IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15586

Intelligent Fingerprint Storage and Management System for Authentication Applications on Cloud Storage

Vaasthava Sree Sai Reddy N [1] ,Subhamay Parya[2], Spoorti Patil[3], vaishnavi Reddy[4], Dr.SoniaMariaD'souza[5]

Student, Artificial Intelligence and Machine Learning, New Horizon College Of Engineering, Bengaluru,India[1]

vaasthavanhce@gmail.com

Student, Artificial Intelligence and Machine Learning, New Horizon College Of Engineering, Bengaluru, India[2]

subhamayparya15@gmail.com

Student, Artificial Intelligence and Machine Learning, New Horizon College Of Engineering, Bengaluru, India[3]

spoortipatil6361@gmail.com

Student, Artificial Intelligence and Machine Learning, New Horizon College Of Engineering, Bengaluru, India[4]

vaishnavireddy5853@gmail.com

Associate Professor, Department of Artificial Intelligence and Machine Learning, New Horizon College of Engineering, Bengaluru, India[5]

s1985md@gmail.com

Abstract: Data security has become highly necessary in our digital era. This paper proposes a Fingerprint Storage System (FSS) on cloud storage that provides users a secure way to access their files through fingerprint authentication and not password-based authentication**.** The OFR is used to recognize and authenticate users. Files stored are also encrypted via AES-256 algorithm in order to prevent any unauthorized access and data breach. This paper eliminates the threat of password thefts, phishing, and unauthorized access since passwords would no longer be necessary. The proposed solution is intended to operate in practical applications such as banking, health care, educational institutes, and enterprises.

Keywords: Cloud Technology, Fingerprint accessibility, AES-256 encryption, Biometric Security,Secure Cloud Storage

I. INTRODUCTION

Cloud computing has a great impact on many fields such as education, healthcare, banking and data management systems in recent years. The use of cloud technology has led to more efficient, accessible, and secure data storage and retrieval processes. One important application area is fingerprint based storage and authentication systems which provide secure and reliable access to digital information.

Most of the traditional storage methods are based on physical storage devices like pen drives and hard disks or they depend on password based authentication systems. These methods are susceptible to data loss, theft, unauthorized access and hardware failure. Furthermore, manual storage and retrieval processes can be time-consuming and less efficient.

The aim of this research is to overcome these limitations by proposing a cloud based fingerprint storage system, using an Optical Fingerprint Reader (OFR) for fingerprint analysis and authentication. The system captures fingerprint data from a biometric sensor, processes the fingerprint using biometric feature extraction and matching techniques algorithms and stores the encrypted files in cloud storage. Authorized users can retrieve their stored data by using fingerprint verification instead of passwords.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.15586

The proposed system is aimed at enhancing the storage security, minimizing the dependence on physical storage devices, increasing the accuracy of authentication and faster access to data stored in the cloud. The dependability, uniformity and effectiveness of the storage process are improved using biometric authentication along with cloud computing and machine learning technologies.

The main goal of this research is to design a robust, efficient and intelligent cloud storage system that employs fingerprint authentication for the protection of confidential data and enhancement of overall storage management performance.

II. LITERATURE REVIEW

Cloud computing is one of the most common technologies for data storage and management due to its scalability, flexibility and cost efficiency. However, the growth of cloud storage usage has posed a significant challenge in ensuring the security of data and user authentication. Traditional password-based authentication systems are vulnerable to hacking, phishing, and unauthorized access. So, the need for more secure authentication mechanisms is clear.

Biometric authentication systems have gained much attention. Fingerprints are unique to each individual and difficult to replicate. A. K. Jain et al. discussed biometric recognition system and showed the reliability and accuracy of fingerprint based authentication for security applications. Fingerprint authentication is widely used in banking systems, mobile devices, healthcare applications and secure access control systems.

Some researchers have proposed secure cloud storage systems integrated with biometric authentication techniques. Meenakshi and Arthi built a secure cloud-based storage system that uses biometric authentication to improve user security and reduce reliance on passwords. Their work revealed that biometric authentication provides a higher level of security against unauthorized access compared to traditional authentication methods.

Cloud security is still a key research area as sensitive user data stored in cloud environments are subject to cyber attacks and data breaches. Subashini and Kavitha conducted a survey on security issues in cloud computing service models and highlighted the importance of encryption techniques to secure cloud data. Encryption algorithms such as AES (Advanced Encryption Standard) are commonly used to protect the confidentiality and integrity of stored files.

