International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 05 | May - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

"Three Layer Based Intelligent Data Privacy in Cloud Computing"

Mr.Omkar Jeurkar, Mr.Shubham Bhuvad, Mr.Atharva Kulkarni, Mr.Aditya Darode

UG Student, Department of Electronics and telecommunication, Sinhgad Institute of Technology and Science, Narhe, Pune.

Mr. M. D. Patil

Professer , Department of Electronics and Telecommunication, Sinhgad Institute of Technology and Science, Narhe, Pune.

Abstract: The rapid advancement of cloud computing technology, coupled with the exponential increase in unstructured data, has led to heightened interest and significant progress in cloud storage solutions. However, cloud service providers often lack insights into the data they store and manage globally across their platforms. To address privacy concerns, various encoding technologies have been developed to enhance data protection. This paper proposes a three-tiered security framework for cloud storage that optimally utilizes cloud resources while safeguarding data privacy. Our approach involves segmenting data into multiple components, ensuring that the loss of any single piece results in the loss of the entire dataset. We implement a bucket-based algorithm to secure the data, demonstrating both protection and efficiency within our proposed model. Furthermore, leveraging process intelligence, this algorithm will assess the distribution ratios of data stored across cloud, fog, and local environments.

Keywords: Cloud Storage Security, Cloud Storage, Three-Layer Storage Security, Privacy Protection, DLP

INTRODUCTION

Overview of Project

With growing reliance on cloud storage, data privacy has become a major concern. This project introduces a three-layer architecture for enhanced data security. Each layer addresses distinct functions: collection, transmission, and access control. Data is segmented and distributed across cloud, fog, and local systems. Intelligent algorithms adapt privacy levels in real time based on data location. Advanced encoding techniques ensure confidentiality and prevent breaches. The system is scalable, efficient, and resource-optimized. It protects sensitive data from unauthorized access and loss. This model offers a balanced approach to privacy and performance. It supports secure and intelligent cloud adoption for organizations.

Related work

The field of data privacy in cloud computing has garnered significant attention from researchers and practitioners alike, leading to the development of various frameworks, algorithms, and strategies aimed at enhancing data security. This section reviews some of the key contributions in the area of cloud data privacy, highlighting the evolution of techniques and the gaps that our project seeks to address.

Encryption Techniques: Numerous studies have focused on encryption as a primary method for securing data in the cloud. Traditional encryption methods, such as symmetric and asymmetric encryption, have been widely adopted. However, these methods often face challenges related to key management and computational overhead. Recent advancements, such as homomorphic encryption, allow computations to be performed on encrypted data without decryption, thus preserving privacy.

Data Segmentation and Sharding: The concept of data segmentation, where data is divided into smaller, manageable pieces, has been explored in various works. Techniques such as sharding not only enhance data availability but also improve security by distributing data across multiple locations. However,ensuring the integrity and consistency of segmented data remains a challenge, particularly in dynamic cloud environments.

Despite progress in cloud security, a unified framework for data privacy is still lacking.Our project, "Three-Layer Based Intelligent Data Privacy in Cloud Computing," addresses this gap.It combines data segmentation, adaptive algorithms, and strong privacy techniques.The goal is to enhance cloud data security by building on and improving existing methods.

LITERATURE SURVEY

Sahai A, Waters B (2005) Fuzzy identity-based encryption. Advances in Cryptology - EUROCRYPT 2005, 2005: 457–473.

Sahai and Waters (2005) introduced Fuzzy Identity-Based Encryption (Fuzzy IBE). This encryption method allows decryption when the recipient's identity attributes are "close enough" to those used for encryption, using a defined metric. This error-tolerant approach is valuable for scenarios like biometric data and enables attribute-based access control for privacy-preserving data sharing, especially in cloud systems.

Brakerski Z, Vaikuntanathan V (2011) Efficient fully homomorphic encryption from (standard) LWE. Proceedings of the 2011 IEEE 52nd Annual Symposium on Foundations of Computer Science (FOCS): 97–106.

