JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

REVIEW ON CLOUD SECURITY, PRIVACY AND INTEGRITY USING BLOCKCHAIN TECHNOLOGY

[1]Anil Kumar, [2]Kavya G L, [3]Manasa K
[1]Assistant Professor, Department of ISE, CIT, Gubbi, Tumakuru
[2] Student, Department of ISE, CIT, Gubbi, Tumakuru
[3] Student, Department of ISE, CIT, Gubbi, Tumakuru

Abstract : **In the quickly developing field of cloud computing security, this study presents novel approaches to ongoing problems. It suggests all-encompassing methods for protecting private information kept on cloud servers, making use of blockchain-based key management and dynamic AES encryption keys for improved security and decentralized governance. Furthermore, without jeopardizing user privacy or disclosing confidential data, a privacy-preserving verification scheme guarantees the integrity of deep packet inspection services in untrusted clouds. Furthermore, a Searchable Encryption that Preserves Privacy (PPSE) method ensures data security and privacy while facilitating effective keyword searches over encrypted data by utilizing both public and private blockchains. To address worries about cloud data security, these systems include strong encryption, decentralized key management, and defense against illegal access. In modern cloud systems, they guarantee users' data security by offering scalable and flexible solutions.**

***Index Terms* – Cloud storage, certificateless encryption, AES, Searchable Encryption.**

I. INTRODUCTION

Cloud computing is a revolutionary technology that offers secure and effective online computing and storage services. Users can benefit from its special features, which include scalability, flexibility, and anytime, anywhere access to data. Especially cloud storage has become more and more popular since it is more economical, effective, and adaptable than traditional storage methods. Even if cloud computing has numerous advantages, there are drawbacks to its quick expansion, particularly with regard to the security and privacy of data kept in the cloud. Malicious actors find cloud service providers (CSPs) to be appealing targets, which raises worries about data tampering and breaches. Maintaining data integrity and secrecy in the cloud is essential to cloud technology development.

Different data auditing techniques have been created to solve these issues; in order to ensure data integrity, third-party auditors, or TPAs, are frequently involved. However, as TPAs could be motivated to access or alter user data, protecting data privacy is crucial during audits. Proxy servers (PS) can be used to improve overall data security by distributing computing workloads and guaranteeing timely data updates. One of the most important aspects of cloud data protection is encryption. The chosen degree of security determines whether cryptography technique is used: symmetric or asymmetric. Additionally, blockchain technology has shown to be a dependable means of boosting cloud service provider trust and data security. It enhances data security and integrity by offering a decentralized, immutable ledger for transaction recording.

Schemes for dynamic searchable encryption, or SE, have been developed in response to the demand for safe and adaptable cloud data searching. By enabling users to update data dynamically and protecting both forward and backward privacy, these techniques guard against unauthorized access to private data. In conclusion, even if cloud computing has many advantages, it is critical to guarantee the security, integrity, and privacy of data stored on the cloud. Blockchain technology, encryption, and dynamic SE systems allow consumers to improve trust and safeguard their data in cloud contexts.

II. INTEGRITY:

Data integrity verification is the main job of the M-MHT authenticated binary tree structure. Its goal is to swiftly and securely show if a set of components has been changed or damaged. As a result, the integrity of every leaf node is guaranteed by the root node authentication of M-MHT. The M-MHT root node, which can be signed by the user and stored on the server, is the main tool for ensuring data security. Conventional bloom filters (BF) support only insertion and search query actions on elements; deletion operations are not supported, therefore data records saved in BF cannot be removed. This problem is addressed by the counting bloom filter (CBF), which permits insert, modify, and delete operations on CBF by substituting an array of counters for the array of bits in BF. This makes each bit location a little counter. To satisfy the efficiency of data structures, however, the usage of traditional CBF is insufficient; this work suggests NCBF structure, which is based on CBF structure. In addition to facilitating data dynamic operations, NCBF can be linked to the location of stored data, which can significantly increase the effectiveness of data dynamic processing and data lookup verification.

