IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN:2349-2163
Volume 13, Issue 04, April https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2026.v1304.02

Securing Cloud Systems with Smart Authentication and Adaptive Encryption

G.Kasi Reddy
Assistant Professor, Department of CSE,
Guru Nanak Institute of Technology, Hyderabad, India
gkasireddy.gnit@gniindia.org
https://orcid.org/0009-0000-5001-7992
N.Gouri Sahithi Lakshmi Priya,S.Pandu,S.Mamatha
UG Student, Department of CSE
Guru Nanak Institute of Technology, Hyderabad, India
gourisahithi5@gmail.com, Pandusabavat59@gmail.com, sirishamamatha10@gmail.com

Publication History
Manuscript Reference No: IJIRAE/RS/Vol.13/Issue04/AEAP26.APAE10081
Research Article | Open Access | Double-Blind Peer-Reviewed| ArticleID: IJIRAE/RS/Vol.13/Issue04/AEAP26.APAE10181
Received:02,March 2026, Revised: 29, March 2026, Accepted: 10,April 2026,Published Online: 22, April 2026.
https://www.ijirae.com/volumes/Vol13/iss-04/02.AEAP26.APAE10081.pdf
Article Citation: Kasi,Gouri,Pandu,Mamatha(2026),Securing Cloud Systems with Smart Authentication and Adaptive Encryption, IJIRAE: International Journal of Innovative Research in Advanced Engineering, Volume 13, Issue 04 of 2026 pages 735-741 **Doi:>** https://doi.org/10.26562/ijirae.2026.v1304.02 BibTeX Key: **Kasi@2026Securing**
IJIRAE papers should be cited as IJIRAE (International Journal of Innovative Research in Advanced Engineering, AM Publications, India 2026, ISSN 2349-2163, https://doi.org/10.26562/ijirae.2026.v1304.02 The journal's official abbreviation is IJIRAE. Orcid: https://orcid.org/0009-0004-9398-7488

Abstract: The necessity for sophisticated security measures to safeguard private information on distant servers is highlighted by the cloud computing industry's explosive growth. To protect these data, authentication is essential. Vulnerabilities continue despite the different approaches that have been suggested. Using data mining approaches based on an intrusion-detection system, this research presents a revolutionary multi-factor authentication system coupled with a hybrid cryptographic framework that dynamically changes encryption algorithms. The proposed system employs passwords, conditional attributes, and fingerprint authentication to derive the encryption key from fingerprint data. It uses a dual-encryption strategy that combines five algorithm pairs: AES + HMAC (SHA-256), ECC + HMAC (SHA-512), HMAC-MD5 + PBKDF2, Twofish + Argon2, and Blowfish + HMAC SHA3-256. In order to secure the data, a hybrid model dynamically modifies an encryption algorithm to anticipate and categorize threats. Strong resistance to brute force, spoofing, phishing, guessing, and impersonation attacks was demonstrated by the framework. By putting this paradigm into practice in a cloud authentication environment, data confidentiality is greatly improved and unwanted access is prevented. This project demonstrates how multi-factor authentication and adaptive cryptography may be combined to create strong cloud security solutions.

I. INTRODUCTION

Cloud computing has become an essential part of modern digital systems, enabling users to store, manage, and access data remotely with ease. However, as the usage of cloud platforms increases, security concerns such as unauthorized access, data breaches, and privacy issues have also grown significantly. Traditional authentication methods like simple passwords are no longer sufficient to ensure data protection. Therefore, there is a strong need for advanced security mechanisms that can safeguard sensitive information stored in cloud environments while maintaining usability and efficiency. To address these challenges, the proposed system "Securing Cloud Systems with Smart Authentication and Adaptive Encryption" introduces a secure framework that enhances data protection in cloud storage. The system integrates smart authentication techniques such as OTP-based verification to ensure that only authorized users can access the system. In addition, adaptive encryption is used to protect data by dynamically applying encryption techniques based on sensitivity levels. This approach ensures that files are securely stored and transmitted, reducing the risk of data leakage and unauthorized access.

A. Objective

The main objective of this project is to develop a secure cloud-based system that ensures the protection of sensitive data using advanced security techniques. The system aims to provide strong user authentication by implementing multi-factor authentication mechanisms such as password verification and OTP validation. Another objective is to enhance data security by applying encryption techniques before storing the data in the cloud, ensuring that unauthorized users cannot access the information. The project also focuses on implementing adaptive encryption, where different levels of encryption are applied based on the sensitivity of the data[1,2,3].

B. Problem Statement

With the rapid growth of cloud computing, a large amount of sensitive data is being stored and accessed over cloud platforms. However, most existing cloud systems rely mainly on single-factor authentication mechanisms such as usernames and passwords, which are highly vulnerable to security threats like phishing attacks, brute-force attacks, and unauthorized access.

Additionally, many systems use static encryption techniques that apply the same level of security to all types of data, without considering the sensitivity of the information. This lack of adaptive protection increases the risk of data breaches, especially when highly confidential data is involved.

