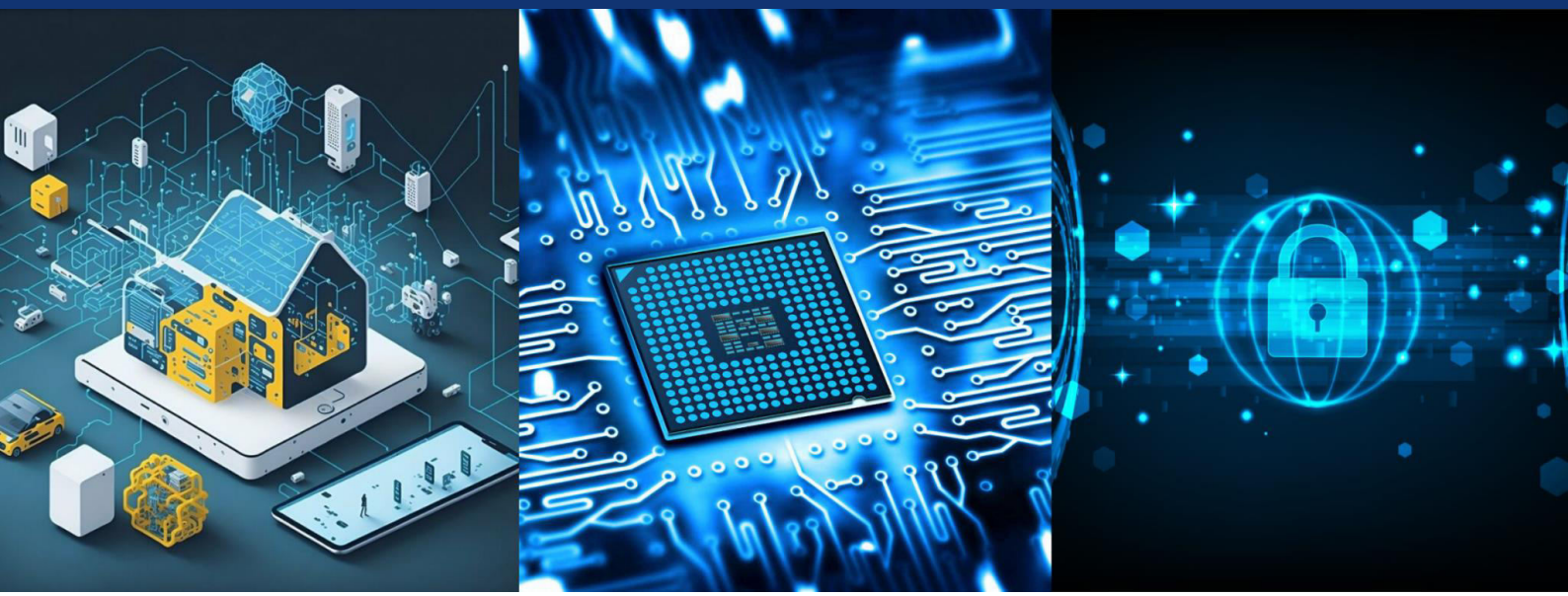
IJIRCCE

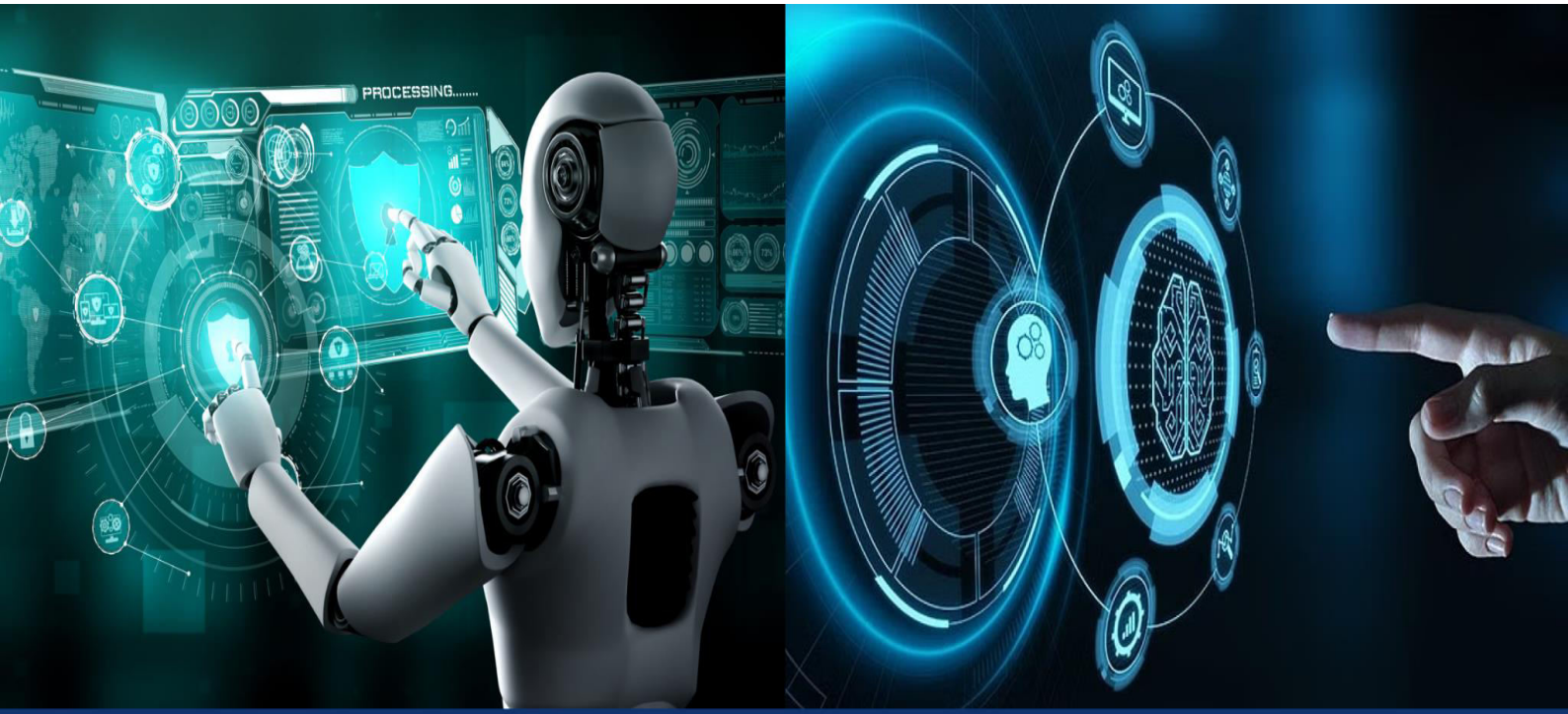
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.771

Volume 14, Issue 4, April 2026

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404147

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Secure Cloud File Storage with Hybrid Cryptography and Advanced Access Control

Chinthala Sweety[1], Lavudya Sushmitha[2], Dr.Meera Alphy[3], Mrs.N.Musrat Sultana[4], Dr.V. Subbaramaiah[5], Dr.K. Rajitha[6]

Student, Department of Computer Science and Engineering, Mahatma Gandhi Institute of Technology, Telangana, India [1,2]

Assistant Professor, Department of Computer Science and Engineering, Mahatma Gandhi Institute of Technology, Telangana, India[3,4,5,6]

ABSTRACT: Cloud storage has become a critical infrastructure for modern data management, enabling scalable and ubiquitous access to digital resources. However, the increasing sophistication of cyberattacks and the emergence of quantum computing pose severe challenges to existing cloud security frameworks. Traditional hybrid cryptography models, primarily using AES for data encryption and RSA for key exchange, face limitations in computational efficiency and quantum resilience. It presents a Secure Cloud File Storage System that integrates Elliptic Curve Cryptography (ECC) to enhance key management efficiency and strengthen security. The proposed hybrid model combines AES and ECC, achieving robust encryption with reduced computational overhead and improved scalability. To further reinforce data protection, the system implements two-factor authentication (2FA) and role-based access control (RBAC) for fine-grained authorization. Blockchain-based immutable audit trails are incorporated to ensure transparency and accountability in data access operations. Additionally, client-side encryption safeguards user data against unauthorized access, even from untrusted cloud providers. The system supports expiring secure share links, enabling controlled and time-bound data sharing. The framework maintains lightweight performance suitable for both enterprise and personal cloud environments.

