How to Cite:
Faritha Banu, J., Kirti, S., Archana, T., & Pandey, U. K. (2022). Third-party enabled auditing for uniqueness-based integrity and data sharing with information hiding. *International Journal of Health Sciences*, *6*(S2), 9083–9091. https://doi.org/10.53730/ijhs.v6nS2.7373

Third-party enabled auditing for uniqueness-based integrity and data sharing with information hiding

Faritha Banu J
Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, India
Corresponding author email: banujahir@gmail.com

Shruti Kirti
Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, India
Email: sk5466@srmist.edu.in

Archana T
Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, India
Email: achu.cse@gmail.com

Utsav Krishna Pandey
Department of Computer Science and Engineering, SRM Institute of Science and Technology, Ramapuram, Chennai, India
Email: up4789@srmist.edu.in

***Abstract*---**The majority data are now kept in the cloud. There are many Cloud storage applications used to exchange data that range from normal to highly sensitive. Among the most essential security measures in cloud is Cloud auditing. It is the process of validating the reliability of data stored in the cloud. As of the inevitability of hardware problems, system failures and errors by people these data may be corrupted or lost. An efficient auditing system to determine whether or not the data is corrupted is a challenging task among the recent research. This paper proposes a third-party enabled auditing methodology to ensure data integrity, privacy data sharing and protect against outside attackers in the public cloud. In this proposed method, the record / data owner generates signatures or add sanitizer before importing sensitive data blocks into the cloud. The record blocks that report sensitive data are sanitized, and the signatures of those records blocks are converted into legitimate ones for the sanitized report. As a result, the records saved in the cloud have the

identical signature. Then a third-party auditor is implemented to confirm the cloud's storage accuracy by validating the reliability of the cloud records on the person's behalf.

Keywords---image retrieval, histogram, content-based retrieval, image fusion, image segmentation**.**

Introduction

Nowadays, storing the data in the cloud is essential for many real time applications. It might range from routine data to highly sensitive information. Cloud computing is a widely used computer paradigm that allows end users to access customizable resources from any device, at any time, from anywhere. Cloud computing has advanced considerably during the last few years. However, as the Internet of Things grows, the downsides of cloud computing (such as excessive latency) are being revealed between the cloud and end users. As a result, it is proposed to use Data Auditing to ensure the privacy of such sensitive information. A variety of audits are frequently required when creating and receiving approval for a quality management of cloud storage system. These audits are carried out by various bodies both within and outside the business. When a firm chooses to establish a quality management system (QMS) that complies with a set of standards, such as ISO 9001, it employs an independent agency to conduct an audit to certify that it has satisfied these requirements. Certification organizations are non-profit organizations that conduct audits to confirm that the QMS meets all of the standards of the stated specification and maintains compliance over time. Firms that have been approved by them are subsequently given certification. This can be used to convince clients that the certified company's QMS complies with the stated standard's standards.

Similarly, the suggested system employs a third-party auditor (TPA) to ensure and maintain the privacy of data kept in the public cloud, as well as to safeguard against outside threats. The device has a sanitizer that is used to sanitize the information blocks that contain sensitive data. The file's sensitive data blocks are sanitized, and their signatures are converted for the sanitized file into legitimate ones. As a result, all cloud-based data of the user will have the same signature. In the proposed approach, a third-party auditor verifies the reliability of cloud data on behalf of the user. There is no conflict of interest with the audited body because they are independent. Fog computing, which extends the cloud to the network's edge. Fog computing, in particular, Processes communication between the cloud and end users through a fog intermediary layer. As a result, fog computing is typically considered a cloud computing extension. Because of the fog layer's inherent data security and privacy design challenges, data protection methods cannot readily be applied to fog computing [1,12].

Literature Survey

In order to keep the data shared safe and secure, several solutions are implemented that allow third-party auditors to assess data without extracting all of the users' data from the cloud. A unique privacy-aware public auditing

technique for public cloud storage data is built by generating a homomorphic reliable group signature. Unlike other techniques, this one necessitates collaboration between at least to set of managers to recover a trace key, prohibiting misuse of sole-authority power and ensuring non-frameability. This approach also ensures that users may trace data changes using a tree structure and restore the most recent correct data block if the present information block becomes corrupted [2].

SeShare is a blockchain-based data storage system that achieves signature uniqueness, solving the problem of multiple group users creating signatures for the same file at the same time. When a file has multiple signatures, it is recorded in a blockchain in linear order, and only one individual is permitted to add additional signatures at the end of the chain. SeShare, on the other hand, presents a public auditing mechanism for data expenditures. In contrast to the preceding stable CECS method, this scheme minimizes (slash) integrity when a group user exits the group to provide a safe way to share data [3,10].