C. Scope of the Project

The scope of this project is to develop a secure cloud-based system that enhances data protection through the integration of smart authentication and adaptive encryption techniques. The system is designed to support multiple user roles such as admin, owner, and user, each with specific functionalities and access controls. It allows users to securely register, log in using multi-factor authentication methods including OTP verification, and access cloud services safely. The project also focuses on protecting data before storing it in the cloud by applying encryption mechanisms that vary based on the sensitivity level of the data, thereby improving both security and performance [4,5,6].

II. LITERATURE SURVEY

Tan et al. [12] introduced a more secure biometric authentication approach using ring learning with error cryptography (ring-LWE), a post-quantum cryptosystem designed to protect user data. They proposed a delay-optimized high-accuracy method for efficiently extracting fingerprint features from images. After extraction, the ring-LWE technique was applied, and number theoretic transform (NTT) polynomial multiplications were used to accelerate the process of encoding and decoding. This leads to a significant decrease in the processing time for fingerprint authentication, ensuring the effective protection of fingerprint data. The simulation results demonstrate that the framework has a minimal processing duration and is suitable for real-time authentication systems. However, further research and analysis are required to fully understand the security and limitations of ring-LWE cryptography in fingerprint authentication systems.

Charanjeet et al. [13] developed a three-tier multi-factor authentication solution specifically for cloud computing. This approach integrates two-level password encryption, OTP verification, andgraphical screen interaction. The two-level encryption feature enhances security by combining the SHA-1 and AES algorithms. Multi-factor authentication significantly reduced the risk of data leakage.

Sagar et al. [14] proposed a password authentication framework that enhances security by integrating elliptic curve cryptography (ECC) and attribute-based encryption. In this framework, passwords are converted into hash values using ECC, and then transformed into negative passwords using a specialized algorithm. These negative passwords are further encrypted into Encrypted Negative Passwords (ENPs) using multi-iteration encryption that combines cryptographic hash functions, negative passwords, and symmetric key algorithms. This method strengthens the protection against dictionary attacks without requiring additional elements. Future improvements in negative password generation algorithms could increase complexity and randomness, further enhancing security.

Another study [15] aimed to improve the cloud image security by introducing a biometric authentication technique. The proposed approach has two stages: picture compression with the discrete wavelet transform method, and encryption with a hybrid of SHA and Blowfish. However, this method is vulnerable to spoofing.

In this study [16], the authors introduced a secure authentication approach combining layered encryption with a two-step verification process, specifically designed to prevent cyber intrusion, such as replay and MiTM attacks.

Khan et al. [11] presented a secure system that authenticated patients by using their names, passwords, and biometric data. The SHA-512 algorithm was used to ensure data integrity. Once verified, the patient's mobile sensor device is activated and continuously sends information to the cloud system. To securely transmit sensor information, the system employs a Caesar cipher and enhanced elliptic-curve cryptography (IECC).The combination of improved ECC and SHA-512 enhances data integrity and security, with the upgraded ECC incorporating an additional secret key for increased security. However, the report did not provide a comprehensive comparison with the other encryption algorithms.

III. SYSTEM DESIGN

A. System Architecture

The system architecture represents the overall structure and workflow of the proposed cloud security system. It consists of three main entities: Admin, Owner, and User, each performing specific roles. The frontend is developed using JSP and HTML, providing an interactive interface for users [7]. The backend is implemented using Java Servlets, which handle the application logic and processing.

B. Methodology

The proposed methodology for the project "Securing Cloud Systems With Smart Authentication And Adaptive Encryption" is designed as a layered system that the system starts with user registration and login using secure authentication methods including OTP verification [8,9,10]. After successful login, the owner uploads files which are encrypted before storage in the database. Users can search for files and send access requests to the admin or owner. The admin verifies and approves the requests to ensure secure access control. Once approved, the user downloads the encrypted file, which is decrypted securely for authorized use [17].

C. Modules

1) User Interface: This module provides the front-end interface for user interaction with the system. It allows users to perform operations like registration, login, file upload, and download.

2) Smart Authentication: This module ensures secure user authentication using advanced techniques like OTP and multi-factor authentication.

3) Data Classification: This module categorizes data based on its sensitivity level such as high, medium, or low. Based on classification, appropriate security measures are applied.

4) Adaptive Encryption: This module dynamically adjusts encryption techniques based on data sensitivity and user access level. Highly sensitive data is encrypted with stronger algorithms.

5) Cloud Storage: This module manages secure storage of encrypted files in the cloud environment. It ensures that all uploaded data is safely stored and easily retrievable. . The module supports scalability and high availability of data. It also prevents unauthorized access to stored files [18,19].

6) User Registration and Profile Management: This module allows users to create and manage their accounts within the system. It stores user details securely and provides options to update profile information.