KEYWORDS: Key Management and Access Control Server,Elliptic Curve Cryptography,Advanced Encryption Standard , Two-Factor Authentication,Role-Based Access.

I. INTRODUCTION

Cloud computing has transformed data storage by providing scalability, cost-efficiency, and accessibility. However, it also brings significant challenges concerning data confidentiality, integrity, and access control. As organizations increasingly depend on cloud services for storing sensitive data, the need for secure storage mechanisms has become critical. Traditional cloud storage models rely on single providers and basic encryption, exposing systems to breaches, insider threats, and unauthorized data access. To overcome these vulnerabilities, hybrid cryptography and distributed storage techniques are emerging as effective solutions. It aims to design a secure file storage framework that ensures confidentiality, authenticity, and controlled access. The proposed system employs a combination of symmetric (AES) and asymmetric (Elliptic Curve Cryptography – ECC) cryptography for efficient and secure data protection. Additionally, advanced access mechanisms such as Two-Factor Authentication (2FA), blockchain-based audit trails, and role-based permissions are integrated to strengthen data accountability and transparency. By combining encryption efficiency with modern authentication and auditing, the proposed model aims to create a robust, scalable, and tamper-resistant cloud storage framework suitable for real-world applications.

II. LITERATURE SURVEY

Nitesh Bharot et al.[1] presents an architecture utilizing Multi-cloud slicing and a Hybrid Cryptosystem. It highlights the advantage of avoiding a single-point failure through data distribution across multiple cloud providers.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Shivarama Krishna et al.[2] This explores a framework leveraging AES, OTP, RSA, and Key Management techniques. It demonstrates how to achieve strong confidentiality and adaptive key management with time-limited access.

yaser M.A. Abualkas et al.[3]This paper introduces a hybrid approach combining ECC (Elliptic Curve Cryptography), AES, and Blockchain integration. It highlights the benefits of a lightweight solution that provides tamper-proof logs via the blockchain.

Jiangyi Yi et al.[4] This research utilizes Blockchain, OPRF (Oblivious Pseudorandom Function), and Digital Twin technology for enhanced key management. It highlights the strength of combining Blockchain + OPRF to effectively resist brute force attacks and improve the key lifecycle.

Firas M. Khalaf et al.[5] This paper explores a hybrid model utilizing AES and RSA with Blockchain integration. It demonstrates how the system provides guaranteed auditability and tamper-proof access records.

III. PROBLEM DEFINITION

storage and controlled data sharing remain major challenges. Traditional cloud systems rely on basic encryption and password-based authentication, which are vulnerable to brute-force attacks, credential theft, and unauthorized access. Many systems also lack fine-grained access control and proper logging, making it difficult to track file usage or detect malicious activity.

Centralized cloud storage creates a single point of failure, where server compromise or downtime can make data inaccessible. Existing hybrid cryptography methods such as AES and RSA provide moderate security but are computationally expensive and may not be suitable for future security threats. Additionally, the absence of tamper-proof audit logs and automatic access expiration mechanisms increases the risk of data leakage and misuse.

IV. PROPOSED SYSTEM

The proposed system introduces a Secure Cloud File Storage Framework that enhances security, efficiency, and transparency by integrating hybrid cryptography with advanced access control mechanisms. It uses Elliptic Curve Cryptography (ECC) for secure key exchange and management, replacing RSA to achieve higher strength with shorter key sizes and better resistance to quantum threats. ECC also accelerates encryption and decryption processes, making the system lightweight and suitable for large-scale cloud environments. On the client side, files are encrypted using AES before uploading, ensuring that even the cloud provider cannot view the contents. The system employs Two-FactorAuthentication(2FA),combining password verification with OTP or biometric validation to prevent unauthorized access. Every file operation—upload, download, update, or deletion is recorded on a blockchain-based immutable audit trail, ensuring transparency.

