iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 9 **Issue:** XII **Month of publication:** December 2021

DOI: https://doi.org/10.22214/ijraset.2021.39352

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: 7.429
Volume 9 Issue XII Dec 2021- Available at www.ijraset.com

A New Framework Approach Enhances Security to Efficient Remote Collaboration in TPA Scheme for Cloud Storage

Pallapu Himavanth Reddy[1], Gandicheruvu Vishwak Sein[2]
[1]*Department of CSE, TKR College Of Engineering and Technology, Hyderabad*
[2]*Department of MECH, MVSR Engineering College, Hyderabad*

Abstract: ***Cloud computing provides customers with storage as a service, allowing data to be stored, managed, and cached remotely. Users can also access it online. A major concern for users is the integrity of the data stored in the cloud, as it is possible for external invaders or criminals to attack, repair, or destroy the data stored in the cloud. Data auditing is a trending concept that involves hiring a third-party auditor to perform a data integrity test (TPA). The main purpose of this project is to provide a safe and effective testing system that combines features such as data integrity, confidentiality, and privacy protection. The cloud server is only used to store encrypted data blocks in the proposed system. It is not subject to any additional computer verification. TPA and the data owner are in charge of all the functions of the scheme. A variety of materials are used to evaluate the proposed audit process. The proposed solution meets all the processes while minimizing the load on cloud servers. Data dynamics actions such as data review, deletion, and installation will be performed in the future.***
Keywords: Cloud storage; Third Party Auditor; Public Auditing; Privacy Preserving; Integrity;

I. INTRODUCTION

"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction," according to the National Institute of Standards and Technology (NIST) definition [1].

Cloud computing is a type of computer-based system in which various services are delivered online to company computers and devices [2]. Data privacy, data security, data acquisition, data location, and secure data transfer are just a few issues to consider when it comes to cloud data security. Threats, data loss, service disruption, malicious external attacks, and multiple recruitment problems are just a few of the cloud security challenges. Data integrity refers to the accuracy of data stored in the cloud by users. Unauthorized users should not be able to modify or hack cloud-based data. Cloud computing companies are entrusted with ensuring the accuracy and integrity of the data. Users prefer to store their important and confidential data in the cloud, so data confidentiality is an important factor for them. To maintain data privacy, authentication, and access, control methods are used. The data privacy issue can be solved by ameliorating the reliability of cloud computing. As a result, from the user's perspective, data security, data integrity, privacy, and confidentiality of cloud-stored data are critical considerations [2]. New processes or strategies should be created and used to meet this need.

Data testing is a novel computer concept related to secure data storage. Testing is the process of verifying the accuracy of user data. It can be a user (data owner) or a third-party administrator (TPA). Helps to store data stored in the cloud. The verification function is divided into two categories: the first is the private audit, which only allows the user or owner of the data to check the integrity of the database. No one else has the authority to investigate the server for data. However, it often increases user authentication further. The second feature is a public research, which enables TPA to query a cloud server and validate data. TPA is a legal entity appointed to represent the client. It has all the necessary knowledge, skills, knowledge, and expertise to perform tasks to ensure integrity. It also lowers client overhead. TPA should monitor cloud data in a timely and efficient manner. There should be no idea which data is stored on the cloud server. It should not place the owner of cloud data under any additional Internet load [3].

Three network companies namely data owners, cloud servers, and TPA are located in the cloud. The data owner is responsible for storing the data on the storage server provided by the cloud service provider (CSP). TPA keeps a check on client data by ensuring the integrity of the data needed. Notify the data owner if any variance or error is detected in the data owner's data. Fig.1 shows the cloud data storage architecture.

