IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12719

A Three-Layer Based Intelligence Data Protection Scheme In Cloud Storage

Dr Siddaraju[1], Ranjitha R[2]

Vice-Principal, Computer Science and Engineering M.Tech, Dr Ambedkar Institution of Technology, Bengaluru, India[1]

Student, Computer Science and Engineering M.Tech, Dr Ambedkar Institution of Technology, Bengaluru, India[2]

Abstract: The rapid adoption of cloud storage services necessitates robust mechanisms for ensuring data privacy and security. This project presents a comprehensive three-layer intelligent data privacy protection scheme tailored for cloud storage, implemented using Java for backend processes, and JSP, HTML, CSS, and JavaScript for the frontend interface. The database management is handled using MySQL, ensuring efficient data storage and retrieval. Our system leverages the AWS Cloud service provider for cloud storage solutions. It introduces a controlled user registration process where new users can only access the system upon administrative approval, enhancing security by preventing unauthorized access. Once registered, users can upload files to the cloud, where the system employs a multi-faceted approach to data protection. Uploaded files are partitioned into three distinct blocks, each encrypted using the Caesar Cipher algorithm. This classical encryption method, despite its simplicity, provides a foundational layer of security. Additionally, our system incorporates a deduplication feature that identifies and manages redundant data uploads, thereby optimizing storage efficiency. To ensure secure access and retrieval, a unique Message Authentication Code (MAC) is generated for each of the three blocks of data. This MAC Code is essential for the decryption process, ensuring that only authorized users can reconstruct and access the original files. The combination of data splitting, encryption, and MAC-based authentication forms a robust framework for maintaining data confidentiality and integrity in cloud environments. This project demonstrates a practical approach to enhancing data privacy in cloud storage systems, offering a scalable and secure solution for both individual users and organizations.

Keywords: cloud storage, data privacy, Message Authentication Code.

I. INTRODUCTION

In an era characterized by the exponential growth of digital data and the widespread adoption of cloud computing, ensuring the privacy and security of sensitive information stored in the cloud has become paramount. Cloud storage offers unparalleled convenience and scalability, enabling users to store, access, and share their data from anywhere at any time. However, the inherent risks associated with storing data in remote servers controlled by third-party providers have raised concerns about data privacy, integrity, and confidentiality.

To address these challenges, this project introduces a novel Three Layer-based Intelligent Data Privacy Protection Scheme tailored specifically for cloud storage environments. Leveraging advanced encryption techniques, efficient deduplication mechanisms, and secure access controls, the system aims to provide comprehensive protection for users' data while maintaining usability and performance.

The project utilizes a multi-layered approach to data privacy protection, incorporating modules for user management, file upload and storage, encryption and decryption, user interface, and database management. By integrating these modules seamlessly, the system offers a holistic solution for secure data handling and user interaction in the cloud.

Through the use of modern web technologies such as Java, JSP, HTML, CSS, and JavaScript, coupled with the robust storage capabilities of the AWS Cloud service provider, the project ensures a user-friendly and reliable cloud storage experience. The system's controlled user registration process, intelligent deduplication mechanisms, and secure encryption algorithms enhance data security and integrity, mitigating risks associated with unauthorized access and data breaches.

Overall, the project aims to contribute to the advancement of data privacy and security in cloud storage systems, providing users with a trustworthy and resilient platform for storing, managing, and accessing their data securely in the digital age. Through continuous innovation and adaptation to emerging threats and technologies, the project seeks to empower individuals and organizations to embrace the benefits of cloud storage while safeguarding their most valuable asset—their data.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12719

Fog computing is being used to design a three-tier storage framework. The proposed framework can take full advantage of cloud storage while still protecting your data's anonymity. To divide the data into separate pieces, the Caesar Cipher code technique is utilised. There is missing data information if one piece of data is missing. To safeguard data information and illustrate the scheme's safety and efficiency, the framework can apply algorithms based on the bucket concept. Furthermore, based on computer intelligence, the algorithm can calculate 80% of the data saved in the cloud, 15% of the data in the fog, and 5% of the data on the local machine. The framework can handle all aspects of cloud storage while maintaining data privacy. Cloud computing has piqued the interest of a unique segment of society in this area. The three-layer cloud garage is divided into three distinct information components.

II. EXISTING SYSTEM

In the existing cloud storage systems, users typically register and log in with minimal oversight, often relying solely on standard user authentication methods such as username and password. Upon successful authentication, users can directly upload, download, and manage their files within the cloud environment. In the existing system, once data is uploaded, it is stored as single, contiguous files within the cloud storage infrastructure. Standard encryption algorithms, if applied, typically encrypt the file as a whole before uploading.

