ISSN: 2278 – 1323
International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)
Volume 5, Issue 9, September 2016

Efficient & Secure Privacy Preserving Public Auditing Scheme For Cloud Storage

N.Ahamadunnisa[1], S. Vasundara[2]
[1]*M.Tech, Dept of CSE, JNTUA, AP, India.*
[2]*Professor, Dept of CSE, JNTUA, AP, India.*

***Abstract*—To regenerate the data at corrupted servers in the cloud storage in absence of data owners, we propose public auditing scheme. Public Auditing Scheme includes TPA (Third Party Auditor) and a Semi Trusted Proxy Server to improve the integrity of data and to regenerate sthe data. To check the integrity of data, TPA done the periodical verification of servers in the cloud. If the faulty server is found it sends it to the proxy to regenerate. The semi trusted proxy server also make the data owners free from online burden. A homomorphic novel authenticator which uses the BLS(Boneh Lynn Schamm) signature is designed which is more appropriate for regenerating the data at corrupted servers. In this privacy preserving is also allowed by using the encryption mechanism. The coefficients of the data are masked with the keyed PRF(Pseudo Random Function) at the initial phase of the auditing scheme which increase the security level in the cloud storage. Extensive comparison is done to evaluate the performance of our scheme.**

***Index Terms*— regenerating data, cloud storage, Public auditing, Privacy Preserving, semi trusted proxy.**

I.INTRODUCTION

Cloud computing offers many services like storage as a service, software as a service, Infrastructure as a service. In this paper we discuss on cloud storage[1] as a service, it has apparent benefits :the data can be accessed without location dependence, the investment on the hardware for storage can be decreased.But this data hosting service has security threats on the users data.

Mechanisms are proposed for checking the integrity[2] of the data under different systems and security models. The two mechanisms PDP (Provable Data Possession) and POR (Proof Of Retrievability) are applied for single server scenario .By using these two mechanisms the correctness of the data in the cloud is checked. The data in the cloud is striped and stored across multi servers[8] by using redundancy schemes like replication, erasure codes[3] and regenerating code.

Regenerating of code at faulty server is done by using the functional repair strategy in which high probability data blocks are generated. This mechanism is already applied for multi server but they used the private auditing. In Private auditing only the data owners who put the data in the cloud are allowed to check the integrity of the data and to repair the faulty servers. If the out sourcing data in the cloud is in large size then the task of auditing and repairing the corrupted data for users can be expensive. The complexity of the users has to be decreased in order to increase the cloud storage service.

Public auditing scheme for regeneration of data in the servers and integrity verification are implemented by semi trusted proxy server and TPA(Third Party Auditor). A homomorphic authenticator based on BLS signature is designed which is appropriate for regenerating data at faulty servers. The authenticators can be computed efficiently by using the linear subspace of regenerating code. To avoid the leakage of the original data the coefficients are encrypted with keyed random function.

Regenerating data:

Regenerating of data at faulty server done by using two repair strategies.

1. Exact repair strategy
2. Functional repair strategy.

Exact repair strategy:

In exact repair strategy ,if any block is corrupted in the server ,the repaired server requires the exact copy of the corrupted block. As exact block is regenerated, the integrity of the data is maintained but it uses higher bandwidth.

Functional repair strategy:

In functional repair strategy, if any block is corrupted in the server, the exact replica of block is not generated yet a new block is generated and sent to the server by connecting to other healthy servers in the cloud. The block which is newly generated is different from corrupted block with high probability.

II.RELATED WORK

The two mechanisms which were used for integrity verification are PDP and POR models.PDP

model is for ensuring the possession of data in the cloud server,it uses the concept of RSA and applying on the randomly selecting few samples of blocks in the server. In addition to this dynamic PDP version is used which is based on MAC ,in the dynamic PDP basic block operations are performed having limited functionality. In order to improve the efficiency of the dynamic PDP, method was introduced based on the merkle hash tree.

Public auditing is used in the PDP model for reducing the online burden of the data owners but the privacy of the data is not maintained.PDP with public auditing scheme is developed by using the cryptography method combining with bilinear property .A formal frame work is designed for fully dynamic PDP scheme and the privacy[5] of the data is also maintained.POR model with spot checking and error correcting codes[6] are used for possession as well as for retrievability.

To discharge the information retriever from online burden for check considered auditability in the PDP model interestingly. In any case, their variation uncovered the direct blend of tests and along these lines gives no information[11] security ensure.

III.PROPOSED WORK

The integrity verification and the regeneration of data at faulty servers are mainly implemented by

1. TPA(Third Party Auditor)
2. Semi Trusted Proxy Server

TPA which conducts public audits[4] on the data in the cloud and it is trusted one, the results produced by TPA is not known to the data owners and also for cloud servers.It done the periodic verification in the cloud servers and if any faulty server is found it sends it to the proxy server where the repair has to performed.

Semi trusted proxy server is used to reduce the overhead computation and the online burden of the data owners. Data owner upload the data and it can stay in off line,if any faulty block in the server is found by the TPA it send to the proxy server,the proxy server repair[7] it by using the partial secret key of the data owner.During this process the data owner need not to stay online.

The computational operations performed by the users after retrieving the data from the cloud server is high by using the direct extension techniques.In this technique,the data block which contained the data is divided into segments and each segment will undergo spot checking method for integrity[9] verification. In the previous method the data is recomputed by using the erasure code and replication ,here the code is produced by using the multi server mechanism.

The same data is distributed over the different servers in the cloud in the replication mechanism,if one server is get corrupted then the user retrieve the data by connecting to the other healthy servers.

