Double Encryption Based Remote Data Integrity Checking With Preserving Data For Cloud Storage

S.Dhara,M.Kamarunisha,S.Aarthi,P.Sasikala

**Department of computer Applications,Dhanalakshmi Srinivasan College of Arts and Science for Women,,Perambalur , 621 212, Tamilnadu, , India.*

Email: dhara78956@yahoo.com *(Dhara S) Corresponding author: Dhara S*

***Abstract*—Cloud computing is a computer technique, and the Internet has become more widespread in recent times. Sharing the software and hardware resources, and providing resources to a user's laptop or mobile phone, is possible. Because cloud computing may combine resources, the customer can benefit from a more efficient service provider. When it comes to a user's perspective, which encompasses both people and IT infrastructures, on-demand cloud storage offers enticing benefits such as the ability to access data from any place and the ability to avoid capital expenditures on hardware or software. There must be no additional load on the cloud user, and the third-party auditor (TPA) must not introduce new vulnerabilities into the user's private information storage, in order for a successful TPA to be implemented. Public auditability suggests that the data owner allows others to verify the data owner's data is inefficient. In well-known, the owner of the data may also have a number of cloud storage provider documents. Statistics owners can't check their information often since doing so would use up their resources, which can't be used for any other purpose. Using the public auditing protocols and the twofold encryption approach, create a privacy-preserving public cloud information auditing machine that fulfils all integrity checks without leaking records. On the other hand, we also investigate the on-line signature method to expand our basic end result into a multi-user environment where TPA may concurrently do numerous auditing requirements. We can use a double encryption technique to encrypt the statistics and cloud server data three times before they are sent over the wire.**

Index Terms—**Cloud Framework, Public Auditing, Data Integrity Protection, Double Encryption, Multi User Setting**

I. INTRODUCTION

Using a large pool of devices, private or public networks, and dynamically expandable infrastructure, cloud computing provides software, data, and file storage services. The costs of processing, software internet hosting, content storage, and delivery have reduced significantly since the beginning of this era. You may reap the benefits of direct rate advantages, as well as change an information centre from a capital-intensive set-up to an environment that is variable-priced. The underlying principle of cloud computing is that IT skills may be repurposed. When compared to "grid computing," "distributed computing," "software computing," or "autonomous computing," cloud computing provides a new set of development opportunities for organisations. Forrester [1] describes the cloud computing model. As a result of this, users and businesses may utiliseprogrammes without having to install them on their computers, as well as view their personal papers from any computer with internet connection. With the assistance of centralising data storage, processing, and bandwidth, this generation allows for much more unskilled computing. Yahoo mail, Gmail, and Hotmail are all instances of cloud computing. Despite the fact that cloud computing has been around for a long time, its present expansion necessitates a closer examination of its real-world impact on privacy and confidentiality concerns. It is impossible to use standard cryptographic primitives for data security since consumers no longer physically control the storage space in their records. Due to I/O and transmission rate costs, it's not feasible to download all data and perform a complete integrity check at a later date. Public auditing services will play an important role in helping this new cloud financial system emerge as fully integrated, in which customers will require methods for risk and reward assessment to be taken into account within the cloud. Figure 1 depicts the cloud's fundamental structure.

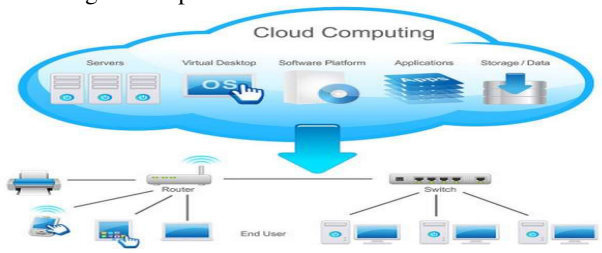

Fig 1: Cloud Deployment Model

II. RELATED WORK

In the words of G. Ateniese and others: Leakage-resistant ID methods may be built using publicly verifiable proofs of storage (PoS) that may be computationally zero-information. [1] (ZK). Customers may use PoS to verify that a server is doing what it says it's doing when it comes to keeping track of their purchases. This means that a PoS may be validated publically if everyone who has access to a user's public-key can verify the server's storage and that it is computationally ZK if the verification segment leaks no helpful information about the document to a bound adversary. We show how to put together a scheme based on the assumption of RSA. This protocol's secret key is a randomly created record encoded with the generic public key for PoS, and its public secret is the state information produced by encoding this document. The prover uses the PoS verification phase with the verifier to prove that it possesses the file in order to identify itself. An identity protocol may be built using 0-understanding proof-of-garage methods in the bounded retrieval version (BRM). Leakage-resistant identification protocols may now be built on this version of BRM, thanks to our framework, which gives new insights into the BRM.

