Map Based Dynamic Data Possession Using Cloud Service Providers

G. Jyothsna
M.Tech Student, Department of CSE, AVN Institute of Engineering & Technology, India.

G. Dayakar
Associate Professor, Department of CSE, AVN Institute of Engineering & Technology, India.

Dr. Shaik Abdul Nabi
Professor, Head of CSE Department, AVN Institute of Engineering & Technology, India.

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 will rent the storage infrastructure from the cloud carrier providers to store their data by method of paying costs. Hence the purchasers should verify whether or not the server possesses the initial data and should have powerful assurance that the service provider is storing all of the data copies issued as per the contract. During this method the problems just like data security, data dynamics, integrity security and multi cloud storage have remained the essential endeavor. The data owner update one in every of the copies from Cloud Service provider and therefore the remaining data should be updated by the Cloud Service provider. By the method Message Authentication Code is additionally been updated then the client will 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.

Index Terms – Cloud Service Provider, Secure Hash Algorithm.

1. INTRODUCTION

Cloud Service provider (CSP) is permits store additional knowledge on non-public automatic data processing system. The data storage infrastructure to store and retrieve data and it store unlimited quantity of knowledge [1]. this can be from of cloud computing that has virtualized computing resources over the net. This model is third party provider hosts hardware, software, server, storage and different infrastructure part on behalf of its users. the purchasers pay on a per-use basis, usually by the hour, week or month. Some provider conjointly charge customers supported the quantity of virtual machine area they use. PDP is technique for confirmative remote knowledge integrity checking could be a crucial technology in cloud computing. the 2 provably-secure PDP schemes[2] that square measure additional economical than previous solutions, even compared with schemes that succeed weaker guarantees. especially, the overhead at the server is low (or even constant), as opposition linear within the size of the data. Experiments victimization our implementation verify the utility of PDP and reveal that the performance of PDP [2] is finite by disk I/O and not by cryptanalytic computation. In remote knowledge integrity checking protocols, the client will challenge the server regarding the integrity of an exact record, and also the server generates responses proving that it's access to the whole and uncorrupted knowledge. the fundamental necessities square measure that the client doesn't have to be compelled to access the whole original record once performing arts the verification [3] of knowledge integrity, which the client ought to be ready to verify integrity for a limiteless range of times. Juels et al describe a “proof of retrievability” (PoR) model and provides a additional rigorous proof of their theme. during this model, spot-checking and error-correcting codes square measure accustomed guarantee each “possession” and “retrievability” of knowledge files on archive service systems. Specifically, some special blocks known as “sentinels” square measure every which way embedded into the data file F for detection purpose and F is additional encrypted to safeguard the positions of those special blocks. However, like [6], the amount of queries a client will perform is additionally a set priori and also the introduction of pre-computed “sentinels” prevents the event of realizing dynamic knowledge updates. additionally, public verifiability isn't supported in their theme. though themes with non-public verifiability can do higher scheme potency, public verifiability permits anyone, not just the client (data owner), to challenge the cloud server for correctness of data storage while keeping no private data. Presently a day’s Outsourcing data to a remote cloud administration providers permits association to stores more data on the CSP [4] 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) [2] and we propose distinctive techniques to review the data put away on remote servers. The prior Advanced Encryption [5] 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 [4] 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.

2. RELATED WORK

1. 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 [5]. 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 [6] 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[4] 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.

2. 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 [7] 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.

3. G. Ateniese, Provable data possession at untrusted stores[3].

We introduce a model for provable data possession (PDP) that allows a client that has stored data at an untrusted server to verify that the server possesses the original data without retrieving it. The model generates probabilistic proofs of possession by sampling random sets of blocks from the server, which drastically reduces I/O costs.

The client maintains a constant amount of metadata to verify the proof. The challenge/response protocol transmits a small, constant amount of data, which minimizes network communication. Thus, the PDP model for remote data checking supports large data sets in widely-distributed storage systems. We present two provably-secure PDP [3] 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.

3. SYSTEM WORK

In this paper for implementation of provable data possession can be done by the following:

A. Data Owner Registration

B. Data Uploading

C. Users Request

D. Users Accessing Data

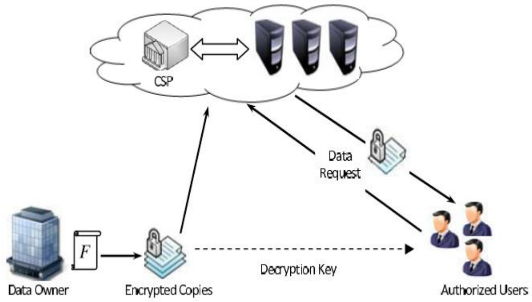

Fig. 1: System Architecture

DATA OWNER REGISTRATION: Data men of affairs have gotten to register the most points. Then decide the info. A knowledge owner which will be a company should hold the info hold on among the clouds info. A cloud service [8] provider maintains the cloud servers and presents paid space for storing to the user. A user may be a cluster of owner and clients having the proper to access the far off server and its data.