Using homomorphic linear authentication tags, Ateniese et al. offered public auditing in a Provable Data Possession (PDP) architecture. Later on, they suggested a dynamic variation of this plan. To lessen the burden of user auditing, Wang et al. created a publicly verifiable PDP scheme with a trustworthy TPA. Publicly verifiable homomorphic authentication tags were used by Shacham et al. to improve the Proof of Retrievability (PoR) that Juels et al. had suggested. Numerous public auditing techniques utilizing homomorphic signatures were influenced by these efforts. However, because duplicate authentication tags are involved, deploying these to secure deduplication systems would result in considerable storage expenditures. By simultaneously supporting data auditing and deduplication, Yuan et al. established the first cloud storage system that increased storage efficiency by deduplicating authentication tags in addition to plaintext. Blockchain was utilized by Xu et al. to assist plaintext deduplication.

Li et al.'s technique, which generates authentication tags by using a fully trusted proxy server, is expensive when utilized across insecure networks. The enhanced plan by Liu et al. did away with the requirement for a completely trusted proxy server, but also necessitated users to remain online during audits, which added expense and hassle. The problem of auditing result dependability for low-entropy data remains unresolved in contemporary cloud storage systems allowing auditing and deduplication over encrypted data, as Gao et al.'s proposed approach addressed reliability difficulties for the initial uploader but not for successive uploaders.

Although Yuan et al.'s plan uses blockchain auditing to solve TPA dependability, it lacks deduplication to authentication tags, which results in inefficient storage. Tian et al.'s method for auditing via blockchain ignores OP leakage and auditing result forgeability for low-entropy data in favor of using two CSPs, raising costs and requiring users to remain online for tag updates.

III.PRIVACY

An extensive security design can be put into place to improve privacy in accordance with the threat model. By encrypting fresh papers with previously searched keywords and applying a unique keyword tag for every document, forward privacy can be attained. Attackers are unable to link searches to particular documents as a result. To guarantee backward privacy at a Type II level, make sure that after a document is erased, no information about it can be retrieved, including query results and update timings.

Before being stored on the blockchain, data should be encrypted. Smart contracts should be used to create an access control mechanism that limits access to authorized users only, preventing hackers from accessing private data. Enterprise traffic privacy can be maintained by employing methods like BlindBox, Embark, and PrivDPI, which enhance encrypted traffic inspection and use encrypted token matching.

Furthermore, mitigation and defense strategies should be used in cloud computing and mobile networks to solve security and privacy issues. Examples of how to protect data exchange and authenticate operating devices include using lightweight anonymous authentication approaches and hybrid encryption methods.

Privacy-Preserving Searchable Encryption Scheme Based on Public and Private Blockchains	Ruizhong Du	• Confidentiality: Since only authorized persons with the required keys may decrypt data, the encryption technique guarantees that information stays secret. • Searchable Encryption: This technique preserves the confidentiality of encrypted data while enabling searches on it. • Privacy-Preserving inquiries: Before being delivered to the blockchain network, user inquiries are converted into encrypted queries.

		- Decentralization: Maintaining decentralization, which is essential for privacy, is made possible by using both public and private blockchains.
Privacy-Preserving and Lightweight Verification of Deep Packet Inspection in Clouds	Xiaoli Zhang	- Deep Packet Inspection (DPI) Privacy: This strategy tackles issues of privacy pertaining to DPI, which is a method of examining network traffic. - Lightweight Verification: Deep packet inspection verification is made to be as light-weight as possible, requiring little in the way of computational or resource overhead. - Anonymity Preservation: During deep packet inspection, the plan might include methods to protect network users' anonymity. - Selective Disclosure: During deep packet inspection, users are in charge of what information is revealed
A Blockchain-Assisted Certificateless Public Cloud Data Integrity Auditing Scheme	JIANMING DU	- Data Privacy: The plan makes sure that the privacy of data stored in public clouds is not jeopardized during the integrity auditing process. - Certificateless Encryption: The system does away with the requirement for conventional public key certificates, which occasionally provide privacy concerns, by employing certificateless encryption. - Blockchain Privacy: The system's blockchain component guarantees data integrity without jeopardizing the auditing process's confidentiality. - User Anonymity: The plan might include safeguards to preserve users' privacy when they take part in the data integrity auditing procedure.

