A Secure Data Dynamics and Public Auditing Scheme for Cloud Storage

Prof.S.S. Bhuite[1*], Swapnali Aware[2], Chaitali Bandgar[3], Prajakta Giram[4], Swapnali Patil[5]

[1]Assistant Professor, Department of Computer Science and Engineering, Brahmdevdada Mane Institute of Technology, Solapur, Maharashtra, India

[2]UG Student, Department of Computer Science and Engineering, Brahmdevdada Mane Institute of Technology, Solapur, Maharashtra, India

Corresponding Author Email: bhuite.sagar@gmail.com

Abstract—

This paper introduced a robust and efficient framework designed to ensure secure dynamic data handling and public auditing in cloud storage systems. The primary goal was to strengthen data integrity and user confidentiality using advanced cryptographic methods and privacy-aware third-party auditing (TPA). An in- depth analysis of existing cloud security models was conducted to uncover persistent challenges such as secure management of data updates, protection of user privacy, and reliable auditing within potentially untrusted cloud environments.

To address these issues, a modular system architecture was developed that supports dynamic data operations—including insertion, deletion, and modification—while enabling secure data outsourcing. The auditing mechanism allows a trusted third party to verify data integrity without exposing sensitive information, ensuring both transparency and privacy. Additionally, the framework incorporates lightweight cryptographic algorithms aimed at reducing computational and communication costs.A comprehensive feasibility study was performed, and the necessary hardware and software requirements were identified to support real-world implementation. The proposed solution demonstrated high potential for scalability, efficiency, and user trust. Overall, the framework offers a practical pathway toward secure, transparent, and user-centric cloud data management, making it a valuable contribution to advancing cloud storage security.

Keywords:

Cloud Storage Systems, Secure Dynamic Data Handling, Public Auditing, Data Integrity, User Confidentiality, Cryptographic Methods, Privacy-Aware, Third-Party Auditing (TPA), Cloud Security Models, Data Updates, User Privacy, Untrusted Cloud Environments, Modular System Architecture, Dynamic Data Operations, Secure Data Outsourcing, Auditing Mechanism, Trusted Third Party, Lightweight Cryptographic Algorithms, Computational Costs, Communication Costs, Feasibility Study, Hardware Requirements, Software Requirements, Scalability, Efficiency, User Trust, Transparent Data Management, Cloud Data Security.

INTRODUCTION

The rise of cloud computing has revolutionized data storage and management by offering scalable, on-demand resources with reduced infrastructure costs. However, outsourcing data to third-party cloud providers introduces significant concerns regarding data integrity, confidentiality, and user control. Users often face limitations in verifying whether their stored data remains intact over time, especially when they no longer maintain local copies. Furthermore, traditional security approaches fall short in providing both privacy and auditability in dynamic cloud environments, where data modifications such as insertions, deletions, and updates are frequent.

To address these challenges, this paper proposes a secure data dynamics and public auditing scheme tailored for cloud storage systems. The scheme allows users to perform dynamic operations on their data while enabling a trusted third-party auditor (TPA) to verify data integrity without accessing the actual content. Leveraging homomorphic authenticators, random masking, and batch auditing techniques, the proposed system ensures robust data security, privacy preservation, and efficient audit performance. This framework offers a practical solution for maintaining trust and control in outsourced cloud storage environments.

I. LITRATURE REVIEW

Existing literature in the field of secure data dynamics and public auditing for cloud storage predominantly addresses the challenge of maintaining data confidentiality, integrity, and accessibility while ensuring the integrity of the cloud storage system. Key research focuses on cryptographic methods, where public key cryptography and homomorphic encryption are often employed to ensure that data remains secure while allowing authorized third parties (auditors) to verify its integrity without accessing the actual content. Various auditing schemes have been proposed, integrating both provable data possession (PDP) and proof of retrievability (PoR) to guarantee data correctness over time.

