International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 03 Issue 14
October2016

Provable Multicopy Data Possession in Cloud Computing System Applications

Kumari Jelli
Asst.Professor, Department Of Cse
Vignana Bharathi Institute Of Technology
J.Rajashekar
Asst.Professor, Department Of Cse
Vignana Bharathi Institute Of Technology
S.Adilakshmi
Asst.Professor, Department Of Cse
Vignana Bharathi Institute Of Technology

Abstract: In Provable data possession scheme the client outsources the data to the remote cloud service provider which is in charge for storing and maintaining the data. Customers can hire the storage infrastructure from the cloud carrier providers to store their data by way of paying prices. Hence the clients must verify whether the server possesses the original data and must have powerful assurance that the service provider is storing all of the data copies issued as per the contract. In this process the issues similar to data security, data dynamics, integrity security and multi cloud storage have remained the essential undertaking. The data owner update one of the copies from Cloud Service Provider and the remaining data must be updated by the Cloud Service Provider. By the way Message Authentication Code is also been updated and then the client can send the request and receive the data from the Cloud Service Provider. By using the Secure Hash Algorithm-1 the client can check the integrity of the data, whether it is updated or not. This mechanism will increase the security when compared to the existing process.

Key Words: Provable data possession (PDP), storage security, Cloud Service Provider(CSP), Cloud Computing, Dynamic Data.

I. INTRODUCTION

Presently a day's Outsourcing information to a remote cloud administration suppliers permits association to stores more information on the CSP than on private PC frameworks. Such outsourcing of data storages enable organizations to focuses on development and soothe the weight of steady server overhauls and other registering issues. The privacy issue can be taken care of by scrambling touchy information before outsourcing to remote server.

All things considered, its crucials requests of client to have solid confirmation that the cloud servers still have their information and it's being tamparated with or mostly erase over times. Therefore, numerous specialists have concentrated on the issue of provable data possessions (PDP) and we propose distinctive techniques to review the information put away on remote servers. The prior Advanced Encryption system (AES) makes use of a combination of Exclusive-OR (XOR), octet substitution, row and column rotations, and a mix column. AES allow block sizes of 128, 168, 192, 224 and 256 bits, and a key measurement of 128 bits. Each byte within the matrix is up-to-date utilising an eight bit substitution box,which is derived from the multiplicative inverse of nonlinear houses. The inverse function is combined with an invertible affine transformation to hinder attacks established on simple algebraic homes. The bytes in each row are shifted in a cyclic method making use of a specified offset, through maintaining the primary row unchanged. The demerits of the prevailing procedure entails the important thing size of the existing AES approach was too small. knowledge stored in the CSPs are susceptible to insecurity. the key size of the MAC, MD-5 is decrease than the Sha-1 cloud provider providers will create the trust for the CSP among algorithm.

II. RELATED WORKS

These schemes was applicable for the data present in the hierarchical cloud. The performance of the proposed work was proved using its ability to proof

unforgeability andin distinguishability. Yang, et al[5] constructed a novel design for effective public auditing. The proposed framework shared data over the cloud by preserving the identity and traceability. The blind signature approach was adopted to provide data privacy and to generate authenticators.Wei, et al[6] presented the efficient and dynamic multi copy possession scheme with their optimal features. The data owner can utilize Fully Homomorphic Encryption (FHE) algorithm for multi copy generation. It allowed dynamic block data operation. The public verification of third party auditor became possible with the proposed scheme. It was able to resist the forgery, other attacks and replacements.Barsoum[7] proposeda pairing-based provable multi-copy data possession (PB-PMDP) scheme,in which, the strategies to be followed for replication, security and integrity of outsourced data in the cloud were discussed. The creation of multiple copies of data was verified over the un trusted cloud servers. It gave the user with the access to data as well as to archive the data desired by the data owner.