IV.SECURITY

A strong approach to data security can be achieved by combining dynamic encryption with the AES encryption standard and the security features of our scheme. Beyond conventional encryption techniques, dynamic encryption provides an additional layer of security by guaranteeing data protection from the moment it is created or accessed. Data is further protected by AES's robust security and performance features, which encrypt data using 128-, 192-, or 256-bit keys, depending on the required level of security.

The objectives of dynamic encryption and AES are nicely aligned with our scheme's focus on data confidentiality, auditing result dependability, ownership privacy (OP) protection, and resistance to duplicate faking attack (DFA). our plan lowers the risk of data breaches and unauthorized access by making sure that sensitive data is encrypted and safeguarded at all times, especially in critical areas like cloud computing, secure communications, financial transactions, and healthcare.

By offering tools for guaranteeing data authenticity and guarding against hostile actions, the employment of cryptographic hash functions, (hash based message authentication code) HMAC-based signatures, and authenticated AC (Authenticated Cipher) automaton in our scheme enhances data security even further. All things considered, integrating dynamic encryption with AES and the security features in our scheme can offer a thorough approach to data protection, assisting in the defense of sensitive data against a variety of attacks.

.

Dynamic AES Encryption and Blockchain Key Management: A Novel Solution for Cloud Data Security	MOHAMMEDY	• Dynamic AES Encryption: Cloud data security is guaranteed by the use of Advanced Encryption Standard (AES) encryption. • Key management: By offering a decentralized, unhackable platform for storing encryption keys, the use of blockchain technology for key management improves security. • Blockchain Security: The solution's blockchain component provides built-in security features like decentralized consensus, immutability, and transparency. • Dynamic Key Generation: To produce fresh encryption keys on a regular basis, the solution uses techniques for dynamic key generation.
Privacy-Preserving and Lightweight Verification of Deep Packet Inspection in Clouds	Xiaoli Zhang	• Authentication: To verify the legitimacy of the parties engaged in the DPI process, security measures are put in place. • Secure Communication Channels: The plan makes use of secure communication channels to keep network devices and cloud infrastructure safe during DPI. Encryption: During DPI activities, encryption techniques may be used to safeguard data confidentiality. • Access Control: To guarantee that only authorized individuals can start or supervise DPI activities, security measures are in place to implement access control standards.

V. SUMMARY OF REVIEW

Although cloud computing provides scalable and adaptable online computing and storage capabilities, privacy and data security are becoming more and more of a worry as a result of its quick growth. To solve these issues, a number of strategies have been developed, including blockchain technology, data audits, and encryption. Data confidentiality is safeguarded by encryption, while data integrity is helped by data audits by outside auditors. Blockchain offers a decentralized ledger, which improves security and trust. While maintaining privacy protection, dynamic searchable encryption enables flexible and safe cloud data searching. Methods such as M-MHT, CBF, and NCBF guarantee the accuracy and efficiency of the data. Data security and efficiency are increased by public auditing programs and blockchain-assisted techniques, however certain issues still exist, such as low-entropy data auditing and data duplication.

A comprehensive approach to data protection can be provided by utilizing cryptographic hash functions, HMAC-based signatures, and dynamic encryption in conjunction with AES. These precautions are essential for protecting sensitive data from unwanted access and data breaches in cloud computing, secure communications, financial transactions, and healthcare.

VI. CONCLUSION AND FUTURE WORK

Cloud computing's incorporation of blockchain technology and cutting-edge encryption methods provides a complete solution to guarantee data security, integrity, and privacy. These techniques improve the security of cloud data auditing procedures by doing away with the complications associated with certificate administration and key escrow. Data privacy and integrity are ensured by the use of encrypted index storage and decentralized security mechanisms in private blockchains, which reduce the danger of hostile servers and users. Furthermore, implementing blockchain and dynamic AES keys for encryption key management improves file-level security and guards against illegal access during transmission and storage. These developments not only solve important security issues with cloud computing, but they also increase user confidence and trust in cloud services, enhancing their security and dependability. All things considered, these methods constitute a major advancement in cloud data security and lay the groundwork for secure and effective cloud computing systems.