Brakerski and Vaikuntanathan (2011) introduced an efficient Fully Homomorphic Encryption (FHE) method based on the Learning With Errors (LWE) problem. This scheme significantly improved FHE by reducing complexity and enabling practical implementation, allowing direct computation on encrypted data and laying the groundwork for privacy-preserving cloud computing. This

breakthrough enables computations on encrypted data, preserving confidentiality for sensitive cloud applications.

Sandhu R, Coyne E, Feinstein H, Youman C (1996) Role-based access control models. IEEE Computer 29(2): 38–47.

Sandhu et al.'s 1996 paper introduced RBAC, a model where permissions are tied to roles, simplifying user access management. RBAC offers advantages like least privilege and easier administration, with a family of models (RBAC96) of increasing complexity. This foundational work established RBAC as a key access control method..

K. Liang, M. H. Au, J. K. Liu, W. Susilo, D. S. Wong, G. yang, Y. Yu,

and A. Yang, "A secure and efficient Ciphertext-Policy Attribute-Based Proxy Re-Encryption for cloud data sharing," Future Gener. Comput. Syst., vol. 52, pp. 95-108, 2015, DOI: 10.1016/j.future.2014.11.016.

Liang et al.'s 2015 paper introduces a way to securely share cloud data. It uses a technique called Ciphertext-Policy Attribute-Based Proxy Re-Encryption. This allows sharing based on user attributes while keeping the data protected. Published in Future Generation Computer Systems.

Ahmed E, Mahmood A, Hu J (2016) A survey of network anomaly detection techniques. Journal of Network and Computer Applications 60: 19–31.

Ahmed, Mahmood, and Hu's 2016 survey paper in the Journal of Network and Computer Applications reviews various network anomaly detection methods. It categorizes techniques into statistical, knowledge-based, machine learning-based, and specification-based approaches.

Kaur S, Singh S, Kumar A (2018) A multi-layer security framework for cloud computing. International Journal of Computer Applications 182(12): 1–6.

The Gentry's approach involves a lattice-based cryptographic system that supports both addition and multiplication operations on ciphertexts, paving the way for secure, privacy-preserving computations across various applications in cloud computing, data analytics, and beyond. This work remains foundational in cryptographic research and applications in secure data processing.

Alazab M, Venkatraman S, Alazab M (2019) Context-aware security for cloud computing. Journal of Cloud Computing: Advances, Systems and Applications 8(1): 1–15.

This paper explores the core security challenges in cloud computing, including data protection, secure access control, and privacy management. Zissis and Lekkas propose a holistic approach to security that combines encryption, access control, and trust management to mitigate vulnerabilities inherent in cloud environments.

Gap Research

Despite the significant advancements in data privacy and security within cloud computing, several gaps remain that hinder the effective protection of sensitive information. Existing frameworks often focus on isolated aspects of data security, such as encryption or access control, without considering the interplay between these components in a cohesive architecture. Additionally, many current solutions lack adaptability to dynamic environments, where data distribution and user behavior can change rapidly. The reliance on traditional security models may not adequately address the evolvingthreat landscape, leading to vulnerabilities that can be exploited by malicious actors.

Aim

"The primary aim of this project, "Three Layer Based Intelligent Data Privacy in Cloud Computing," is to develop a comprehensive and adaptive framework that enhances data privacy in cloud environments."

Problem Statement

"As organizations increasingly migrate to cloud computing, the protection of sensitive data has become a critical concern. Current data privacy solutions often fall short in providing a holistic approach that addresses the multifaceted nature of cloud security The lack of an integrated framework that combines data segmentation, intelligent processing.

