RESEARCH ARTICLE OPEN ACCESS

NOVEL METHOD FOR DELEGATABLE PROOFS OF STORAGE TO PREVENT DATA LEAKAGE IN CLOUD STORAGE

Ms.Madhuri Desale
Dr. Babasaheb Ambedkar Technological University, Lonere.
Department of Computer Engineering
Godavari College of Engineering, Jalgaon
madhuridesale11120@gmail.com

Abstract

Cloud storage is associate increasingly customary application of cloud computing, which could provide on-demand outsourcing knowledge services for every organizations and folks. because of the data outsourcing, however, this new paradigm of data hosting service collectively introduces new security challenges that need associate freelance auditing service to examine the data integrity within the cloud. Some existing remote integrity checking ways in which will solely serve for static archive information and so can't be applied to the auditing service since the data within the cloud unit of measurement generally dynamically updated. we have a tendency to take into account the trip of permitting a 3rd Party reviewer (TPA), for the good thing about the cloud client, to verify the trait of the dynamic knowledge hangs on within the cloud. Proofs of storage (including Proofs of Retrievability and demonstrable information Possession) might be a cryptologic tool, that allows knowledge owner or third party auditor to audit integrity of data hold on remotely in Associate in Nursing very cloud storage server, whereas not keeping a district copy {knowledge|of information} or downloading data back throughout auditing.

KEYWORDS: – **Multi-Cloud storage, Proof of Storage, Cloud Computing, Third Party Auditor**

I. INTRODUCTION

Cloud computing is extensively developed technology employed in business, IT industries that give services like network access, resources, infrastructure, platform, and speedy resource snap as per user would like. The user can gain access of services anytime, anywhere on-demand. In cloud computing the data of user is centralized to the cloud storage. several users from remote location use services continuously therefore there may arise some issues like info security, info integrity, dynamic updates. once it's unimaginable for user to check the data is being consistent that's hold on cloud storage. therefore user forever wants that cloud server ought to have to be compelled to maintain info integrity and privacy. Cloud service suppliers square measure the separate entities that store info and provide services to the user. to confirm the data security and integrity and to chop back on-line burden it's of importance to alter public auditing service for cloud storage, so as to audit the data. TPA wills the auditing methodology on behalf of the user. The TPA has capabilities and skill which can periodically check the integrity of the data hold on in cloud. The user does not have the capabilities that the TPA has.

TPA keeps the info in original state and it conjointly verifies the correctness performs this task by user permission. sanctioning public auditing service can play AN awfully very important role for privacy knowledge security & minimizing the info risk from hackers. Documented capability wants guarantee with regard to the legality of learning on capability, particularly that capability servers have learning. It's meager to search out that info ar adjusted or erased once reaching to the info, as a result of it's aiming to be past the purpose wherever it's potential to recoup lost or broken info. Safe reposition servers hold large measures of data, next to no of that ar gotten to. They conjointly hold info for intensive stretches of it slow amid that there's in addition introduction to info misfortune from ad succor blunders on the grounds that the physical execution of capability advances, e.g., reinforcement and restore, info movement to new systems, and systematically dynamic enrollments in shared frameworks. to deal with the issues of existing in public verifiable POS schemes, we've got a bent to propose a replacement variant formulation said as Delegatable Proofs of Storage (DPOS), that on one hand supports delegation of information auditing task, like in public verifiable POS schemes, and on the other hand is as economical as a privately verifiable POS theme. Public verifiability of POS permits any third party auditor to visualize the first contents of information in cloud storage that significantly eliminates the burden of information owner. an issue that supports delegation of information equally as a result of it's economical as POS in privately verifiable theme is DPOS.

If there is changed in data, that we'll verify victimization third party auditor. It checks for original content and might show acceptable message to user. to supply extra security, we've got a possible to area unit visiting divide the knowledge files into blocks and aiming to use double cryptography by victimization two algorithmic programs Bastion and altered RSA algorithmic program, initial we'll inscribe the knowledge victimization Bastion and ciphertext area unit aiming to be re-encrypted mistreatment modified RSA algorithm. thus data go es to be safer as twin cryptography is given in projected system. Once we've got a bent to urge twin encrypted ciphertext, it's going to be divided in blocks and theses blocks area unit aiming to be stick with it all completely different servers. equally as once secret is generated it'll even be divided in blocks to stay it safe from someone, as he got the secret writing key he will get solely key therefore attack won't be taken place and knowledge will not be disclosed and can be further secured. Planned Bastion and adjusted RSA formula, a topic that ensures the confidentiality of encrypted data even once the someone has the cryptography key, and each one but re-encrypted ciphertext blocks. Bastion is best suited to settings where the ciphertext blocks area unit hold on in multi-cloud storage systems and adjusted RSA generates long bit cryptography key therefore data got to keep secure even the someone tries to rewrite it. in addition as cryptography key area unit divided and should be hold on inside the blocks for added security.

