iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 10 **Issue:** V **Month of publication:** May 2022

DOI: https://doi.org/10.22214/ijraset.2022.42714

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 10 Issue V May 2022- Available at www.ijraset.com

An approach for Preserving Privacy in Public Auditing of Cloud data

Shreya Mugal[1], Prof. K.K. Chhajed[2]
[1, 2]*Department of Computer science and Engineering, Sant Gadge Baba Amravati University*

Abstract: ***Cloud users can remotely store their data and appreciate the on demand high quality applications and services from a shared pool of configurable computing resources, regardless of local data storage and maintenance. However, the fact that users no longer have physical possession of the out sourced data makes the data integrity protection in Cloud computing a formidable task, especially for users with constrained computing resources. This paper study the problem of ensuring the integrity of data storage in Cloud Computing. In particular, wet ask of allow in gathird party auditor (TPA), on behalf of the cloud client, to verify the integrity of the dynamic datastored in the cloud. To securely introduce an effective third-party auditor (TPA), and determine various techniques and algorithms for strengthen the Security.***
Keywords: TPA, Cloud Computing, CSP, RSA

I. INTRODUCTION

By victimization Cloud storage, users will access applications, services, software system whenever they needs over the internet. Users will place their data remotely to cloud storage and obtain advantage of on-demand services and application from the resources. The cloud should need to guarantee data integrity and security of knowledge of user. the problem concerning cloud storage is integrity and privacy of data of user will arise. therefore the basic motivation behind this work is:

1) To overkill this issue, public auditing process is introduced for cloud storage that users can make use of a third-party auditor (TPA) to check the integrity of data.
2) Not only verification of data integrity, the planned system additionally supports data dynamics. The work that has been exhausted this line lacks information dynamics and true public auditability. The auditing task monitors data modifications, insertions and deletions.
3) The proposed system is capable of supporting public auditability, data dynamics and Multiple TPA are used for the auditing process.

II. LITERATURE SURVEY

Ateniese et al. [6] are the primary to consider public auditability in their outlined “provable data possession” (PDP) model for guaranteeing possession of files on untrusted storages. In their theme, utilize RSA primarily based homomorphic tags for auditing outsourced data, so public auditability is achieved. However, Ateniese et al. don't contemplate the case of dynamic data storage, and therefore the direct extension of their scheme from static data storage to dynamic case could suffer design and security issues.

In [7], Ateniese et al. propose a dynamic version of the previous PDP scheme. However, the system imposes a priori certain on the quantity of queries and doesn't support absolutely dynamic data operations, i.e., it only permits very basic block operations with restricted practicality, and block insertions can't be supported.

In [17], Wang et al. contemplate dynamic data storage in a very distributed situation, and also the proposed challenge-response protocol will each confirm the data correctness and find possible errors. the same as [7], they only contemplate partial support for dynamic data operation.

Juels et al. [10] describe a “proof of retrievability” (PoR) model, wherever spot-checking and errorcorrecting codes ar accustomed guarantee each “possession” and “retrievability” are files on archive service systems. Specifically, some special blocks known as “sentinels” are indiscriminately embedded into the data file F for detection purpose, and F is additional encrypted to shield the positions of those special blocks. However, like [7], the quantity of queries a client will perform is additionally a fixed priori, and also the introduction of precomputed “sentinels” prevents the development of realizing dynamic data updates.

Shacham et al. [16] design associate improved PoR scheme with full proofs of security within the security model outlined in [10]. They use in public verifiable homomorphic authenticators designed from BLS signatures , supported that the proofs are often aggregative into atiny low authenticator price, and public retrievability is achieved. Still, the authors only contemplate static data files.

rway et al. [9] was the primary to explore constructions for dynamic obvious data possession. They extend the PDP model in [6] to support obvious updates to stored data files exploitation rank-based authenticated skip lists. The scheme is basically a completely dynamic version of the PDP answer. To support updates, particularly for block insertion, they eliminate the index information within the "tag" computation in Ateniese"s PDP model [6] and use authenticated skip list data structure to authenticate the tag information of challenged or updated blocks 1st before the verification procedure. However, the efficiency of their scheme remains unclear.