This approach ensures that the data is protected during transmission and while at rest in the cloud. However, the encryption and decryption processes are straightforward, usually involving symmetric or asymmetric key algorithms managed by the user or the cloud service provider. The existing system may also include basic measures for data integrity, such as checksums or hashing techniques, to ensure that the files have not been altered during transmission.

Additionally, some systems may offer rudimentary deduplication processes to identify and eliminate duplicate files to optimize storage space. Overall, the existing system provides a basic level of security and functionality, allowing users to store and retrieve their files from the cloud with standard encryption and integrity verification measures in place.

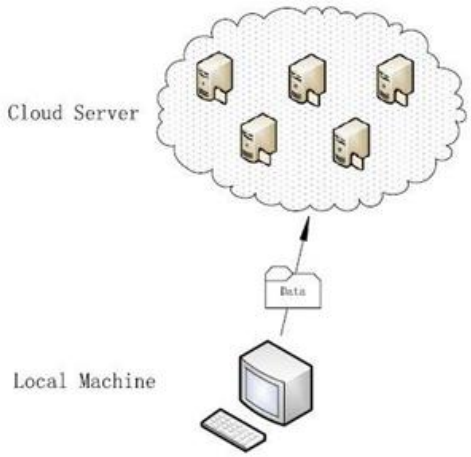

Fig.1 Existing System Architecture

III. PROPOSED SYSTEM

The proposed system introduces a multi-layered approach to enhance data privacy and security in cloud storage, addressing several critical aspects through advanced mechanisms and structured processes.

Controlled User Registration: The system enforces an administrative approval process for new user registrations. This ensures that only verified and authorized users gain access to the cloud storage platform, significantly reducing the risk of unauthorized access.

Data Upload and Storage: When a user uploads a file, the system splits the file into three distinct blocks. Each block is then encrypted separately using the Caesar Cipher algorithm. This segmentation and individual encryption add an additional layer of security, making it more difficult for unauthorized parties to reconstruct the original file.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12719

Cloud Storage with AWS: The encrypted data blocks are stored in the cloud using the AWS Cloud service provider. AWS provides a reliable and scalable cloud storage solution, supporting the secure storage requirements of the proposed system.

Deduplication Mechanism: The system incorporates an intelligent deduplication process that checks for duplicate files during the upload. If the same file has been previously uploaded, the system identifies it and manages the storage efficiently, ensuring optimal use of storage resources.

MAC Code Generation for Security: For each of the three encrypted blocks, the system generates a unique Message Authentication Code (MAC). This MAC code is essential for the decryption process, serving as a secure key that ensures only authorized users can decrypt and download the stored files.

Frontend and Database Management: The frontend of the system is developed using JSP, HTML, CSS, and JavaScript, providing a user-friendly interface for interacting with the cloud storage. MySQL is used for database management, ensuring efficient data handling and storage operations.

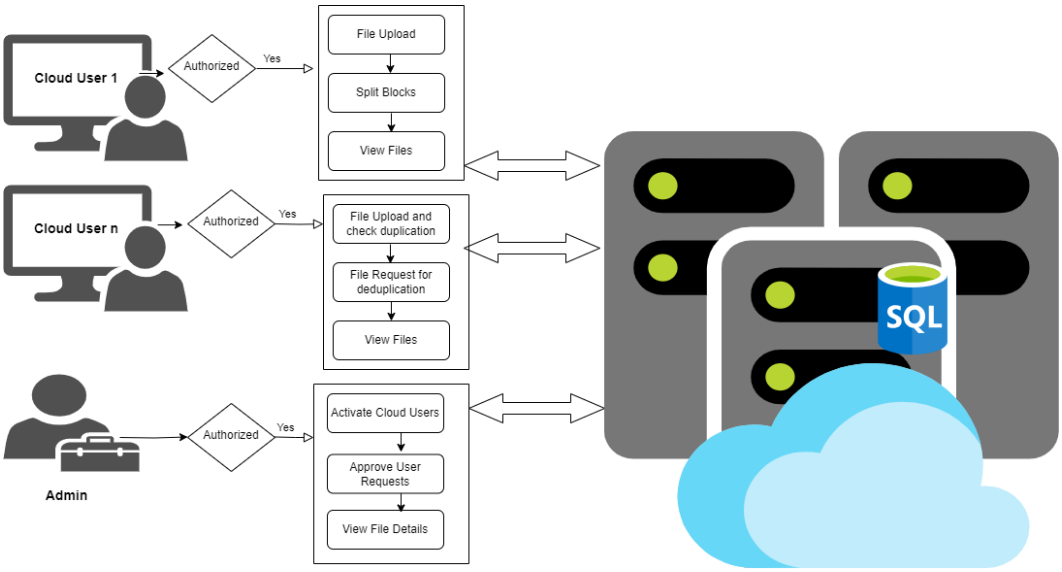

Fig.2 Proposed System Architecture

IV. RELATED WORK

User Management Module:
This module facilitates the registration and management of users within the system. It includes functionalities for user registration, login, and profile management. Additionally, administrative features for approving new user registrations and managing user accounts are included. The module ensures secure user authentication and access control, enforcing strict validation processes to prevent unauthorized access to the system.