Recent studies emphasize the importance of dynamic data operations (such as updates, deletions, and additions) in cloud storage environments, addressing the need for secure and efficient ways to handle these operations without compromising the security of the entire system. Research often explores the trade-offs between performance and security, seeking lightweight solutions that do not impose excessive computational burdens on cloud resources. Advanced cryptographic primitives, such as signature-based verification and zero-knowledge proofs, are frequently discussed for their ability to facilitate secure auditing with minimal data exposure.

In the context of cloud storage for developing countries, such as India, specific challenges have been identified, including the potential for network instability and the need for cost-effective solutions. Studies show that deploying secure and dynamic data auditing systems in such environments requires careful attention to bandwidth constraints, latency issues, and energy- efficient implementations. While there has been some work on tailoring auditing systems for these regions, many systems fail to address the unique operational challenges in developing countries, particularly with respect to the heterogeneity of users' devices and the varying trust models.

Another important aspect in the literature is the growing trend towards integrating blockchain technology into auditing systems for cloud storage. Blockchain’s decentralized and immutable nature makes it an ideal candidate for enhancing data integrity and trust in public auditing systems. Researchers have proposed blockchain-based solutions to ensure transparent and tamper- proof auditing mechanisms for cloud storage, though scalability and energy efficiency remain areas of active investigation.

While these advancements have been significant, there remains a gap in literature concerning the practical implementation of these secure data dynamics and auditing systems, particularly in low-resource settings. This project seeks to address this gap by exploring efficient, scalable, and secure auditing mechanisms for cloud storage, tailored to environments with limited computational and network resources, while also ensuring the systems remain secure and reliable for dynamic data operations.

II. ALGORITHM

To support core functionality and security in the proposed system, multiple algorithms have been integrated. These algorithms ensure secure data handling, integrity verification, and privacy-preserving auditing within a cloud storage environment.

1. **Data Segmentation and Signature Generation Algorithm** This algorithm handles the initial processing of user data before it is uploaded to the cloud. It splits the entire file into fixed-size data blocks (e.g., 4 KB each), which are easier to manage, modify, or audit individually. Each data block is then signed using a cryptographic signing function such as a homomorphic authenticator based on RSA or BLS (Boneh–Lynn–Shacham) signatures. These signatures are later used to verify data possession and correctness without accessing the actual content.

2. **Dynamic Data Operation Algorithm** This component supports operations such as block insertion, deletion, and modification directly within the cloud storage. It ensures that when a block is modified, its associated signature is recalculated to reflect the new content. When a block is inserted or deleted, both the storage structure and metadata (such as block indices and tags) are updated to maintain consistency. This allows for real-time, flexible cloud data management while retaining verifiability.

3. **Public Auditing Algorithm** In this algorithm, a Third-Party Auditor (TPA) can verify the integrity of cloud-stored data on behalf of the user. Without retrieving the full data, the TPA sends a challenge to the cloud containing randomly selected block indices. The server responds with a computed proof that aggregates the corresponding block data and signatures using algebraic operations over finite fields. The TPA then verifies the proof using the public key and predefined hash functions.

4. **Batch Auditing Algorithm** :This algorithm enables the TPA to verify multiple audit requests—either from the same user or from multiple users—in a single batch. Instead of checking each file or user data independently, it uses algebraic aggregation of multiple responses into one combined proof. This drastically reduces the amount of time and communication bandwidth required, especially in multi-user cloud systems.

5. **Challenge-Response Protocol:** The core auditing process uses a challenge-response mechanism. The TPA selects a small random sample of data blocks and assigns a random coefficient to each. The cloud then computes a linear combination of the selected blocks using those coefficients and combines the corresponding signatures. This proof is then sent to the TPA, who verifies whether the result matches the expected signature of the computed value, confirming data correctness.

6. **Privacy-Preserving Masking Algorithm** This algorithm adds a layer of random masking to the data during the audit response. Even though the TPA receives the result of a linear combination of data blocks, random values are introduced to obfuscate actual data values. This ensures that the TPA can perform integrity verification but cannot infer any meaningful information about the data content, thereby preserving user confidentiality during public audits.

