IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 6, June 2025
Impact Factor: 7.67

Fingerprint Based File Encryption-Decryption System

Rohit Bankar, Bhushan Chaware, Om Ghope, Venkat Ghodke
Electronics and Telecommunication,
AISSMS Institute of Information Technology, Pune, India

Abstract: *The emerging digital security threats require strong data protection methods to provide confidentiality, integrity, and accessibility of sensitive documents. Conventional password-based security solutions are vulnerable to attacks like weak passwords, lost credentials, and unauthorized access. To overcome such shortcomings, this paper proposes a Fingerprint-Based File Encryption-Decryption System, combining biometric verification and cryptographic encryption to offer an extremely secure and easy-to-use file security solution. The system to be developed utilizes fingerprint identification to act as the encryption and decryption key so that only authorized users can read files. It uses AES (Advanced Encryption Standard) for encryption and takes advantage of biometric-based dynamic generation of keys for additional security. In contrast to systems that traditionally use static passwords, this method reduces the vulnerability of data breaches and key compromises. A user-friendly Python Tkinter-based graphical user interface (GUI) adds usability, providing real-time authentication feedback, encryption status feedback, and error handling facilities. Arduino-based fingerprint sensors are included in the system through serial communication, giving biometric verification accurately. Multithreading also allows smooth, responsive operation. With biometric security, cryptographic encryption, and interactive user interface, this system enhances protection of data and eradicating password weaknesses, thus making it suitable for corporate settings, legal document protection, and individual data security.*

Keywords: Biometric Security, Fingerprint Authentication, Cryptographic Encryption, AES Encryption, Secure File Management, Data Protection

I. INTRODUCTION

In today's digital era, information security has emerged as a key component of managing information. With the rise in the use of electronic storage and transmission of sensitive data, the dangers of unauthorized access, data loss, and cyber attacks have also grown. The age-old traditional security measures like passwords and PINs have been found wanting as they are vulnerable to attacks like brute force, phishing, and credential exposure. In response to these vulnerabilities, biometric authentication has been the most potent alternative as it provides better security through exclusive physiological characteristics like fingerprints, facial features, and iris scanning.

The Fingerprint-Based File Encryption-Decryption System is the focus of this study. The system combines biometric verification and cryptographic encryption methods to provide added security for data protection. In contrast to traditional password-based encryption, where file security is dependent on user-created credentials, this system employs fingerprints as the encryption and decryption key. The non-replicability and uniqueness of fingerprints lower the possibility of unapproved access, and the system only allows registered users to retrieve or edit encrypted files.

The system to be implemented utilizes the Advanced Encryption Standard (AES), one of the most popularly used encryption algorithms that has the security and performance benefits. When a user logs in using a fingerprint reader, the system creates a special cryptographic key based on the biometric information. It uses such a key to encrypt or decrypt a file so that it can only be accessed by the authenticated user. As opposed to static passwords that are vulnerable to theft or guessing, biometric authentication does away with the need for users to memorize complicated passwords, thus improving security and convenience.

Copyright to IJARSCT
www.ijarsct.co.in

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 6, June 2025
Impact Factor: 7.67

For better accessibility and usability, the system has been implemented with an interactive Graphical User Interface (GUI) based on Python's Tkinter framework. The GUI enables users to select files in a convenient manner, scan their fingerprints, and track encryption or decryption in real time. Further, the system incorporates serial communication with an Arduino Nano for effective fingerprint recognition. The Arduino Nano, combined with a fingerprint sensor module, takes and verifies the fingerprint of the user prior to executing encryption or decryption processes. This prevents any unauthorized user from bypassing security measures.

The main aim of this research is to improve data security by replacing standard password-based encryption with biometric authentication. By removing password-related risks including weak passwords, lost passwords, and brute-force attacks, the system drastically minimizes the threat of unauthorized access. The incorporation of an easy-to-use interface makes file encryption and decryption uncomplicated without sacrificing security, providing real-time authentication with minimal delay.