V. DESIGN AND METHODOLOGY

5.1 System architecture

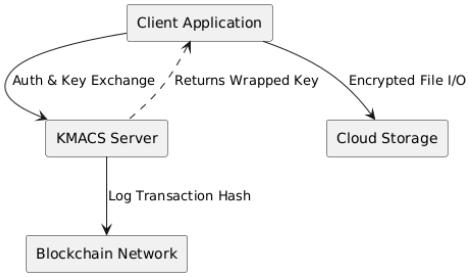
The system architecture shows secure cloud storage using client-side AES encryption, KMACS for key management and access control, cloud storage for encrypted files, and blockchain for immutable audit logging.The client securely uploads and retrieves encrypted files, while KMACS handles authentication, key wrapping/unwrapping, and records transaction hashes on the blockchain for auditability.

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404147

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



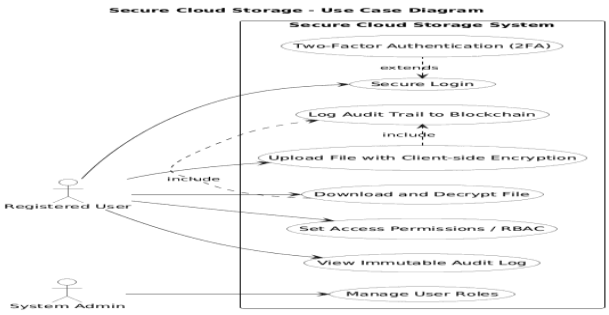
5.1 system architecture

5.2 working methodology

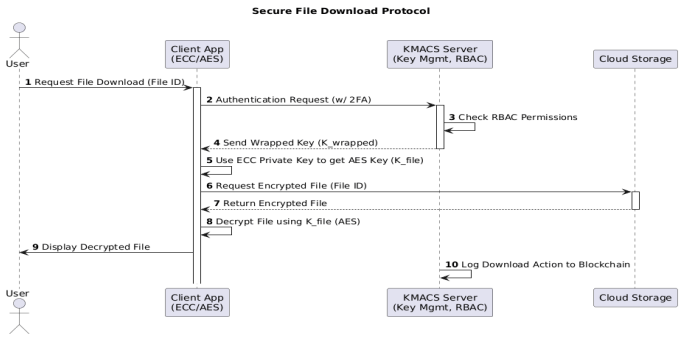
The system authenticates users and allows them to upload files through a dashboard. Each file is encrypted using AES, while the AES key is secured using ECC. The encrypted file is stored in cloud or local storage, and its metadata and hash are saved in the database. All actions are recorded in a blockchain for auditability. During download, the system verifies access, decrypts the file, and provides it to the user, ensuring security and controlled access.

5.3 UML Diagrams

The system is described using UML diagrams to show its design and workflow. The Use Case Diagram shows user interactions like login, upload, and download. The Class Diagram represents system structure with entities like user, file, encryption, and blockchain. The Sequence and Activity Diagrams explain the step-by-step process of file handling. The Component Diagram shows how modules interact, and the Deployment Diagram represents the system setup with client, server, database, cloud, and blockchain.