Panda, a public data auditing protocol, has recently been proposed to assure the accuracy of sahred data. Panda is notable for its data sharing and user cancelation capabilities. Panda is inappropriately weak in that it allows a cloud server to keep data loss from being discovered. It demonstrates that if some stored blocks are lost, the server may still produce a valid proof by substituting another block and signature pair for the missing data blocks [4].

Prior public auditing techniques for shared cloud data kept group members' identities hidden for security reasons. However, unrestricted identity anonymity would create a new dilemma, in which a group member might maliciously edit shared data while remaining anonymous. Because uncontrolled malicious adjustments to shared data can degrade its usability, identity traceability should be preserved in data sharing. Yang, G et al. developed a public auditing system that preserves group members identify privacy while also allowing them to trace their identities. This cloud data sharing framework formalizes the establishment of a public auditing technique for shared data in cloud that supports identity confidentiality and traceability, as well as the addition of a manager to support members in establishing authenticators to ensure identity confidentiality. Two lists are utilized to track who made the most recent change on each block in order to accomplish identity traceability. Furthermore, the approach uses the blind signature technique to ensure data privacy during authenticator generation [5].

The long-term validity of cloud shared data can be confirmed via a third-party verification [11]. It's challenging to handle group membership dynamics efficiently at the same time because of the important volume of processing required to add the signatures on shared information. B. Wang et. al proposed a public auditing system for shared cloud data that preserves anonymity. Without having to download the whole file from the cloud or knowing the group members' secret identifying information, a public verifier can confirm the integrity of shared data. Group dynamics are handled by outsourcing activities using a secure substitution re-signature technique [6].

M. Thangavel and P. Varalakshmi in 2020 proposed a singular integrity verification framework primarily based totally on Ternary Hash Tree (THT) and Replica primarily based totally Ternary Hash Tree for protecting cloud garage, with a view to be utilized by TPA to adopt records auditing. In comparison to previous work, the suggested device performs Block-, File-, and Replica-level auditing, as well as tree block and garage block ordering, to ensure data integrity and availability throughout the cloud. This framework is used to cover blunders localization with records correctness, dynamic updates in the cloud using block update, insert, and delete operations, and blunders localization with records correctness [7].

Tao, Y proposed a unique stable record looking and sharing strategy. Earlier, this method is useful in phrases of defensive the privateness of IoT gadgets and person non-public keys. This machine assures cloud records secrecy, secure records sharing and looking, and avoids failure. In phrases of performance, the experimental consequences propose that delegating the bulk of cryptographic operations to facet servers significantly saves consumers' computational computing and communique price for building a trapdoor [8,9].

Proposed System

The most essential safety measure is cloud storage auditing. It checks the data stored in the public/private cloud. Auditing procedures for cloud storage has gained a lot of importance in recent years and have been extensively investigated. These protocols concentrate on a variety of areas of auditing, with one of the most important problems being how to attain high bandwidth and computing efficiency.

The risk of data on clouds is being corrupted or tampered with is a fundamental factor when adopting multi-cloud. The proposed system is Efficient for distributed optimization at a low deployment cost. It also maintains a consistent degree of control overhead. The Cloud Storage Auditing Architecture is shown in Figure 1.

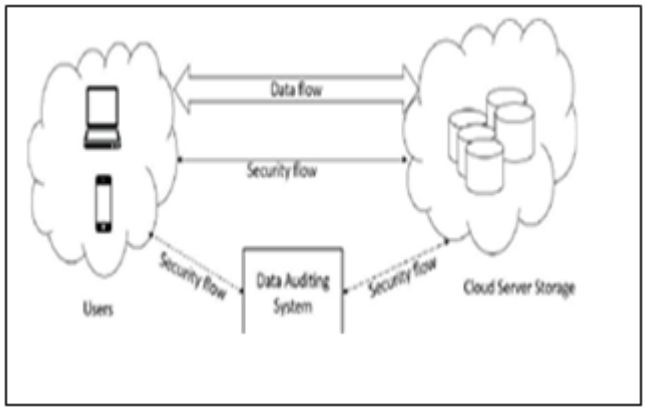

Fig. 1. Cloud Storage Auditing

The key impediment inside the layout of information storing auditing protocol is the data confidentiality problem (i.e., the auditing protocol must preserve data confidentiality from the auditor). Because of the following factors:

1. For public facts, the auditor can get better the facts blocks from the facts evidence and retrieve the facts information.
2. In the case of encrypted facts, the auditor can be capable of get content material keys through any precise channels and so decrypt the facts.