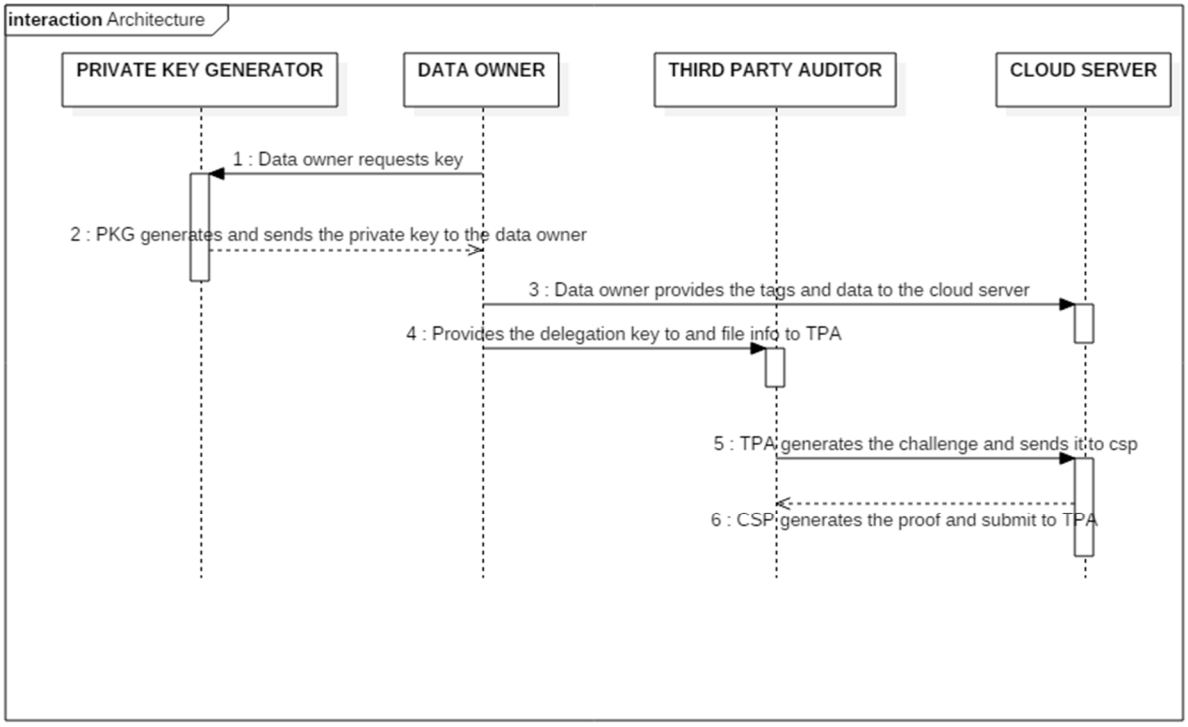


Fig. 1. System architecture

II. LITERATURE SURVEY

Cloud computing has a number of difficulties regarding the integrity and confidentiality of users' data stored in the cloud. From a user's perspective, developing a secure and effective solution to ensure the integrity and confidentiality of data stored in the cloud is essential. Wang et al. [4] presented a public auditing approach that preserves privacy. Data tested by independent TPA. A public key based on the Homomorphic linear authenticator (HLA) is used in conjunction with random hides for this purpose. However, existing phishing attacks, such as a message attack from a hard cloud server and an external attacker, are possible. Wang et al. [3] provided a new improved approach to this problem, much more secure than the previously recommended protocol [4]. With TPA, it is also a public research methodology. Designed for the purpose of conducting data research on behalf of users. Hides data using HLA created from BLS signature (Boneh-Lynn-Shacham short signature) and random encryption method. The new method uses a complex computer-based compilation process, which makes it inefficient. It is actually used in the Amazon EC2 model, which ensures that the design works quickly both in the cloud and at the end of the auditor. However, its full implementation in the public commercial cloud is yet to be confirmed. As a result, it is impossible to expect it to work reliably with large amounts of data [5].