Shah et al.[13] introduce TPA thought to take care of data integrity and preserve privacy. It reduces on-line burden and keeps the privacy preserve. Chen et al.[8] provides mechanism for auditing the correctness of data with multiple server.

III.SYSTEM ARCHITECTURE

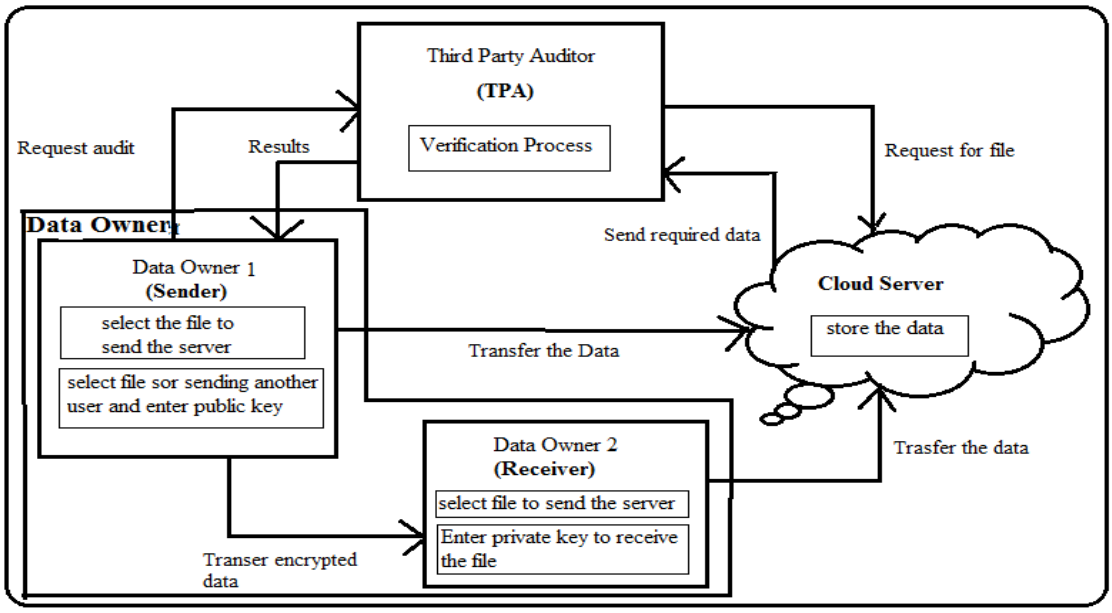


Fig 1: Auditing scheme Architecture

There is a requirement to develop an efficient public auditing protocol that overcomes the limitation of the present auditing scheme. The proposed system is developed to verify the correctness of cloud knowledge by TPA, periodically or on demand while not retrieving the complete data or while not introducing extra online burden to the cloud users and cloud servers. It assure that no data content is leaked to TPA throughout the auditing method. It maintains storage correctness of data, integrity and confidentiality of stored data.

The proposed scheme consists of 3 basic entities; they're

1) *Data Owner:* Data owner is a very important a part of our proposed system. It performs most of the responsibility associated with the data. within the proposed auditing scheme, the data owner 1st performs login and registration with cloud server and TPA. The new user needs to first register itself by filling the registration type and be the active member of the system. A message for prospering registration are going to be provided. If a user is already the member of the system then he or she will be able to perform login process. If the user name and password exist within the database, then they'll be login successfully for being valid users as an alternative they'll receive miscalculation message. Once with success login, the data owner an error choose the file he or she want to store on the cloud server. The file will by him/her then transferred to the cloud server. If user want to send file to a different user. to produce security to the communication we tend to use RSA algorithm. 1st sender encode the file by getting into public key and so send the file and so receiver receives enters the non-public key to decode the file and receives it.
2) Cloud Server Storage: Cloud server stores that is transferred by data owner and send the requested data to the third party auditor.