II. RELATED WORK

Proofs of storage (including Proofs of Retrievability and obvious information Possession) may be a scientific discipline tool, that enables information owner or third party auditor to audit integrity of data keep remotely in Associate in Nursing passing cloud storage server, whereas not keeping a section copy {of *knowledge|of information|of information} or downloading data back throughout auditing. Delegatable proofs of storage permits info owner to delegate auditing task to a third party auditor, and within the in the meantime retains the power to perform audit task by her, whether or not or not the auditor colluded with the cloud storage server. Our formulation to boot support revoking and shift auditors manifestly [1].

The shopper keeps up a seamless with amount of knowledge to substantiate the confirmation. The test/reaction convention transmits slightly, consistent live of learning, that limits prepare correspondence. throughout this way, the PDP show for remote information checking underpins immense information sets in typically circulated capability frameworks. we tend to tend to blessing 2 provably-secure PDP plans that area unit more cost effective than past arrangements, even analyzed with plans that succeed extra fragile certifications. Especially, the overhead at the server is low (or even steady), as operation conferred to straight among the span of the info [2].

Numerous capability frameworks accept replication to broaden the accessibility and strength of learning on untrusted storage frameworks. At present, such capability frameworks give no solid proof that varied duplicates of the data are literally place away. Capability servers will attempt to kind it seem like they're stroke away some duplicates of the info, whereas actually they fully store one duplicate. we tend to tend to handle this deformity through numerous copy demonstrable knowledge possession (MR-PDP): A provably-secure got wind of that permits a shopper that stores t copys of a document throughout a capability framework to substantiate through a take a glance at reaction convention that (i) all of a kind reproduction are going to be created at the season of the take a glance at which (ii) the potential framework utilizes t times the capability required to store a solitary copy [3].

By utilizing Cloud storage, shoppers can get to applications, administrations, programming at despite purpose they wants over Infobahn. Shoppers can place their data remotely to distributed storage and notice advantage of on-request administrations and application from the assets. The cloud ought to got to guarantee info uprightness and security of information of client. the issue regarding distributed storage is honorableness and protection of information of client can emerge. to stay up to gratuitous excess this issue here, we've an inclination to square measure giving open reviewing methodology for distributed storage that shoppers can produce utilization of AN outsider examiner (TPA) to check the attribute of information. Not merely confirmation of information honorableness, the projected framework additionally underpins data elements. The work that has been drained this line wishes data elements and real opens auditability. The inspecting endeavor screens data alterations, additions and erasures [4].

We think regarding the issue of proficiently demonstrating the honesty of data place away at untrusted servers. among the plain information possession (PDP) show, the shopper preprocesses the information associate degreed later on sends it to Associate in Nursing untrusted server for capability, whereas keeping a small amount live of knowledge. we tend to gift a definitional structure and effective developments for dynamic obvious information possession (DPDP) that expands the PDP model to help obvious updates to position away information. we've an inclination to utilize a replacement kind of valid word references addicted to rank information [5].

Confirmations of capability (PoS) square measure intuitive conventions enabling a consumer to check that a server firm stores a record. Past work has incontestable that evidences of capability square measure typically developed from any homomorphic straight appraiser (HLA). The latter, generally, square measure mark/message confirmation plans where 'labels' on varied messages square measure typically homomorphically consolidated to yield a 'tag' on any direct we've got a bent to at that point tell easyst|the only|the best} because of make over any open key HLA into a freely simple PoS with correspondence varied nature autonomous of the autoimmune disease length and supporting Associate in Nursing limitless sort of confirmations [6].