Z. Fu, K. Ren, et. al., and a host of others

[2] Searchable encryption is a common method for searching encrypted data, and a number of useful techniques have been proposed for various uses. As a result, searchable encryption systems based on keywords can no longer meet the challenges of the new challenge and the rising demands of consumers. As a first step, many current methods adopt the "one size fits all" concept, ignoring the unique interests and cultural backgrounds of individual users. There may be a large amount of network bandwidth used in such methods since the cloud returns all files that meet the user's query. Furthermore, it will take a lot of time and resources for the user to sort through a huge number of files to find the ones he is interested in. Because of the value or importance of the query phrases, different users may find various items relevant in the actual application of customised search, showing the need for personalised search. If you can't grasp the user's purpose, how can you develop a search engine that does? Because of this, these systems can't be immediately applied to searchable encryption schemes. The artificial method of gauging term choice has a high degree of unpredictability and fails to take individual users' search histories into account. In addition, most of these methods only allow for specific keyword searches. Because of this, the user's input is all that matters when it comes to the output. The user may be dissatisfied if just a few matching results are provided while searching for phrases that are difficult to find.

Researchers Z.Hao, S.Zhong, et al. [3] It examined the method through which a growing number of consumers save their most important data in the cloud, without keeping a copy on their own computers. Customers must guarantee that the data they save in the cloud is not lost or damaged at all times. Despite the fact that it is simple to verify the integrity of data after it has been downloaded, downloading large amounts of data only to verify the integrity of data is a waste of communication capacity. There have therefore been a number of efforts to build remote statistics integrity checking protocols that enable the integrity of the facts to be confirmed without downloading the facts. Consequently. Consumers may ask the server about the integrity of a particular data document using remote information integrity checking protocols, and the server responds with evidence that it has access to the whole and uncorrupted statistics. Simply said, customers need to be able to check record integrity in an endless number of ways without gaining access to the whole genuine facts report during record integrity verification. As a result, the protocol wants to be protected against a hostile server that tries to pass the facts integrity verification without access to the whole and uncorrupted data set. Those enhanced skills may be required at the same time in a real-world application. When it comes to document management, don't forget to include an online document machine. It is also possible for the client and her companions to work together on a file. As soon as a client or a member of her group makes changes to a document, the report and the tags should be updated as well.

Implemented by H.Liu, L. Chen, and others

A slew of benefits to this unique storage approach are driving up the popularity of Cloud storage. There are already millions of people throughout the globe using cloud storage systems like Amazon S3, Google Cloud, and Microsoft Skydrive. Cloud storage offers a number of advantages over conventional storage methods, such as reducing the burden of storage management, eliminating capital investment on hardware, software, and people upkeep, and providing access to data from a variety of geographic locations. Using this paper, we demonstrate that the structure is not secure in their security model or in a correct security model. It is possible for a malicious cloud server to respond to an audit challenge from a third-party auditor (TPA) even if all of a user's files have been wiped or corrupted by the server. Malicious cloud servers may discard data that has not been or is rarely accessed for financial reasons because cloud servers are not fully trusted. To ensure that their data on the cloud is safe and secure, cloud users need to have strong evidence that their data is not tampered with or partially deleted. To ensure data confidentiality, the auditing process cannot be used to recover the entire file, which is similar to one-way encryption. Since no scheme can be demonstrated to be safe in this model's framework, the model's concept of security is unrealistic.

A study by J. K. Liu, et al. [5] found that end users access cloud-based apps through a web browser or thin client, while the business software and user data are kept on faraway servers. There are several advantages to using web-based cloud computing services, such as lower expenses and capital expenditures, improved operational efficiency, and the capacity to scale up and down as needed. The new cloud computing paradigm has many benefits, but security and privacy are major problems, particularly for web-based cloud services. First of all, it is quite normal to share a computer with many others. It's simple for hackers to install spyware on a web browser and get access to a user's login password [6]-[12].

