IJARST
International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
ISSN: 2457-0362
www.ijarst.in

Cloud Security Enhancement via Data Integrity and Replication Detection

M. Anitha[1], CH. Satyanarayana Reddy[2], L. Anil Kumar[3]

#1 Assistant Professor & Head of MCA Department, SRK Institute of Technology, Vijayawada.
#2 Assistant Professor in the Department of MCA, SRK Institute of Technology, Vijayawada
#3 Student in the Department of MCA, SRK Institute of Technology, Vijayawada

Abstract : In today's digital era, the utilization of cloud servers for data storage has become ubiquitous, offering a myriad of benefits to users and customers alike. Leading cloud service providers such as Google Cloud Platform, Microsoft Azure, and others have revolutionized data management practices, providing scalable solutions to address diverse storage needs. However, despite the convenience afforded by cloud storage, concerns regarding data security persist, particularly in sensitive sectors such as healthcare and private enterprises.To address these concerns, implementing robust data security measures is imperative to ensure the confidentiality and integrity of stored data. One approach to bolstering data security in the cloud is through the utilization of Authorized Client-Side Deduplication, leveraging techniques such as Ciphertext-Policy Attribute-Based Encryption (CP-ABE). The proposed system employs CP-ABE to encrypt user data prior to uploading it to the cloud, thereby ensuring that sensitive information remains protected from unauthorized access. By incorporating user attributes into the encryption process, the system enhances data security while facilitating efficient access control mechanisms. Furthermore, the system incorporates deduplication functionality to mitigate storage issues and optimize cloud storage utilization. When a file is uploaded to the cloud, the system identifies any duplicate copies and prevents redundant uploads, thereby conserving storage space and improving overall system efficiency. The suggested approach to authorized client-side deduplication strikes a balance between storage space efficiency and security considerations, making it well-suited for deployment in hybrid cloud architectures. By adopting this innovative security measure, organizations can safeguard their data assets while maximizing the benefits of cloud storage solutions.

1.INTRODUCTION

CSP can dispose of sometimes utilized data to save space. Due to its low startup costs, low maintenance costs, and universal access to data regardless of location or device, capacity as a service has emerged as a business alternative to local data storage. Regardless of cost investment funds, accessibility, effortlessness of purpose, changing, and sharing, it acts security gambles with like information is at the control of the cloud supplier (CSP). It is possible for it to mislead about information debasement and misfortune as a result of programming or equipment failure. Verify who owns the information stored in distributed storage.

Traditional data trustworthiness cryptographic solutions either require a local copy of the data, which data users (DUs) do not possess, or permit DUs to download the entire data. The first arrangement necessitates more space, while the second raises costs for document transport. Several proposals propose using square less confirmation to evaluate trustworthiness without downloading all data to resolve this issue. These works let the open verifier affirm, which is alluring. DUs can design the evaluating system with open survey v. (TPA). It can persuade CSP and DU. By randomly confirming a few squares, these proposals use proven information ownership (PDP) to guarantee ownership of information in unconfidential distributed storage.

As of late, proposition have been made to permit TPA to check cloud information's precision. There are pros and cons to each plan. When inspecting, TPA shouldn't use the response from the cloud server. There are no life-saving plans. Information owners are able to embed, modify, and delete data without altering the meta-information of other blocks thanks to the information elements requirement, which is not met by the processes provided in. Then, plans like "couldn't meet clump checking requirement" guarantee that the TPA can deal with multiple DU check requests at once. Costs for CSP and TPA correspondence and computation are reduced as a result. Plans make use of blending-based cryptographic processes that take more time. A secure and effective information ownership protection scheme (SEPDP) is provided by us.

SEPDP supports dynamic information duties, group reviewing, and information owners. a probabilistic look at the squares of CSP. We contrasted the proposed plan's show with notable frameworks.

The proposed plan's full scale check time is not exactly the current arrangement's. Because of this, low-controlled devices can be effectively tested by SEPDP. The rest of this paper follows. clarified prerequisites for the elements.