Information administrations for the two associations and others. yet, purchasers may not absolutely believe the cloud specialist co-ops (CSPs) in this it's exhausting to see if the CSPs live up to their lawful needs for information security. throughout this fashion, it's basic to create skillful reviewing methods to fortify data proprietors' trust and trust in distributed storage. throughout this paper, we've got an inclination to gift a novel open examining created for secure distributed storage hooked in to distinctive hash table (DHT), that's another two-dimensional data structure placed at a third equality examiner (TPA) to record the knowledge} property knowledge for dynamic inspecting. Variable from the present works, the projected created moves the approved data from the CSP to the TPA and through this fashion primarily diminishes the method expense and correspondence overhead. among the interim, misusing the basic preferences of the DHT, our set up can likewise accomplish higher refreshing productivity than the only at college set ups [7].

Distributed computing has been notional as a result of the forefront engineering of IT Enterprise. It moves the applying

Programming and databases to the brought on massive server farms, where the administration of the data and administrations may not be totally dependable. This novel worldview achieves varied new security challenges, that haven't been sure enough knew. This work examines the issue of guaranteeing the righteousness of information storage in Cloud Computing. Specifically, we have a tendency to expect relating to the enterprise of permitting a third party examiner (TPA), inside the interest of the cloud shopper, to check the righteousness of the dynamic knowledge place away inside the cloud. the help for knowledge elements through the foremost broad forms of info activity, for example, sq. alteration, addition, and cancellation, is additionally a remarkable advance toward reasonableness, since administrations in Cloud Registering do not appear to be restricted to file or reinforcement knowledge as a result of it were. Whereas earlier chips away at guaranteeing remote knowledge uprightness of times does not have the help of either open auditability or dynamic knowledge tasks, this paper accomplishes every [8].

In spite of the particular incontrovertible fact that the advantages square measure clear, such Associate in nursing administration is likewise surrendering clients' physical possession of their redistributed data that inescapably presents new security dangers toward the accuracy of the information in cloud. In request to handle this new issue and any accomplish a secure and trustworthy distributed storage administration, we have a tendency to tend to propose throughout this paper a labile sent storage righteousness inspecting system, victimization the homomorphic token and disseminated obliteration coded data. The planned configuration permits purchasers to review the distributed storage with exceptionally light-weight correspondence and calculation price. The reviewing result ensures solid distributed storage accuracy guarantee, yet in addition at the identical time accomplishes quick data mistake limitation, i.e., the ID of acting mischievously server [9].

Due to the data redistributing, be that as a result of it may, this new worldview of information facilitating administration likewise presents new security challenges, that desires associate autonomous reviewing administration to check the data honesty at intervals the cloud. Some current remote trustworthiness checking strategies can serve for static document data and consequently can't be connected to the reviewing administration since the data at intervals the cloud is more and more reinvigorated. Consequently, associate economical and secure dynamic evaluating convention is required to influence data proprietors that the data ar accurately place away at intervals the cloud. we've got a possible to first organize a reviewing structure for distributed storage frameworks what is loads of, propose a talented and protection safeguarding examining convention. At that point, we've got an inclination to stretch out our reviewing convention to help the data dynamic tasks, that's practiced and provably secure at intervals the irregular prophet demonstrate. we've got an inclination to a lot of broaden our examining convention to assist cluster reviewing for every varied proprietors and numerous mists, whereas not utilizing any confided in arranger. The investigation and recreation results demonstrate that our projected reviewing conventions ar secure and practiced, notably it cut back the calculation worth of the examiner [10].

III. Proposed Algorithm

A. ***Description of the Proposed Algorithm:***

1) **Data Owner:**

- Data owner generate public keys.
- Data owner will be responsible for encrypting files and generating authentication tags also.
- Data owner will upload all this data to cloud.

2) **Cloud Service Provider:**

- Cloud service provider will store all the data i.e. file along with keys and authentication tags.
- Cloud Service Provider will work according to the request and response from the user.

3) **ODA:**

- Verification of file content is done by ODA.
- Check for integrity.

4) **Data User:**

- Data user will request for keys to the Data Owner.
- Data Owner will send keys to the Data user.
- With keys he can decrypt and download the original content of the file.