III. EXISTING METHODOLOGIES

There are many advantages to cloud computing, but it also has serious drawbacks, such as bankruptcy and a lack of security for consumer data. To outsource your data, you're giving up a lot of control since cloud carriers (CSP) are independent

administrative organisations. As a consequence, the accuracy of the data stored in the cloud is in jeopardy for the reasons listed below. Despite the fact that cloud computing infrastructures are more powerful and reliable than private computers, they nonetheless face a broad range of both internal and external risks to data integrity. Examples of cloud service failures and security breaches occur from time to time. It is also possible for CSPs to be dishonest in their dealings with cloud customers on the status of their outsourced statistics. In order to save money, a CSP may dispose of data that is seldom or never accessed, or hide data loss occurrences in order to preserve a positive reputation. Overall, although moving data to the cloud is a cost-effective option for long-term, large-scale storage, there is no guarantee that the data will remain accurate or readily available. If this issue isn't solved, cloud architecture may be hindered. Conventional cryptographic primitives for data security protection cannot be immediately applied since consumers no longer control the storage of their information. To be exact, downloading all the facts for integrity verification isn't a viable option because of the high I/O and transmission costs throughout the community. If you can access the data, it may be difficult to find the data corruption since it doesn't provide customers [2] accuracy guarantee for the un-accessed data and may be too late to repair the data loss or damage.

3.1. WATERMARKING SCHEME

They have full power to inspect the crucial item and send it to the server. Compression technique for watermark photo to decrease verbal exchange overhead may also be used to reduce verbal exchange overhead when watermarking photos, so that statistics or images cannot be detected by attackers in the cloud. Embedded, verbal exchange channel, and detector all play major roles in watermarking. For the purpose of protecting legitimate data, watermark statistics are included into the original picture and then encrypted to ensure their integrity. The name of the game key is used to transmit data across different formats using an encryption approach similar to embedded. Decryption is performed in reverse using the same detector approach as detection. Before the watermarked image is broadcast across the communication channel, the watermark information is incorporated in the legitimate picture to allow the watermark image to be identified at the receiving end.

In the system known as "ORUTA," the goal is to have only one ring that controls everything.

Then ORUTA was built, which is a public auditing solution for shared statistics in an untrusted cloud that maintains anonymity. Using ring signatures, homomorphic authenticators may be built in Oruta, allowing the third birthday celebration auditor to verify the integrity of shared facts for a specific number of clients without having to get the complete data set, all while keeping the signer's identity private in the TPA. To make use of batch auditing, which examines many pieces of shared data at the same time, the method should be enhanced. Even while public audits continue, Oruta maintains data privacy by using random masking, as well as index hash tables, to aid in completely dynamic operations on shared information. A dynamic operation illustrates a single block in shared facts being inserted, deleted, or updated. It is our goal in this research to best recall how cloud-based stats supplied with static agencies may be audited for veracity. Pre-described groups are formed in advance of cloud data storage and client membership in those groups does not alter at some future, as yet undefined, point in time. Real people are responsible for selecting who may share their data before moving it to the cloud. This is a fascinating challenge, since it allows dynamic companies to verify shared data integrity in the cloud while still safeguarding the identity privacy of its members, such as when a new user joins the group and an existing employee member is cancelled.

IV. PROPOSED METHODS

There are three parties involved in this project's Machine version: a cloud server, a group of users, and a third, anonymous third party. Customer types include the actual individual, as well as those who are members of an institution. The legitimate user initially generates shared records in the cloud and shares them with other users of the institution. The firm treats both consumers like people, regardless of whether they are individuals or institutions. There are no restrictions on who has access to or may make changes to the shared information. Data and its verification information (e.g. Signatures) are both stored in the cloud server. It is possible for a 3rd-birthday party auditor (TPA) providing professional information auditing services or an outside records user to publicly certify the integrity of shared information kept on a cloud server. The first step in doing a cloud server audit is sending an auditing project to a public verifier. When a cloud server receives an auditing undertaking, it sends back an auditing evidence to the public verifier. Finally, this public verifier assesses the accuracy of the whole statistics by confirming the auditing proof's correctness. As a general rule, public auditing is a two-way exchange between a public verifier and the cloud's server.

Audits by the government To verify the integrity of information shared in the cloud, public verifiers don't necessarily need to go through all of the data themselves.

Correctness Verifying the integrity of shared information may be done by a public verifier.

Unforgetability Creating valid verification metadata (i.e. signatures) on shared facts may only be done by a single member of the group.

Personal Data Security Through auditing, a public verifier is unable to determine the signer's identity for any block in a shared record.