2.LITERATURE SURVEY

2.1 Secure and constant cost public cloud storage auditing withdeduplication

In order for cloud storage to be effective, data integrity and storage efficiency are two key needs. Data integrity for cloud storage is guaranteed by POR and PDP approaches. Storage efficiency is increased by POW, which safely deletes redundant data from the storage server. To accomplish both data integrity and storage efficiency, however, a minimal combination of the two strategies leads to non-trivial duplication of information (i.e., authentication tags), which is in opposition to POW's goals. Recent solutions to this issue have been shown to be insecure and to incur significant computational and communication costs. In order to offer effective and safe data integrity auditing together with storage deduplication for cloud storage, a new solution is required. In this study, we present a novel strategy for the solution of this open problem, based on homomorphic linear authenticators and polynomial-based authentication tags. Deduplication of files and the related authentication tags is possible thanks to our architecture. Storage deduplication and data integrity auditing are accomplished simultaneously. Constant real-time communication and computational expense on the user's end are further characteristics of our suggested approach. Both batch and public audits are supported. As a result, our suggested method performs better than current POR and PDP schemes while incorporating deduplication as an additional utility. We use the Computational Diffie-Hellman problem, the Static Diffie-Hellman problem, and the t-Strong Diffie-Hellman problem to demonstrate the security of our suggested system. Experimental findings on Amazon AWS and numerical analysis demonstrate how effective and scalable our system is.

2.2 Dupless: Server aided encryption for deduplicated storage

AUTHORS: S. Keelveedhi, M. Bellare, and T. Ristenpart

Deduplication is a technique used by cloud storage service providers like Dropbox, Mozy, and others to store only one copy of each submitted file in order to conserve space. However, savings are lost if clients encrypt their files normally. This strain is alleviated by message-locked encryption, of which convergent encryption is the most notable example. However, brute-force assaults that can retrieve files that belong to a known set are fundamentally possible. We provide an architecture that offers safe deduplicated storage that can withstand brute-force attacks, and we implement it in the DupLESS system. Clients in DupLESS encrypt using message-based keys that they have gotten from a key server via an unaware PRF protocol. It allows users to save encrypted data with a current service and have that service handle deduplication on their behalf. but still manages to secure adequate confidentiality assurances. We demonstrate how performance and space savings from encryption for deduplicated storage can be comparable to those of utilising the storage service with plaintext data.

3.PROPOSED SYSTEM

In this paper, we propose two secure systems, SecCloud and SecCloud-D, in an effort to achieve data integrity and deduplication in the cloud.

By combining the management of a MapReduce cloud with an auditing entity, SecCloud enables its users to ensure the authenticity of data stored in the cloud and to generate metadata tags prior to upload.

SecCloud+ enables the guarantee of file confidentiality in addition to supporting integrity auditing and secure deduplication.

We propose an approach for performing direct audits of encrypted data's integrity.

3.1 IMPLEMENTATION

3.1.1 Cloud Service Provider

We create the Cloud Service Provider module in this module. This organisation offers a public cloud data storage service.
The CS offers the data outsourcing service, stores data on behalf of the users, and uses deduplication to remove redundant data from storage and retain only unique information.

For the purposes of this research, we'll assume that CS is constantly online and has plenty of storage space and processing power.

3.1.2 Data Users Module

➢ A user is a company that wishes to outsource data storage to the S-CSP and afterwards access the data.

➢ In a storage system that allows for deduplication, the user only uploads one-of-a-kind data—which may belong to them or to other users—and does not upload any duplicate data to save on upload bandwidth.

➢ At system setup, the authorised deduplication system grants a set of rights to each user. Each file is secured with a convergent encryption key and privilege keys to enable authorised deduplication with differential privileges.

3.1.3 Auditor

A MapReduce cloud is maintained by the auditor, which also serves as a certificate authority and assists clients with uploading and auditing their outsourced data. This presumption makes the auditor presumed to be connected to a set of public and private keys. It makes its public key visible to the other system entities. The capacity to validate the accuracy of data saved remotely is the primary design objective of this effort. public verification enables verification by anybody, not just the

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362
IJARST

customers who originally stored the material.