7. **Authentication and Access Control Algorithm** This algorithm controls user access by enforcing login and session mechanisms. User credentials (such as passwords) are securely stored using cryptographic hashing (e.g., SHA-256, bcrypt), and tokens or session IDs are used to manage authenticated sessions. Role-based access control (RBAC) is optionally applied to ensure that only authorized users can perform operations like upload, audit request, or deletion.

8. **Input Validation and Error Handling** This algorithm ensures that all incoming user inputs—such as file uploads, block indices, authentication tokens, or operation commands—are sanitized and validated. It rejects malformed or malicious inputs, applies boundary checks, and uses exception handling logic to ensure that the system doesn't crash or leak sensitive data. It contributes to both the robustness and security of the system by preventing injection attacks and runtime failures.

III. SYSTEM ARCHITECTURE

The system architecture defines how different entities interact within the framework for secure cloud storage and public auditing. It involves three primary roles: **User**, **Cloud Server**, and **Third-Party Auditor (TPA)**. The workflow and interaction are described as follows:

.

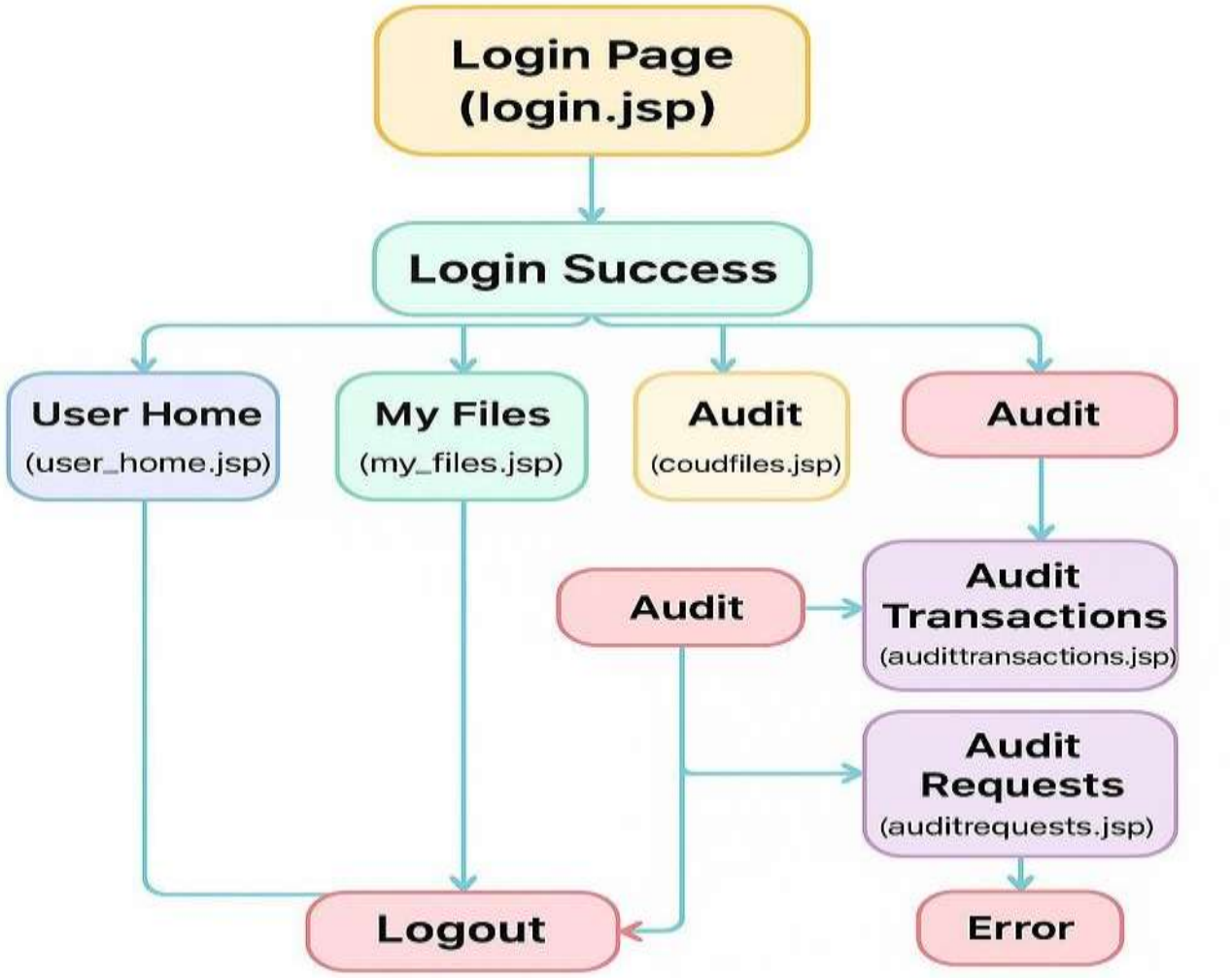
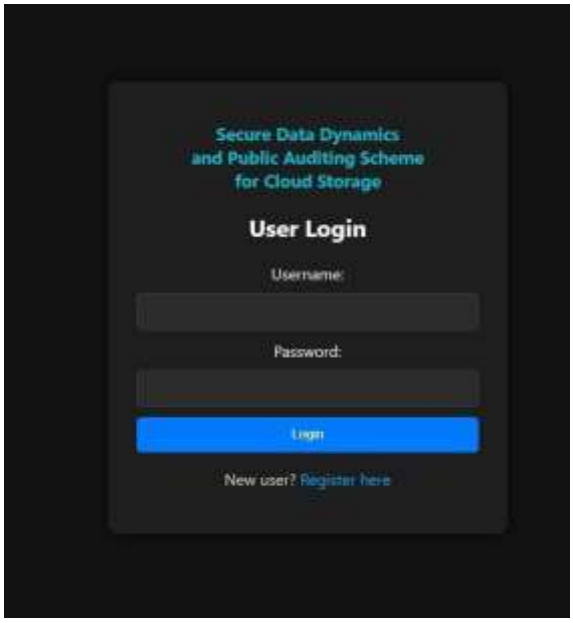