Objectives

The primary objective of the Three Layer Based Intelligent Data Privacy model is to enhance the security and privacy of sensitive data stored in cloud environments. By implementing a comprehensive multi-layered approach, the model aims to protect data from unauthorized access, breaches, and other security threats. At its core, the model leverages advanced encryption techniques to ensure data remains secure both at rest and during transmission

PROPOSED METHODOLOGY

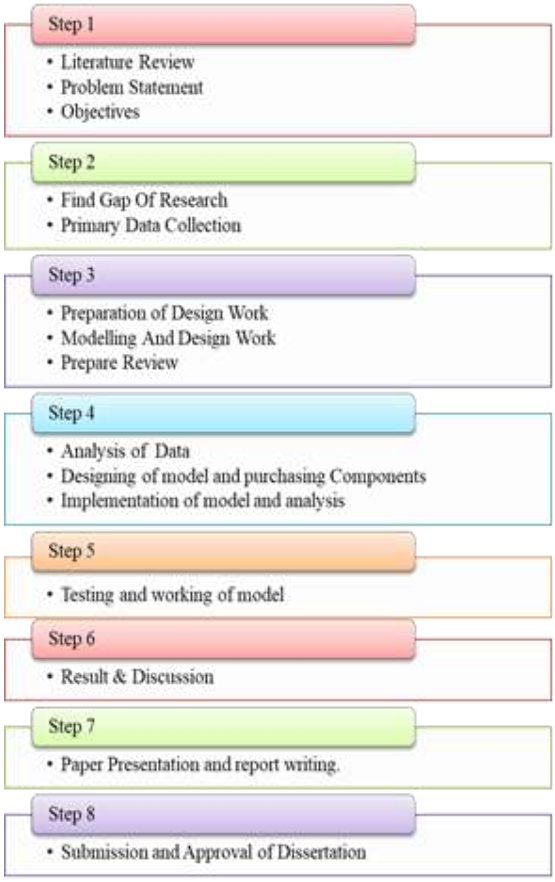
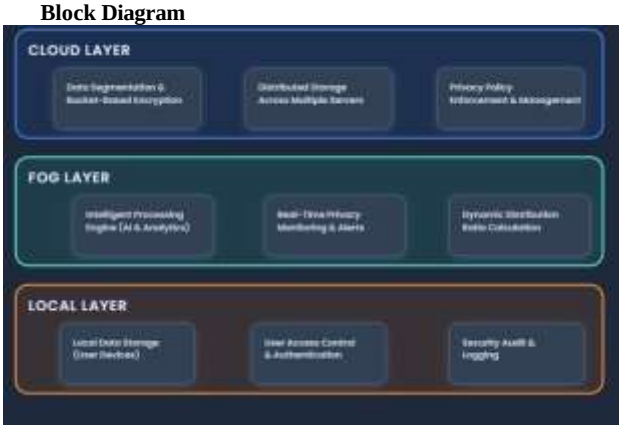


Figure1.1: Research Methodology Flow

Research Work

The research explores a three-layered approach to strengthen data privacy in cloud computing, addressing the limitations of traditional security models. The first layer applies machine learning to automatically classify data sensitivity, enabling tailored privacy measures. The second layer leverages privacy-preserving encryption techniques, selecting the most suitable encryption method for each sensitivity level to balance security and processing efficiency. The third layer focuses on dynamic access control, adjusting permissions based on user roles and continuously monitoring for security threats. Together, these layers form a robust, adaptable framework that ensures data protection, optimized for large-scale, multi-user cloud systems.

Block Diagram



SYSTEM DESIGN

Functional Requirement

Adaptive Privacy-Preserving Techniques:

1. Develop methods that dynamically adjust privacy measures based on real-time analysis of user behavior and data sensitivity.
2. Utilize machine learning algorithms to monitor access patterns and adapt security protocols accordingly. The classification process must be accurate and adapt to new data types in real-time.

Multi-Layer Security Frameworks:

1. A comprehensive security architecture that provides robust protection against various threats in cloud environments. Examine the combination of encryption, access control, and intrusion detection systems.
2. Investigate existing frameworks that integrate multiple layers of security measures.

Real-Time Monitoring and Threat Detection

1. The system should include monitoring tools to track user activity and detect potential threats in real-time.
2. It must alert administrators of suspicious activities, such as unauthorized access attempts or unusual data requests.
3. The threat detection module should adapt to new patterns of suspicious behavior using machine learning.