DATA UPLOADING: Mac generated for the splitted data then the info are encrypted and uploaded into the cloud service provider's space for storing. The info owner contains a file entailing of multi blocks and also the csp [4] bids to store the multi copies of the owner file on varied servers. The vital data ought to be duplicated on multiple servers. On the opposite hand, [10] non-critical, reproducible data are hold on at condensed levels of redundancy. For data confidentiality, the owner encrypts his data before outsourcing to csp.

USERS REQUEST: Users send the invite to the cloud service provider. Cloud service providers send the associated data to the user [9]. A certified user sends a data-access request to the csp and receives a file copy in an encrypted type. Decoding is completed by employing a secret key shared with the owner. The work of the servers ought to be systematic exploitation the load equalization mechanism. The data-access request is directed to the server with all-time low congestion.

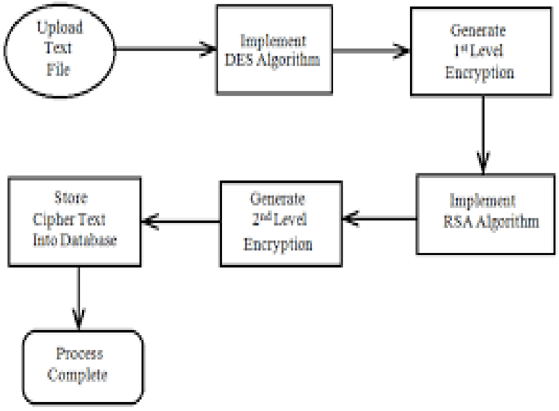
Upload Text File
Implement DES Algorithm
Generate 1st Level Encryption
Implement RSA Algorithm
Generate 2nd Level Encryption
Store Cipher Text Into Database
Process Complete

Fig. 2: Multilevel Encryption

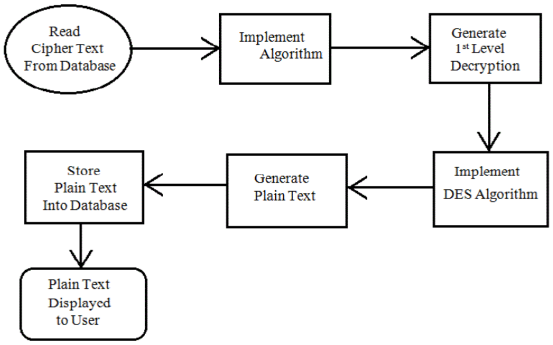
Read Cipher Text From Database
Implement Algorithm
Generate 1st Level Decryption
Implement DES Algorithm
Generate Plain Text
Store Plain Text Into Database
Plain Text Displayed to User

Fig. 3: Multilevel Decryption

USERS ACCESSING DATA: User get the key from the data owner and find the encrypted data from the cloud service [8] provider then decrypts the info. The licensed users have the rights to admission the owner file hold on on the csp. A brand new pdp theme funds outsourcing of multi-copy dynamic data. Data owner having the aptitude to change, scaling and access the info copies hold on within the remote servers.

4. CONCLUSION

In the existing system the data's were send although email. However the user might not understand whether or not he/she got the mail he/she solely understand once logged on to their mail-id, by connecting with the web. But in our projected Map-based Provable Multi Copy Dynamic information Possession, MB-PMDDP makes use of blowfish cryptography reduces the price of storage and computations distressed in it. The user needs to register within the projected theme and add the information that must be keep at intervals the cloud servers. {the information|the info|the information} square measure split and coded victimization SHA1 to own exceptional data integrity. The blowfish cryptography permits the information owner to guard 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 Data 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] F. Seb´e, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J.-J. Quisquater, "Efficient remote data possession checking in critical data 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.

Authors

G. Jyothsna, B.Tech, is currently pursuing M.Tech in the stream of Computer Science and Engineering, AVN Institute of Engineering & Technology, Ibrahimpatnam, Hyderabad, TS, India. She has attended workshops on Network implementation and security. Her areas of interest are OOPS and Data mining.

G. Dayakar is working as Associate Professor in Dept. of CSE, AVN Institute of Engineering & Technology, Hyderabad, T.S, India. He completed his B.Tech (Computer Science and engineering) from JNTU, Hyderabad. He has completed his M.Tech from JNTU Hyderabad campus, India. He is a certified professional in Teaching by National Institute of Technical Teachers Training & Research (Govt of India).

He is having 10 years of Teaching Experience in various Engineering Colleges. His expertise areas are Design and Analysis of Algorithms, Data Structures & UNIX Networking Programming and cloud computing.

Dr. Shaik Abdul Nabi is working as professor & Head of the Dept. of CSE and vice principal in AVN Inst. Of Engg. & Tech, Hyderabad, T.S, India. He completed his B.E (Computer Science and engineering) from Osmania University, Hyderabad. He has completed his M.Tech from JNTU Hyderabad campus and he received Doctor of Philosophy (PhD) in the area of Web Mining from Acharya Nagarjuna University, Guntur, AP, India. He is a certified professional by Microsoft.

He is having 17 years of Teaching Experience in various Engineering Colleges. He has published 18 publications in International / National Journals and presented 10 papers in National / International conferences. His expertise areas are Data warehousing and Data Mining, Data Structures & UNIX Networking Programming, Cloud Computing and Mobile Computing.