Recent advances in machine learning and neural networks have aided in improving fingerprint recognition systems. Neural network techniques help in accurate feature extraction, pattern recognition and reduction of authentication errors. Such methods enhance the performance and reliability of biometric systems, particularly in large-scale cloud settings.

Although there are secure authentication and cloud storage systems, many systems are still constrained by password dependencies, risk of data theft, lack of efficient encryption mechanisms and low authentication accuracy. To solve these problems, the proposed system combines fingerprint authentication, AES-256 encryption and cloud storage technology to provide a secure, reliable and user-friendly storage system.

The proposed work is intended to enhance the security of cloud storage using biometric verification and encrypted file management. This will help to reduce unauthorized access and improve the overall efficiency of data storage systems.

III. METHODOLOGY

The proposed system is a secure cloud-based storage architecture that uses fingerprint authentication to ensure authorized access to user data. The system combines biometric verification with cloud technology to improve security, reliability, and ease of access.

In the proposed model, users must first register their fingerprint using a fingerprint sensor. The fingerprint template is extracted and securely stored in the database. During login, the user scans their fingerprint again, and the system compares it with the stored template. If the fingerprint matches, access to cloud storage is granted.

The architecture consists of four major modules:

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.15586

1. User Registration Module
2. Fingerprint Authentication Module
3. Cloud Storage Module
4. Encryption and Security Module

The system reduces unauthorized access and improves data confidentiality compared to traditional password-based systems.

User Registration Phase

In this phase, the user creates an account and registers their fingerprint.

1) Steps Involved

1. User enters personal details.
2. Fingerprint sensor captures fingerprint image.
3. Pre-processing techniques such as noise removal and normalization are applied.
4. Minutiae points are extracted.
5. Fingerprint template is generated.
6. Template is encrypted and stored in the database.

This phase ensures secure biometric enrollment of users.

Authentication Phase

The authentication phase verifies the identity of the user.

2) Steps Involved

1. User scans fingerprint during login.
2. The system pre-processes the fingerprint image.
3. Feature extraction is performed.
4. Extracted features are compared with stored templates using a matching algorithm.
5. If similarity exceeds threshold value, authentication is successful.
6. Access to cloud storage is granted.

Encryption Technique

To enhance security, files stored in the cloud are encrypted using AES (Advanced Encryption Standard).

3) Encryption Process

- Before uploading, files are encrypted using AES-256.
- Encrypted files are stored in cloud storage.
- Only authenticated users can decrypt and access files.

This ensures data confidentiality even if cloud storage is compromised.

Advantages of Proposed System

- High security through biometric authentication
- Eliminates password theft issues
- Secure cloud data storage

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15586

- Fast authentication process
- Reduced unauthorized access
- Improved user convenience

Algorithm

Fingerprint Authentication Algorithm

1. Start
2. Capture fingerprint image
3. Preprocess image
4. Extract fingerprint features
5. Compare with stored template
6. If match found
    - Grant cloud access
7. Else
    - Deny access
8. Stop

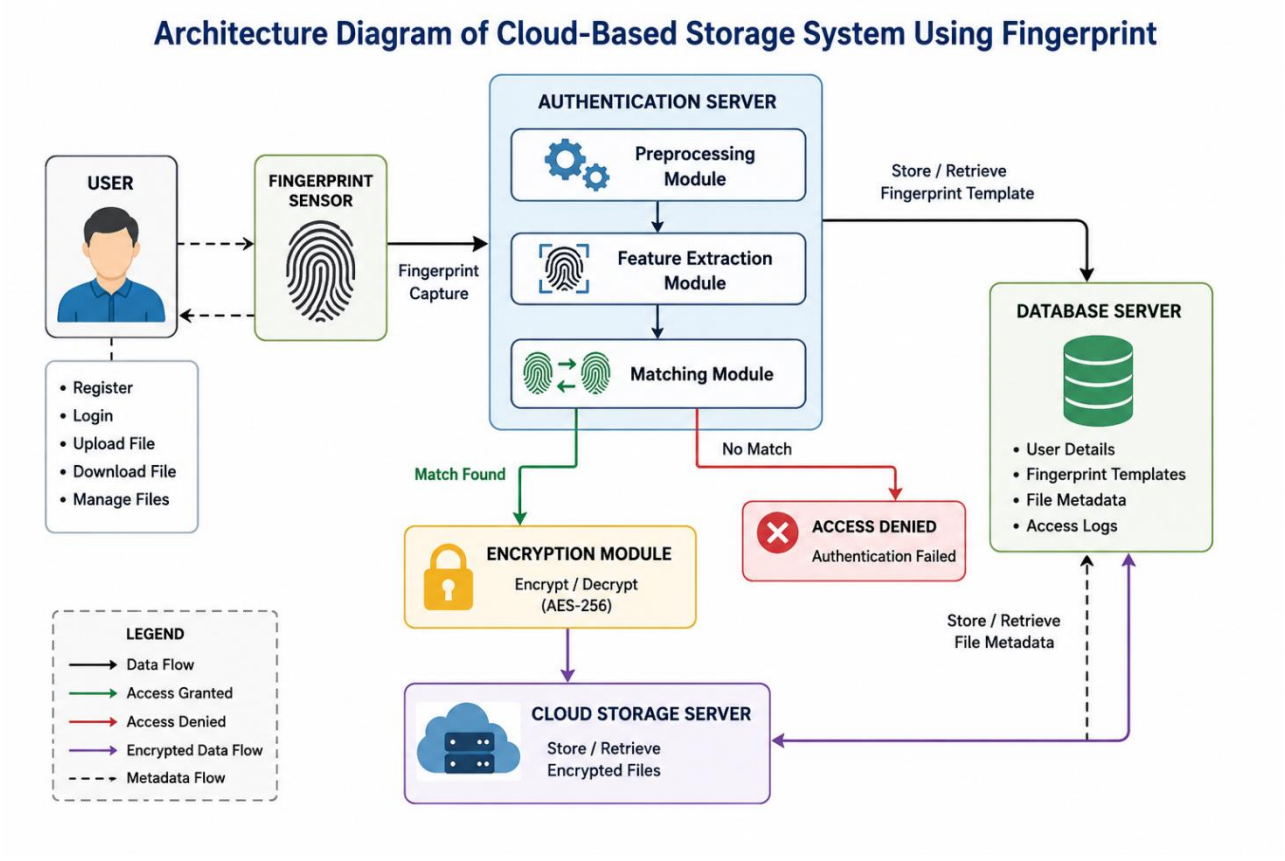


Fig. 1 A sample graph

Table Captions

Tables must be numbered using uppercase Roman numerals. Table captions must be centred and in 10 pt. Captions with table numbers must be placed before their associated tables, as shown in Table 1.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

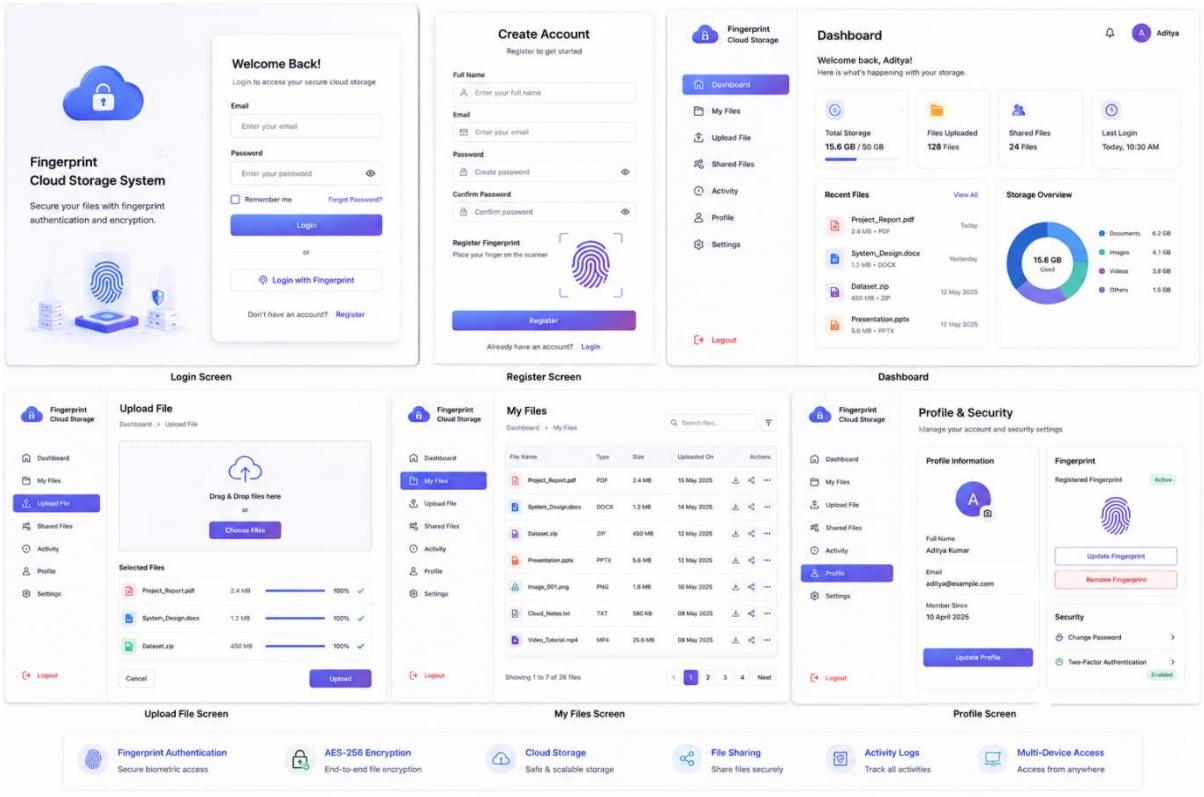
International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15586

IV. EXPECTED OUTCOMES

The implementation and testing of the proposed cloud based fingerprint storage system are expected to result in the followingoutcomes:
Security: AES-256 encryption combined with fingerprint authentication should greatly reduce unauthorized access, compared to traditional password-based systems. As fingerprints are unique to each individual, high accuracy is anticipated in identity verification by the system .
Authentication: The minutiae based fingerprint matching algorithm is designed to provide reliable and fast user authentication with minimum false acceptance and false rejection rates in a real world deployment.
Storage Efficiency: Cloud-based file storage can eliminate the need for physical storage devices, enabling users to access their data securely from any location and at any time.
Scalability: The proposed architecture is supposed to be scalable and can be used in educational institutions, banking systems and healthcare environments.
Future Validation: The accuracy, response time and encryption efficiency of the system will be quantitatively validated in future work by empirical testing using standard fingerprint datasets.



V. CONCLUSION

The proposed cloud-based storage system using fingerprint is expected to improve data security and user authentication in cloud environments. The system combines biometric verification with cloud storage technology to provide secure and reliable access control. Unlike traditional password-based systems, fingerprint authentication reduces the risk of password theft, unauthorized access, and phishing attacks.

The implementation of AES-256 encryption further enhances security by protecting files stored in the cloud from data breaches and unauthorized modifications.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026
DOI: 10.17148/IJARCCE.2026.15586

The proposed system is suitable for applications requiring secure data storage, such as banking systems, healthcare management, educational institutions, and enterprise cloud platforms. The system provides a user-friendly and highly secure solution for protecting sensitive information in cloud environments.

Although the system is designed to perform effectively, future improvements can include multi-factor authentication, AI-based fingerprint recognition, blockchain integration, and mobile cloud access to further enhance security and scalability.

Overall, the proposed system demonstrates that integrating fingerprint biometrics with cloud storage and encryption techniques provides a secure, efficient, and reliable solution for modern cloud security challenges.

VI. ACKNOWLEDGMENT

Hereby, we would like to thank all those people who have helped us in guiding us through the completion of this project titled "**Intelligent Fingerprint Storage and Management System for Authentication Applications on Cloud Storage** ."

We are highly thankful to our project **guide Dr. Sonia D'Souza,PostDoctoral** ,Associate Professor,NHCE for guiding us, encouraging us, and suggesting us all along the development process of this project.

We would also like to extend our gratitude towards the head of the department and all other professors who have contributed towards the successful completion of this work.

Moreover, we would like to acknowledge our college New Horizon College of Engineering for providing us with the platform for this project where we have learned about our technical skills in the areas of cloud computing, biometrics, and machine learning.

Finally, we would like to extend our sincere gratitude towards our team leader **Vaasthava Sree Sai Reddy N** and our fellow teammates
Subhmay Parya, .**Spoorti Patil**, **Vaishnavi Reddy** for their constant encouragement and support during this project.

REFERENCES

[1] A. K. Jain, A. Ross, and S. Prabhakar, "An Introduction to Biometric Recognition," IEEE Transactions on Circuits and Systems for Video Technology, vol. 14, no. 1, pp. 4-20, Jan. 2004.