Future research in these areas might concentrate on improving the suggested solutions scalability and efficiency. This could entail investigating novel cryptography techniques, refining key management plans, and optimizing algorithms. Furthermore, more investigation might be carried out to assess how well the schemes work in actual cloud systems and confirm their applicability and efficacy in safeguarding data security, integrity, and privacy. The creation of standardized frameworks or protocols based on these schemes may be another avenue for future research, as this might help with their uptake and incorporation into already-existing cloud computing systems. Furthermore, investigating the possible effects of cutting-edge technology, such quantum computing, on these systems' security and privacy may be a crucial subject for further study

REFERENCES

[1] Song, M., Hua, Z., Zheng, Y., Huang, H., & Jia, X. (2023). Blockchain-Based Deduplication and Integrity Auditing Over Encrypted Cloud Storage. *IEEE Transactions on Dependable and Secure Computing.* 20(6), 4928.

[2] Du, J., Dong, G., Ning, J., Xu, Z., & Yang, R. (2023). A Blockchain-Assisted Certificateless Public Cloud Data Integrity Auditing Scheme. *IEEE Access*. DOI: 10.1109/ACCESS.2023.3329558

[3] Shakor, M. Y., Khaleel, M. I., Safran, M., Alfahood, S., & Zhu, M. (2024). Dynamic AES Encryption and Blockchain Key Management: A Novel Solution for Cloud Data Security. IEEE Access. DOI: 10.1109/ACCESS.2024.3351119

[4] Du, R., Ma, C., & Li, M. (2023). Privacy-Preserving Searchable Encryption Scheme Based on Public and Private Blockchains. *Tsinghua Science and Technology*,28(1), 13-26. DOI: 10.26599/TST.2021.9010070

[5] Zhang, X., Geng, W., Song, Y., Cheng, H., Xu, K., & Li, Q. (2024). Privacy-Preserving and Lightweight Verification of Deep Packet Inspection in Clouds. *IEEE/ACM Transactions on Networking*, 32(1), 159.

[6] Goswami, P., Faujdar, N., Debnath, S., Khan, A. K., & Singh, G. (2023). ZSS Signature-Based Audit Message Verification Process for Cloud Data Integrity. *IEEE Access*.DOI: 10.1109/ACCESS.2023.3343841

[7] Zhang, X., Zhao, J., Xu, C., Wang, H., & Zhang, Y. (2022). DOPIV: Post-Quantum Secure Identity-Based Data Outsourcing with Public Integrity Verification in Cloud Storage. *IEEE Transactions on Services Computing*, 15(1), 334.

[8] Abdulsalam, Y. S., & Hedabou, M. (n.d.). Security and Privacy in Cloud Computing: Technical Review. DNA Lab, School of Computer and Communication Science, University Mohammed VI Polytechnic, Lot 660, Hay Moulay Rachid, Ben Guerir 43150, Morocco. Contact: abdulsalam.yunusa@um6p.ma.

[9] Bian, G., Zhang, R., & Shao, B. (2022). Identity-Based Privacy Preserving Remote Data Integrity Checking with a Designated Verifier. IEEE Access, 10.1109/ACCESS.2022.3166920.

[10] Arora, S., & Dalal, S. (2019). Integrity Verification Mechanisms Adopted in Cloud Environment. *International Journal of Engineering and Advanced Technology (IJEAT)*, 8(6S3). ISSN: 2249 – 8958.

[11] Fu, A., Yu, S., Zhang, Y., Wang, H., & Huang, C. (2022). NPP: A New Privacy-Aware Public Auditing Scheme for Cloud Data Sharing with Group Users. *IEEE TRANSACTIONS ON BIG DATA*, 8(1), 14.