Access and sharing of cloud-provided resources is made possible via the usage of cloud computing and storage. Cloud storage systems, such as DropBox, iCloud, and Google Drive, have grown more popular because they allow users to share data with others in a group. Perhaps the most effective way to ensure that cloud data is accurate is to use a classic strategy like this. Conventional cloud statistics methods may not be as effective as previously thought. To put it simply, the size of cloud recordings is enormous. Cloud records must be downloaded to ensure data integrity; doing so will cost or even squander the resources of users, especially if the cloud data has been damaged. Public auditing is a term that refers to the

process of verifying the integrity of cloud-based data without having to download all of the data at once, which has recently been suggested by a number of techniques. Statistics are broken down into several little chunks, each of which is separately signed by the owner, and during integrity verification a random mixture of all the blocks is received instead of the whole facts.. Batch auditing techniques may now be designed to execute a variety of tasks simultaneously, while user-stage data protection ensures that no information is leaked. Figure 2 depicts the suggested framework[13-22].

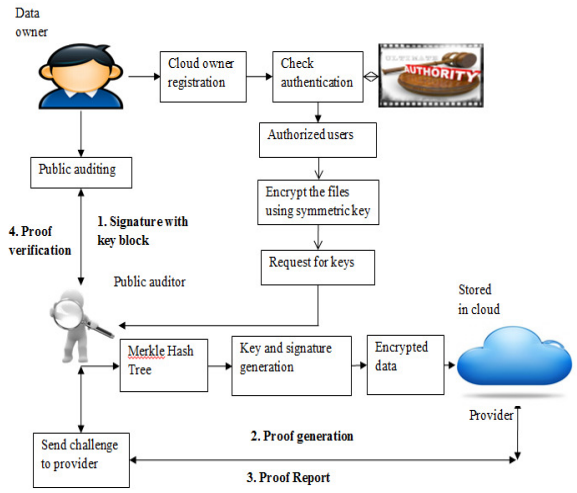

Fig 2. Proposed Framework

V. CONCLUSION

In a prior research, cloud computing security was discussed and assessed. Privacy risks and ways for defeating them are examined in this projectscope. .'s In order to maintain anonymity, some approaches employed standard cryptography methods, while others hid them away and instead relied on trade ways to accomplish so. It's also explored how to maintain confidentiality during public audits. As a result, cloud users need to know that their data is safe and secure at all times, regardless of where it is stored, processed, or accessed. In order to defend against accidental or purposeful rollbacks, data freshness is essential. An authenticated document device that helps migrate an enterprise-magnificence distributed file device into the cloud effectively, transparently, and scalable may be increased by keeping the data up to date. An enterprise tenant may verify that data collected from the record device is up-to-date by authenticating it during the record device's activities. In order to administer the records, the individual must have full access to them. In addition, cloud software should always be accompanied by strong security measures. Many of these would be necessary to achieve the long-awaited vision of secure Cloud Computing in the near future.

REFERENCES

[1] G. Ateniese, A. Faonio, and S. Kamara, “Leakage-resilient identification schemes from zero-knowledge proofs of storage,” in IMA Inte. Conf. Cryptography and Coding, 2015, pp. 311–328.

[2] Z. Fu, K. Ren, J. Shu, X. Sun, and F. Huang, “Enabling personalized search over encrypted outsourced data with efficiency improvement,” IEEE Trans. Parallel Distrib.Syst., doi.10.1109/TPDS. 2015.2506573.

[3] Z. Hao, S. Zhong, and N. Yu, “A privacy-preserving remote data integrity checking protocol with data dynamics and public verifiability,” IEEE Trans. Knowl.Data Eng., vol.23, no.9, pp.1432-1437, 2011.

[4] H. Liu, L. Chen, Z. Davar, and M. Pour, “Insecurity of an efficient privacy-preserving public auditing scheme for cloud data storage,” J. Universal Comput.Sci., vol. 21, no. 3, pp. 473–482, 2015.

[5] J. K. Liu, M. H. Au, X. Huang, R. Lu, and J. Li, “Fine-grained twofactor access control for web-Based cloud computing services,” IEEE Trans. Inf. Forens. Security, vol. 11, no. 3, pp. 484–497, 2016.

[6] F. Seb´e, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J. J. Quisquater, “Efficient remote data possession checking in critical information infrastructures,” IEEE Trans. Knowl. Data Eng., vol. 20, no.8, pp. 1034–1038, 2008

[7] C. Wang, Q. Wang, S. C, K. Ren, and W. Lou, “Privacy-preserving public auditing for secure cloud storage,” IEEE Trans. Comput., vol. 62, no. 2, pp. 362–375, 2013.