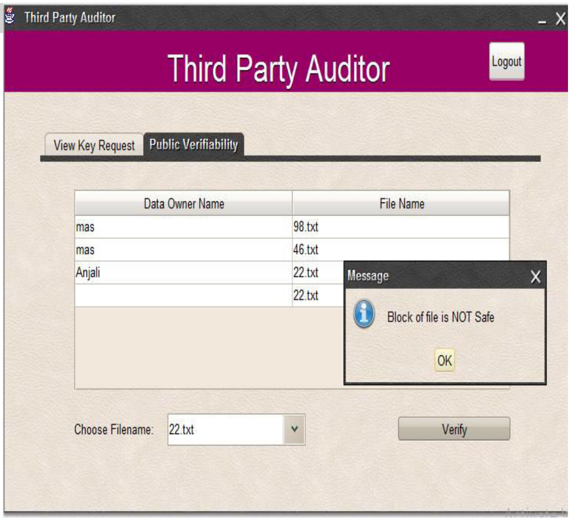
Pseudo Code

File Splitting, Encryption and Decryption:
Input: Text file, secret key
Output: Encrypted Files E (F.1), E (F.2), E (F.3), E (F.4), and E (F.5), Decrypted files.

```
Step 1: Divide the file into blocks.
Step 2: Uploads a file (F) and secret key (SK)
Step 3: Index based files (F.0, F.1, F.2, F.3 and F.4) are created with the same file name.
Step 4: Encrypt each part of the divided file E (F.1), E (F.2), E (F.3), E (F.4), and E (F.5) and upload it to the Cloud server.
Step 5: Provide keys to the to the ODA i.e. Third Party Auditor.
Step 6: ODA will choose the file along with verification key pair and upload it to the cloud.
Step 7: Data user will request for keys to Data Owner and once have them can decrypt and download the file.
Step 8: Enter the File Name (FN) and Secret Key (SK) from the data owner or File owner by making request
Step 9: Perform a search with the filename associated in Cloud storage service provider directory (F.0, F.1, F.2, F.3 and F.4)
Step 10: Pass the secret key (SK) to the data user
Step 11: Data user can download the original file F.
Step 12: End.
```

IV. Results

The proposed framework provides user information protection by taking user information,that is the file square measurement data, which aims to be separated into entirely different blocks.
Then, upload each block to cloud in ciphertext format. If any change in owners data then third party auditor will shows that block of file is safe or not safe.



Data Owner Name	File Name
mas	98.txt
mas	46.txt
Anjali	22.txt
	22.txt

Block of file is NOT Safe

Choose Filename: 22.txt

Fig.1. Block Safe or Not Safe

V. Conclusion and Future Work

Propose system provides security to the user information by taking users information, the data i.e. file square measure aiming to be divided into altogether completely different blocks. Then, these blocks square measure encrypted by applying a pair of altogether completely different algorithms i.e. modified RSA and Bastion algorithmic rule. Through these algorithms we have a tendency to tend to square measure re-encrypting user's information. Once this the data owner goes to be answerable for generating the mix of varied keys like public and secret key. The divided parts of the files will have altogether completely different tags, this tags additionally are created by the data owner. Then all information along side file goes to be uploaded to cloud. Cloud service provider provides the appropriate information, tags and key mix as per the request from altogether completely different users like information owner, data user, and ODA. Here ODA will check for integrity of the user's information, and if there square measure some changes in contents then the appropriate message square measure aiming to be to the user. Information user request for keys to the ODA and gets the keys square measure aiming to be able to rewrite and transfer the file. With this we have a tendency to tend to square measure able to offer further security to user's information, execution time of the planned system is in addition economical.

ACKNOWLEDGMENT

I profoundly grateful to Mr.P.B.Gosavi.for his/her expert guidance and continuous encouragement throughout to see that this project rights its target since its commencement to its completion. I would like to express my deepest appreciation towards PrincipalDr.V.H.Patil., Mr.P.B.Gosavi HOD department of computer engineering and PG coordinator Mr.Rahal Gaikwad.I must express my sincere heartfelt gratitude to all staff members of computer engineering department who helped me directly or indirectly during this course of work. Finally, I would like to thank my family and friends, for their precious support.

REFERENCES

[1] J. Xu, A. Yang, J. Zhou, and D. S. Wong, "*Lightweight Delegatable proofs of storage*," in Proceedings of 21st European Symposium on Research in Computer Security, ESORICS 2016, pp. 324–343, Springer International Publishing, 2016.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "*Provable data possession at untrusted stores*," in Proceedings of the 14th ACM Conference on Computer and Communications Security, CCS 2007, pp. 598–609, ACM.