Figure 1.1 System Architeture

IV. RESULTS


Secure Data Dynamics
and Public Auditing Scheme
for Cloud Storage
User Login
Username:
Password:
Login
New user? Register here


Welcome, Chaitu1404!
My Files
Upload File
Logout


Upload Cloud File


Welcome Admin


My Files

V. REFERENCES

1) C. Wang, S. S. M. Chow, Q.Wang, K. Ren, and W. Lou, "Privacy-Preserving Public Auditing for Secure Cloud Storage," Cryptology ePrint Archive, Report 2009/579, 2009.

2) H. A. Gosavi and M. R. Umale, "Public Auditing and Data Dynamics for Storage Security inCloud Computing," arXiv preprint arXiv:1405.6263, 2014.

3) A. Salim, R. K. Tiwari, and S. Tripathi, "An Efficient Public Auditing Scheme for Cloud Storage with Secure Access Control and Resistance Against DOS Attack by Iniquitous TPA," Wireless Pers. Commun., vol. 117, no. 4, pp. 2929–2954, 2021.

4) S. M. V. Nithya and V. R. Uthariaraj, "Identity- Based Public Auditing Scheme for Cloud Storage with Strong Key-Exposure Resilience," Security and Communication Networks, vol. 2020, Article ID 4838497, 2020.

5) H. Wang, Y. Zhang, X. A. Wang, and X. Yang,"An Improved Identity-Based Public Audit Protocol for Cloud Storage," Heliyon, vol. 10, no. 16, p.e36273, 2024.