[8] C. Wang, Q. Wang, K. Ren, and W. Lou, “Privacy-preserving public auditing for data storage security in cloud computing,” in Proc. IEEE Int. Conf. Comput.Commun. (INFOCOM), 2010, pp. 1–9.

[9] Z. Xia, X. Wang, X. Sun, and Q. Wang, “A secure and dynamic multi-keyword ranked search scheme over encrypted cloud data,” IEEE Trans. Parallel Distrib. Syst., vol. 27, no. 2, pp. 340-352, 2015.

[10] S.Kannadhasan, G.Karthikeyan and V.Sethupathi, A Graph Theory Based Energy Efficient Clustering Techniques in Wireless Sensor Networks. Information and Communication Technologies Organized by Noorul Islam University (ICT 2013) Nagercoil on 11-12 April 2013, Published for Conference Proceedings by IEEE Explore Digital Library 978-1-4673-5758-6/13 @2013 IEEE

[11] L. Zhang, Q. Wu, J. Domingo-Ferrer, B. Qin, and Z. Dong, "Round-efficient and sender-unrestricted dynamic group key agreement protocol for secure group communications," IEEE Trans. Inf. Forens.Security, vol. 10, no. 11, pp. 2352-2364, 2015.

[12] S.Kannadhasan and R.Suresh, EMD Algorithm for Robust Image Watermarking. Recent Advances in Mechanical Engineering and Interdisciplinary Developments Organized by Ponjesly College of Engineering (ICRAMID 2014) Nagercoil on 7-8 March 2014, Published for Advanced Materials Research Vols.984-985 (2014) PP 1255-1260, ISSN No:1022-6680

[13] Singh, D., Buddhi, D., & Karthick, A. (2022). Productivity enhancement of solar still through heat transfer enhancement techniques in latent heat storage system: a review. Environmental Science and Pollution Research, 1-34.

[14] Haseena, S., Saroja, S., Madavan, R., Karthick, A., Pant, B., & Kifetew, M. (2022). Prediction of the Age and Gender Based on Human Face Images Based on Deep Learning Algorithm. Computational and Mathematical Methods in Medicine, 2022.

[15] Jasti, V., Kumar, G. K., Kumar, M. S., Maheshwari, V., Jayagopal, P., Pant, B., ... & Muhibbullah, M. (2022). Relevant-based feature ranking (RBFR) method for text classification based on machine learning algorithm. Journal of Nanomaterials, 2022.

[16] Babu, J. C., Kumar, M. S., Jayagopal, P., Sathishkumar, V. E., Rajendran, S., Kumar, S., ... & Mahseena, A. M. (2022). IoT-based intelligent system for internal crack detection in building blocks. Journal of Nanomaterials, 2022.

[17] Chidambaram, S., Ganesh, S. S., Karthick, A., Jayagopal, P., Balachander, B., & Manoharan, S. (2022). Diagnosing Breast Cancer Based on the Adaptive Neuro-Fuzzy Inference System. Computational and Mathematical Methods in Medicine, 2022.

[18] Saroja, S., Madavan, R., Haseena, S., Pepsi, M., Karthick, A., Mohanavel, V., & Muhibbullah, M. (2022). Human centered decision-making for COVID-19 testing center location selection: Tamil Nadu—a case study. Computational and Mathematical Methods in Medicine, 2022.

[19] Kumar, R. R., Thanigaivel, S., Priya, A. K., Karthick, A., Malla, C., Jayaraman, P., ... & Karami, A. M. (2022). Fabrication of MnO2 Nanocomposite on GO Functionalized with Advanced Electrode Material for Supercapacitors. Journal of Nanomaterials, 2022.

[20] Karthick, A., Mohanavel, V., Chinnaiyan, V. K., Karpagam, J., Baranilingesan, I., & Rajkumar, S. (2022). State of charge prediction of battery management system for electric vehicles. In Active Electrical Distribution Network (pp. 163-180). Academic Press.

[21] Bharathwaaj, R., Mohanavel, V., Karthick, A., Vasanthaseelan, S., Ravichandran, M., Sakthi, T., & Rajkumar, S. (2022). Modeling of permanent magnet synchronous motor for zero-emission vehicles. In Active Electrical Distribution Network (pp. 121-144). Academic Press.

[22] Jayalakshmi, Y., Subramaniam, U., Baranilingesan, I., Karthick, A., Rahim, R., & Ghosh, A. (2021). Novel Multi-Time Scale Deep Learning Algorithm for Solar Irradiance Forecasting. Energies 2021, 14, 2404.