4.RESULTS AND DISCUSSION

Fig 1 User login page

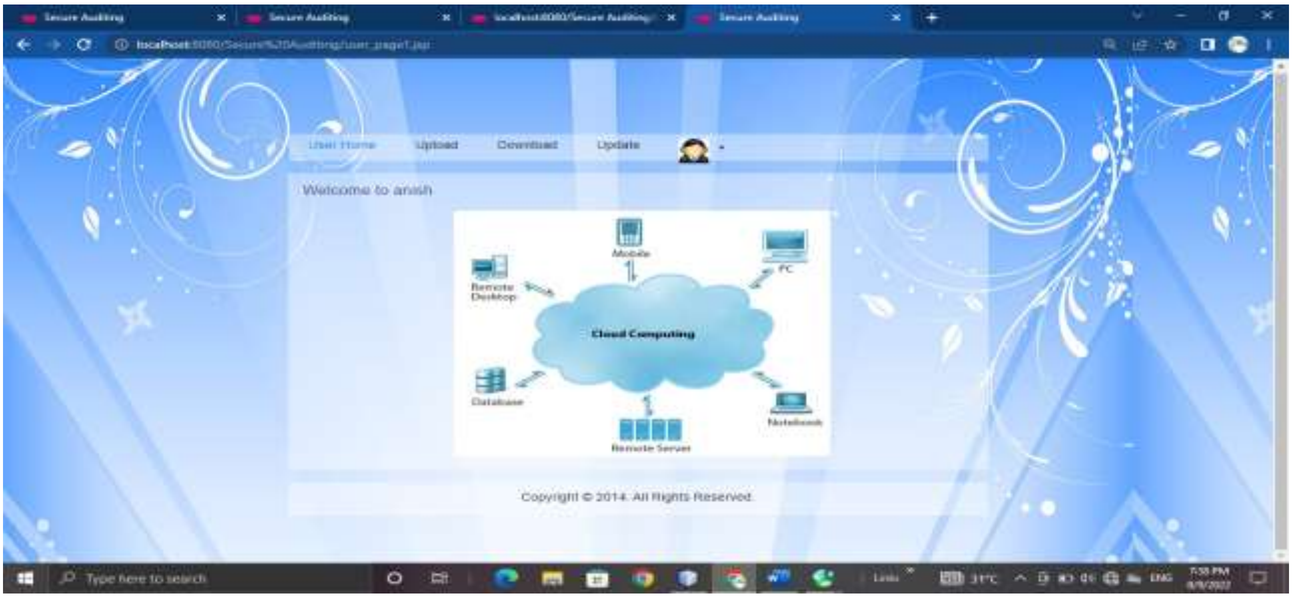

Fig 2: User home page

International Journal For Advanced Research In Science & Technology
A peer reviewed international journal
www.ijarst.in
ISSN: 2457-0362

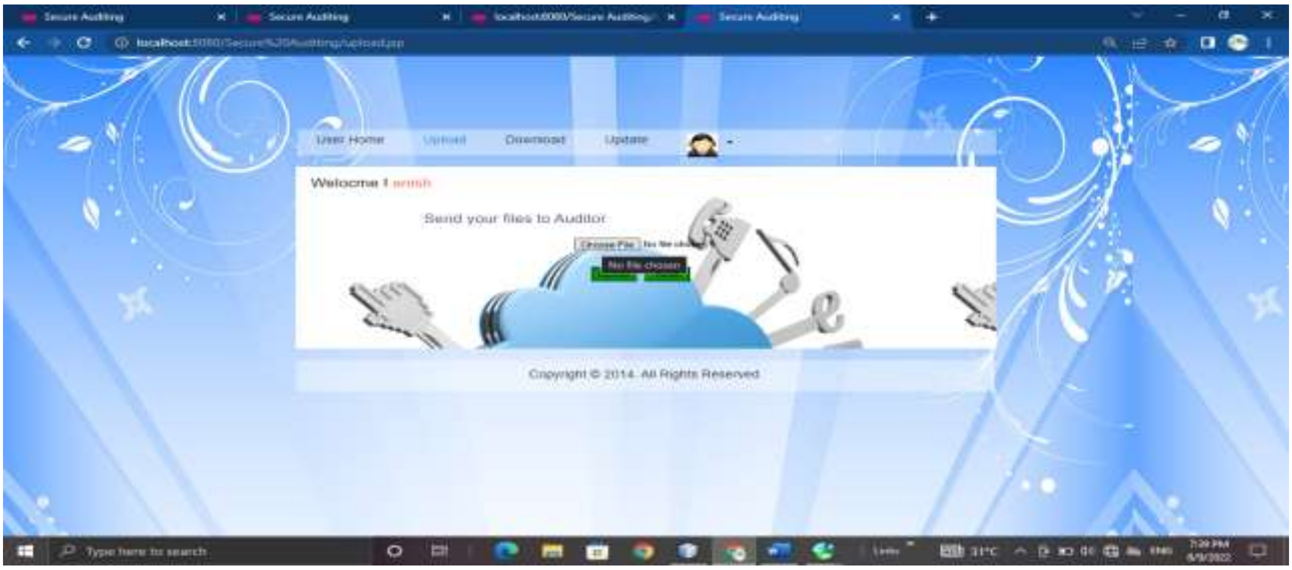

Fig 3: User file upload page

5.CONCLUSION

In conclusion, the proposed approach of enhancing cloud security through data integrity measures such as replication detection and authorized client-side deduplication holds significant promise in addressing the persistent concerns regarding data security in the cloud. By leveraging techniques like Ciphertext-Policy Attribute-Based Encryption (CP-ABE) and deduplication functionality, organizations can ensure the confidentiality, integrity, and efficiency of their data storage practices in cloud environments.