By combining the BLS-based HS with the Merkle Hash Tree, Wang et al. [6] introduced an alternative approach that enables both community assessment and data flexibility (MHT). It guarantees data integrity, but fails to ensure data privacy in the cloud. Wang et al. [7] have developed a system that uses homomorphic token pre-computation to easily detect modified blocks, and then use the coded method to locate the required blocks on several servers. Solomon et al. [8] introduced a protocol with the same level of security as that of Wang et al. [5], but it works very well. Creates a signature set, which is a ordered set of signatures on each file block, resulting in additional calculations and transfer costs. Meenakshi et al. [9] introduced a method that uses TPA to test user data using the Merkle Hash Tree method. Allows data power, but does not guarantee that data stored in the cloud is secure. To establish data integrity through TPA, Tejaswini et al. [10] they rented a Merkle hash tree. Rivest, a Shamir Adleman (RSA)-based cryptographic system, maintains data confidentiality, while Jadhav et al. [11] created an offensive module that constantly monitors data changes in the cloud. Data is encrypted using Advanced Encryption (AES) method, which ensures confidentiality. Arasu et al. [12] has proposed a solution that uses a Hash Message Authentication Code (HMAC) with keys and homomorphic tokens. It tends to improve the safety of TPA. It is a way of ensuring the integrity of data sent between two parties by establishing a shared private key. HMACs are a shared key method based on both sides. An attacker or unauthorized user may generate fraudulent messages if a group key is in danger. Table I compares existing public research schemes that protect privacy.

The task of calculating the integrity of the data integrity test is now done by the cloud server, which is also responsible for storing large amounts of user data. As a result, storage capacity and the task of creating authentication credentials on the cloud server have increased. In the research process, there is a need to raise a system that does not load the load on the cloud server. All of the above factors are important and must be met in order for the system to be reliable. As a result, an effective and secure research system should be developed that can conduct public research effectively while ensuring the integrity and confidentiality of the database.

III. PROPOSED SYSTEM

In order to overcome the limitations of current accounting strategies, it is important to build an effective public auditing protocol. TPA is used to assess the accuracy of cloud data in the proposed system. Conducts periodic or audited audits. During the research process, it ensures that no data content is disclosed to TPA. Ensures the security and integrity of the data you store. Figure 2 shows the design of proposal

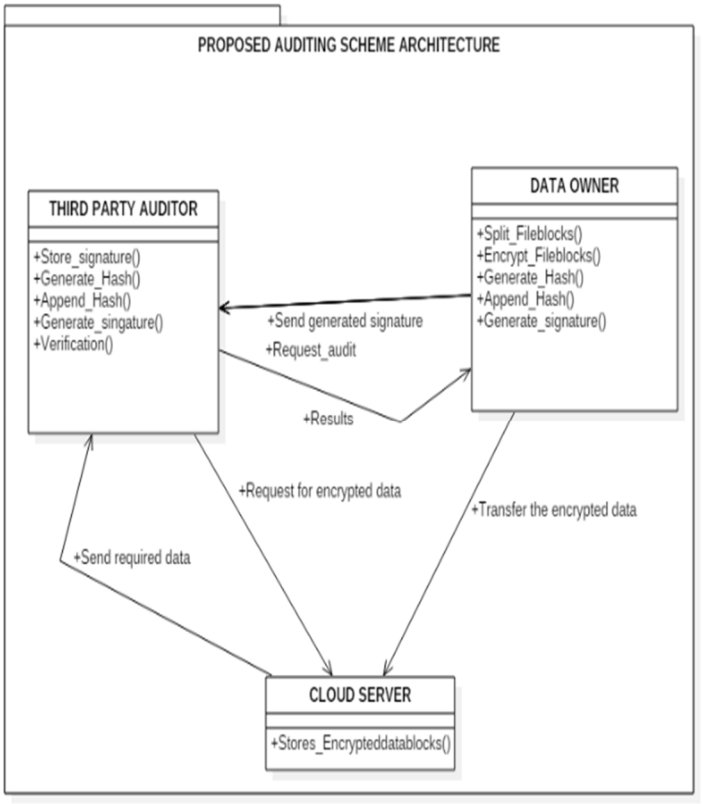


Fig.2. Proposed Auditing scheme Architecture (modified from [17])

Data owner, cloud server storage, and TPA are the three key elements in the proposed concept. The data owner manages to split the selected file into blocks, encrypt those blocks using the AES method, generate a Secured Hash Algorithm-2 (SHA-2) hash for each block, which includes all hashtags, and produces RSA (Rivest , Shamir Adleman) digital signature on it. The choice of the AES algorithm is based on its highest level of safety, speed, efficiency, ease of use, and flexibility [13]. The SHA-2 algorithm enables one-way hashing and non-collision hashing, which are two of the most important features of a solid hashing function. As a result, the proposed system [14] uses SHA-2 for making hashing. RSA's digital signature is used for a variety of purposes, including authentication, integrity, and non-verification.