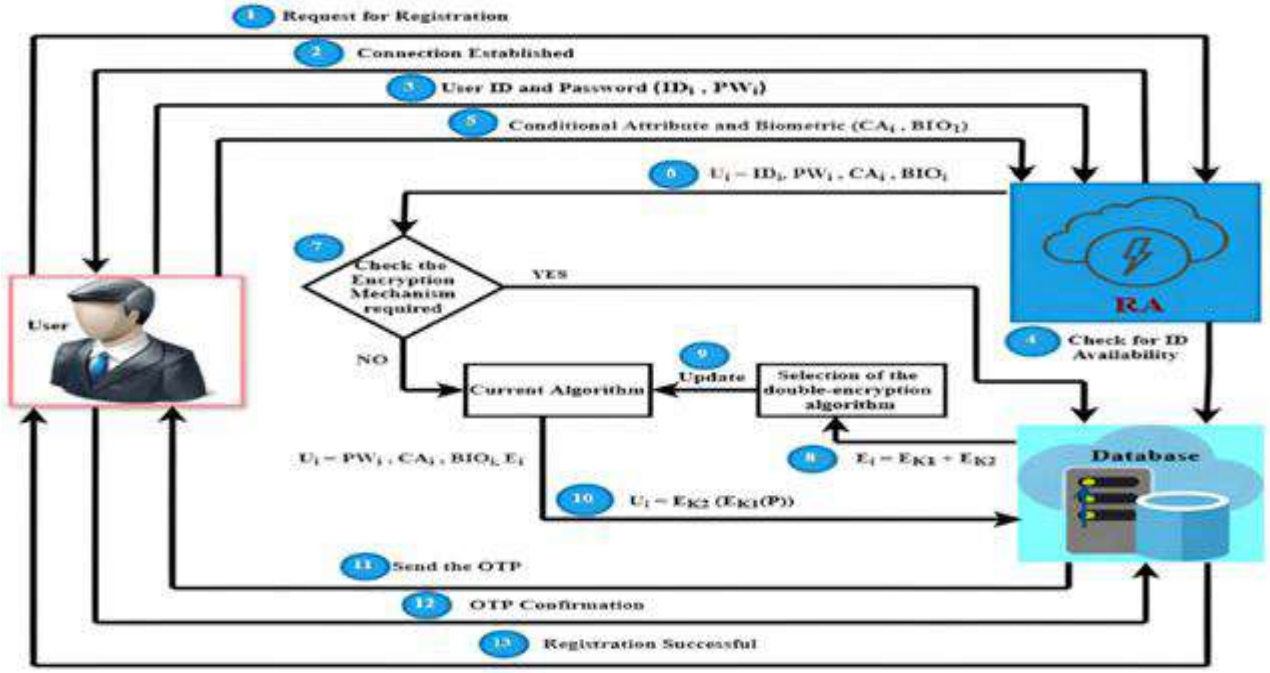

Fig: System Architecture Diagram

IV. EXISTING SYSTEM VS PROPOSED SYSTEM

A. Existing System

Most existing studies has the potential to transform authentication methods by offering more secure and user-friendly options than the traditional approaches. By leveraging behavioral, biometric or contextual data, machine learning can authenticate users and devices more effectively. This involves collecting and analyzing data that reflects the unique characteristics or behaviors of a user or device. Such data may include biometric traits such as facial recognition, fingerprints, voice, or iris scans as well as behavioral patterns such as typing style, mouse movements, or device usage.

B. Proposed System

We propose an innovative framework that enhances security through a multi-factor authentication system using passwords, conditional attributes, and identities, supported by hybrid cryptography techniques that provide multiple layers of protection for user credentials. The security algorithm adapts dynamically based on user numbers and limitations, allowing users to switch authentication methods, as needed. We evaluated the reliability, efficiency, and security of the proposed authentication technique against threats such as man-in-the-middle attacks, eavesdropping, credential stuffing, account hijacking, and impersonation.

V. IMPLEMENTATION

A. System Design and Development Implementation

The system is developed using Java technologies to create a secure and scalable web application. Eclipse IDE is used for coding and debugging, while Apache Tomcat server is used for deployment and execution. The frontend is designed using JSP, HTML, CSS, and JavaScript to provide an interactive and user-friendly interface. The backend is implemented using Java Servlets to handle business logic and data processing efficiently. MySQL database is used to store user details, file information, and access records, with JDBC connectivity enabling communication between the application and database. Proper validation, navigation, and exception handling mechanisms are implemented to ensure smooth functioning of the system.

B.Security, Encryption, and Access Control Implementation

The system ensures security through strong authentication and encryption mechanisms. User authentication is implemented using username, password, and OTP verification, along with role-based access control for Admin, Owner, and User modules. Files are encrypted using AES and RSA algorithms before storing in the cloud to maintain confidentiality. SHA-256 hashing is used to ensure data integrity and detect tampering. A request-based access control mechanism is implemented where users must request permission to access files, and the owner approves or rejects the requests. Only authorized users can download and decrypt files using secure key management techniques, ensuring controlled and protected access to cloud data.

IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN:2349-2163
Volume 13, Issue 04, April https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2026.v1304.02

VI. RESULTS AND DISCUSSION

This section features screenshots that provide visual documentation of the system development, functionality and user interface evidence. The snapshots provide a clear representation of how the application works in real-time, and illustrates main functionality during release.

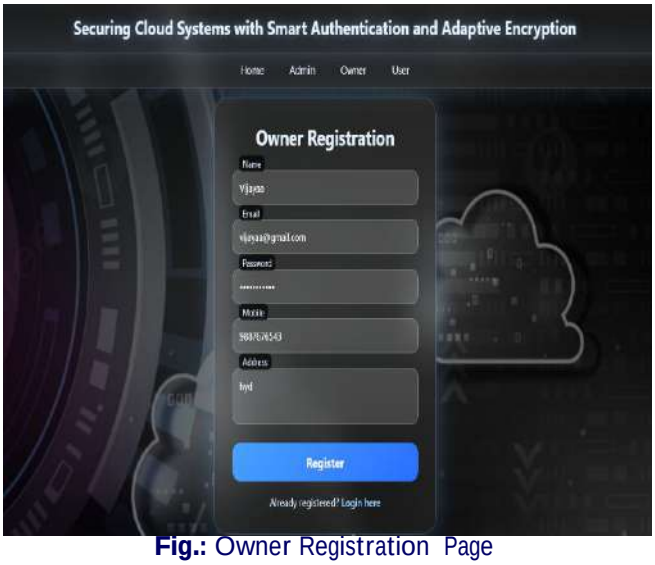

Fig.: Owner Registration Page

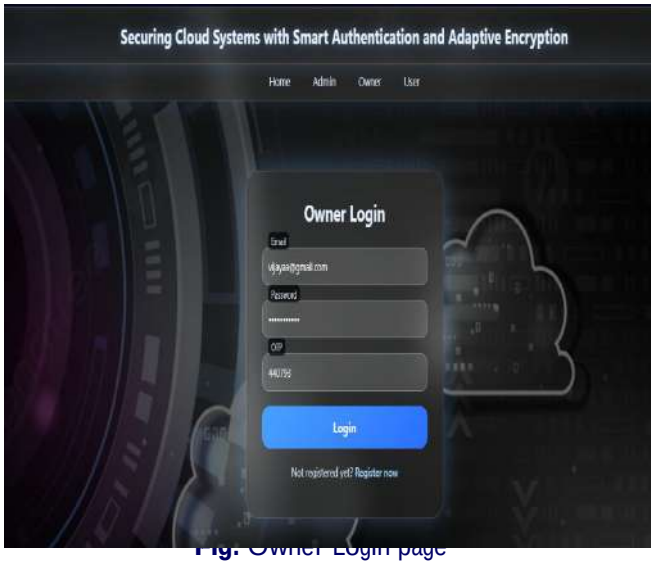

Fig. Owner Login page

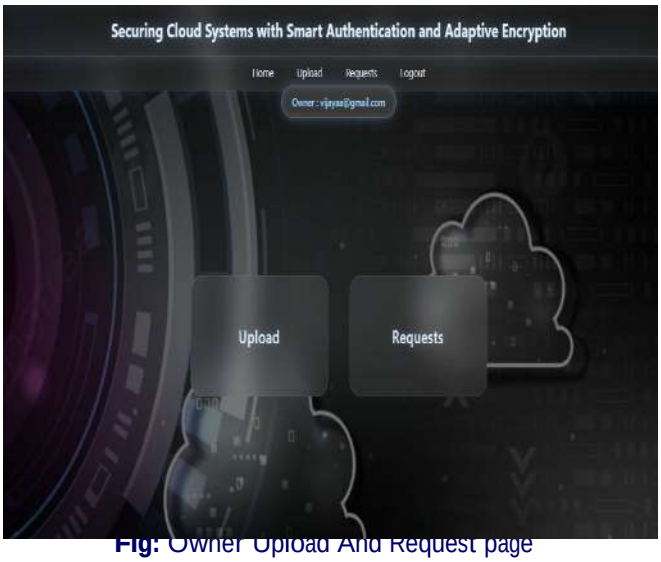

Fig. Owner Upload And Request page

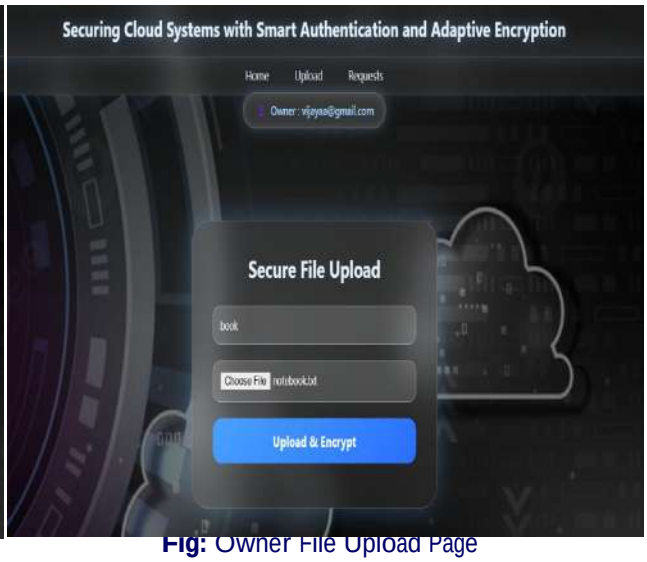

Fig. Owner File Upload Page

IJIRAE:: International Journal of Innovative Research in Advanced Engineering ISSN:2349-2163
Volume 13, Issue 04, April https://www.ijirae.com/archives
https://doi.org/10.26562/ijirae.2026.v1304.02

Fig: Owner Upload and Request page

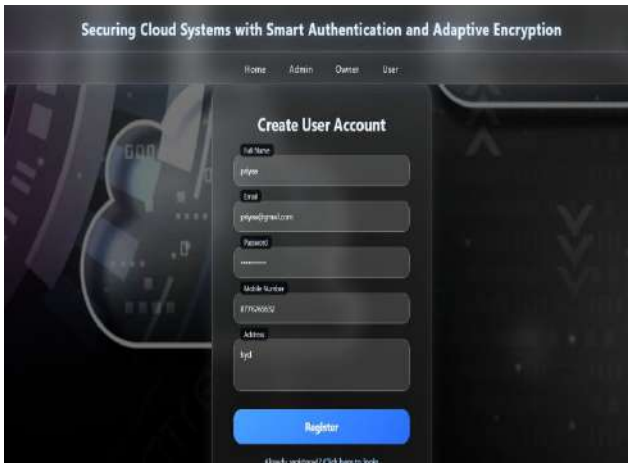

Fig: User Registration Page

Fig: Admin Page

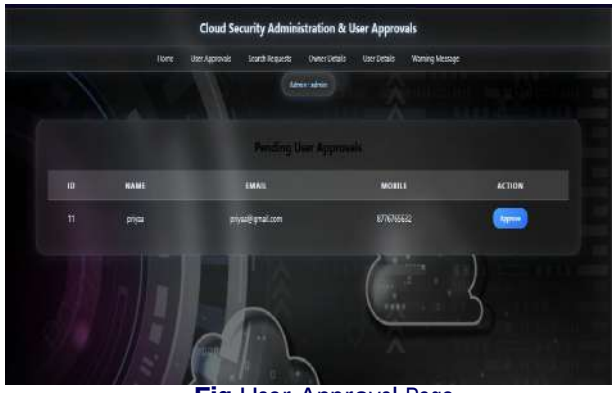

Fig User Approval Page

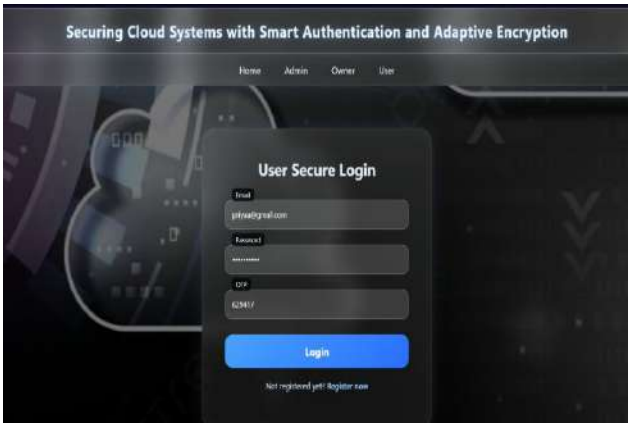

Fig User Login Page

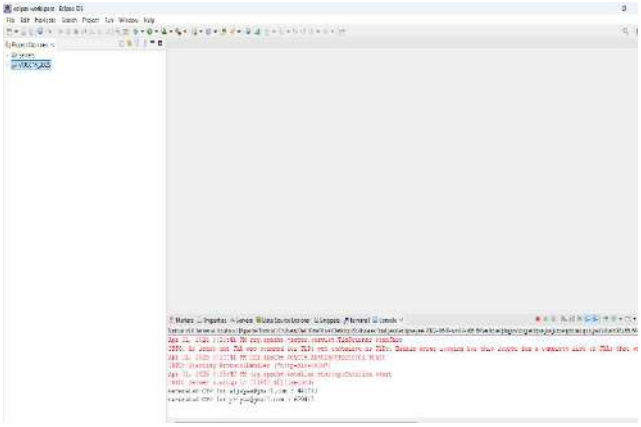

Fig Owner And User OTP Verification Page

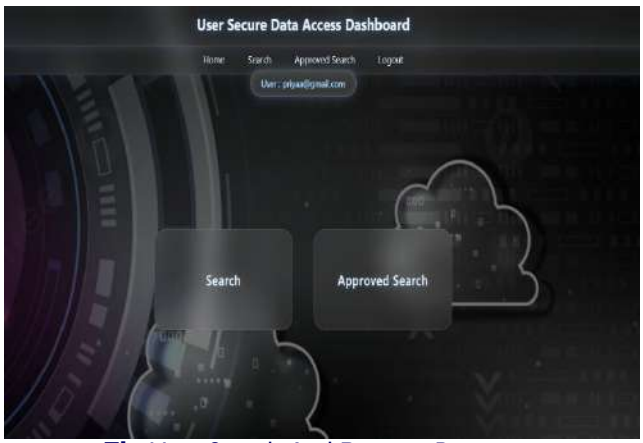

Fig User Search And Request Page

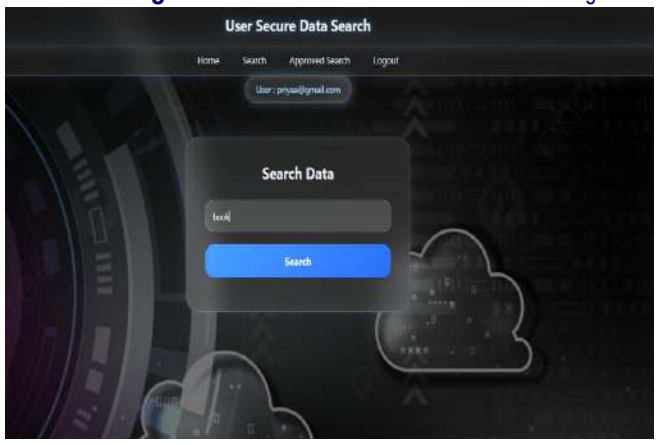

Fig User Search Data Page

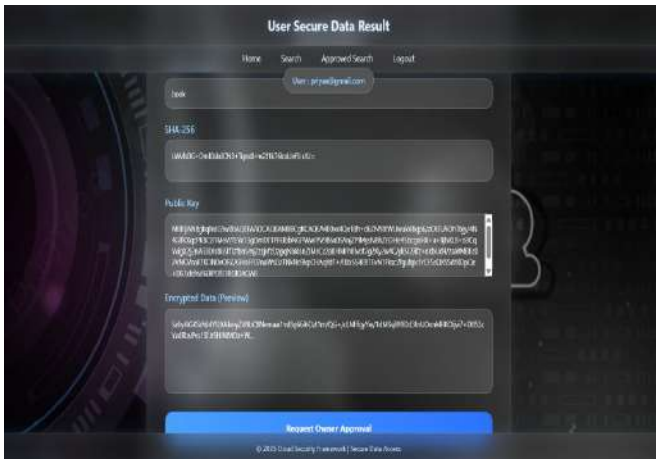

Fig User Search Data Result Page

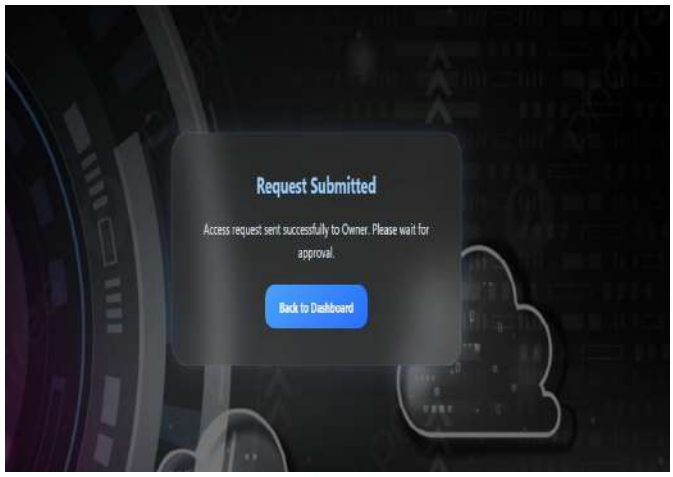

Fig Request Submission Page

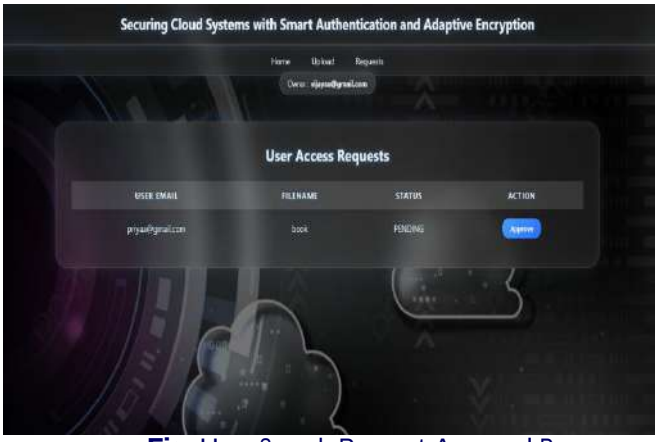

Fig User Search Request Approval Page

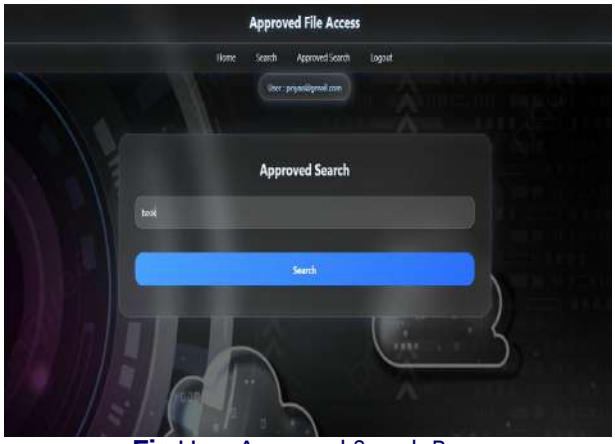

Fig User Approved Search Page

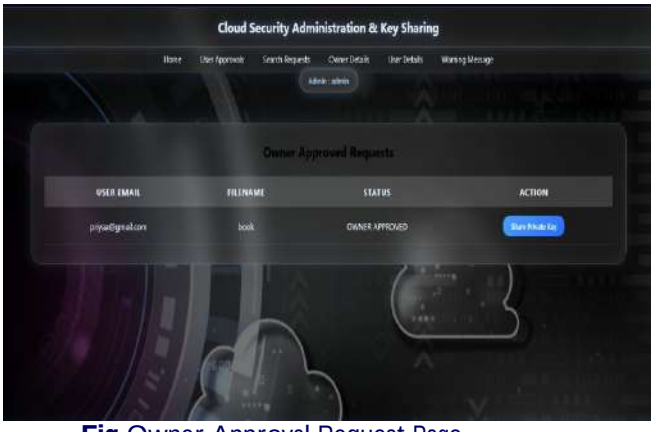

Fig Owner Approval Request Page

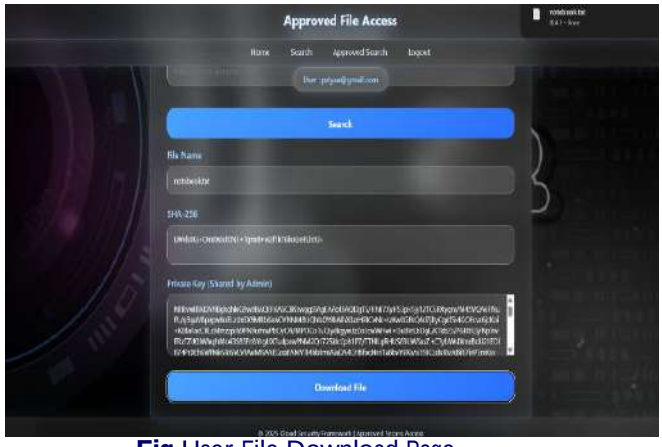

Fig User File Download Page

The proposed system was successfully implemented and tested to ensure secure cloud data management using smart authentication and adaptive encryption techniques. The results show that the system effectively provides role-based access