The proposed approach is rather efficient and provably secure, consistent with the safety and overall performance study. To guarantee the integrity of such sensitive facts, integrity auditing is used. A number of audits are commonly required. To accomplish and maintain the integrity of facts saved withinside the public cloud, in addition to shield towards out of doors intruders, a third-party auditor (TPA) can be utilized. In the proposed gadget, a sanitizer is implemented to sanitize the facts blocks that correspond to the record's sensitive information. It essentially simplifies the time-eating technique of certificates administration. On the cloud, documents are frequently stored as everyday documents. There is no manner to inform if the documents are corrupted or not. There is no dependable technique for figuring out whether or not facts withinside the cloud is saved appropriately. Data is exchanged through cloud storage including Dropbox, and iCloud. These facts can be compromised or misplaced because of the inevitability of software program faults, hardware malfunctions, and human errors. The facts proprietor needs to generate signatures withinside the proposed gadget earlier than importing facts blocks. As a result, all cloud-primarily based totally facts could have the equal signature. The gadget is primarily based totally on a BLS signature and a pseudorandom function.

System Desin and Experimental Results

The user is provided a username and password in order to utilize the Identity-Based Integrity Auditing programme. A permanent registration number that will serve as an IoT identifier. The next step is Generation of Blinded and Sanitized Files. Blinded File Algorithm: Python takes a file and encrypts it with the Pycrypto package. Along with the password, the filename is used as an input parameter. Encryption is accomplished by the use of a key that is generated according to algorithmic requirements. The encrypted file is saved with the prefix (encrypted) in the same directory. The cryptographic hash function produces keys that aid in the security of data that are used for symmetric encryption. The files are primarily password-protected. The password and encrypted file are used as input parameters in the decryption process. Blind and sanitation algorithm is shown in figure 2.

Fig. 2. Implementation of Blind and sanitize algorithm

Advanced Encryption Standards (AES) is one of the most extensively used encryption and decryption technologies. To ensure that data can be kept securely, this encryption method employs a block cypher algorithm. AES works with a four-by-four-column important order matrix of bytes. If it appears like a mouthful, the cryptography network is of the same opinion and has dubbed this manner the state. This is how the cycles work. For 128-bit key, ten rounds are required, For 192, 12 and for 256, 14 are required. The facts is substituted the usage of a substitution desk withinside the first step of the AES encryption manner; the second one transmutation adjustments statistics rows, and the 1/3 shifts columns. The remaining transformation is a simple specific XOR on every column, which makes use of an element of the encryption key for every column. The greater rounds required, the longer the encryption key is. Hashes, on the alternative hand, are a one-manner authentication function. The hash function takes a larger file as input, analyses it, and returns a smaller output that is nearly guaranteed to be the file's unique fingerprint. This makes it simple to compare two files to see if they vary. Even if you change one character, you'll get a different hash output.

Through public verification, the patron can enlist the assist of an unbiased auditor to test the storage accuracy withinside the cloud on his behalf. Then Third-Party Auditor is implemented. It is through public verification the purchaser can enlist the assist of an independent third-party auditor to affirm the storage Party Auditor correctness withinside the cloud on his behalf. Batch audit permits the TPA to deal with numerous jobs from distinct clients on the equal time, growing audit efficiency. It can correctly use a checking scheme to verify the correctness of statistics withinside the cloud. Sanitized blind files are shown in figure 3.

Fig. 3. Sanitized Blinded Files

There are two critical phases in the system as follows.

1. Phase of challenge reaction: The auditor selects the blocks. The variety of blocks queried is blanketed with the task message. It selects a detail at random from the subset s = s1. Sc of the set belongs to [1,n]. The project message is dispatched to the cloud server with the aid of using the auditor. After receiving the task request, it is generated with the aid of using TPA, the server takes an enter record F, a task request query, and a Signature set S. It submits the evidence to the auditor as a response.
2. Phase of Proof Verification: After getting the response, the auditor checks and tests the algorithm to check for integrity. Then the generated signature is then tested to the previous signature which is stored. TPA examines the Certificate using its verification method in the first stage after getting the signature. If it's proven, the response's public key is used to verify it (PK). Otherwise, the integrity check will be stopped. The proof answer is then decrypted using the public key in a second phase. This is done when the certificate's legitimacy has been validated. The signature is then checked to ensure that the server is authenticated. This proposed method can detect data that has been tampered with by an active attacker. In conjunction with certificates, this auditing approach employs a digital signature technique. This certificate is used to verify the server's validity. With the use of digital signatures, certificates connect identifying data such as a username, IP address, and password to a public key. As a result, no one can access the information. The auditing report is shown in figure 4, 5.