IV. SYSTEM EVALUATION

Public auditing scheme is divided into three phases:
1.Set up
2.Audit
3.Repair

Set up: In the set up phase the initialization of parameters used in the audit scheme is done. It includes three polynomial time algorithms.

KeyGen(1k)->(pk,sk): In this algorithm the data owner produces a key pair(spk, ssk)by using two random elements x,y. By using these parameters we determine the public key and secret key[10] as pk_x<-g^x,pk_y<-g^y.

Delegation(sk)->(x): Here a secret key is generated by the data owner and it sends to the semi trusted proxy server for repairing, when an corrupted server is detected.

SigAndBlockGen(sk,F)->(φ,ψ,t): This polynomial time algorithm is used to generate authenticator set and block set and file tag by taking input parameters as secret key and file tag.

Audit: In the audit phase servers are verified by using the TPA which selected the samples randomly. This is the main phase where the corrupted block is identified by the TPA and sends to the proxy for regeneration.

Challenge(Finfo)->(C): In this polynomial time algorithm a challenge is claimed to verify the block is corruted or not.The input parameter is the file information of a particular block.

ProofGen(C, φ, ψ)->(P): Here a proof is generated by taking input parameters as challenge,block set and the authenticator set and output produces whether the code in the data block is manipulated and integrity is checked.

Verify(P,pk,C)->(0,1): This algorithm uses the public key ,challenge claimed by the segment and the proof the data block for verification of the code in the block.the output for this algorithm is either 1 or 0 .if output is 1 then data is manipulated by unauthenticated user.

Repair: In the repair phase the server segments which are corrupted are repaired by using the proxy server.

Claim For Repair(F info)->(Cr): In this algorithm the corrupted block is claimed for regeneration.In put parameter is file information and output is the claim itself.

Gen For Rep(Cr,φ,ψ)->(BA): Here the new block is generated for the corrupted data by taking the claim, authenticator set and block set as input parameters and the output is the repaired block.

BlockAndSigReGen(Cr,BA)->(φ',ψ',T): This polynomial time algorithm is used to generate the secured authenticator set for block set generated in the above algorithm.

V.CONCLUSION

A Public auditing scheme is proposed to regenerate the data at the faulty servers in the cloud where the data owners priviliged to delegate TPA to check the validity of data. To protect the data privacy the coefficients are masked with the pseudo random function in the set up phase rather than applying a blind technique in the audit phase.Public auditing scheme also reduces the online burden of the data owners by introducing proxy server. An authenticator based on BLS signature issued to increase the efficiency of the regenerated data.

REFERENCES

1.K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 9, pp. 1717–1726, Sep. 2013

2. H. C. H. Chen and P. P. C. Lee, "Enabling data integrity protection inregenerating-coding-based cloud storage: Theory and implementation,"*IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 2, pp. 407–416,Feb. 2014.

3.A. G. Dimakis, K. Ramchandran, Y. Wu, and C. Suh, "A survey onnetwork codes for distributed storage," *Proc. IEEE*, vol. 99, no. 3,pp. 476–489, Mar. 2011.

4. C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou,"Privacy-preserving public auditing for secure cloud storage," *IEEETrans. Comput.*, vol. 62, no. 2, pp. 362–375, Feb. 2013.

5.S. G. Worku, C. Xu, J. Zhao, and X. He, "Secure and efficient privacypreservingpublic auditing scheme for cloud storage," *Comput. Elect.Eng.*, vol. 40, no. 5, pp. 1703–1713, 2013.

6.C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," *IEEE Trans. Service Comput.*, vol. 5, no. 2, pp. 220–232, Apr./Jun. 2012.

7. Y. Hu, H. C. H. Chen, P. P. C. Lee, and Y. Tang, "NCCloud: Applying network coding for the storage repair in a cloud-of-clouds," in *Proc. USENIX FAST*, 2012, p. 21.

8. Y. Zhu, H. Hu, G.-J. Ahn, and M. Yu, "Cooperative provable data possession for integrity verification in multicloud storage," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 12, pp. 2231–2244, Dec. 2012

9.J. He, Y. Zhang, G. Huang, Y. Shi, and J. Cao, "Distributed data possession checking for securing multiple replicas in geographicallydispersed clouds," *J. Comput. Syst. Sci.*, vol. 78, no. 5, pp. 1345–1358,2012.

10. C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," *IEEE Trans. Comput.*, vol. 62, no. 2, pp. 362–375, Feb. 2013.

11.Dr. S. Vasundra et.al, CSE, JNTUACEA**,** "Study of Cloud Based Mobile Learning Approaches" published a paper on i-manager's Journal on Cloud Computing, Vol.2 No. 1 November 2014-January 2015

AUTHORS PROFILE:

N.AHAMADUNNISA received B.Tech degree in Computer Science and Engineering from JNTU college of engineering,pulivendula, affiliated to JNTUA University, Anantapuramu, A.P, India, during 2010 to 2014. Currently pursuing M.Tech in Computer Science(Artificial Engineering) from JNTUA College of Engineering, Anantapuramu, A.P, India, during 2014 to 2016 batch. Her area of interests include cloud computing,cloud security.

Dr. S. VASUNDRA, presently working as a Professor and Head of the Department CSE, JNTUACEA. She completed her Ph.D from JNTUA University Anantapuramu, M.Tech from JNTUA and B.E from VTU. She is having 17 years of teaching experience and 5 years of research experience. Published 36 papers in various international journals and 21 National and international conferences. Her areas of interest include MANETS, Cloud Computing, Algorithms, Data Structures and Distributed Computing