Mukundan, et al[8] presented Dynamic Multi-Replica Provable Data Possession Scheme (DMR-PDP) that focused on the dynamic files along with the static data files and to reduce the cost incurred in this proposed scheme. It ensured to check the honesty of the CSP.Sookhak, et al[9] reviewed the auditing of data in the distributed cloud network. The auditing was classified based on the erasure coding, network coding and replication. The study illustrated the uniqueness and similarities of various techniques along with the issues associated with the systems.

Zhao, et al [10]introduced a fully homomorphic encryption algorithm to address the issue of security in cloud computing. The algorithm helped to provide security along with the information retrieval from the encrypted data. Thus the data storage and data transmission was safe. Tan and Teh[11] presented performance evaluation of the resources in the virtual machines by applying machine learning technique and linear regression analysis with reference to TPC-H benchmark data. The real data is not involved hence it was said to be secure during evaluation.Huang, et al[12] generated a novel code to work along with Dynamic Provable Data Possession (DPDP) scheme to overcome the data security problem persisting in the network. The dynamic operations of the proposed scheme is a memory adversary model that improved the system performance as well as the viability. Du, et al[13] formulated the Proofs of Ownership and Retrievability (PoOR) model for mutual validation of the network. Erasure coding was utilized in order to prove the recoverability and security of the system. The storage resource wasmaintained optimally using merkle tree and homomorphic verifiable tags.

Mohan and Katti[14] proposed a new provable secure sigma Provable Data Possession (PDP) scheme to provide computation and communication without complexity. A challenge response protocol helped to transmit small and constant amount of data.Sontakke and Manjrekar[15] suggested multi owner with sharing approach. The work identified the corrupted data copy and corrected it before performing the dynamic operation. The work allowed many owners for the single data on the sharing basis. It verified the data integrity and reconstructed the corrupted copies of data using the Attribute based encryption standard.

III. PROPOSED METHOD

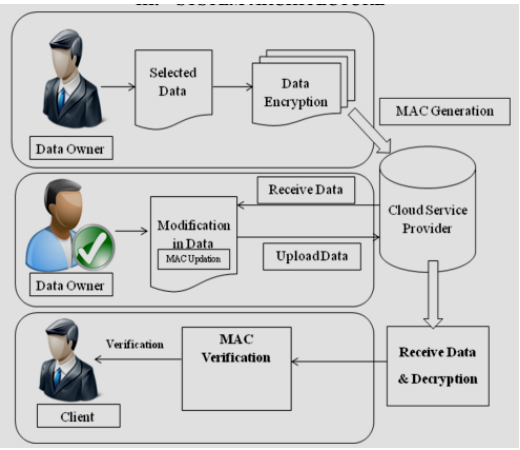

Fig1. System Architecture

A. Data Owner Registration

Data proprietor have got to register the main points. And then pick the data. The data are splitted. A data owner that may be an organization must hold the data stored within the clouds database. A Cloud service provider maintains the cloud servers and

presents paid storage space to the user. A user is a group of owner and clients having the correct to access the far flung server and its data.

B. Data Uploading

MAC generated for the splitted data then the data are encrypted and uploaded into the cloud service provider's storage space. The data owner has a file entailing of multi blocks and the CSP bids to store the multi copies of the owner file on various servers. The critical data should be duplicated on multiple servers. On the other hand, non-critical, reproducible data are stored at condensed levels of redundancy. For data confidentiality, the owner encrypts his data before outsourcing to CSP.