File Upload and Storage Module:
The File Upload and Storage module handle the uploading, partitioning, encryption, and storage of files in the cloud environment. Upon file upload, the system splits the file into three distinct blocks and encrypts each block individually using the Caesar Cipher algorithm. The encrypted blocks are then stored securely in the DriveHQ Cloud service provider. The module incorporates mechanisms for efficient deduplication to identify and manage duplicate files, optimizing storage resources and enhancing system performance.

Encryption and Decryption Module:
This module is responsible for implementing encryption and decryption processes to ensure the confidentiality and security of the stored data. It employs the Caesar Cipher algorithm to encrypt file blocks before storage in the cloud. During file retrieval, authorized users utilize unique Message Authentication Codes (MAC) generated for each block to decrypt and reconstruct the original file. The module handles encryption key management securely, preventing unauthorized access to sensitive data.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12719

User Interface Module:
The User Interface module provides a user-friendly frontend interface for interacting with the cloud storage system. Developed using JSP, HTML, CSS, and JavaScript, the interface offers seamless navigation and intuitive functionalities for users to upload, download, and manage their files. It includes features for displaying file listings, monitoring upload/download progress, and managing user preferences. The module ensures an engaging and responsive user experience, enhancing user satisfaction and adoption.

Database Management Module:
This module manages the storage and retrieval of data from the MySQL database. It stores user information, file metadata, authentication credentials, and system configurations securely. The module includes functionalities for data querying, insertion, updating, and deletion, ensuring efficient data management operations. It enforces data integrity constraints and implements backup and recovery mechanisms to safeguard against data loss or corruption. The module serves as a central repository for critical system information, facilitating seamless integration with other modules.

System Administration Module:
The System Administration module provides administrative functionalities for managing system configurations, user permissions, and access control policies. It includes features for configuring security settings, managing user roles and privileges, and monitoring system activities. The module allows administrators to perform tasks such as approving new user registrations, view cloud files, and auditing system logs. It ensures effective system governance and compliance with security policies, enhancing overall system security and reliability.

V. FUTURE WORK

While the current project provides a solid foundation for intelligent data privacy protection in cloud storage, several avenues for future work and enhancements can be explored to further improve the system's functionality and effectiveness:

Advanced Encryption Techniques: Investigate and implement more advanced encryption algorithms beyond the Caesar Cipher to enhance data security further. Techniques such as AES (Advanced Encryption Standard) or RSA (Rivest-Shamir-Adleman) can offer stronger cryptographic protection against modern threats.

Enhanced Deduplication Strategies: Develop and integrate more sophisticated deduplication algorithms to improve the identification and elimination of duplicate files. Machine learning-based approaches or content-aware deduplication techniques can enhance deduplication accuracy and efficiency.

Intelligent Access Control Policies: Implement dynamic access control policies based on contextual factors such as user behavior, location, and device characteristics. Adaptive access control mechanisms can provide finer-grained access control and adapt to changing security requirements dynamically.

Multi-Cloud Integration: Extend the system to support multi-cloud environments, allowing users to distribute their data across multiple cloud service providers for redundancy and fault tolerance. Implementing interoperability standards and seamless data migration mechanisms can facilitate multi-cloud integration.

Comprehensive Security Auditing: Develop robust mechanisms for continuous security auditing and monitoring to detect and respond to security incidents proactively. Implement intrusion detection systems (IDS), anomaly detection algorithms, and real-time monitoring tools to ensure the system's resilience against evolving threats.

Blockchain Integration for Data Integrity: Explore the integration of blockchain technology to enhance data integrity and tamper resistance. Utilizing blockchain-based distributed ledgers can provide immutable records of data transactions and ensure transparent and auditable data storage and access.

User-Centric Privacy Controls: Empower users with more granular control over their privacy settings and data sharing permissions. Implement features such as data anonymization, pseudonymization, and selective data sharing to give users greater control over their personal information and ensure compliance with data privacy regulations.