Encrypted file blocks are only stored on the cloud server. As a result, they are not burdened with the added burden of proofreading. Proof of proof refers to the process of producing hashes of encrypted block hashes, assembling them, and creating a digital signature for verification. TPA is responsible for completing this task. Sequential diagram is used to show how the proposed system works. Shows interaction between data owner, TPA, and cloud server. The connection between user, data holder, TPA, and cloud server is shown in Figure 3.

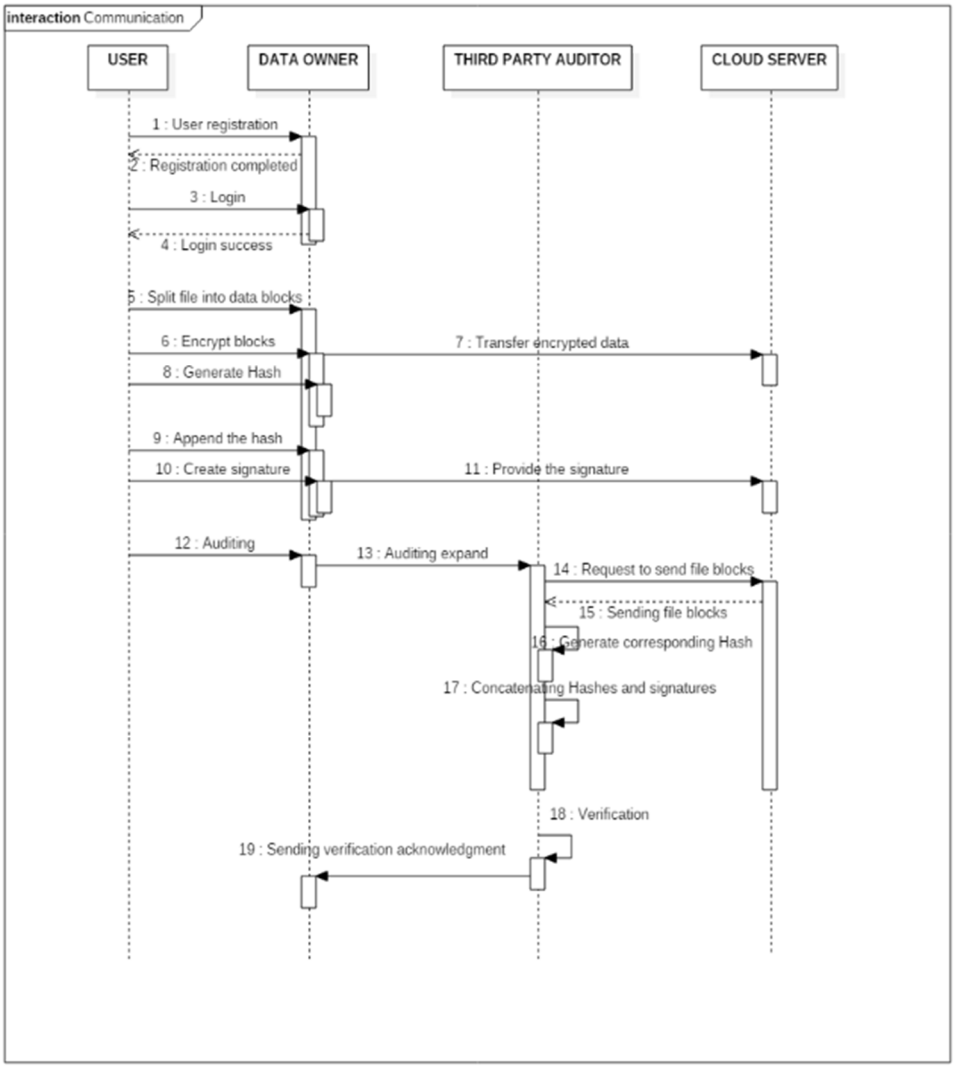


Fig.3. Communication between User, Data owner, TPA and Cloud server

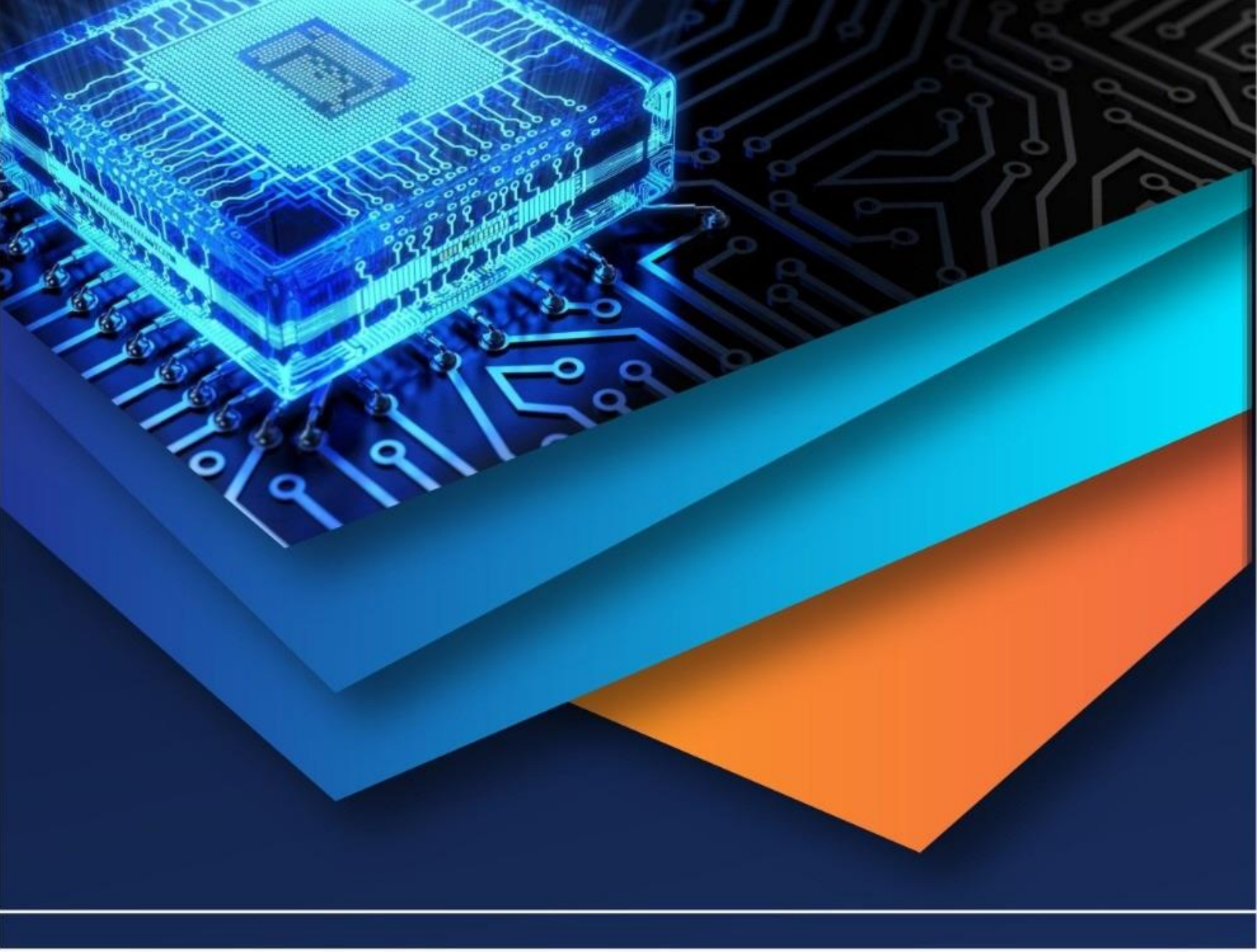
When TPA receives a data test request from a data owner or user, it immediately requests the encrypted data blocks on the cloud server. It calculates the hash value of each block of files encrypted after receiving data, using the same speed method used by the data owner to generate hashes. It then compiles hash values and generates RSA digital signature on it. TPA compares the signature issued by the TPA with the one stored in the TPA compiled by the data holder throughout the verification process to ensure the integrity of the data. If they are identical, it means that the data stored in the cloud is secure and has not been compromised by outsiders. If they do not match, then data integrity is compromised. The owner of the data receives notification of receipt of the integrity check of the research process data.