Data Segmentation and Sharding Approaches:

1. Explore innovative techniques for segmenting and sharding data to improve security and performance.

Non-Functional Requirement

- Performance: The system should be able to handle a minimum of 1000 concurrent users without significant degradation in response time.
- Scalability: The architecture must support horizontal scaling to accommodate increasing data volumes and user loads without requiring significant redesign.
- Usability: The user interface should be intuitive and user-friendly, allowing users to navigate and manage their data privacy settings with minimal training.
- Interoperability: The system must be compatible with existing cloud services and platforms, allowing for seamless integration with third-party applications and services.

Figure1.2: Block Diagram Web Page Description:

Admin Login Page:

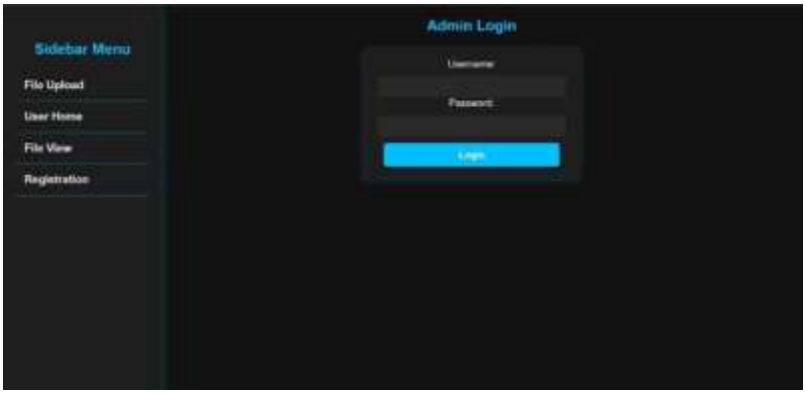


Figure1.3: Admin Login

- The Users enter basic information such as their name, email, gender, contact no, date of birth, state and country.
- The page includes strong password requirements to enhance account security, and multifactor authentication (MFA) is available to add an extra layer of protection.

New File Upload:

Figure1.4: New File Upload

- The interface enables users to upload files directly from their local device to the cloud infrastructure. The design features a dark-themed UI with a central file selection box and a clearly labeled "Upload" button to initiate the transfer.
- On the left-hand side, a sidebar menu provides easy navigation between key functionalities such as User Home, File Upload, Registration, and Cloud Storage.

Admin Dashboard:

Figure1.5: Admin Dashboard

- This figure shows the Admin Dashboard interface.The dashboard provides a table view listing uploaded files, along with key metadata such as Plagiarism Similarity (%), User Reason, and Actions for moderation.
- The administrator can review submissions, enter the respective username, and take action by clicking either Approve or Reject.

Admin Approved Files:

Figure1.6: Admin Approved File

- The main panel displays a welcome message, followed by the prompt "Please Upload your file", encouraging users to submit documents for admin approval.
- Once approved, the files are listed under the section "Admin Approved Files", each file being identifiable via a unique ID and file extension (Before accessing any file, users must enter the MAC key

Plagiarism Checking and Detection:

Figure1.6: Plagiarism Detection

- When a file is submitted and identified to have 100.00% similarity with a previously uploaded file, the system triggers a warning: "Plagiarism Detected"

- To proceed, the system presents a Request Approval dialog box, prompting the user to provide a justification for re-uploading the file.

Plagiarism Detected

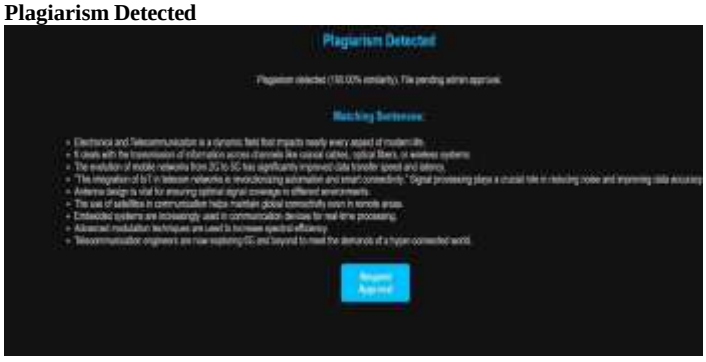


Figure1.6: Plagiarism Detected

- Identifies a file with 100.00% similarity but also extracts and highlights the matching sentences from the uploaded content.