Scalability and Performance Optimization: Optimize the system's scalability and performance to accommodate increasing data volumes and user loads efficiently. Implement techniques such as horizontal scaling, load balancing, and caching mechanisms to ensure seamless performance even under high-demand scenarios.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.311 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 7, July 2025

DOI: 10.17148/IARJSET.2025.12719

By pursuing these avenues for future work, the project can evolve into a more robust and comprehensive solution for intelligent data privacy protection in cloud storage, addressing emerging challenges and meeting the evolving needs of users and organizations in an increasingly digital landscape.

VI. CONCLUSION

In conclusion, the project presents a comprehensive and intelligent data privacy protection scheme tailored for cloud storage environments. By leveraging a multi-layered approach and advanced encryption techniques, the system addresses critical challenges in ensuring the confidentiality, integrity, and availability of data stored in the cloud. Through modules such as user management, file upload and storage, encryption and decryption, user interface, and database management, the system provides a robust framework for secure data handling and user interaction. The controlled user registration process, efficient de-duplication mechanisms, and secure key management enhance the overall security posture of the system, mitigating risks associated with unauthorized access, data duplication, and data breaches.

REFERENCES

[1]. P. Mell and T. Grance, "The NIST definition of cloud computing," *Nat. Inst. Stand. Technol.*, vol. 53, no. 6, pp. 50–50, 2009.

[2]. H. T. Dinh, C. Lee, D. Niyato, and P. Wang, "A survey of mobile cloud computing: Architecture, applications, and approaches," *Wireless Commun. Mobile Comput.*, vol. 13, no. 18, pp. 1587–1611, 2013.

[3]. J. Chase, R. Kaewpuang, W. Yonggang, and D. Niyato, "Joint virtual machine and bandwidth allocation in software defined network (sdn) and cloud computing environments," in *Proc. IEEE Int. Conf. Commun.*, 2014, pp. 2969–2974.

[4]. H. Li, W. Sun, F. Li, and B. Wang, "Secure and privacy-preserving data storage service in public cloud," *J. Comput. Res. Develop.*, vol. 51, no. 7, pp. 1397–1409, 2014.

[5]. Y. Li, T.Wang, G.Wang, J. Liang, and H. Chen, "Efficient data collection in sensor-cloud system with multiple mobile sinks," in *Proc. Adv. Serv. Comput., 10th Asia-Pac. Serv. Comput. Conf.*, 2016, pp. 130–143.

[6]. L. Xiao, Q. Li, and J. Liu, "Survey on secure cloud storage," *J. Data Acquis. Process.*, vol. 31, no. 3, pp. 464–472, 2016.

[7]. R. J. McEliece and D. V. Sarwate, "On sharing secrets and reed-solomon codes," *Commun. ACM*, vol. 24, no. 9, pp. 583–584, 1981.

[8]. J. S. Plank, "T1: Erasure codes for storage applications," in *Proc. 4th USENIX Conf. File Storage Technol.*, 2005.

[9]. R. Kulkarni, A. Forster, and G. Venayagamoorthy, "Computational intelligence in wireless sensor networks: A survey," *IEEE Commun. Surv. Tuts.*, vol. 13, no. 1, pp. 68–96, First Quarter 2011.

[10]. Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, "A privacy preserving and copy-deterrence content-based image retrieval scheme in cloud computing," *IEEE Trans. Inf. Forensics Security*, vol. 11, no. 11, pp. 2594–2608, Nov. 2016.

[11]. J. Shen, D. Liu, J. Shen, Q. Liu, and X. Sun, "A secure cloud-assisted urban data sharing framework for ubiquitous-cities," *Pervasive Mobile Comput.*, vol. 41, pp. 219–230, 2017.

[12]. Z. Fu, F. Huang, K. Ren, J.Weng, and C.Wang, "Privacy-preserving smart semantic search based on conceptual graphs over encrypted outsourced data," *IEEE Trans. Inf. Forensics Security*, vol. 12, no. 8, pp. 1874–1884, Aug. 2017.

[13]. J. Hou, C. Piao, and T. Fan, "Privacy preservation cloud storage architecture research," *J. Hebei Acad. Sci.*, vol. 30, no. 2, pp. 45–48, 2013.

[14]. Q. Hou, Y. Wu, W. Zheng, and G. Yang, "A method on protection of user data privacy in cloud storage platform," *J. Comput. Res. Develop.*, vol. 48, no. 7, pp. 1146–1154, 2011.

[15]. P. Barham *et al.*, "Xen and the art of virtualization," *ACM SIGOPS Oper. Syst. Rev.*, vol. 37, no. 5, pp. 164–177, 2003.

