International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 04 Issue-17
December 2017

Efficient Way Of Verifying Multiple Copies Of Data In Cloud Servers

M. Swetha, G. Sravan Kumar, Dr.Suresh Akella

[1]M.Tech Computer Science Engineering Sreyas Institute of Engineering and Technology, Beside INDU Aranya,Nagole, Hyderabad

[2]B.Tech.,M.Tech. Associate Professor, Department of Computer Science And Engineering Sreyas Institute of Engineering and Technology, Beside INDU Aranya,Nagole, Hyderabad

[3]Principal Sreyas Institute of Engineering and Technology, Beside INDU Aranya,Nagole, Hyderabad

Abstract: *In Provable data possession theme the client outsources the data to the remote cloud service provider that is responsible 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 exploitation the Secure Hash Algorithm-1 the client will check the integrity of the data, whether or not it's updated or not. This mechanism can increase the safety in comparison to the present method.*

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

I. INTRODUCTION

Cloud Service Provider (CSP) is allows store more data on private computer system. The data storage infrastructure to store and retrieve data and it store unlimited amount of data. This is from of cloud computing that provides virtualized computing resources over the internet. This model is thirdparty provider hosts hardware, software, server, storage and other infrastructure component on behalf of its users. The customers pay on a per-use basis, typically by the hour, week or month. Some provider also charge customers based on the amount of virtual machine space they use. PDP is technique for validating remote data integrity checking is a crucial technology in cloud computing. The two provably-secure PDP schemes that are more efficient than previous solutions, even when compared with schemes that achieve weaker guarantees. In particular, the overhead at the server is low (or even constant), as opposed to linear in the size of the data. Experiments using our implementation verify the practicality of PDP and reveal that the performance of PDP is bounded by disk I/O and not by cryptographic computation. In remote data integrity checking protocols, the client can challenge the server about the integrity of a certain data file, and the server generates responses proving that it has access to the complete and uncorrupted data. The basic requirements are that the client does not need to access the complete original data file when performing the verification of data integrity, and that the client should be able to verify integrity for an unlimited number of times. Juels et al describe a “proof of retrievability” (PoR) model and give a more rigorous proof of their scheme. In this model, spot-checking and error-correcting codes are used to ensure both “possession” and “retrievability” of data files on archive service systems. Specifically, some special blocks called “sentinels” are randomly embedded into the data file F for detection purpose and F is further encrypted to protect the positions of these special blocks. However, like [11], the number of queries a client can perform is also a fixed priori and the introduction of pre-computed “sentinels” prevents the development of realizing dynamic data updates. In addition, public verifiability is not supported in their scheme. Although schemes with private verifiability can achieve higher scheme efficiency, public verifiability allows anyone, not just the client (data owner), to challenge the cloud server for correctness of data storage while keeping no private information.

Presently a day’s Outsourcing data to a remote cloud administration providers permits association to stores more data 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 data before outsourcing to remote server. All things considered, its crucials requests of client to have solid confirmation that the cloud servers still have their data 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 data 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 knowledge stored in the CSPs are susceptible to was too small. 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.

Bing Rao, Zhigang Zhou, Hongli Zhang, Shuofei Tang and Renfu Yao, Outsourcing Cloud Data Privacy-Preserving Based on Over-Encryption[1]. Cloud computation allows the users with limited computing power outsource their data to the cloud of large-scale computing power through payment method. However, the security issue has been always the obstacles to the widely use of the computing outsourcing, especially when the end-user’s privacy data need to be processed on the cloud. Secure outsourcing mechanisms are in great need to not only protect privacy data, but also protect customers from malicious behaviors by validating the computation result. A mechanism of general secure computation outsourcing was recently shown to be feasible in theory, but to design mechanisms that are practically efficient is a very challenging problem. General research is based on a basic model. The model we used in this paper including Data Owner (DO), Cloud Service Provider (CSP) and End-User (EU). Focus on considering the DO, CSP and EU. Over-encryption is a good method to protect the security of the users’ data. Our proposal is based on the application of selective encryption as a means to enforce authorizations. Two layers of encryption are imposed on the data blocks. This paper talks about the over-encryption mechanism and proposes a novel over-encryption mechanism which can protect the security of the data on the Cloud. Last, we do some experiments to verify the performance of our mechanism.

Yongjun Ren, Zhenqi Yang, Jin Wang and Liming Fang, Attribute based Provable Data Possession in Public Cloud Storage[2]. Cloud storage is now an important development trend in data technology. To ensure the integrity of data storage in cloud storing, researchers have present some provable data possession (PDP) schemes. In some cases, the ability to check data possession is delegated by data owners. Hence, the delegable provable data possession and proxy provable data possession are proposed. However the PDP schemes are not secure since the proxy or designated verifier stores some delegation data in cloud storage servers. In this paper, we propose an attribute based provable data possession scheme, which utilizes attribute based signature to construct the homomorphic authenticator. In the scheme, the homomorphic authenticator contains an attribute strategy. Only the verifier, who satisfied the strategy, can check the data integrity. In particular, the cloud storage service (CSS) in our scheme is stateless and independent of verifier. Moreover the scheme has more security features, including strong anonymity, unlink ability and conspiring to resistance.

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.

III. PROPOSED METHOD

In proposed system uploaded data are stored in multiple server (Multi copy).In this system one scheme and three algorithms were used. They are KeyGen, CopyGen, and TagGen. If user upload the data, automatically prepare three copies then stores that data in three servers for security and to avoid server overload. Those copies are encrypted so that

cloud service provider or any others can’t hack the data. When user uploads the data, servers automatically convert it to zip format. So servers reduce the file size automatically. User shares the file to authorized user.

Then authorized user send the file request to cloud server again, server send the encrypted data to authorized use and authorized user get the decrypt key from data owner. In this system AES algorithm is used for data security.

Proposed System Advantages:

•Multicopy Data reduce access time and communication cost for user.

•If one copy is corrupted it will be redirected to another server and the file can be downloaded.

•Convert Zip format upload the data.

•In this system used AES algorithm. It is most secure 256-bit key length.

Algorithms

(PK, SK) ← KeyGen(). This algorithm is run by he data owner to generate a public key PK and a private key SK. The private key SK is kept secret by the owner, while PK is publicly known. Ẽ← CopyGen (CNi , E)1≤i≤n. This algorithm is run by the data owner. It takes as input a copy number CNi and a file F, and generates n copies Ẽ= {Ẽi} 1≤i≤n. The owner sends the copies Ẽ to the CSP to be stored on cloud servers.Φ← TagGen (SK, Ẽ). This algorithm is run by the data owner. It takes as input the private key SK and the file copies Ẽ, and outputs tags/authenticators set Φ, which is an ordered collection of tags for the data blocks. The owner sends Φ to the CSP to be stored along with the copies Ẽ.

IV. CONCLUSION

In the existing system the data's were send though email. But the user may not know whether he/she got the mail he/she only know when logged on to their mail-id, by connecting with the internet.But in our proposed scheme, the first is to address multiple copies of dynamic data. The communication between the authorized users and the CSP is measured in our system, where the authorized users can effortlessly access a data copy received from the CSP using a single secret key shared with the data owner. Furthermore, the proposed scheme supports public verifiability, allows arbitrary number of auditing, and allows possession-free verification where the verifier has the capability to verify the data integrity even though they neither possesses nor retrieves the file blocks from the server.

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

[3] 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.

[4] 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 Data and System Security, Vol. 14, No. 1, Article 12, Publication date: May 2011.

[5] 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.

[6] 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.

[7] 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.

[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.