International Journal of Engineering Research ISSN:2319-6890)(online),2347-5013(print)
Volume No.5, Issue No.7, pp : 640-642 1 July 2016

Responsibility Handler TPA: Auditing and Repairing of Data in Cloud Storage

Miss.Shilpa Singh , Mrs. Padmavathi B.
,Department of computer engineering,G. H. Raisoni College of Engineering And Management,wagholi,pune
Shilpa1991singh@gmail.com ,b.padmavathi@raisoni.net

Abstract: Now a day's to protect data and back up for damaged data is very important. This scheme is for the public auditing and repairing from the regenerating-code-based cloud storage. It solve problem of authenticators in the absence of files owners, a proxy will regenerate the authenticators. Thus, the scheme will completely release files owners from online burden. And repairing of damaged files using generated checksum provides the backup for the same. And the model will provide the auditing and repairing of files to the file owners.

Keywords :TPA,regenerating code,repairing,proxy.

I.INTRODUCTION

Cloud computing is trending technology with shared resources, low cost and rely on pay per use according to the file owner demand. Due to many circumstances it affected on IT market and also impacted on security, security issues and privacy. Customer do not know that where the data are stored in cloud, who manages data and other vulnerabilities that can happen. Following are some issues and problems that can be faced by CSP while implementing services provided in cloud.

*(i)Privacy Issues:*As per the human right their private and sensitive information must be secure. In cloud area privacy occur according to the cloud deployment model and structure. In Public cloud (accessed through the Internet and shared amongst different consumers) is one of the dominant or main architecture when cost reduction is concerned topic, but relying on a CSP to manage and hold file owners information raises many privacy concerns.

(ii)Lack of user control: According to SAAS,environment service provider only responsible to control files or data. Now the question arises how customer can retain its control on files or data when information is processed or stored. It is the legal and required requirement of them and also to make trust and maintain dignity between customer and vendor.

(iii)Unauthorized Secondary Usage: The major threats can occur if data or file is placed for illegal or for wrong intentionally uses. Cloud computing standard business structure tells that the service provider can reach in profits from authorized secondary uses of user files.

II.LITERATURE SURVEY

1. A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "Above the clouds: A Berkeley view of cloud computing," Dept. Electrical Eng. and Computer. Sciences,University of California, Berkeley, Rep. UCB/EECS, vol. 28, p. 13, 2009.

Cloud Computing, the long-held dream of computing as a utility, has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. Developers with innovative ideas for new Internet services no longer require the large capital outlays in hardware to deploy their service or the human expense to operate it. They need not be concerned about over-provisioning for a service whose popularity does not meet their predictions, thus wasting costly resources, or under-provisioning for one that becomes wildly popular, thus missing potential customers and revenue. Moreover, companies with large batch-oriented tasks can get results as quickly as their programs can scale, since using 1000 servers for one hour costs no more than using one server for 1000 hours. This elasticity of resources, without paying a premium for large scale, is unprecedented in the history of IT.

2.G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proceedingsof the 14th ACM Conference on Computer and Communications Security, ser. CCS '07. New York, NY, USA: ACM, 2007, pp. 598–609.

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 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.A. Juels and B. S. Kaliski Jr, "Pors: Proofs of irretrievability for largefiles," in Proceedings of the 14th ACM conference on Computer andcommunications security. ACM, 2007, pp. 584–597.

Cloud computing has been envisioned as the paramount solution to the rising storage device costs of IT Enterprises. With the high costs of data storage devices as well as the rapid rate at which data is being generated it proves expensive for enterprises or individual users to frequently update their hardware. Apart from reduction in storage costs data

ISSN:2319-6890)(online),2347-5013(print)
1 July 2016

outsourcing to the cloud also helps in reducing the maintenance. Cloud storage moves the user's data to large data centres, which are remotely located, on which user does not have any control. However, this unique feature of the cloud rises many new security challenges which need to be clearly understood and resolved. One of the important concerns that need to be addressed is to assure the data integrity to customer. I.e. correctness of his data in the cloud. As the data is physically not accessible to the user the cloud should provide a way for the user to check if the integrity of his data is maintained or is compromised. In thispaper a scheme is proposed which gives a proof of data integrity in the cloud which the customer can employ to check the correctness of his data in the cloud. This proof can be agreed upon by both the cloud and the customer and can be incorporated in the Service level agreement (SLA). This scheme ensures that the storage at the client side is minimal which will be beneficial for the organization

4.R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "Mr-pdp: Multiplereplicaprovable data possession," in Distributed Computing Systems,
2008. ICDCS'08. The 28th International Conference on. IEEE, 2008, pp. 411–420.