5.2 use case diagram



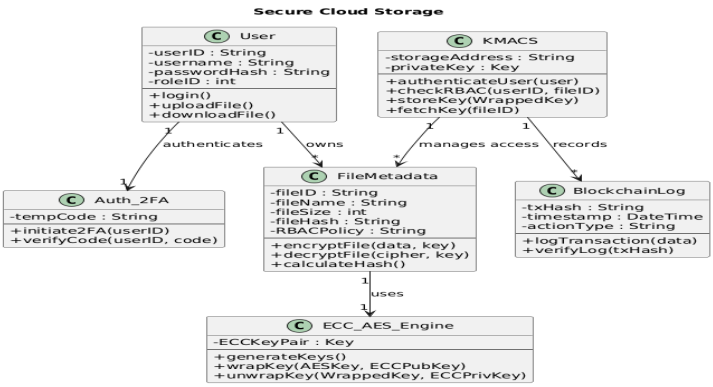
5.3 sequence diagram

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404147

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



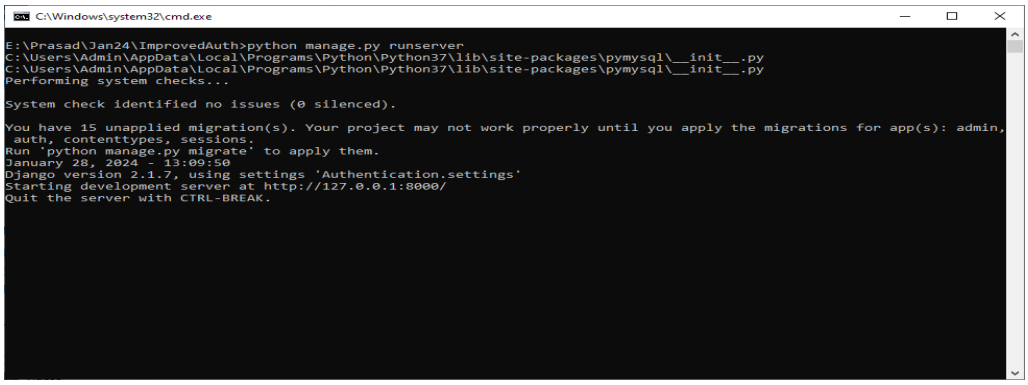
5.4 class diagram

VI. RESULTS AND DISCUSSION

The Secure Cloud File Storage system was successfully implemented with features like user authentication, encrypted file upload, and controlled file access. Hybrid cryptography (AES and ECC) ensures data security, while file hashes maintain integrity. The system also records file activities using blockchain for transparency. The results show that the system provides secure and reliable file storage with proper access control.

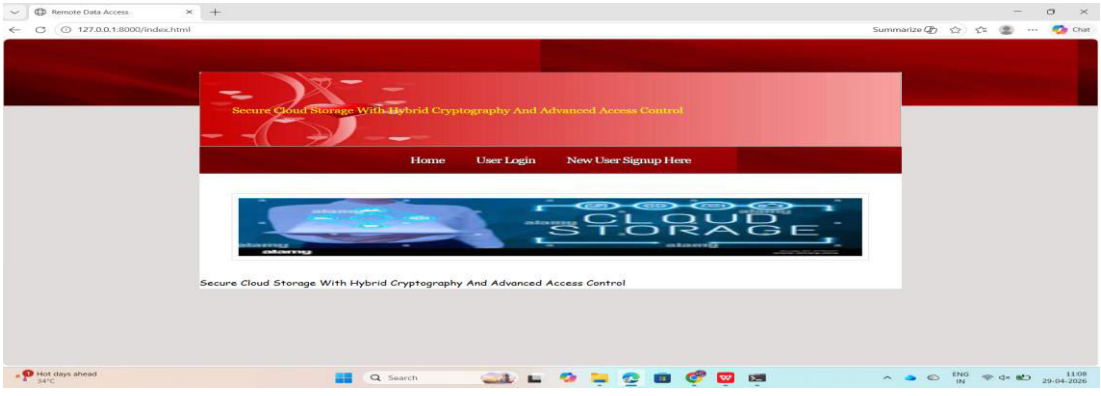
6.1 server

To run project double click on 'run.bat' file from to start python Cloud server and get below page



6.2 home page

Displays the login interface for user authentication.Users enter credentials to access the system securely



© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404147

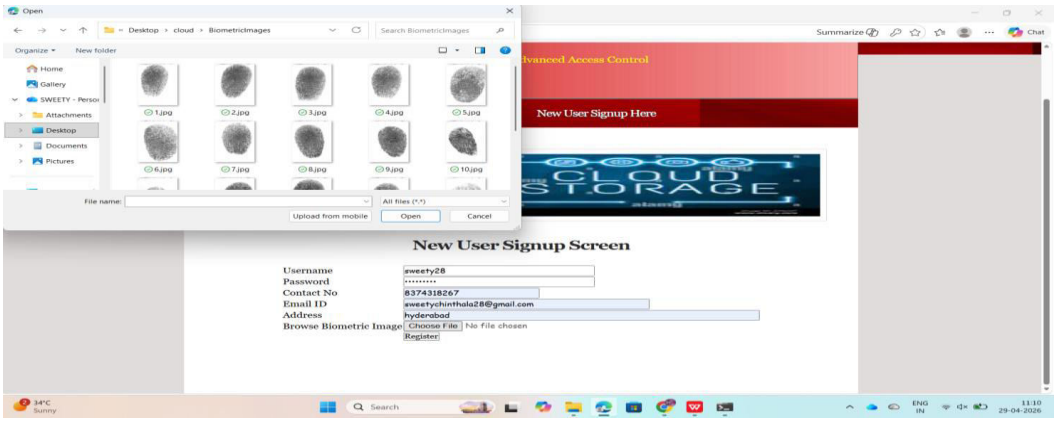
www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