[2] Jian Shen, Tianqi Zhou, Debiao He, Yuexin Zhang, Xingming Sun, and Yang Xiang, "Block Design-Based Key Agreement for Group Data Sharing in Cloud Computing," IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 6, pp. 996-1010, Nov.-Dec. 2019.

[3] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, 2nd ed., Springer, 2009.

[4] S. Subashini and V. Kavitha, "A Survey on Security Issues in Service Delivery Models of Cloud Computing," Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1-11, Jan. 2011.

[5] M. Armbrust et al., "A View of Cloud Computing," Communications of the ACM, vol. 53, no. 4, pp. 50-58, Apr. 2010.

[6] William Stallings, Cryptography and Network Security: Principles and Practice, 7th ed., Pearson Education, 2017.

[7] R. Buyya, C. S. Yeo, and S. Venugopal, "Market-Oriented Cloud Computing: Vision, Hype, and Reality for Delivering IT Services as Computing Utilities," Proceedings of the 10th IEEE International Conference on High Performance Computing and Communications, pp. 5-13, 2008.

DOI: 10.17148/IJARCCE.2026.15586

[8] Meenakshi and R. Arthi, "Cloud-Based Secure Storage System Using Biometric Authentication," International Journal of Advanced Research in Computer Science, vol. 8, no. 5, pp. 1200-1205, 2017.

[9] A. Ross, K. Nandakumar, and A. K. Jain, Handbook of Multibiometrics, Springer Science & Business Media, 2006.

[10] National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)," Federal Information Processing Standards Publication 197, Nov. 2001.

BIOGRAPHY

Vaasthava Sree Sai Reddy N is an undergraduate student specializing in Artificial Intelligence and Machine Learning at New Horizon College of Engineering, Bangalore, India. At the age of 18, Vaasthava has demonstrated a profound interest and commitment to the fields of artificial intelligence and deep learning. He has actively participated in and coordinated several workshops related to deep learning, gaining recognition for both participation and leadership in these technical events. This hands-on experience has enhanced Vaasthava's understanding of advanced AI concepts and practical applications. His academic pursuits are focused on exploring cutting-edge technologies and applying machine learning techniques to address complex real-world challenges. With a portfolio of innovative ideas and projects, Vaasthava is dedicated to advancing expertise and making significant contributions to the field of AI and ML through both academic research and practical applications.

Subhamay Parya is an undergraduate student specializing in Artificial Intelligence and Machine Learning at New Horizon College of Engineering, Bangalore, India. At the age of 19, subhamay has demonstrated a profound interest and commitment to the fields of artificial intelligence and deep learning. He has actively participated in and coordinated several workshops related to deep learning, gaining recognition for both participation and leadership in these technical events. This hands-on experience has enhanced Subhmay's understanding of advanced AI concepts and practical applications. His academic pursuits are focused on exploring cutting-edge technologies and applying machine learning techniques to address complex real-world challenges. With a portfolio of innovative ideas and projects, Subhmay is dedicated to advancing expertise and making significant contributions to the field of AI and ML through both academic research and practical applications.

Spoorti Patil is an undergraduate student specializing in Artificial Intelligence and Machine Learning at New Horizon College of Engineering, Bangalore, India. At the age of 20, Spoorti has demonstrated a profound interest and commitment to the fields of artificial intelligence and deep learning. She has actively participated in and coordinated several workshops related to deep learning, gaining recognition for both participation and leadership in these technical events. This hands-on experience has enhanced Spoorti's understanding of advanced AI concepts and practical applications. Her academic pursuits are focused on exploring cutting-edge technologies and applying machine learning techniques to address complex real-world challenges. With a portfolio of innovative ideas and projects, Spoorti is dedicated to advancing expertise and making significant contributions to the field of AI and ML through both academic research and practical applications.

Vaishnavi Reddy is an undergraduate student specializing in Artificial Intelligence and Machine Learning at New Horizon College of Engineering, Bangalore, India. At the age of 20, vaishnavi has demonstrated a profound interest and commitment to the fields of artificial intelligence and deep learning. She has actively participated in and coordinated several workshops related to deep learning, gaining recognition for both participation and leadership in these technical events. This hands-on experience has enhanced vaishnavi's understanding of advanced AI concepts and practical applications. Her academic pursuits are focused on exploring cutting-edge technologies and applying machine learning techniques to address complex real-world challenges. With a portfolio of innovative ideas and projects, vaishnavi is dedicated to advancing expertise and making significant contributions to the field of AI and ML through both academic research and practical applications.