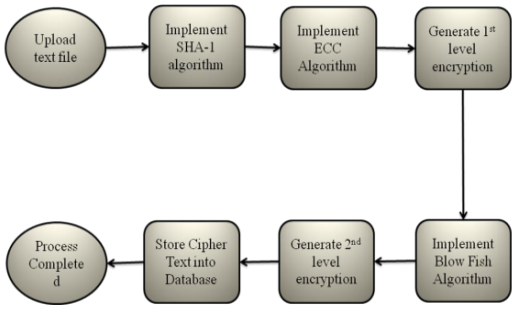

Fig2. Multilevel Encryption

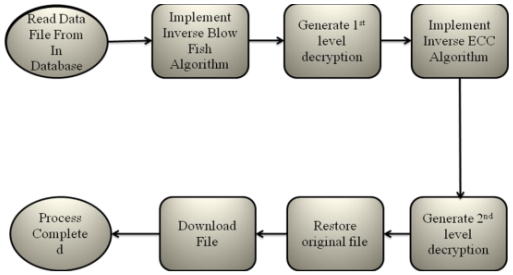

Fig 3. Multilevel Decryption

C. Users Request

Users send the invitation to the cloud service provider. Cloud service providers send the associated data to the user. An authorized user sends a data-access request to the CSP and receives a file copy in an encrypted form. Decryption is done by using a secret key shared with the owner. The work of the servers should be systematized using the load balancing mechanism. The data-access request is directed to the server with the lowest congestion.

D. Users Accessing Data

User get the key from the data owner and get the encrypted data from the cloud service provider then decrypts the data. The authorized users have the rights to admission the owner file stored on the CSP. A new PDP scheme funds outsourcing of multi-copy dynamic data. Data owner having the capability to updating, scaling and access the data copies stored in the remote servers.

IV. CONCLUSION

The proposed Map-based Provable Multi Copy Dynamic data Possession, MB-PMDDP makes use of blowfish encryption reduces the cost of storage and computations worried in it. The user desires to register in the proposed scheme and add the data that needs to be stored within the cloud servers. The data are split and coded using SHA1 to have exceptional data integrity. The blowfish encryption enables the data owner to protect and share keys for authenticating the approved users.

REFERENCES

[1] Bing Rao, Zhigang Zhou, Hongli Zhang, Shuofei Tang and Renfu Yao "Outsourcing Cloud Data Privacy-Preserving Based on Over-Encryption," Communications in Computer and Information Science pp 109-116.

[2] Swapna Lia Anil and Roshni Thanka "A Survey on Security of Data outsourcing in Cloud," International Journal of Scientific and Research Publications, Volume 3, Issue 2, February 2013.

[3] Y. Deswarte, J.-J. Quisquater, and A. Saïdane "Remote integrity checking," in Proc. 6th Working Conf. Integr. Internal Control Inf. Syst. (IICIS), 2003, pp. 1–11.

[4] Yongjun Ren, Zhenqi Yang, Jin Wang and Liming Fang "Attribute based Provable Data Possession in Public Cloud Storage," Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2014.

[5] G. Ateniese "Provable data possession at untrusted stores," in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), New York, NY, USA, 2007, pp. 598–609.

[6] Giuseppe Ateniese, Randal Burns, Reza Curtmola, Joseph Herring, Osama Khan, Lea Kissner, Zachary Peterson and Dawn Song "Remote Data Checking Using Provable Data Possession," ACM Transactions on Information and System Security, Vol. 14, No. 1, Article 12, Publication date: May 2011.

[7] F. Seb´e, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J.-J. Quisquater, "Efficient remote data

possession checking in critical information infrastructures," IEEE Trans. on Knowl. and Data Eng., vol. 20, no. 8, 2008.–247.

[8] R. Mukundan, S. Madria, M. Linderman, and N. Rome, "Replicated Data Integrity Verification in Cloud," IEEE Data Eng. Bull., vol. 35, pp. 55-64, 2012.

[9] M. Sookhak, A. Gani, H. Talebian, A. Akhunzada, S. U. Khan, R. Buyya, et al., "Remote data auditing in cloud computing environments: a survey, taxonomy, and open issues," ACM Computing Surveys (CSUR), vol. 47, p. 65, 2015.

[10] F. Zhao, C. Li, and C. F. Liu, "A cloud computing security solution based on fully homomorphic encryption," in 16th International Conference on Advanced Communication Technology (ICACT), 2014, 2014, pp. 485-488.

Author's Profile

Kumari Jelli working as Asst.Professor, Department of CSE in **Vignana Bharathi Institute Of Technology.**

J.Rajashekar working as Asst.Professor, Department of CSE in **Vignana Bharathi Institute Of Technology.**

S.Adilakshmi working as Asst.Professor, Department of CSE in **Vignana Bharathi Institute Of Technology.**