IV. CONCLUSION AND FUTURE WORK

The safest and most effective public research methodology while promoting anonymity is suggested. With the help of the TPA, public audits can be performed while maintaining confidentiality. Checks without receiving a copy of the data, respecting the privacy of the data. Data is categorized and stored in an encrypted cloud, which ensures data privacy. TPA confirms the integrity of the data at the request of the data owner by comparing two signatures, one created by the data owner and the other produced by TPA. It just confirms if the saved data has been looted and notifies the data owner. Only encrypted version of the data stored on the cloud server. Because the cloud server does not include a virtual computer verification, the Internet load of the cloud server decreases. The proposed solution meets all test methods while minimizing the load on cloud servers. Flexible data actions such as data updates, deletions, and insertions will be performed in the future.

REFERENCES

[1] P. Mell and T. Grance, "The NIST definition of cloud computing," Communications of the ACM, vol. 53, no. 6, 2010.
[2] D. Zissis and D. Lekkas, "Addressing cloud computing security issues," Future Generation Computer Systems, vol. 28, no. 3, pp. 583–592, Mar. 2012.
[3] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," http://eprint.iacr.org/2009/579.pdf.
[4] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving and public auditing service for data storage in cloud computing," INFOCOM, 2010 Proceedings IEEE, pp. 1–9, 2010.
[5] C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," IEEE Transactions on Computers, vol. 62, no. 2, pp. 362–375, Feb. 2013.
[6] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling Public Auditability and data dynamics for storage security in cloud computing," IEEE Transactions on Parallel and Distributed Systems, vol. 22, no. 5, pp. 847–859, May 2011.
[7] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," IEEE Transactions on Services Computing, vol. 5, no. 2, pp. 220–232, Apr. 2012.
[8] S. G. Work u, C. Xu, J. Zhao, and X. He, "Secure and efficient privacy preserving public auditing scheme for cloud storage," Computers & Electrical Engineering, vol. 40, no. 5, pp. 1703–1713, Jul. 2014.
[9] M. IK and S. George, "Cloud server storage security using TPA," International Journal of Advanced Research in Computer Science & Technology (IJARCST), 2014.
[10] V. Tejaswini, K. Sunitha, and S. K. Prashanth, "Privacy-preserving and public auditing service for data storage in cloud computing," Paripex - Indian Journal Of Research, vol. 2, no. 2, pp. 131–133, Jan. 2012.
[11] S. Jadhav and B. R. Nandwalkar, "Privacy-preserving and batch auditing in secure cloud storage using AES," Proceedings of 13th IRF International Conference, 2014.
[12] A. S Ezhil, B. Gowari, and S. Ananthi, "Privacy-preserving public auditing in the cloud using HMAC algorithm, "International Journal of Recent Technology and Engineering (IJRTE) ISSN, vol. 2277, 2013.
[13] N. Penchalaiah and R. Seshadri, "Effective Comparison and evaluation of DES and Rijndael Algorithm (AES)," International Journal of Computer Science and Engineering, vol. 2, no. 05, p. 1641—1645, 2010.
[14] C. Paar and J. Pelzl, Understanding Cryptography: A textbook for students and practitioners. Heidelberg: Springer-Verlag Berlin and Heidelberg GmbH & Co. K, 2009.
[15] S Dhanaya. Privacy-preserving third-party auditing in the cloud. Dissertation report, 2015.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY