IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

MULTI CLOUD SHARE SECURITY SYSTEM FOR PRIVACY PROTECTING DATA USING BIGDATA

[1]K. Sathiya Priya, [2]Karthick.J, [3]R. Nithish Kumar, [4]S. Karthikeyan
[2,3,4]Bharath Institute of Higher Education and Research, Selaiyur, 600073,
[1]Assistant Professor from Bharath Institute of Higher Education and Research, Selaiyur, 600073

Abstract: ***Cloud storage services offer users the convenience of storing and accessing data from anywhere. However, this convenience comes with the risk of data loss since users relinquish direct control over their data. To address this issue, various cloud storage auditing techniques have been developed. One such technique is a public auditing scheme for shared data that ensures data privacy, identity traceability, and group dynamics. However, we highlight a security flaw in this scheme: its vulnerability to tag forgery or proof forgery attacks. This means that the cloud server can generate valid proof of accurately storing data even after deleting some outsourced data. To counter this vulnerability, we propose a new scheme that offers the same functionalities while being secure against such attacks. Additionally, we conduct a comparative analysis of our*** *scheme* ***with others in terms of computation and communication costs.***

Key Words: ***Cloud Storage, Data Loss, Auditing techniques, public auditing scheme.***

I. *INTRODUCTION:*

The challenges in shared cloud environments revolve around data privacy and integrity, where ensuring authorized access while enabling public auditing poses a significant hurdle. Previous solutions have been limited by vulnerabilities like tag or proof forgery attacks. To address these limitations, this project proposes a novel scheme designed to withstand such attacks, thereby enhancing audit security. The solution utilizes advanced cryptographic methods to uphold data integrity and authenticity while safeguarding user privacy. A critical aspect of the system involves secure group management, ensuring only authorized members can access and audit shared data, thus bolstering system security. Leveraging cutting-edge cryptographic techniques, the project aims to establish a secure and privacy-preserving environment for auditing shared cloud data. The diverse nature of data generated by multi-cloud share systems requires normalization, standardization, and governance before analysis.

Cloud computing:

Cloud computing refers to the delivery of computing services over the internet, providing users with access to a wide range of resources such as storage, processing power, and applications, without the need for local infrastructure or management. These services are typically provided by cloud service providers who maintain and manage the underlying hardware and software infrastructure. Cloud computing offers scalability, flexibility, and cost-effectiveness, allowing users to scale resources up or down as needed and pay only for what they use. This includes different service models such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS) to meet different needs and preferences. Overall, cloud computing revolutionizes how businesses and individuals' access and utilize computing resources, enabling greater efficiency, agility, and innovation.

Cloud Security

In the context of multi-cloud share systems for privacy-protecting data using big data, security plays a crucial role in safeguarding information and information assets. Security involves the use of technology, processes, and training to defend against unauthorized access, disclosure, disruption, modification, inspection, recording, and destruction of data. While security focuses on protecting data from malicious attacks and the misuse of stolen data for profit, data privacy is concerned with the use and governance of individual data. It involves setting up policies to ensure that consumers' personal information is collected, shared, and utilized appropriately. Although security is fundamental for protecting data, it is not sufficient for addressing privacy concerns. In the context of big data generated by multi-cloud share systems, several privacy requirements need to be addressed. The diverse nature of data generated by these systems requires normalization, standardization, and governance before analysis. Data security and privacy protection are critical factors of concern in cloud computing. The distributed nature of data in the cloud makes security and privacy protection particularly important. Techniques and challenges related to data security and privacy in both software and hardware aspects of cloud architecture have been extensively investigate.

II. RELATED WORK

Existing systems for multi-cloud shared security system for privacy protecting data using bigdata prioritize user privacy while facilitating public auditing of cloud-shared data. They employ advanced cryptographic methods like ring signatures to compute audit verification information without compromising individual privacy. Mechanisms like oruta ensure identity privacy while allowing public auditing. Introducing third-party auditors (tpas) enhances data integrity protection. However, challenges include maintaining efficiency and scalability as data size and user numbers increase. Continuous research is crucial to bolster security against evolving attack models. Overall, these systems represent significant progress in cloud data security, yet future efforts are needed to enhance efficiency and security further. The Disadvantage are Performance Degradation**:** As the number of users and the volume of data in the shared cloud environment increase, the system may experience performance degradation. This could be due to the increased computational load required for cryptographic operations and the management of group memberships. Complexity in Auditing**:** The public auditing aspect of the system may become more complex as the number of participants and the variety of data increase. Ensuring that audits remain efficient and accurate as the system scales can be a challenge. Potential for Attacks: While the system is designed to be resistant to common attacks, new and more sophisticated attacks could emerge that exploit vulnerabilities in the cryptographic techniques or the system's architecture.

III. MODULES:

1. Authentication Module:

Every detail pertaining to the verified user is contained in this module. A user can only access his login if he has been authenticated; otherwise, he cannot access it without his username and password. Verifying a user's identification through the acquisition of credentials and application of those credentials to confirm the user's identity is the process known as authentication. The authorization process begins if the credentials are legitimate. The authorization process always comes after the authentication process. As volunteers who pass a community evaluation procedure, administrators take on these duties. It's not like they're using it. Their tools are never compelled to be used, and they must never be used to their benefit in a dispute where the other party needs secure access to their database.

2. Security Policies Module

In order to guarantee end-to-end data security in cloud storage systems, attribute-based encryption, or ABE, has become a viable method. Data owners are able to establish access policies and encrypt their data according to them, limiting access to the data to users whose attributes match the policies. Since data owners may alter data access policies dynamically and regularly, policy updating becomes a major concern as more and more businesses and organizations outsource their data to the cloud.

3. **Audit Logging Modules**
   - **Audit Trail Generation**: Modules that generate and store audit trails of all access and modifications to data, including who accessed what data, when, and how.
   - **Privacy-Preserving Auditing:** Modules that implement privacy-preserving techniques such as differential privacy or homomorphic encryption to ensure that auditing does not compromise data privacy.
4. **Secure Group Management Modules**
   - **Group Creation and Management**: Modules that support the creation and management of groups, including adding members and setting permissions for group access.
   - **Secure Communication**: Modules that ensure secure communication between group members, possibly using encrypted channels.
5. **Cloud Storage Integration Modules**
   - **Cloud Storage API Integration**: Modules that integrate with cloud storage services (e.g., AWS S3, Google Cloud Storage) to store and retrieve encrypted data.
   - **Security and Compliance**: Modules that ensure compliance with relevant security standards and regulations, such as GDPR or HIPAA, when handling shared cloud data.

IV. ALGORITHM

1. Advanced Encryption Standard (AES)

Establishing the Advanced Encryption Standard (AES) in 2001, the National Institute of Standards and Technology (NIST) of the United States provides a specification for the encryption of electronic data. Even while AES is more difficult to build than DES and triple DES, it is nevertheless frequently used today since it is significantly stronger. Important things to keep in mind:

• AES encrypts data in blocks of 128 bits each;
• It is a block cipher;
• The key size can be 128/192/256 bits.

In other words, 128 bits of encrypted cipher text are output after 128 bits of input are received. Because AES operates on the substitution-permutation network principle, it replaces and shuffles incoming data through a sequence of interconnected processes.

ENCRYPTION

Cloud encryption involves transforming data from its original plain text format into an unreadable format, known as ciphertext, before it is transferred to and stored in the cloud. Encryption ensures that even if the data is lost, stolen, or accessed by unauthorized users, it remains indecipherable without the encryption keys. AES treats each block as a 16-byte grid (4 **bytes** x 4 byte**s** = 128) in a basic column layout.

```
[ b0 | b4 | b8 | b12 |
| b1 | b5 | b9 | b13 |
| b2 | b6 | b10| b14 |
| b3 | b7 | b11| b15 ]
```

SubBytes:

This step performs the replacement. In this step, each byte is **replaced** by another byte. This is done using a lookup **table,** also called **an** S-box. This replacemen**t** is done in **such** a way that a byte is never replaced by itself **or** by another byte **that** is **the** complement of the current byte. **This** step results in a 16-byte (4 x 4**)** matrix as before. The next two steps apply the permutation.

Shift Rows

This step is **exactly what** it **sounds like.** Each row

is **moved** a **certain** number of times.
• The first row is not **moved**
• The second row is **moved left once.**
• The third row is **moved left twice.**
• The fourth row is **moved left. three times.**
(Circular movement to the **left.)**

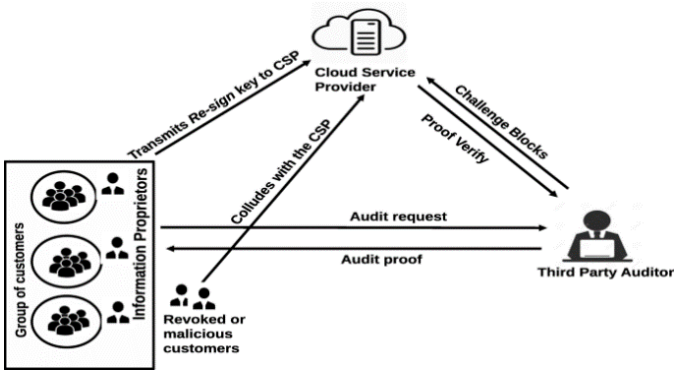
```
[ b0 | b1 | b2 | b3 ]        [ b0 | b1 | b2 | b3 ]
| b4 | b5 | b6 | b7 |   ->   | b5 | b6 | b7 | b4 |
| b8 | b9 | b10 | b11 |      | b10 | b11 | b8 | b9 |
[ b12 | b13 | b14 | b15 ]    [ b15 | b12 | b13 | b14 ]
```

DECRYPTION

The process of restoring encrypted material to its original, readable form is known as decryption. It requires a secret key or password to access the encrypted information. Purpose: The main purpose of decryption is to ensure the confidentiality of sensitive information. By encrypting data, unauthorized parties are prevented from reading or accessing the information. Decryption allows authorized parties to retrieve and view the original data. Security: Decryption plays a crucial role in securing sensitive information, such as passwords, login IDs, and other confidential data. It ensures that only authorized individuals with the correct decryption key or password can access the encrypted data

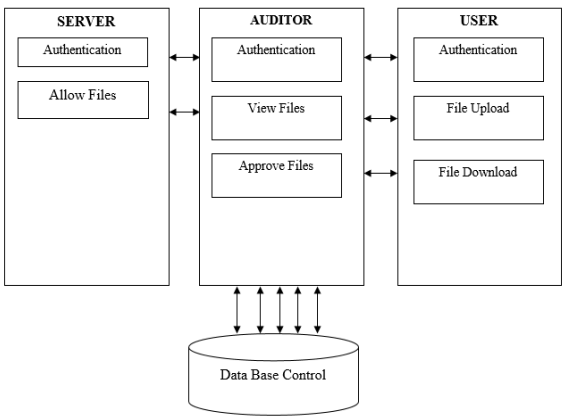
2. PUBLIC AUDITING ALGORITHM

Public auditing of algorithms refers to the process of assessing and evaluating algorithms used in various domains to ensure transparency, fairness, and accountability. It involves independent reviews and assessments of algorithms by external entities, such as regulatory bodies, public auditors, or specialized organizations. The goal is to identify and mitigate potential issues, biases, or risks associated with algorithmic decision-making systems. Key Takeaways: The field of public auditing algorithms is still in its early stages of development. Public sector involvement may be necessary to incentivize an ex-ante approach to algorithm auditing efforts to proactively find and fix problems in algorithmic systems have proven sluggish to get going. Public auditing algorithms is an important process to ensure the responsible and ethical use of algorithms in various domains. It promotes transparency, accountability, and trust in algorithmic systems. While the field is still in its early stages, efforts are being made to develop guidelines, standards, and best practices for effective algorithm auditing. Collaboration between stakeholders is key to addressing the challenges and ensuring the integrity of algorithmic decision-making systems. Public auditing algorithms play a crucial role in ensuring the ethical and responsible use of algorithms in various domains. Here are some reasons why public auditing is important: Transparency**:** Public auditing promotes transparency by providing external scrutiny of algorithms and their decision-making processes. It helps uncover any hidden biases, discriminatory practices, or unintended consequences. Accountability**:** Auditing algorithms holds organizations accountable for the impact of their algorithms on individuals and society. It helps identify and rectify any unfair or harmful practices. Trust and Confidence**:** Public auditing helps build trust and confidence in algorithmic systems by ensuring that they are fair, unbiased, and aligned with societal values. It provides assurance to stakeholders that algorithms are being used responsibly. Mitigating Risks**:** Auditing algorithms helps identify and mitigate risks associated with algorithmic decision-making, such as privacy breaches, security vulnerabilities, or unintended consequences.



V. PROPOSED SCHEME

Implementing a, multi-cloud shared security system for privacy protecting data using bigdata as proposed in the sources, involves leveraging cryptographic techniques to ensure data integrity and privacy. The proposed systems utilize AES achieve efficient and secure auditing without compromising user privacy. Preservation of Identity Privacy: The system effectively maintains the privacy of the users who sign each block of shared data in the cloud. This is crucial for groups where the identity of the signer may indicate their role or the importance of the data, they are responsible for. By keeping the identity of the signer private from third-party auditors (TPAs), the system ensures that sensitive information about the group's operations or data priorities remains confidential. Verification Without Disclosure: The mechanism allows for the verification of the integrity of shared data without the need for the TPA to access the entire file. This is particularly useful for auditing large datasets or for performing audits on data stored in untrusted cloud environments, where data integrity is subject to skepticism and scrutiny Ring Signatures for Efficiency: The use of ring signatures in the proposed system contributes to its efficiency. Ring signatures enable the computation of verification information needed to audit the integrity of shared data without revealing the identity of the signer. This approach ensures that the TPA can verify the integrity of the shared data without retrieving the entire file, making the auditing process more efficient. The proposed system aims to achieve efficient auditing operations to minimize computational overhead and reduce the communication costs between the cloud service provider and the users. This efficiency is crucial, especially when dealing with large-scale shared cloud data.



VI. *FUTURE ENHANCEMENTS:*

Enhancing Security and Privacy Measures

• **Improving Identity Privacy**: The current system aims to preserve the identity of signers on each block during public auditing, which is a critical aspect of privacy. Future work could explore more sophisticated cryptographic techniques or novel identity-preserving protocols to further enhance the privacy of users while maintaining the integrity and authenticity of the audited data.

• **Resilience Against Attacks**: While the proposed system is designed to be resistant to common attacks, continuous research is needed to develop more advanced attack models and countermeasures. This includes exploring new types of attacks that could exploit vulnerabilities in the system and developing robust defences against them

.

Scalability and Efficiency

- **Optimizing Cryptographic Primitives**: The system's performance and efficiency are crucial, especially as cloud environments scale. Future research could focus on optimizing cryptographic primitives used in the system, such as bilinear maps, to ensure they remain efficient even as the size of the data and the number of users grow.
- **Efficient Public Auditing Mechanism**: The size of verification metadata in public auditing mechanisms can become a significant issue as the system scales. Future work could aim at designing more efficient public auditing mechanisms that reduce the size of verification metadata while maintaining the integrity and authenticity of the audited data.
- **Strengthened Security** Measures: As the research by Tian et al. highlighted, existing schemes were vulnerable to tag forgery or proof forgery attacks. Future research could focus on developing more secure auditing schemes that are resistant to such attacks. This would involve exploring cryptographic techniques that ensure the integrity and authenticity of audit proofs, thereby strengthening the overall security framework.
- **Performance Optimization**: The comparison of computational and communication costs in the study suggests that there is room for optimization in terms of performance. Future work could aim to reduce the overhead associated with auditing processes, making them more efficient without compromising on security or privacy. This could involve leveraging advancements in hardware and software technologies to streamline the auditing process

VII. *CONCLUSION:*

In conclusion, the project on multi cloud share security for privacy protecting data using bigdata represents a significant advancement in the realm of cloud data security and integrity. By addressing the critical challenges of ensuring data privacy while facilitating public auditing capabilities, this project has the potential to revolutionize the way shared cloud data is managed and audited. The integration of advanced cryptographic techniques and secure group management within the cloud environment not only enhances the privacy and security of individual users' data but also allows for the integrity and authenticity of shared data to be verified by auditors. This approach ensures that only authorized members of a group can access and audit the shared data, further safeguarding the privacy and security of the system. Moreover, the proposed system's resistance to common attacks like tag forgery or proof forgery underscores its robustness and reliability**.** The implementation of a multi-cloud security system involves addressing various challenges, such as data confidentiality, integrity, availability, access control, computation, analysis, management, reliability, and scalability. These challenges can be overcome through optimized big data management, scheduling workflows with privacy protection constraints, and other techniques that enhance security and privacy in cloud computing. It is important to note that the search results do not provide a specific conclusion on the topic of multi-cloud share security systems for privacy-protecting data using big data. However, the information provided highlights the importance of security and privacy in cloud computing, the challenges involved, and the need for comprehensive solutions to protect data in multi-cloud environments.

VIII. *REFERENCES:*

1. (Apr. 2021). Cloud Storage-Global Market Trajectory and Analytics. [Online]. Available: https://www.researchandmarkets.com/reports/ 5140992/cloud-storage-global-market-trajectory-and

2. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, ‘‘Provable data possession at untrusted stores,’’ in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), 2007, pp. 598–609.