III.PROPOSED APPROACH FRAMEWORK AND DESIGN

This scheme is for the public auditing and repairing from the regenerating-code-based cloud storage. It solve problem of authenticators in the absence of files owners, a proxy will regenerate the authenticators. Thus, the scheme will completely release files owners from online burden. it protect the confidentiality of sensitive file an repair the damaged files by using generated checksum. And repairing of damaged files using generated checksum provides the backup for the same. And the model will provide the auditing and repairing of files to the file owners.

We are going to implement authorized data de-duplication system in which differential privileges of users are further considered.

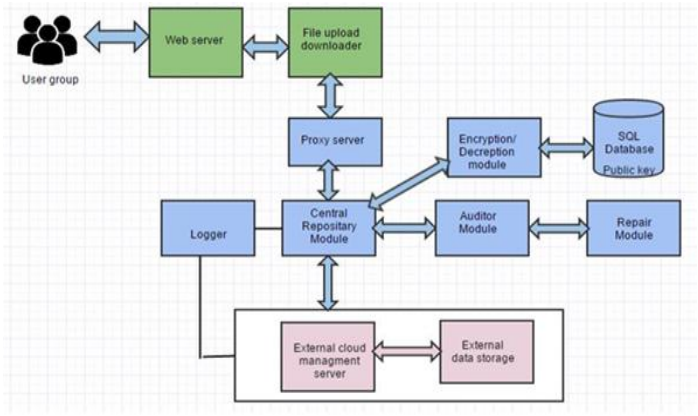


Fig. 1 System Architecture

*(i)Proxy Server:*A proxy agent acts on behalf of information the info the information owner to regenerate authenticators and data blocks on the servers throughout the repair procedure. Notice that the information owner is restricted in machine and storage resources compared to alternative entities and should become off-line when the knowledge transfer procedure. The proxy, UN agency would continuously be on-line, is meant to be rather more powerful than the information owner however less than the cloud servers in terms of computation and memory capability. To save resources as well as the on-line burden doubtless brought by the periodic auditing and accidental repairing, the knowledge house owners resort to the TPA for integrity verification and delegate the reparation to the proxy. Considering that the information owner cannot continuously keep on-line in observe, so as tokeep the storage offered and verifiable when a malicious corruption, we have a tendency to introduce a semi-trusted proxy into the system model and supply a privilege for the proxy to handle the reparation of the coded blocks and authenticators. It generates signature exploitation OAEP primarily based key delegation that provides distinctive non-public and public key for every cluster registered within the cloud. Therefore the users will access the document provided by its own cluster solely. The users will read alternative team's document exploitation non-public key of the opposite teams. If he modifies alternative cluster content he are revoked by the cloud server.

*(ii)TPA:*TPA is trusty and its audit result's unbiased for each knowledge homeowners and cloud servers; and a proxy agent, UN agency is semi-trusted and acts on behalf of the knowledge information} owner to regenerate authenticators and data blocks on the unsuccessful servers throughout the repair procedure. Noticethat the info owner is restricted in procedure and storage resources compared to alternative entities and will becomes off-line even once the info transfer procedure. The proxy, who wouldalways be on-line, is meant to be far more powerful than the info owner however but the cloud servers in terms of computation and memory capability. to avoid wasting resources likewise because the on-line burden probably brought by the periodic auditing and accidental repairing, the info homeowners resort to the TPA for integrity verification and delegate the reparation to the proxy.

IV.MATHEMATICAL MODEL

Let,S = fI,P,R,Og
Where,
S: Service Recommendation system
I: Set of inputs
P: Set of processes
R: Rules or constraints
O: Set of outputs/Final output
I = f i1 ,i2 g
Where,
i1: Files containing text.
i2: Private and Public Key
P = fp1, p2, p3, p4, p5, p6, p7,p8,p9 g
Where ,
p1: User Registration
p2: Public and Private Key Generation.
p3:File upload and Download
p4:File Replication ,Encryption and Checksum Creation.
p5: Storing Checksum and Encrypted data on Cloud.
p6: Perform Audit.

