby saving the amount of data stored in the cloud and reducing the redundancy.

IV. EXPERIMENTAL RESULTS

In this paper experiments are done on text document and shown how the data is encoded and hashed before uploading to the cloud,In the experiment we divide the data into not only three different parts but also divides in many parts to test the relationship between the encoding,decoding time with the divided parts,to check the efficiency of the algorithm.

Consider the change of storage efficiency and the coding efficiencywhenthenumberofk increases.Apparently, the tendency of storage efficiency is contrary to the tendency of coding. It means there must be a value of k which can achieve a best efficiency of the whole system.Figure 4(a) shows the tendency of encoding time with different number of data blocks. When the number of data blocks k increases, the encoding time grows

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

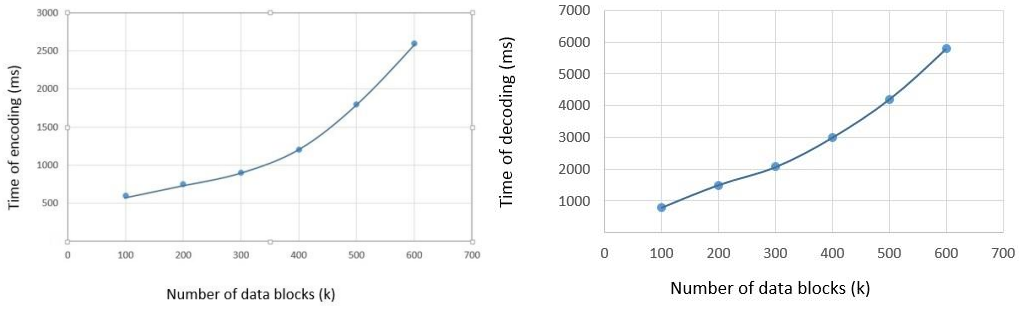
International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 8, August 2019

exponentially.Accordingly,inthereal scenario,one shouldconsider delay degree that user can ensure and adjust the value of k according to the user's machine performance dynamically.



(a)Growth of encoding time with respect to k (b) Growth of decoding time with respect to k

FIGURE 4: Shows the Relationship between encoding timeand decodingtime with respect to number of data blocks (k)

As shown in the Figure 4(b) see how the decoding time increases with the increase in the number of data blocks. When the number of data blocks k increases from 100 to 600, the decoding time increases at express speed. One can see, the decoding process costs more time than the encoding process does, so one should pay more attention to enhance decoding efficiency in real scenario.

V. CONCLUSIONS

The development of cloud computing brings us a lot of benefits.Cloud storage is a convenient technology which helps users to expand their storage capacity. However, cloud storage also causes a series of secure problems. When using cloud storage, users do not actually control the physical storage of their data and it results in the separation of ownership and management of data.In order to solve the problem of privacy protection in cloud storage, this paper propose a framework that fragments data into different parts and design a Hash-Solomon algorithm. Through the theoretical safety analysis, the scheme is proved to be feasible. By allocating the ratio of data blocks stored in different servers reasonably, this can ensure the privacy of data in each server. On another hand, cracking the encoding algorithm is a way difficult. Besides, using hash transformation can protect the fragmentary information. Through the experiment test, this scheme can efficiently complete encoding and decoding without influence of the cloud storage efficiency.

REFERENCES

[1] Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacypreserving and copy-deterrence content-based image retrieval scheme in cloud computing," IEEE Trans. Inf. Forensics Security, vol. 11, no. 11, pp. 2594–2608, Nov. 2016.
[2] J. Shen, D. Liu, J. Shen, Q. Liu, and X. Sun, "A secure cloud-assisted urban data sharing framework for ubiquitous-cities," Pervasive Mobile Compute., vol. 41, pp. 219–230, 2017.
[3] Z.Fu,F.Huang,K.Ren,J.Weng,andC.Wang,"Privacy-preservingsmart semantic search based on conceptual graphs over encrypted outsourced data,"
IEEE Trans. Inf. Forensics Security, vol. 12, no. 8, pp. 1874–1884, Aug. 2017.
[4] J. Hou, C. Piao, and T. Fan, "Privacy preservation cloud storage architecture research," J. Hebei Acad. Sci., vol. 30, no. 2, pp. 45–48, 2013.
[5] Q. Hou, Y. Wu, W. Zheng, and G. Yang, "A method on protection of user data privacy in cloud storage platform,"J.Comput.Res.Develop.,vol.48, no. 7, pp. 1146–1154, 2011.
[6] P. Barham et al., "Xen and the art of virtualization," ACM SIGOPS Oper. Syst. Rev., vol. 37, no. 5, pp. 164–177, 2003.
[7] G.Kulkarni,R.Waghmare,R.Palwe,V.Waykule,H.Bankar,andK.Koli, "Cloud storage architecture," in Proc. 7th Int. Conf. Telecommun. Syst., Serv.,
Appl., 2012, pp. 76–81.
[8] L. Wei et al., "Security and privacy for storage and computation in cloud computing," Inf. Sci., vol. 258, pp. 371–386, 2014