3) *TPA:* within the proposed scheme, to perform the task of data auditing a TPA is been used for this purpose. TPA performs data auditing either sporadically or on demand by the client. On receiving the auditing request from user or data owner, the TPA starts its auditing process. Later it compares the two signature in verification process. If it matches then it means that the integrity of data is maintained and otherwise not maintained. this suggests that data isn't been tampered or modified. The results for a similar is provided to the data owner by the TPA.

IV. METHODS AND EXECUTION

A. *Methodology*

To provide the security to the communication between the data owners this dissertation used RSA algorithm The RSA algorithm ensures that the keys, are as secure as possible. The following steps highlight how it works:

1) Generating the keys
2) Encryption
3) Decryption

B. *System Execution*

When user enters the system , then they have to authenticate their self. Once registration of user is completed users are allow to authenticate their self. Fig 1 shows login form of a system. When one user want to send any message or any file to another user. This system provide security to the communication by using RSA algorithm. When one user wants to communicate with another user, at that time dynamic public and private keys are generated. The public and private key generation is shown in fig 2. There is a one tab in project folder called keys user can able to see there dynamically generated keys in the tab which is shown in fig. 3. When user wants to create a new folder, then by click on create new folder, a new folder is created. Then if user want to upload the file in created folder. They have to first enter the private key to enter the file. Fig. 4 shows Upload file by entering private key. Once a dynamic private key is entered by user, users are allowed to upload the file. Here users are allowed to send the file to another user with message. While uploading the data by data owner the data is encrypted by using RSA algorithm. The data owner or receiver are allowed to see the received files. And can download the received files by click on the download file. Fig 5 shows Enter Public Key page. When receiver wants to download the file, User must enter the public key first. Fig. 6 shows Downloaded File page. Once a public is entered by user, then users are allowed to see the file with message by click on it. Also the message and file get decrypted. Screenshot 4.7 shows TPA scan page. The Most important feature in this dissertation is TPA (Third Party Auditor). TPA SCAN each and every file in user directory. Keep and watch on every file, Its source file details and current file status. IF any mismatched found means there is an Unauthorized Accessed to the file. If someone intruder deleted file from server then TPA shows message “Danger! Some one deleted File.” If the file is secure then show message “Secured File.”