ISSN:2319-6890)(online),2347-5013(print)
1 July 2016

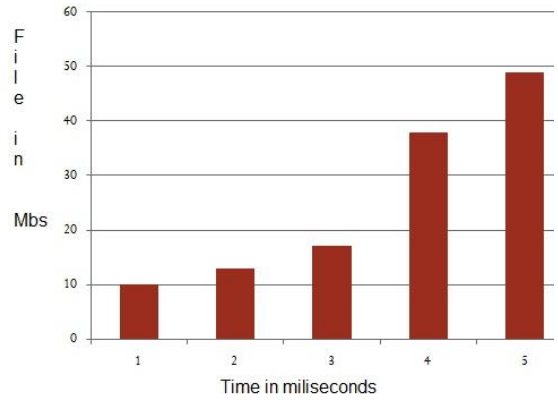
p7: Repair Corrupted data.
p8: Generate logs and Results.
p9: Send Results as Email.
R = fr1, r2 g
Where ,
r1 =During replication store data on more than one server.
r2 = Use Proxy server to audit automatically without user intervention.
O = o1 , o2
Where,
o1 = Perform Successful audit on Replicated data.
o2 = Corrupted file Recovered successfully.

VI. SCOPE OF WORK

Main goal of this system is to develop a new approach for authentication of file owners and repairing of damaged data while comparing the original encrypted data.To develop improvement in performance of recommendation system by use of relevance feedback.

VI.RESULT

1.To provide secured and efficient system for managing the personal information or files including sensitive and non sensitive data and repair the damaged files.



2.The following table shows the time required to audit the file. The program was run on a 1 GHz Pentium IV computer running GNU/Linux.

File ID	File Size	Regeneration Time (MS)
1	50 KB	10
2	67KB	13
3	100KB	17
4	1MB	38
5	2MB	49

VII.CONCLUSION AND FUTURE WORK

System will protect and repair the confidentiality of files. To implement authorized file details system in which differential privileges of users are further considered. And block level encryption provides additional security to user Files and where the files owners are privileged to delegate Third Party Authenticator for their files validity checking and repairing for the same. To protect the original data privacy against the TPA and repaired the damaged files and provide the originality.

VIII.REFERENCES

i. *Jian Liu, Kun Huang, Hong Rong, Huimei Wang and Ming Xian,Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage, IEEE TRANSACTIONS ON INFORMATION AND SECURITY Vol 1 No 2015.*

ii. *Bo Chen, Reza Curtmola,Remote Data Checking for Network Coding-based Distributed Storage Systems, Department of Computer Science,New Jersey Institute of Technology,The 28th International Conference on. IEEE, 2008,pp. 411420.*

iii. *Dan Boneh, Ben Lynn, and Hovav Shacham,Short signatures from the Weil pairing,Computer Science Department, Stanford University, ACM, 2009, pp. 187198.*

iv. *KennethW. Shum and Yuchong Hu,Functional-Repair-by-Transfer Regenerating Codes,IEEE Transactions on, vol. 25, no. 2, pp. 407416,Feb 2014.*

v. *K. D. Bowers, A. Juels, and A. Oprea, "Hail: a high-availability andintegrity layer for cloud storage," in Proceedings of the 16th ACMconference on Computer and communications security. ACM, 2009,pp. 187–198.*

vi. *J. He, Y. Zhang, G. Huang, Y. Shi, and J. Cao, "Distributed datapossession checking for securing multiple replicas in geographically dispersedclouds," Journal of Computer and System Sciences, vol. 78,no. 5, pp. 1345–1358, 2012.*

vii. *B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote datachecking for network coding-based distributed storage systems," inProceedings of the 2010 ACM workshop on Cloud computing security workshop. ACM, 2010, pp. 31–42.*

viii. *H. Chen and P. Lee, "Enabling data integrity protection in regenerating coding-based cloud storage: Theory and implementation," Parallel andDistributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 407–416,Feb 2014.*

ix. *K. Yang and X. Jia, "An efficient and secure dynamic auditing protocolfor data storage in cloud computing," Parallel and Distributed Systems,IEEE Transactions on, vol. 24, no. 9, pp. 1717–1726, 2013.*

x. *Y. Zhu, H. Hu, G.-J. Ahn, and M. Yu, "Cooperative provable datapossession for integrity verification in multi-cloud storage," Parallel and Distributed Systems, IEEE Transactions on, vol. 23, no. 12, pp. 2231–2244, 2012.*

xi. *A. G. Dimakis, K. Ramchandran, Y. Wu, and C. Suh, "A survey onnetwork codes for distributed storage," Proceedings of the IEEE, vol. 99,*