- A "Request Approval" button is provided at the bottom, allowing users to formally submit a request to re-upload or validate the content.

CONCLUSION

This research presents a novel three-layer architecture for intelligent data privacy in cloud computing, integrating data segmentation, bucket-based encryption, and real-time monitoring to enhance security and user control. The proposed methodology addresses critical challenges in data privacy, paving the way for more secure cloud environments.
By leveraging data segmentation, bucket-based encryption, and real-time monitoring through the Cloud, Fog, and Local layers, this methodology effectively mitigates risks associated with unauthorized access and data breaches. The integration of intelligent processing allows for dynamic adaptation to emerging threats, while strict access control measures empower users to manage their data privacy actively.

REFERENCES

1. Sharma, A., & Gupta, R. (2023). Machine learning for data privacy in cloud computing: A review. Future Generation Computer Systems, 132, 1-15. doi: 10.1016/j.future.2022.10.001

2. Bertino, E., & Sandhu, R. (2005). Digital identity management and access control in cloud computing. IEEE Security & Privacy, 3(6), 24-31. doi:10.1109/MSP.2005.139

3. 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.

4. I. Chillotti, N. Gama, M. Georgieva, and M. Izabachène, ''TFHE: Fast fully homomorphic encryption over the torus,'' *J. Cryptol.*, vol. 33, no. 1, pp. 34–91, Jan. 2020.

5. H. Deng, Z. Qin, Q. Wu, Z. Guan, and Y. Zhou'Flexible attributebased proxy re-encryption forefficient data sharing,'' *Inf. Sci.*, vol. 511, pp.113, Feb. 2020

6. Singh, R., & Pasupuleti, S. (2017). A Multi-Layered Security Model for Cloud Computing. *International Journal of Advanced Research in Computer Science*, 8(5), 54-58.

7. Zissis, D., & Lekkas, D. (2012). Addressing Cloud Computing Security Issues. *Future Generation Computer Systems*, 28(3), 583-592.

8. Gentry, C. (2009). A Fully Homomorphic Encryption Scheme. Stanford University.

9. Sahai, A., & Waters, B. (2005). Fuzzy Identity-Based Encryption. *Advances in Cryptology – EUROCRYPT 2005*, 457-473.

10. Li, M., Yu, S., Zheng, Y., Ren, K., & Lou, W. (2013). Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption. *IEEE Transactions on Parallel and Distributed Systems*, 24(1), 131-143.

11. Chen, D., & Zhao, H. (2012). Data Security and Privacy Protection Issues in Cloud Computing. *2012 International Conference on Computer Science and Electronics Engineering*, 1, 647-651.

12. Wang, C., Wang, Q., Ren, K., Cao, N., & Lou, W. (2012). Toward Secure and Dependable Storage Services in Cloud Computing. *IEEE Transactions on Services Computing*, 5(2), 220-232.

13. Ranjan, R., & Bansal, A. (2020). A comprehensive review on data privacy in cloud computing. Journal of Cloud Computing: Advances, Systems and Applications, 9(1), 1-20. doi:10.1186/s13677-020-00167-5

14. Garg, S., & Kaur, A. (2022). Intelligent data privacy in cloud computing: A survey. Journal of King Saud University - Computer and Information Sciences. doi:10.1016/j.jksuci.2022.01.001

15. Khan, M. K., & Alghamdi, A. (2021). A three-layer architecture for secure data storage in cloud computing. Journal of Information Security and Applications, 58, 102-110. doi:10.1016/j.jisa.2020.102110