[3] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "*MR-PDP: Multiple-replica provable data possession*," in Proceedings of the 28th International Conference on Distributed Computing Systems, ICDCS 2008, pp. 411–420, IEEE, 2008.

[4] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "*Privacy preserving public auditing for secure cloud storage*," IEEE Transactions on Computers, TC 2013, vol. 62, no. 2, pp. 362–375, 2013.

[5] C. C. Erway, A. K¨upc¸ ¨ u, C. Papamanthou, and R. Tamassia, *"Dynamic provable data possession*," ACM Transactions on Information and System Security, vol. 17, pp. 15:1–15:29, April 2015.

[6] G. Ateniese, S. Kamara, and J. Katz, "*Proofs of storage from homomorphic identification protocols*," in Advances in Cryptology -ASIACRYPT 2009, vol. 5912 of LNCS, pp. 319–333, Springer, 2009.

[7] Hui Tian, Yuxiang Chen, Chin-Chen Chang, "*Dynamic-Hash-Table Based Public Auditing for Secure Cloud Storage,*" IEEE TRANSACTIONS ON SEVICE COMPUTING, MANUSCRIPT ID

[8] Qian Wang, Cong Wang, Kui Ren, Wenjing Lou "*Enabling Public Auditability and Data Dynamics for Storage Security in Cloud Computing,*" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 22, NO. 5, MAY 2011

[9] Cong Wang, Qian Wang, Kui Ren, Ning Cao, and Wenjing Lou, "*Toward Secure and Dependable Storage Services in Cloud Computing,*" IEEE TRANSACTIONS ON SERVICES COMPUTING, VOL. 5, NO. 2, APRIL-JUNE 2012

[10] G. Ateniese, S. Kamara, and J. Katz, "*Proofs of storage from homomorphic identification protocols*," in Advances in Cryptology -ASIACRYPT 2009, vol. 5912 of LNCS, pp. 319–333, Springer, 2009

[11] I. G. Aniket Kate, Gregory M. Zaverucha, "*Constant-Size Commitments to Polynomials and Their Applications,*" in Advances in Cryptology - ASIACRYPT 2010, pp. 177–194.

[12]] J. Alwen, Y. Dodis, and D. Wichs, "*Leakage-Resilient Public-Key Cryptography in the Bounded-Retrieval Model*," in CRYPTO '09: Annual International Cryptology Conference on Advances in Cryptology, pp. 36–54, 2009.

[13] Dan Boneh, Ben Lynn, and Hovav Shacham, "*Short Signatures from the Weil Pairing,*" J. Cryptology (2004) 17: 297–319

[14] G., Burns, R., Curtmola, R., Herring, J., Khan, O., Kissner, L., Peterson, Z., and Song, "*Remote Data Checking Using Provable Data Possession,*" ACM Trans. Info. Syst. Sec. 14, 1, Article 12

[15] A. Juels and J. Burton S. Kaliski, "*PORs: Proofs of retrievability for large files*," in Proceedings of the 14th ACM Conference on Computer and Communications Security, CCS 2007, pp. 584–597, ACM, 2007.

[16] H. Shacham and B. Waters, "*Compact proofs of retrievability*," in Advances in Cryptology - ASIACRYPT 2008, vol. 5350 of LNCS, pp. 90–107, Springer, 2008.

[17] B.Wang, B. Li, and H. Li, "*Oruta: Privacy-preserving public auditing for shared data in the cloud,*" in Proceedings of 5th International Conference on Cloud Computing, Cloud 2012, pp. 295–302, IEEE, 2012.

[18] T. Okamoto, "*Provably secure and practical identification schemes and corresponding signature schemes,*" in CRYPTO '92: Annual International Cryptology Conference on Advances in Cryptology, pp. 31– 53.

[19] J. Alwen, Y. Dodis, and D. Wichs, "*Leakage-Resilient Public-Key Cryptography in the Bounded-Retrieval Model*," in CRYPTO '09: Annual International Cryptology Conference on Advances in Cryptology, pp. 36–54, 2009.

[20] Jiawei Yuan, Shucheng Yu, and Song, "*Proofs of retrievability with Public Verifiability and Constant Communication Cost in Cloud,*" ACM Trans. May 8, 2013, Hangzhou, China.

[21] Dan Boneh, Ben Lynn, and Hovav Shacham, "*Short Signatures from the Weil Pairing,*" J. Cryptology (2004) 17: 297–319