This renders the system feasible for use in real-world scenarios where confidentiality is paramount. The growing uptake of biometric technology across different sectors attests to its efficacy in enhancing security systems. Through the combining of fingerprint recognition and cryptographic encryption, this research seeks to further the development of secure file management solutions. The system has been designed with a very secure, efficient, and user-oriented way of protecting files, making it an important resource for individuals and organizations looking to have better digital security systems.

II. PAGE LAYOUT

Introduces a scheme in which cryptographic keys are derived from fingerprint minutiae, instead of conventional passwords, to improve security and usability. While not biometric, outlines a USB-protected symmetric encryption scheme that can be expanded with fingerprint authentication. Introduces a basic method for creating secure keys from fingerprint characteristics along with handling error tolerance. Fingerprint recognition is merged with public key infrastructure (PKI) for digital access security, with an emphasis on template protection. Discusses fingerprint key generation with a focus on revocability and attack resistance like template inversion. Suggests a hybrid AES-RSA scheme in which AES keys generated from the fingerprint minutiae facilitate efficient and secure file encryption. Introduces cancelable biometrics for secure, revocable, and non-invertible fingerprint-based file encryption. Discusses identity-based encryption to ensure secure access to cloud storage using fingerprints, which can also be used for local systems. Strengthens authentication by integrating fingerprints with behavioral biometrics such as keystroke dynamics for multi-layer key creation. The second (duplicate numbering) is an irreversible encryption process via chaotic systems and SVD, providing high recognition rates along with attack resistance. Focuses on irreversible fingerprint transforms that are invulnerable to inverse and brute-force attacks and revocability support. Uses fuzzy extractors and side information to create secure keys from fingerprint scans, thus no need for storing keys and high security when accessing encrypted files.

III. METHODOLOGY

The suggested Fingerprint-Based File Encryption-Decryption System combines biometric verification with cryptology to provide safe and convenient file protection. It starts with fingerprint identification, where the fingerprint of the user is scanned, hashed, and stored safely during enrollment. At authentication, the system authenticates by matching the scanned fingerprint with the stored template in order to provide access. After successful authentication, a biometric key-generated dynamic AES-256 encryption key is used to encrypt specified files. These encrypted files are stored securely locally on the user's device, circumventing the risks linked to cloud storage. Decryption is the reverse of encryption, with re-authentication and regeneration of the biometric key necessary to view the original file. A Tkinter GUI allows easy interaction for file handling, encryption, and decryption, while in-built error management provides smooth operations. Also, the system has real-time access control and records failed authentication attempts, enhancing security and facilitation of forensic tracing.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 6, June 2025
Impact Factor: 7.67

IV. RESULT AND DISCUSSION

The testing of the Fingerprint-Based File Encryption-Decryption System proved its efficiency, security, and ease of use. Biometric verification was highly accurate, with low false acceptance and rejection rates, and performed consistently under different environmental conditions. The AES-256-based encryption and decryption operations were effective, preserving data integrity and making sure that files were accessible to authorized users only. The system provides added security through dynamic generation of encryption keys directly from fingerprints, obviating the need for storing or memorizing passwords and making brute-force or keylogging attacks impossible. An interactive Tkinter GUI offers ease of use with real-time feedback and error handling, facilitating even for non-technical users. Storage on a local machine adds privacy and integrity while preventing cloud breaches. Compared to conventional password-based systems, the biometric method was more secure, quicker, and simpler to utilize. Overall, the system presents a strong, secure, and practical approach to safeguarding sensitive information, with future possibilities for multi-biometric support and cloud integration.

V. FUTURE SCOPE

Future developments of the Fingerprint-Based File Encryption-Decryption System will greatly enhance security, scalability, and user access. Adding multi-biometric authentication—fingerprints, facial recognition, and iris scanning—can offer resistance to spoofing and enhanced reliability, particularly for high-security applications. Cloud storage integration will allow secure, location-transparent access to encrypted files, with more sophisticated controls such as time-limited access and geo-blocking. Embedding blockchain technology can decentralize the management of keys and keep tamper-proof access records, enhancing transparency and minimizing risk of key theft. Anomaly detection powered by AI can also enhance security further by picking up on abnormal access patterns and invoking further authentication. For ultimate usability, the system can be made cross-platform and deployable in enterprise contexts across industries such as healthcare, finance, and government. Together, these technologies will evolve the system into a more resilient, intelligent, and future-proof solution for safe data management.

VI. CONCLUSION

Fingerprint-Based File Encryption-Decryption System offers a safe and effective method for secure protection of sensitive digital files by combining biometric verification with AES encryption. Contrary to conventional password-based systems, it employs distinctive fingerprint identification to provide protected access to encrypted information only for approved users. Easy-to-use Tkinter GUI makes file handling and verification easy, while Arduino-based serial communication safely takes in biometric input without storing constant passwords. Future extensions such as support for multi-biometrics, cloud storage, blockchain-based key management, and AI-based anomaly detection can further enhance its functionality. The system in general provides a scalable, future-proof solution appropriate for personal, corporate, and governmental data security requirements.

VII. AKNOWLEDGEMENT

We gratefully appreciate and acknowledge that the project has been successfully done. We take this privilege to thank our guide Prof. Venkat Ghodke, Department of Electronics and Telecommunication for all her tireless efforts and guidance in taking this attempt as a grand success. We are thankful to Dr. Mohini Sardey, Department of Electronics and Telecommunication and HOD for their precious advice.

REFERENCES

[1] Ranjith Jayapal, Pramod Govindan, ”Fingerprint Encryption System for Increased Security”, Department of Electrical Engineering, University of North Florida (UNF),Jacksonville, Florida, USA.
[2] XUE Juntao, WANG Ye, WANG Shucheng, “File Encryption System Based on Fingerprint”, Proceeings of 31st Chinese Control Conference July 25-27,2012, Hefei, China.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 6, June 2025
Impact Factor: 7.67

[3] Mehta Manisha Pravinchandra, Hiteishi Milind Diwanji & Jagdish Shantilal Shah, "Performace Analysis of Encryption and Decryption using Genetic Based Cancelable Non-Invertible Fingerprint based Key in MANET", 2012 International Conference on Communication Systems and Network Technologies

[4] Alex Stoianov, Ann Cavoukian, "Fingerprint Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy"

[5] Kehe Wu, Yakun Zhang, Wenchao Cui, Ting Jiang, "Design and implementation of encrypted and decrypted filesystem based on USB Key and hardware code", AIP Conf. Proc. 1839, 020215 (2017).

[6] Mouad .M .H .Ali , Vivek H. Mahale, Pravin Yannawar, A. T. Gaikwad, "Overview of Fingerprint Recognition System", International Conference on Electrical, Electronics, and Optimization Techniques (ICEEOT) – 2016.

[7] Sheikh Imroza Manzoor, Arvind Selwal, "An Analysis of Biometric Based Security Systems", 5th IEEE International Conference on Parallel, Distributed and Grid Computing(PDGC-2018), 20-22 Dec, 2018, Solan, India.

[8] Hemalatha S, "A systematic review on Fingerprint based Biometric Authentication System", 2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE).

[9] Singampalli Gowthami, 2Kezia Rani Badhiti, "Encrypting Biometric File using Enhanced AES and Storing on the Cloud", International Journal of Creative Research Thoughts (IJCRT) Issue 2 April 2018.

[10] Melisha Kaur A/P Narinder Singh, Julia Juremi, "PiFortify: A Raspberry Pi-based Encryption Tool with Biometric Authentication", Journal of Applied Technology and Innovation (e -ISSN: 2600-7304) vol. 8, no. 2, (2024).