3. A. Juels and B. S. Kaliski, ‘‘PORs: Proofs of retrievability for large files,’’ in Proc. 14th ACM Conf. Comput. Commun. Secur. (CCS), Oct. 2007, pp. 584–597.

4. H. Shacham and B. Waters, ‘‘Compact proofs of retrievability,’’ in Proc. Int. Conf. Theory Appl. Cryptol. Inf. Secur. Berlin, Germany: Springer, 2008, pp. 90–107.

5. C. Wang, Q. Wang, K. Ren, and W. Lou, ‘‘Privacy-preserving public auditing for data storage security in cloud computing,’’ in Proc. IEEE INFOCOM, Mar. 2010, pp. 1–9.

6. 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, Sep. 2011.

7. K. Yang and X. Jia, ‘‘An efficient and secure dynamic auditing protocol for data storage in cloud computing,’’ IEEE Trans. Parallel Distrib. Syst., vol. 24, no. 9, pp. 1717–1726, Sep. 2013.

8. C. Wang, S. S. M. Chow, Q. Wang, K. Ren, and W. Lou, ‘‘Privacy preserving public auditing for secure cloud storage,’’ IEEE Trans. Comput., vol. 62, no. 2, pp. 362–375, Feb. 2013.

9. K. He, C. Huang, K. Yang, and J. Shi, ‘‘Identity-preserving public auditing for shared cloud data,’’ in Proc. IEEE 23rd Int. Symp. Quality Service (IWQoS), Jun. 2015, pp. 159–164.

10. C. Erway, A. Küpçü, C. Papamanthou, and R. Tamassia, ‘‘Dynamic provable data possession,’’ in Proc. 16th

ACM Conf. Computer. Commun. Secured. (CCS), New York, NY, USA, 2009, pp. 213–222.

11. Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, ''Enabling public auditability and data dynamics for storage security in cloud computing,'' IEEE Trans. Parallel Distrib. Syst., vol. 22, no. 5, pp. 847–859, May 2011.

12. Y. Zhu, G.-J. Ahn, H. Hu, S. S. Yau, H. G. An, and C.-J. Hu, ''Dynamic audit services for outsourced storages in clouds,'' IEEE Trans. Services Comput., vol. 6, no. 2, pp. 227–238, Apr./Jun. 2013.

13. J. Shen, J. Shen, X. Chen, X. Huang, and W. Susilo, ''An efficient public auditing protocol with novel dynamic structure for cloud data,'' IEEE Trans. Inf. Forensics Security, vol. 12, no. 10, pp. 2402–2415, Oct. 2017.

14. B. Wang, B. Li, and H. Li, ''Knox: Privacy-preserving auditing for shared data with large groups in the cloud,'' in Proc. 10th Interfaces Conf. Appl. Crypto. Netw. Secur., 2012, pp. 507–525.

15. B. Wang, B. Li, and H. Li, ''Oruta: Privacy-preserving public auditing for shared data in the cloud,'' IEEE Trans. Cloud Comput., vol. 2, no. 1, pp. 43–56, Jan./Mar. 2014.

16. B. Wang, B. Li, and H. Li, ''Panda: Public auditing for shared data with efficient user revocation in the cloud,'' IEEE Trans. Serv. Comput., vol. 8, no. 1, pp. 92–106, Jan./Feb. 2015.

17. T. Jiang, X. Chen, and J. Ma, ''Public integrity auditing for shared dynamic cloud data with group user revocation,'' IEEE Trans. Comput., vol. 65, no. 8, pp. 2363–2373, Aug. 2016.

18. J. Yuan and S. Yu, ''Efficient public integrity checking for cloud data sharing with multi-user modification,'' in Proc. IEEE Conf. Computer. Communication. (IEEE INFOCOM), Apr. 2014, pp. 2121–2129.

19. J. Yuan and S. Yu, ''Public integrity auditing for dynamic data sharing with multiuser modification,'' IEEE Trans. Inf. Forensics Security, vol. 10, no. 8, pp. 1717–1726, Aug. 2015.

20. G. Yang, J. Yu, W. Shen, Q. Su, Z. Fu, and R. Hao, ''Enabling public auditing for shared data in cloud storage supporting identity privacy and traceability,'' J. Syst. Softw., vol. 113, pp. 130–139, Mar. 2016.