Fig. 4. Blockchain Report

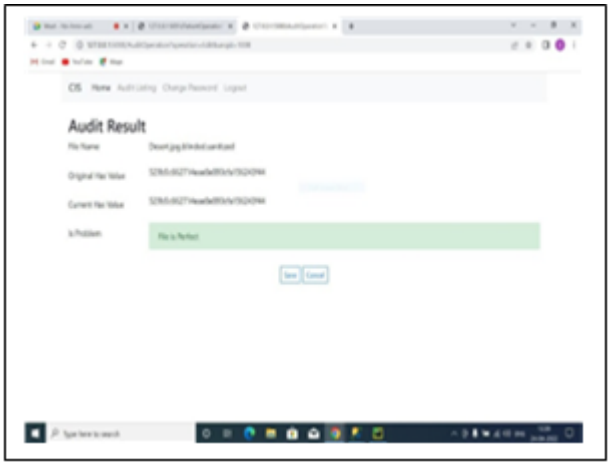

Fig. 5. Audit Report

Conclusion

In order to ensure cloud data security, availability, and integrity, Linear Authenticator as a third-party authenticator in a public auditing system is implemented. During the auditing process, TPA verifies data integrity without acquiring knowledge of the data, data access management and data protection from unauthorized data users. It also minimizes the number of keys necessary for data decryption and the overhead associated with key management. By applying numerous encryption mechanisms at various levels, the Secure Cloud system ensures data security and privacy. In the future, the system will be implemented to work in a multiple cloud based environment and to sum up the security mechanisms to prevent data loss in the event of a cyber-attack.

References

1. Guan, Y., Shao, J., Wei, G., & Xie, M. (2018). Data security and privacy in fog computing. IEEE Network, 32(5), 106-111.

2. Fu, A., Yu, S., Zhang, Y., Wang, H., & Huang, C. (2017). NPP: a new privacy-aware public auditing scheme for cloud data sharing with group users. IEEE Transactions on Big Data.
3. Huang, L., Zhang, G., Yu, S., Fu, A., & Yearwood, J. (2019). SeShare: Secure cloud data sharing based on blockchain and public auditing. Concurrency and Computation: Practice and Experience, 31(22), e4359.
4. Yu, Y., Ni, J., Au, M. H., Mu, Y., Wang, B., & Li, H. (2014). Comments on a public auditing mechanism for shared cloud data service. IEEE Transactions on Services Computing, 8(6), 998-999.
5. Yang, G., Yu, J., Shen, W., Su, Q., Fu, Z., & Hao, R. (2016). Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability. Journal of Systems and Software, 113, 130-139.
6. Wang, B., Li, H., & Li, M. (2013, June). Privacy-preserving public auditing for shared cloud data supporting group dynamics. In 2013 IEEE International Conference on Communications (ICC) (pp. 1946-1950). IEEE.
7. Sowmiya, B., Abhijith, V. S., Sudersan, S., Sakthi Jaya Sundar, R., Thangavel, M., & Varalakshmi, P. (2021). A survey on security and privacy issues in contact tracing application of COVID-19. SN computer science, 2(3), 1-11.
8. Tao, Y., Xu, P., & Jin, H. (2019). Secure data sharing and search for cloud-edge-collaborative storage. IEEE Access, 8, 15963-15972.
9. Wang, T., Mei, Y., Liu, X., Wang, J., Dai, H. N., & Wang, Z. (2021). Edge-based auditing method for data security in resource-constrained internet of things. Journal of Systems Architecture, 114, 101971.
10. Sun, S., Du, R., & Chen, S. (2021). A Secure and Computable Blockchain-Based Data Sharing Scheme in IoT System. Information, 12(2), 47.
11. Gupta, K., Yadav, K., & Singh, A. (2022). A Comparative Study on Securely Sharing and Searching Data Using Edge of Cloud-Supported Internet of Things. In ICT with Intelligent Applications (pp. 155-163). Springer, Singapore.
12. Costa, B., Bachiega Jr, J., de Carvalho, L. R., & Araujo, A. P. (2022). Orchestration in Fog Computing: A Comprehensive Survey. ACM Computing Surveys (CSUR), 55(2), 1-34.