control for admin, owner, and user. All modules such as registration, login with OTP verification, file upload, request handling, and file download were executed successfully. The encryption mechanism ensured that the data remained secure during storage and transmission. The system also demonstrated smooth performance with quick response time and user-friendly navigation across all pages. From the discussion, it is observed that the integration of multi-factor authentication and encryption significantly improves the security level compared to traditional cloud systems. The admin plays a crucial role in managing and approving user requests, which helps in maintaining controlled access. The system reduces the risk of unauthorized access and data breaches. Overall, the proposed model proves to be reliable, efficient, and secure for cloud-based data storage and access. Future improvements can further enhance performance and scalability of the system.

VII. CONCLUSION

The project "Securing Cloud Systems with Smart Authentication and Adaptive Encryption" successfully demonstrates how cloud data can be safeguarded through advanced authentication techniques and dynamic encryption mechanisms. In today's digital world, where sensitive information is frequently stored and accessed over cloud platforms, ensuring privacy and preventing unauthorized access have become critical challenges. This project addresses these concerns by implementing a multi-layered security model that combines user authentication, biometric verification, conditional access, and adaptive encryption. The use of smart authentication ensures that only legitimate users can access their data, while adaptive encryption dynamically strengthens data protection based on its sensitivity. Additionally, the integration of OTP verification and secure key management minimizes the risk of hacking and data leakage.

ACKNOWLEDGMENT

The authors express sincere gratitude to Mr.G.Kasi Reddy, Assistant Professor, CSE Department, for his valuable guidance and continuous support. They also thank Dr.B.Santhosh Kumar, Head of the Department, for expert supervision, and the faculty members and lab technicians of the CSE Department, Guru Nanak Institute of Technology, Hyderabad, for their assistance and cooperation throughout this project.

REFERENCES

1. G.Ramesh,J.Logeshwaran,V.Aravindarajan,"A secured database monitoring method to improve data backup and recovery operations in cloud computing," BOHR Int.J.Comput.Sci.,vol.2,no.1 https://doi.org/10.54646/bijcs.019
2. B.T.Rao,"A study on data storage security issues in cloud computing," ProcediaComput. Sci., vol. 92, pp. 128–135, 2016, https://doi.org/10.1016/j.procs.2016.07.335.
3. K.Latha and T.Sheela, "Block based data security and data distribution on multi cloud environment," J. Ambient Intell. Humanized Comput., vol. 15, 2024, Art. no. 53, https://doi.org/10.1007/s12652-019-01395-y
4. K.Raju,M.Chinnadurai,"An identity-based secure and optimal authentication scheme for the cloud computing environment," Comput., Mater. Continua, vol. 69, no. 1, pp. 1057–1072, 2021, https://doi.org/10.32604/cmc.2021.016068
5. A.Ometov, S.Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: A survey," Cryptogr., vol. 2, no. 1, pp. 1–31, 2018, https://doi.org/10.3390/cryptography2010001
6. S.Sudha and S.S.Manikandasaran, "A survey on different authentication schemes in cloud computing environment," Int. J. Manage., IT Eng., vol. 9, no. 1, pp. 359–375, 2019.
7. A.Alhothaily, C.Hu, A.Alrawais, T.Song, X.Cheng, and D.Chen, "A secure and practical authentication scheme using personal devices," IEEE Access, vol. 5, pp. 11677–11687, 2017, https://doi.org/10.1109/ACCESS.2017.2717862.
8. N.Anusha and N.R.Suma, "A review on secured file system using multi-factor authentication with visual cryptography for cloud environment," Int. Res. J. Modernization Eng. Technol. Sci., vol. 4, no. 6, pp. 4433–4436, 2012.
9. Cybersecurity, "What is password encryption and how does it work," Accessed: Jun. 15, 2023. [Online]. Available: https://teampassword.com/blog/what-is-password-encryption-and-how-much-is-enough.
10. M.Hazratifard, F.Gebali, and M.Mamun, "Using machine learning for dynamic authentication in telehealth: A tutorial," Sensors, vol. 22, no. 19, 2022, Art. no. 7655, https://doi.org/10.3390/s22197655.
11. N.Siddiqui, L.Pryor, and R.Dave, "User authentication schemes using machine learning methods—A review," in Proc. Int. Conf. Commun. Comput. Technol., Singapore, 2021, pp. 703–723, https://doi.org/10.1007/978-981-16-3246-4_54
12. T.N.Tan and H.Lee, "High-secure fingerprint authentication system using ring-LWE cryptography," IEEE Access, vol. 7, pp. 23379–23387, 2019, https://doi.org/10.1109/ACCESS.2019.2899359.
13. C.Singh and D.Singh, "A 3-level multifactor authentication scheme for cloud computing," Int. J. Comput. Eng. Technol., vol. 10, no. 1, pp. 184–195, 2019. [Online]. https://www.ssrn.com/abstract=3537621
14. S.A.Sagar, O.Bhat, M. Raina, and S. Patil, "Authentication system using cryptographic secure password storage," Int. J. Innov. Res. Eng. Multidisciplinary Phys. Sci., vol. 6, no. 6, pp. 76–78, 2018.
15. V.Kakkad,M.Patel,M. Shah, "Biometric authentication and image encryption for image security in cloud framework," Multiscale Multidisciplinary Model.Exp. Des, vol. 2, no. 4,pp. 233–248, 2019, https://doi.org/10.1007/s41939-019-00049-y.
16. Rao,Ch.C.,Hiwarkar,T.Kumar,B.S.(2023).Cloud-based data security transactions employing blowfish and spotted hyena optimisationalgorithm. JournalofControlandDecision, 10(4), 494–503. https://doi.org/10.1080/23307706.2022.2105267.
17. Kumar,B.S., Karthik, S. & Arunachalam, V.P. Upkeeping secrecy in information extraction using 'k' division graph based postulates. Cluster Comput 22 (Suppl 1), 57–63 (2019). https://doi.org/10.1007/s10586-018-1705-2.
18. Prabu, M. K., Kumar, B. S., & Karthik, S. (2015). Optimized scheduling for data anonymization in cloud using top down specialization. Int J Appl Eng Res (IJAER), 10(41), 30546-30549.
19. Rao, C.,Hiwarkar, T., & Kumar, B. S. (2021). Enhanced effective and privacy preserving multi keyword search over encrypted data in cloud storage using blowfish algorithm. Turkish Journal of Computer and Mathematics Education, 12(2), 2845-2853.
20. Joshi, Y., Totad, S. G., Geeta, R. B., & Prasad Reddy, P. V. G. D. (2018). Mobile agent-based frequent pattern mining for distributed databases. In S. Bhalla, V. Bhateja, A. Chandavale, A. Hiwale, & S. Satapathy (Eds.), Intelligent computing and information and communication (Vol. 673). Springer. https://doi.org/10.1007/978-981-10-7245-1_9