Fig 1: User Login

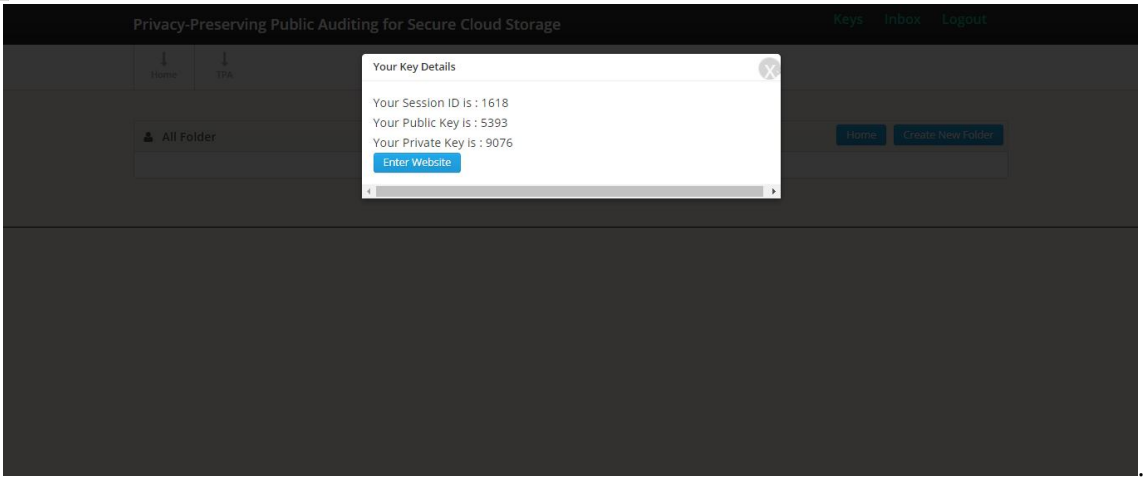


Fig 3: public and private key generation

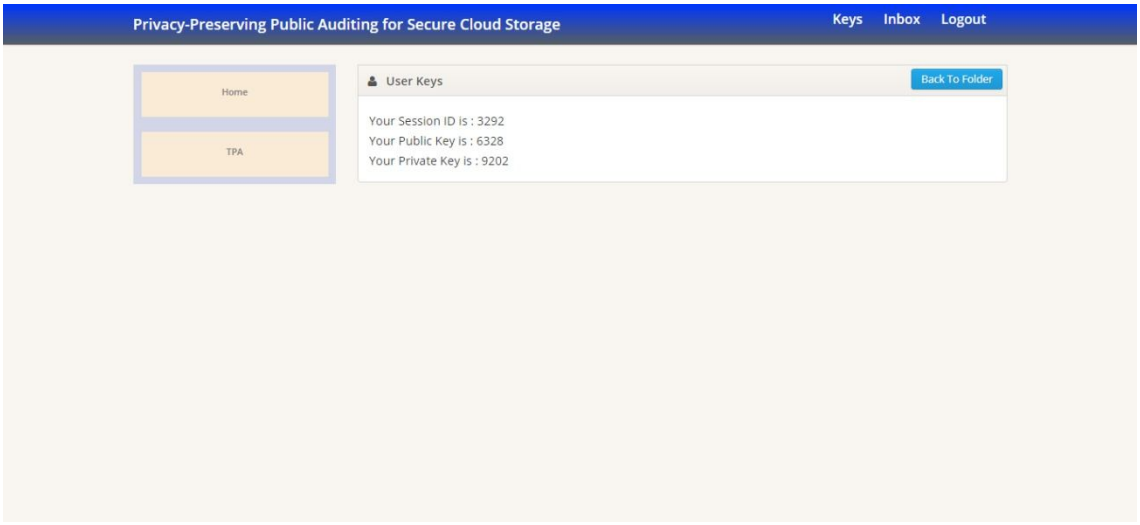


Fig 4: Dynamic key generation

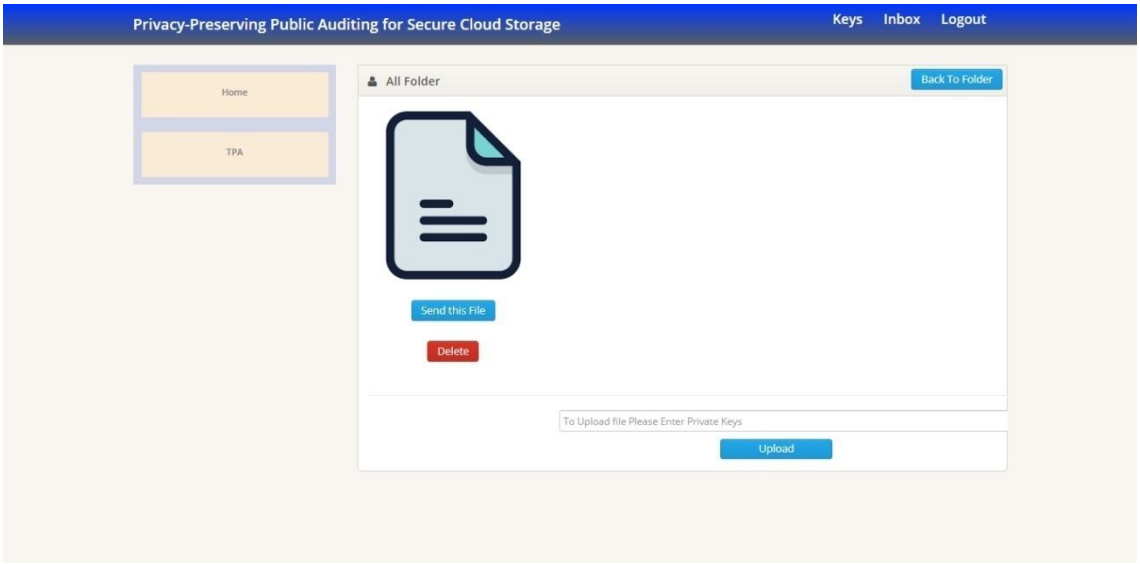


Fig 5: Upload file by entering private

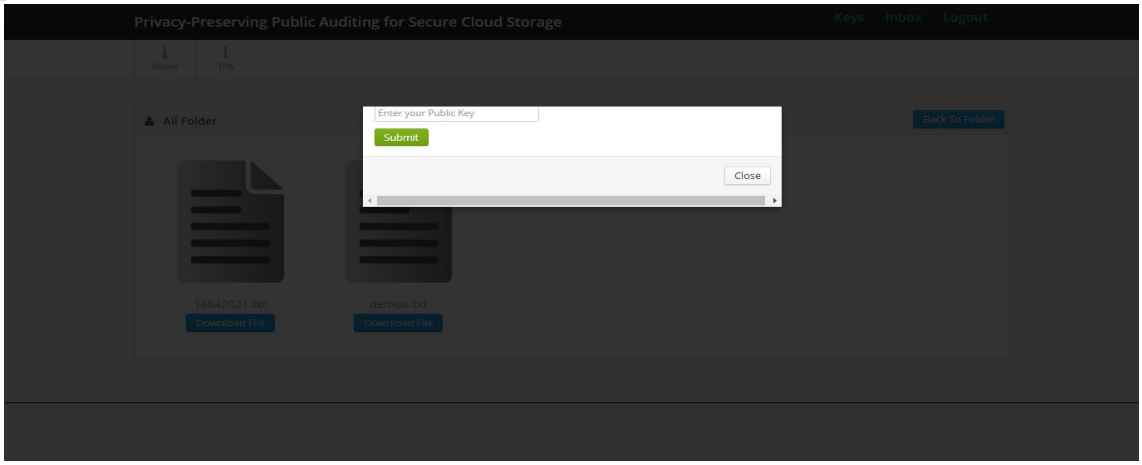


Fig 6: Enter Public Key

Fig 7: Downloaded File

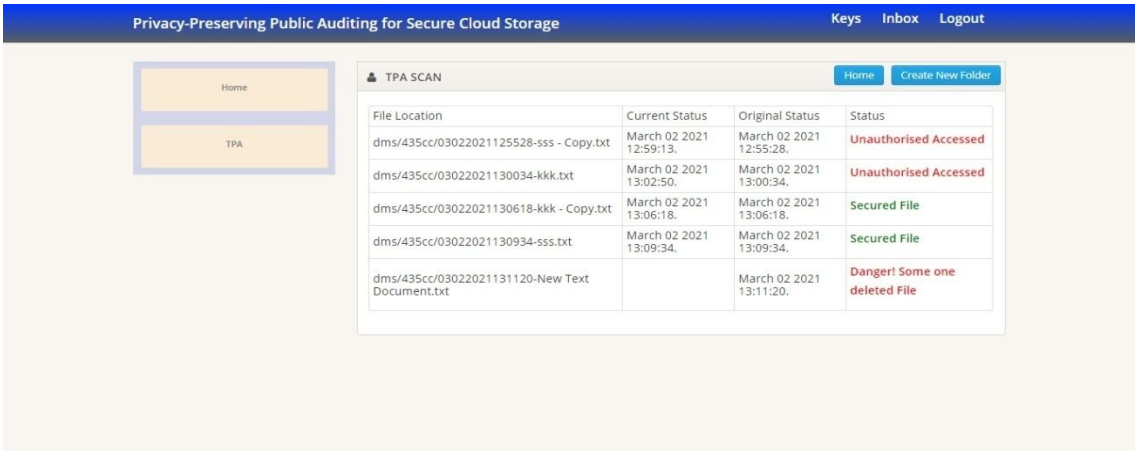


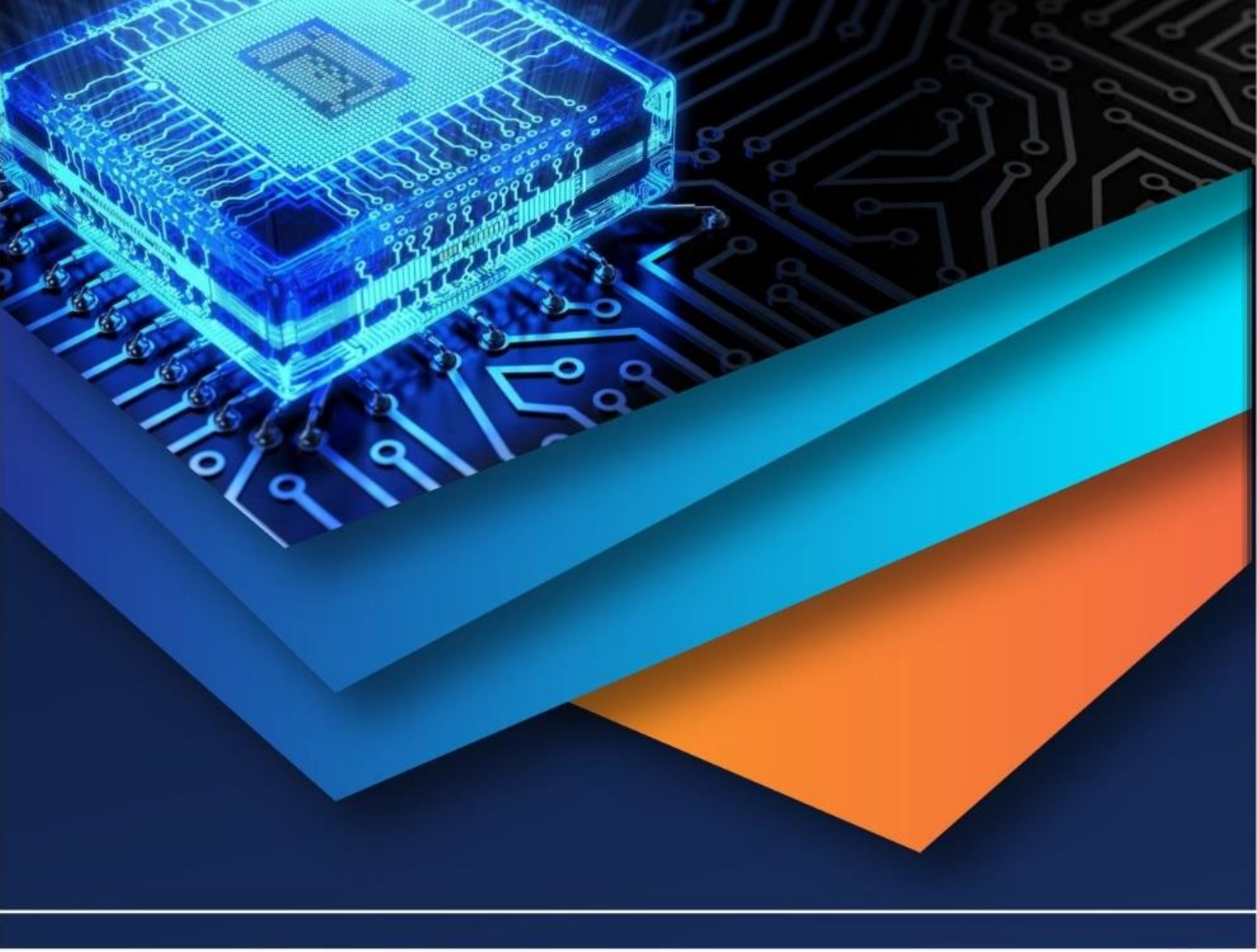
Fig 8: TPA Scan

V. CONCLUSIONS

A secure and economical privacy preserving public auditing scheme is been proposed. It achieves privacy preserving and public auditing for cloud by employing a TPA (Third Party Auditor), that will the auditing while not retrieving the data copy, thus privacy is preserved. the data stored within the encrypted format within the cloud storage, so maintaining the confidentiality of data. the data integrity is verified by. It only checks whether or