The integration of CP-ABE encryption enhances data security by encrypting user data prior to uploading it to the cloud, thereby protecting sensitive information from unauthorized access. Additionally, the incorporation of deduplication functionality optimizes storage utilization by identifying and preventing the upload of duplicate files, conserving storage space and enhancing overall system efficiency.

Furthermore, the proposed approach strikes a balance between security considerations and storage space efficiency, making it well-suited for deployment in hybrid cloud architectures. By adopting this innovative security measure, organizations can mitigate security risks while maximizing the benefits of cloud storage solutions.

Moving forward, it is essential for researchers and practitioners to continue exploring and refining data integrity measures to keep pace with evolving cloud security challenges. By staying abreast of emerging technologies and best practices, organizations can proactively safeguard their data assets and maintain trust and confidence in cloud computing technologies.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, ―A view of cloud computing,‖ *Communication of the ACM*, vol. 53, no. 4, pp. 50–58, 2010.

[2] J. Yuan and S. Yu, ―Secure and constant cost public cloud storage auditing with deduplication,‖ in *IEEE Conference on Communications and Network Security (CNS)*, 2013, pp. 145–153.

[3] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg, ―Proofs of ownership in remote storage systems,‖ in *Proceedings of the 18th ACM Conference on Computer andCommunications Security*. ACM, 2011, pp. 491–500.

[4] S. Keelveedhi, M. Bellare, and T. Ristenpart, ―Dupless: Serveraided encryption for deduplicated storage,‖ in *Proceedings of the 22Nd USENIX Conference on Security*, ser. SEC'13. Washington, D.C.: USENIX Association, 2013, pp. 179–194. [Online]. Available: https://www.usenix.org/conference/usenixsecurity13/technicalsessions/presentation/bellare

[5] 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*, ser. CCS '07. New York, NY, USA: ACM, 2007, pp. 598–609.

[6] G. Ateniese, R. Burns, R. Curtmola, J. Herring, O. Khan, L. Kissner, Z. Peterson, and D. Song, ―Remote data checking using provable data possession,‖ *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 12:1–12:34, 2011.

[7] G. Ateniese, R. Di Pietro, L. V. Mancini, and G. Tsudik, ―Scalable and efficient provable data possession,‖ in *Proceedings of the 4th International Conference on Security and Privacy in Communication Netowrks*, ser. SecureComm '08. New York, NY, USA: ACM, 2008, pp. 9:1–9:10.

[8] C. Erway, A. K¨upc¸ ¨u, C. Papamanthou, and R. Tamassia, ―Dynamic provable data possession,‖ in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, ser. CCS '09. New York, NY, USA: ACM, 2009, pp. 213–222.

[9] 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. on Knowl.and Data Eng.*, vol. 20, no. 8, pp. 1034–1038, 2008.

Author's Profiles

Ms. M. Anitha Working as Assistant Professor & Head of MCA Department, in SRK Institute of technology in Vijayawada. She done with B. Tech, MCA, M. Tech in Computer Science. She has 14 years of Teaching experience in SRK Institute of Technology, Enikepadu, Vijayawada, NTR District. Her area of interest includes Machine Learning with Python and DBMS.

Mr. CH. Satyanarayana Completed his Bachelor of Computer Application at Acharya Nagarjuna University. He completed Master of Computer Application at Acharya Nagarjuna University. Currently working as an Assistant Professor in the Department of Computer Application SRK Institute of Technology, Enikepadu, Vijayawada, NTR District. His area of interest includes Networks, Machine Learning & Artificial Intelligence.

Mr. L. Anil Kumar is an MCA Student in the Department of Computer Application at SRK Institute of Technology, Enikepadu, Vijayawada, NTR District. He has Completed Degree in B.Sc. (MPC) from P. B. Siddhartha College of Arts & Science. His area of interest are Networks, Cloud Computing and Machine Learning with Python.