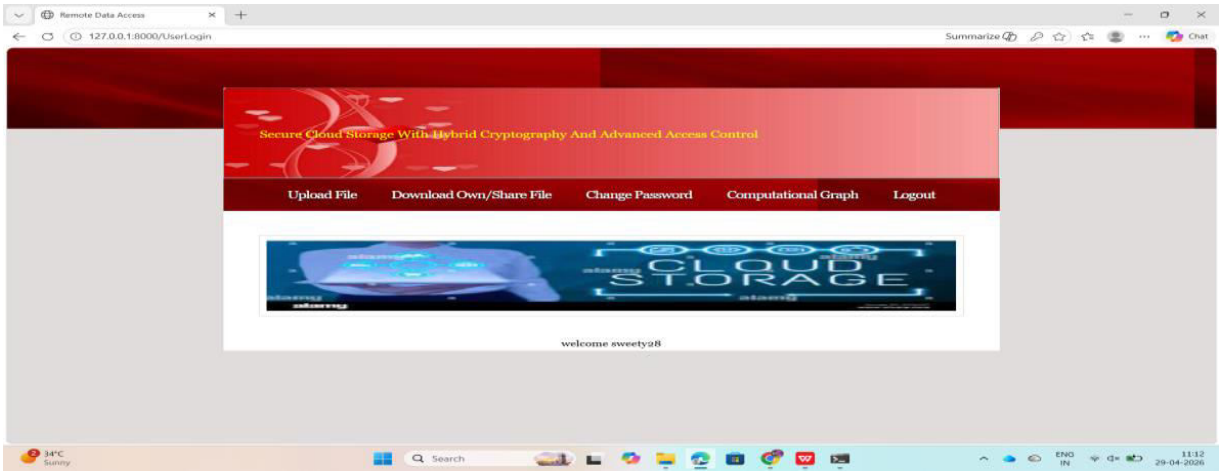
6.3 Registration page

Allows new users to create an account. User details are stored securely in the database.



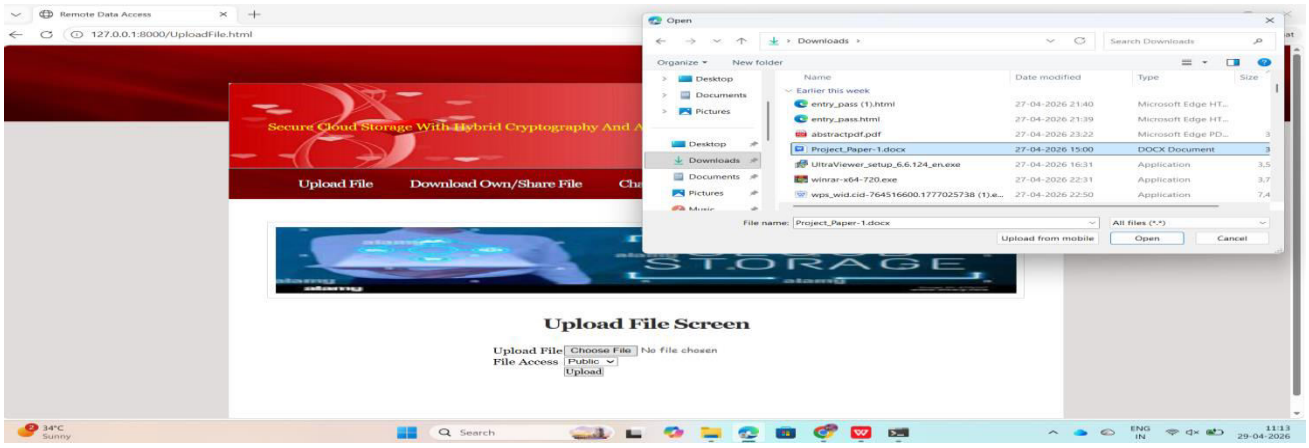
6.4 Login Success / Dashboard

shown after successful login. Provides access to file upload and file management features.



6.5 Upload File Screen

User selects a file and uploads it to the system. The file is encrypted using AES and ECC before storage.



© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404147

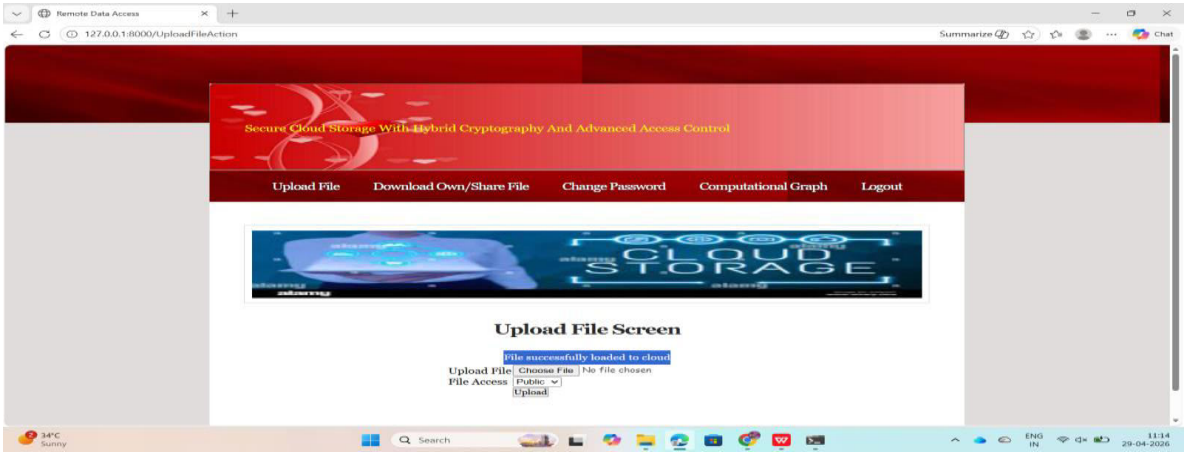
www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

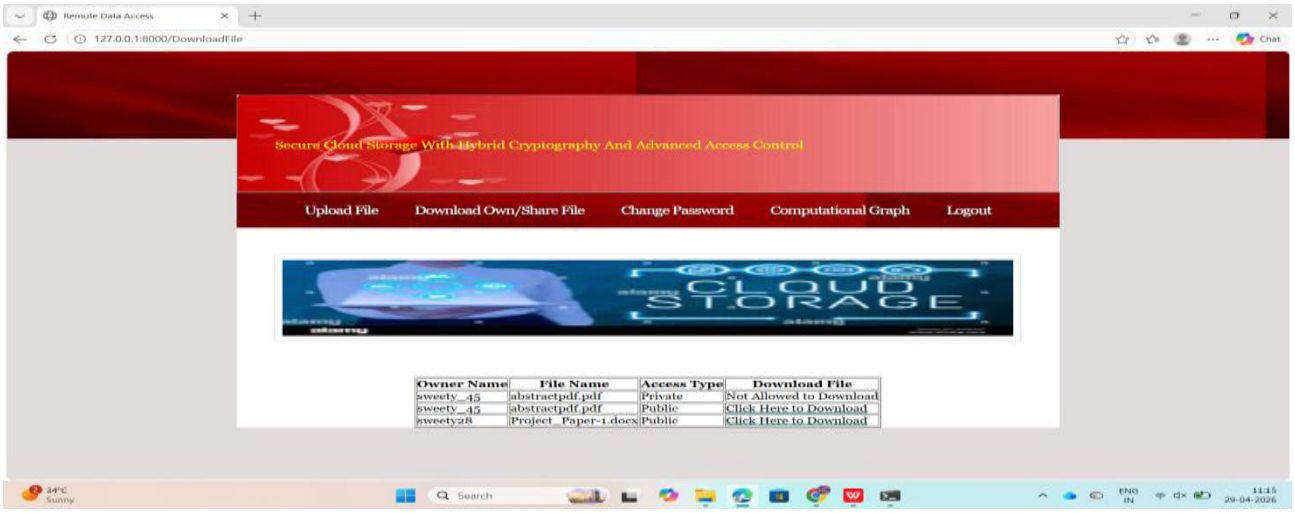
6.6 File Stored (Encrypted)

Confirms that the file is saved in encrypted form. Ensures confidentiality of data in storage.



6.7 Uploaded Files Table

Displays list of uploaded files with ID, name, and hash. Allows users to view and manage their files.



6.8 Download File Screen

User selects and downloads a file. File is decrypted and provided in original format.

© 2026 IJIRCCE | Volume 14, Issue 4, April 2026 DOI: 10.15680/IJIRCCE.2026.1404147

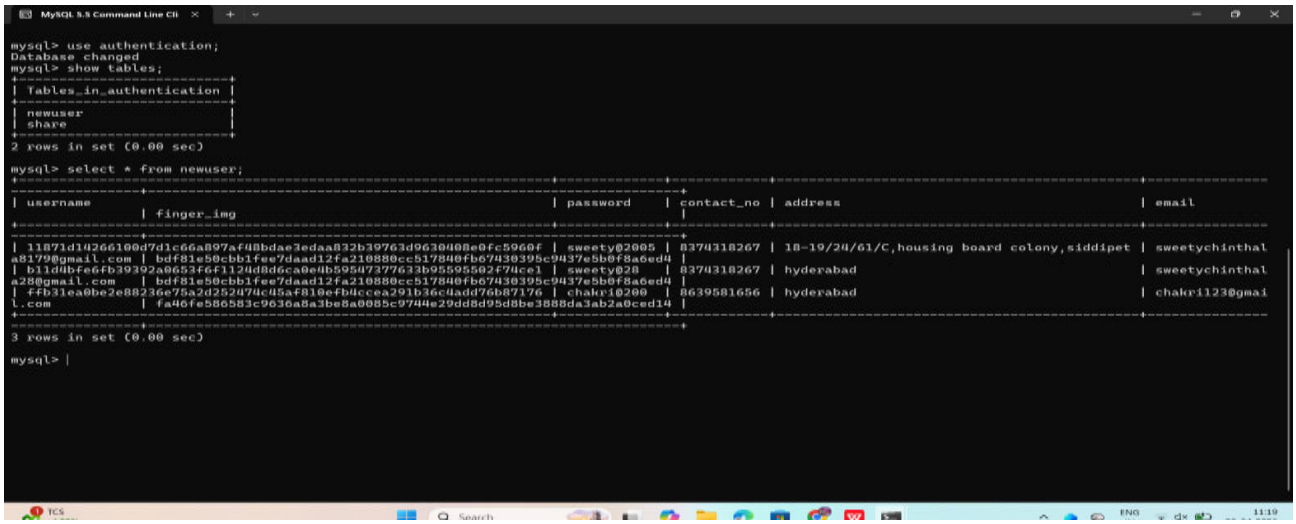
www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 8.771| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

6.9 Database View

Shows stored file details and metadata. Used to verify integrity and stored records.



VIII. CONCLUSION

The Secure Cloud File Storage system was successfully developed to provide safe and controlled data storage using hybrid cryptography. The integration of AES and ECC ensures strong data confidentiality, while hashing and blockchain logging maintain integrity and transparency. The system allows users to securely upload, store, and access files with proper authentication. Overall, the project demonstrates an effective approach for secure and reliable cloud-based file management

REFERENCES

[1]. Nitesh Bharot et al., "CloudLock: Secure Data Sharing Using a Hybrid Cryptosystem in Multi-Cloud Data Storage", 2025.
[2]. D. Shivarama Krishna et al., "A Novel Hybrid Cryptographic Framework for Secure Data Storage in Cloud Computing (AES-OTP + RSA)", 2023.
[3]. Yaser M. A. Abualkas et al., "Hybrid Approach to Cloud Storage Security Using ECC AES Encryption and Key Management Techniques", 2024.
[4]. Jiangyi Yi et al., "The Key Security Management Scheme of Cloud Storage Based on Blockchain and Digital Twins", 2024.
[5]. Firas M. Khalaf et al., "A Hybrid Encryption Model with Blockchain Integration for Secure Cloud Data Storage and Retrieval", 2025.
[6]. Jian-Foo Lai et al., "Secure File Storage on Cloud Using Hybrid Cryptography", 2022.
[7]. Biao Jin et al., "BCAS: Blockchain-Based Secure Access and Sharing Scheme for EHR Data", 2024.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details