not the stored data is tampered or not and informs regarding it to the user. a shot is made to overcome the restrictions of scheme auditing theme.

REFERENCES

[1] C. Wang, Q. Wang, K. Ren, a n d W. Lou, “Privacy- Preserving Public Auditing for Storage Security in Cloud Computing,” Proc. IEEE INFOCOM ¨10, Mar. 2010.
[2] P. Mell and T. Grance, “Draft NIST Working Definition of Cloud Computing,” http://csrc.nist.gov/groups/SNS/cloud- computing/index.html, June 2009.
[3] Pearson, S. 2012. Privacy, Security and Trust in Cloud Computing. Privacy and Security for Cloud Computing,3-42.
[4] Cloud Security Alliance, “Top Threats to Cloud Computing,” http://www.cloudsecurityalliance.org, 2010
[5] M. Arrington, “Gmail Disaster: Reports of Mass Email Deletions,” http://www.techcrunch.com/2006/12/28/gmail disasterreports- of-mass-email-deletions/, 2006.
[6] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, “Provable Data Possession at Untrusted Stores,” Proc. 14th ACM Conf. Computer and Comm. Security (CCS ¨07), pp. 598-609, 2007.
[7] G. Ateniese, R.D. Pietro, L.V. Mancini, and G. Tsudik, “Scalable and Efficient Provable Data Possession,” Proc. Int¨l Conf. Security and Privacy in Comm. Networks (SecureComm ¨08), pp. 1-10, 2008.
[8] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, “Remote Data Checking for Network Coding-based Distributed Stroage Systems,” in Proc. ACM Cloud Computing Security Workshop (CCSW), 2010, pp.31– 42.
[9] C. Erway, A. Kupcu, C. Papamanthou, and R. Tamassia,“Dynamic Provable Data Possession,” Proc. 16th ACM Conf.Computer and Comm. Security (CCS ¨09), 2009.
[10] A. Juels and J. Burton, S. Kaliski, “PORs: Proofs of Retrievability for Large Files,” Proc. ACM Conf. Computer and Comm. Security (CCS ¨07), pp. 584-597, Oct. 2007.
[11] M. Franz, P. Williams, B. Carbunar, S. Katzenbeisser, and R. Sion, “Oblivious Outsourced Storage with Delegation,” in Proc. Finan-cial Cryptography and Data Security Conference (FC), 2011, pp. 127– 140.
[12] R. L. Rivest, A. Shamir, and Y. Tauman, “How to Leak a Secret,” in Proc.International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT). Springer-Verlag, 2001, pp. 552– 565.
[13] M.A. Shah, M. Baker, J.C. Mogul, and R. Swaminathan, “Auditing to Keep Online Storage Services Honest,” Proc. 11th USENIX Workshop Hot Topics in Operating Systems(HotOS ¨07), pp. 1-6, 2007.
[14] R. Curtmola, O. Khan, and R. Burns, “Robust Remote Data Checking,” Proc. Fourth ACM Int¨l Workshop Storage Security and Survivability (StorageSS ¨08), pp. 63-68, 2008.
[15] K.D. Bowers, A. Juels, and A. Oprea, “Proofs of Retrievability: Theory and Implementation,” Proc. ACM Workshop Cloud Comput- ing Security (CCSW ¨09), pp. 43-54, 200



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY