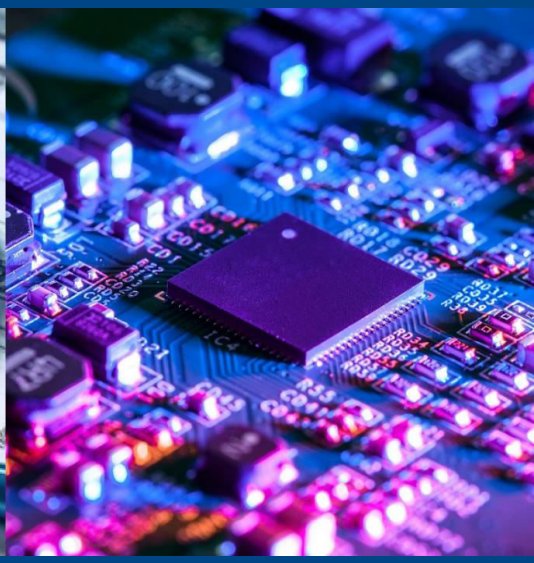
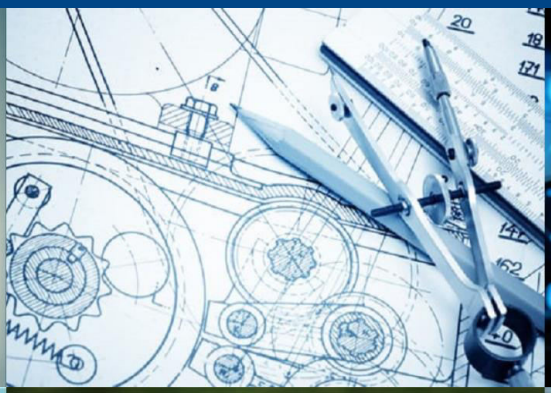
ISSN: 2582-7219

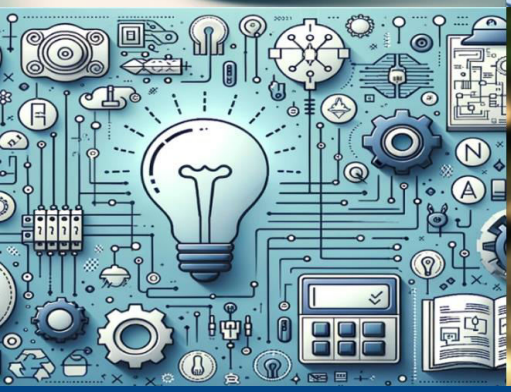




International Journal of Multidisciplinary Research in Science, Engineering and Technology

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



Impact Factor: 8.206 **Volume 9, Issue 3, March 2026**

© 2026 IJMRSET | Volume 9, Issue 3, March 2026 DOI:10.15680/IJMRSET.2026.0903182

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

Cyber-Secure File Vault with Hardware Key Using Raspberry PI 5

Arfat Haju[1], Pranav Gulve[2], Altaf Jamkhandi[3], Nilesh Bangar[4], Azhar Bandri[5]

U.G Student, Department of Computer Science and Engineering, JSPM University, Pune, India [1,2,3]

Professor, School of Computational Sciences, Faculty of Science and Technology, JSPM University, Pune, Maharashtra, India[4]

Industry Guide, Chief Operating Officer(COO), Pleximus Inc., Ratnagiri, Maharashtra, India[5]

ABSTRACT: Government organizations and defense institutions handle massive volumes of confidential and mission-critical data, including classified intelligence, citizen identity records, and national security documents. Traditional password-based systems and simple encryption mechanisms have proven inadequate due to increasing cyber threats such as phishing, credential theft, insider misuse, and brute-force attacks. This paper presents the Cyber Secure File Vault with Hardware Key, a multi-layered cyber defense architecture built on the Raspberry Pi 5 platform. The system combines biometric authentication, hardware-based key verification, and advanced cryptographic protocols to create a highly secure digital vault. The proposed solution employs AES-256 for symmetric encryption, RSA/Elliptic Curve Cryptography (ECC) for asymmetric key exchange, SHA-3 for integrity verification, and TLS 1.3 for encrypted data transmission. Role-Based Access Control (RBAC) governs user permissions across each Raspberry Pi 5 node, while secure synchronization with a centralized cloud server ensures backup, recovery, and scalability. An AI-driven destruct mode automatically encrypts or wipes sensitive data upon detection of intrusion or tampering attempts. Experimental results demonstrate that the system achieves enterprise-grade security at a fraction of the cost of traditional secure servers, providing a scalable, tamper-proof solution for government, defense, healthcare, finance, and enterprise cybersecurity infrastructures.

KEYWORDS: AES-256 encryption; biometric authentication; cyber security; elliptic curve cryptography; hardware token; Raspberry Pi 5; role-based access control; secure file vault; TLS 1.3.

I. INTRODUCTION

The rapid digitization of government and enterprise operations has resulted in the storage of highly sensitive information such as defense files, citizen records, and confidential policy drafts. Traditional security systems that rely primarily on passwords and rudimentary encryption have become increasingly inadequate against modern threats including phishing attacks, credential theft, ransomware, and insider misuse [1].

The proliferation of connected devices and cloud infrastructure has expanded the attack surface available to malicious actors. Existing hardware security solutions such as YubiKey and enterprise-grade HSMs offer strong authentication but remain cost-prohibitive for large-scale government adoption. Cloud storage providers introduce concerns around data sovereignty and centralized trust. This creates an urgent demand for a cost-effective, multi-factor, and user-friendly secure file vault capable of ensuring the confidentiality, integrity, and availability of sensitive data.

This paper presents the Cyber Secure File Vault with Hardware Key, a Raspberry Pi 5-based system that delivers enterprise-class security through a layered combination of biometric authentication, cryptographic algorithms (AES-256, RSA/ECC, SHA, TLS 1.3), and an AI-driven tamper response mechanism. The system targets government agencies, law enforcement, healthcare institutions, financial organizations, and SMEs requiring robust, affordable, and scalable data protection.

A. Motivation

Current storage systems overwhelmingly rely on single-factor authentication. Password-based vaults such as BitLocker and VeraCrypt, while widely deployed, are susceptible to credential compromise. Cloud vaults introduce remote attack

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

surfaces. The absence of integrated hardware-level offline security makes these solutions inadequate against determined adversaries. The Raspberry Pi 5 platform, with its improved computational capabilities, presents an opportunity to close this gap at low cost.

B. Contributions

The key contributions of this work are:

- A hardware-anchored, multi-factor authentication pipeline combining fingerprint biometrics and a USB hardware token.
- Integration of AES-256, RSA/ECC, SHA-3, and TLS 1.3 into a unified encryption framework on embedded hardware.
- Role-Based Access Control (RBAC) with per-machine encrypted vaults and audit logging.
- An AI-based anomaly detection and data destruct mechanism for tamper response.
- A private NAS cloud backend built on ESP32 for secure, administrator-controlled cloud synchronization.

II. LITERATURE REVIEW

1. Overview

The literature focuses on cryptography, multi-factor authentication (MFA), hardware security, role-based access control (RBAC), and embedded systems. These domains collectively form the foundation for designing a secure file vault integrated with hardware authentication.

2. Cryptographic Algorithms for Data Security

AES-256 is widely used for secure data encryption due to its strong resistance to attacks. RSA enables secure key exchange, while ECC provides similar security with smaller key sizes suitable for embedded systems. SHA-3 ensures data integrity, and TLS 1.3 secures communication with improved security and performance.

3. Multi-Factor Authentication (MFA) Systems

MFA combines passwords, biometrics, and hardware tokens to enhance security. Fingerprint authentication provides high accuracy, and NIST recommends hardware-based authentication for the highest assurance level (AAL3), supporting the proposed system design.

4. Hardware Security Tokens and Modules

Hardware tokens like YubiKeys offer strong protection against phishing attacks. However, they introduce risks such as physical tampering. Integrating hardware verification within the system improves control, reduces cost, and enhances overall security.

5. Role-Based Access Control (RBAC)

RBAC assigns permissions based on roles, simplifying access management and improving security. It supports role hierarchy and separation of duties, ensuring only authorized users access sensitive data.

6. Raspberry Pi and Embedded System Security Platforms

Raspberry Pi provides a cost-effective platform capable of handling encryption and biometric authentication. It supports real-time operations and hardware interfacing, making it suitable for secure embedded systems.

7. Cloud Storage Security

Cloud storage introduces risks like data breaches. Encrypting data before uploading ensures confidentiality. Private cloud solutions improve control and auditability while maintaining data availability.

8. AI and Anomaly Detection in Security Systems

Machine learning algorithms like Isolation Forest detect abnormal access patterns. AI-based systems can identify unknown threats and trigger automatic responses such as system lockdown or data destruction.

9. Summary and Research Gap

Existing solutions focus on individual components but lack integration. The proposed system fills this gap by combining cryptography, MFA, RBAC, AI-based detection, and secure cloud storage into a unified, low-cost platform.

© 2026 IJMRSET | Volume 9, Issue 3, March 2026 DOI:10.15680/IJMRSET.2026.0903182

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

III. RELATED WORK AND STATE OF THE ART

Data security research has produced a range of solutions spanning software vaults, cloud-based storage, hardware tokens, and biometric authentication, each presenting distinct trade-offs.

Software Vaults (BitLocker, VeraCrypt) offer AES encryption but rely solely on software credentials — no hardware barrier, tamper detection, or AI response.

Cloud Storage (Google Drive, Dropbox, OneDrive) provides encryption and optional MFA, but centralized third-party dependency raises privacy, sovereignty, and security gap concerns.

Hardware Tokens (YubiKey/FIDO2) deliver strong phishing-resistant 2FA but are costly at scale and lack built-in vault or biometric functionality.

Biometric Systems offer high accuracy yet remain expensive and vulnerable to spoofing when used alone — combining them with hardware tokens significantly strengthens security.

Raspberry Pi Security Systems have been used for intrusion detection and VPN endpoints, but no prior work integrates biometric MFA, cryptographic vault management, RBAC, cloud sync, and AI-driven destruct mode on a single embedded platform**.**

IV. SYSTEM ARCHITECTURE AND DESIGN

A. Overall Architecture

The proposed system is built around three interconnected tiers: (1) the user-facing authentication layer, (2) the local encrypted vault layer running on Raspberry Pi 5, and (3) a private NAS cloud layer implemented on an ESP32 module. Figure 1 illustrates the overall process flow. A user initiates an access request, which triggers sequential validation through the hardware key module and the biometric fingerprint sensor. Upon successful MFA, the RBAC engine evaluates the user's assigned role and grants appropriate vault permissions. Unauthorized access attempts activate the AI-based destruct module. Authorized sessions can trigger encrypted cloud backup to the ESP32-based NAS server.

B. Authentication Module

The authentication pipeline enforces strict two-factor verification. In the first factor, a USB hardware token is physically inserted and cryptographically verified against a stored hash. In the second factor, a fingerprint scanner validates the biometric template. Both factors must succeed independently; failure in either blocks all vault access. Authentication operations are targeted to complete within 3-5 seconds.

C. Encryption and Security Module

File confidentiality is achieved through AES-256 encryption in CBC mode using PyCryptodome. Key exchange during cloud synchronization employs RSA/ECC asymmetric cryptography, eliminating shared-secret exposure. Data integrity is enforced via SHA-3 hash verification computed before and after every file operation. All communication between the local vault and the cloud NAS is wrapped in TLS 1.3, the most current version of the Transport Layer Security protocol.

D. Role-Based Access Control Module RBAC is configured with three principal roles: Administrator, Government User, and Academic/Corporate User. Each role carries a defined permission set governing allowable operations (upload, download, rename, delete, cloud backup, destruct). Each Raspberry Pi 5 node maintains a unique, isolated vault directory. Access logs capturing timestamp, username, role, and operation type provide a traceable audit trail.

E. AI-Based Destruct Module Anomaly detection is implemented using a lightweight Scikit-learn model trained on baseline access behavior. Upon detection of abnormal access patterns, repeated failed authentication attempts, or physical tampering signals, the module automatically initiates vault destruction: encrypted files are overwritten with random data and subsequently deleted, eliminating any possibility of forensic recovery. The destruct action is also manually accessible to authorized administrators via a confirmation dialog.

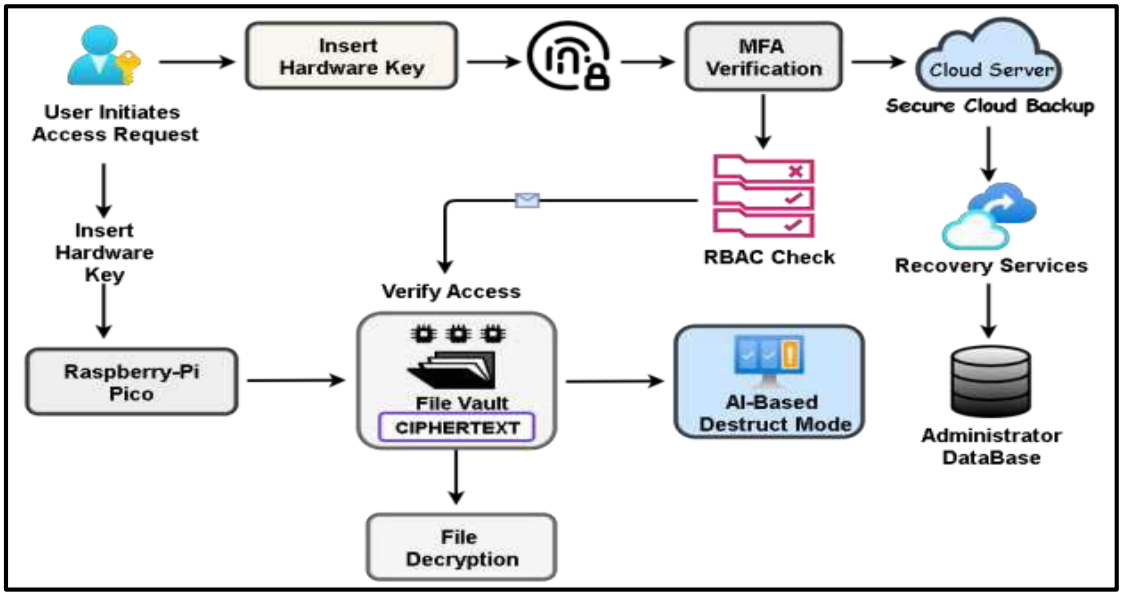
F. Cloud Integration Module A private Network-Attached Storage (NAS) server is implemented on an ESP32 microcontroller, accessible over the local network at a static IP address. The PiVault5 Cloud web interface provides file upload, download, rename, and delete operations restricted to authenticated administrator sessions. This hybrid local-plus-cloud architecture ensures data availability and disaster recovery without dependence on third-party cloud provders.

© 2026 IJMRSET | Volume 9, Issue 3, March 2026 DOI:10.15680/IJMRSET.2026.0903182

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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



V. SYSTEM REQUIREMENTS SPECIFICATION

A. Hardware Requirements

The system hardware stack consists of a Raspberry Pi 5 (8GB RAM) as the primary compute node, a USB fingerprint scanner module for biometric capture, a USB hardware security key as the second authentication factor, an external SSD/HDD for encrypted vault storage, a 16GB microSD card for OS and boot media, an ESP32 Wi-Fi module for NAS functionality, a Raspberry Pi Active Cooler, and a USB-C power supply adapter.

B. Software Requirements

The software stack includes Python 3.11 as the primary development language, C++ for low-level ESP32 firmware development, MySQL for session and user data management, and VS Code as the integrated development environment. The system targets Linux-based operating systems, specifically Raspberry Pi OS, for compatibility and portability.

C. Non-Functional Requirements The system is designed to meet the following non-functional criteria: end-to-end encryption with no plaintext data at rest; authentication latency not exceeding 5 seconds; modular codebase enabling integration of future cryptographic standards; compliance with ISO/IEC 27001 and India IT Act 2000; and scalability to support multiple concurrent vault nodes across a departmental network.

Component	Library / Technology
AES-256 Encryption	PyCryptodome (Crypto.Cipher.AES, CBC mode)
RSA / ECC Key Exchange	Python cryptography library (hazmat.primitives)
SHA-3 Integrity Hashing	hashlib (sha3_256)
TLS 1.3 Communication	Python ssl module / OpenSSL
Anomaly Detection (AI)	Scikit-learn / TensorFlow (Isolation Forest)
UI Framework	Tkinter (desktop), Flask (NAS web interface)
Database	MySQL (user/session management)
Cloud NAS Firmware	C++ on ESP32, Arduino framework

Table I: Technology Stack and Libraries

© 2026 IJMRSET | Volume 9, Issue 3, March 2026 DOI:10.15680/IJMRSET.2026.0903182

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

VI. IMPLEMENTATION

A. Cryptographic Libraries and Frameworks

Table I: Technology Stack and Libraries

B. Module Implementation Workflow

The user launches the application and is presented with a landing screen. Upon clicking 'Go to Login', the RBAC login screen prompts for a username, password, and role selection (Government, Academic, or Corporate). Credentials are validated against a hashed user database. A mismatched role or incorrect password triggers an 'Access Denied' alert.
Following successful credential validation, the system transitions to the Hardware Key Verification screen, which detects USB insertion events. A cryptographic challenge-response confirms key authenticity. Upon hardware key verification, if a fingerprint scanner is connected, a biometric scan is initiated and the captured template is compared against registered data.

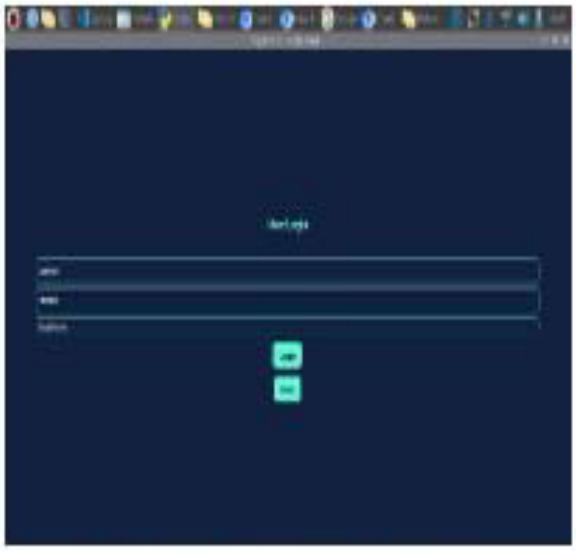
Once both MFA factors are satisfied, the Secure Vault Access dashboard is presented, offering options to Open Vault Folder, Backup to Cloud (Simulated), Destroy Vault Data, or Logout. Vault folder access reveals the encrypted file directory on the Raspberry Pi filesystem. Cloud backup initiates an authenticated upload to the ESP32 NAS server over the local network.

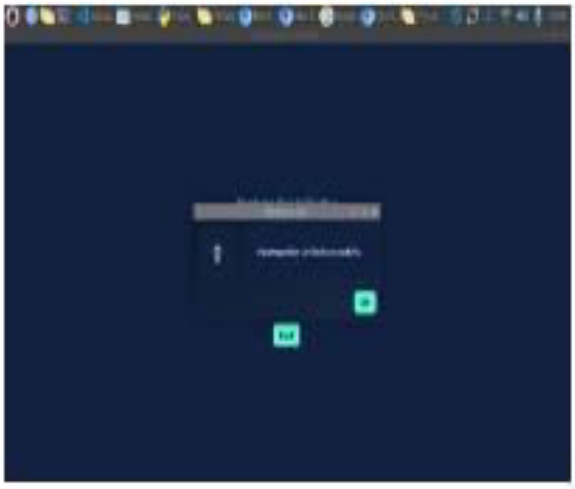
© 2026 IJMRSET | Volume 9, Issue 3, March 2026 DOI:10.15680/IJMRSET.2026.0903182

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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



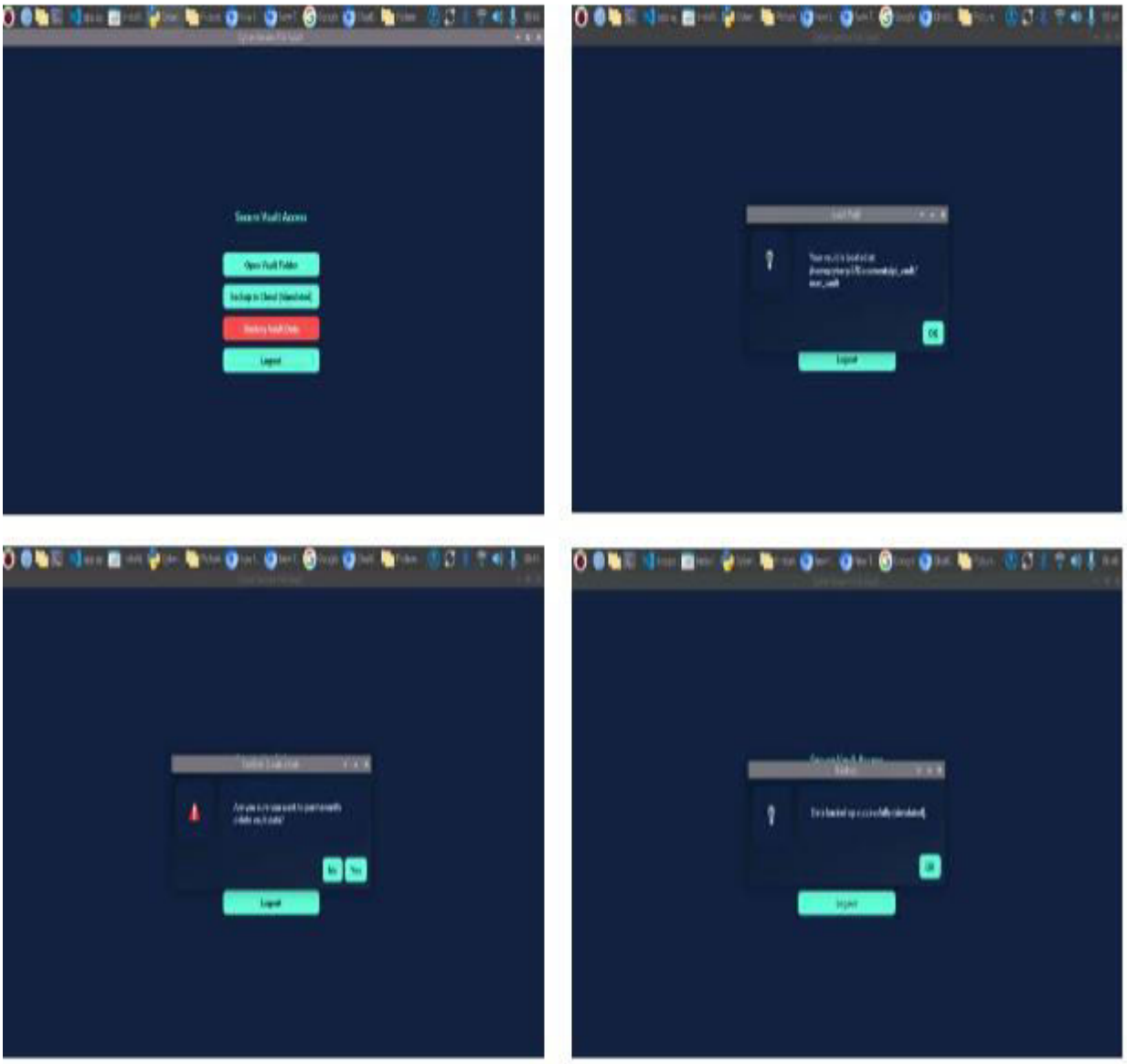


© 2026 IJMRSET | Volume 9, Issue 3, March 2026 DOI:10.15680/IJMRSET.2026.0903182

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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



VII. TESTING AND RESULTS

A. Unit Testing

Individual modules were validated in isolation using the Python unittest framework. The biometric authentication module was tested with enrolled and non-enrolled fingerprint samples to verify acceptance and rejection rates. The AES-256 and RSA encryption and decryption routines were validated for correctness by comparing encrypted output hashes against expected values. Hardware key recognition was verified by simulating both valid key insertion events and unauthorized device connections.

B. Integration Testing

Integration testing verified correct data flow between the biometric module, encryption engine, vault storage directory, hardware key handler, and cloud NAS endpoint. All modules successfully interacted without data mismatch or cryptographic key-handshake failures. The cloud backup integration was tested by uploading files of varying sizes and confirming byte-for-byte integrity upon download.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

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

C. System Testing

End-to-end functional testing covered the complete pipeline from authentication through file encryption, upload, retrieval, and secure deletion. The AI-based destruct mode was triggered by simulating abnormal access patterns, including repeated authentication failures and role mismatches, and was confirmed to initiate data destruction within the expected detection window. RBAC enforcement was verified across Government, Academic, and Corporate role scenarios.

D. User Acceptance Testing (UAT)

UAT was conducted with a simulated group of government department personnel. Participants evaluated ease of operation, clarity of authentication prompts, alert responsiveness, and confidence in the system's security posture. Feedback indicated smooth operation, strong perceived security, and an intuitive user experience, with authentication completing within the target 3-5 second window in all test runs.

VIII. CONCLUSION AND FUTURE WORK

A. Conclusion

This paper presented the Cyber Secure File Vault with Hardware Key, a multi-layered, Raspberry Pi 5-based security architecture integrating biometric authentication, hardware token verification, AES-256/RSA/ECC/SHA-3 cryptography, RBAC, AI-driven tamper response, and private cloud synchronization. The system demonstrates that enterprise-grade data security is achievable on affordable embedded hardware without sacrificing usability. The offline-first design eliminates reliance on third-party cloud providers while audit logging ensures full accountability. Testing confirmed functional correctness, security policy enforcement, and sub-5-second authentication latency. Approximately 30% of the full system has been implemented to date, with the fingerprint and hardware key integration pipeline validated and operational.

B. Future Work

Future development directions include:

[1] Full physical integration of the fingerprint scanner and NFC-based hardware token with the Raspberry Pi 5 GPIO interface. [2] Deployment of the AI anomaly detection model on real-world access log data for improved detection accuracy and reduced false-positive rates. [3] Extension of the RBAC model to support dynamic, policy-driven permission delegation across multi-node government department deployments. [4] Integration of post-quantum cryptographic primitives (CRYSTALS-Kyber, CRYSTALS-Dilithium) to future-proof the system against quantum computing threats.

REFERENCES

[1] W. Stallings, Cryptography and Network Security: Principles and Practice, 7th ed. Pearson, Upper Saddle River, NJ, USA, 2016.

[2] A. Menezes, S. Vanstone, and P. Oorschot, "Elliptic curve cryptosystems," Journal of Cryptology, vol. 8, no. 3, pp. 179-200, Summer 1995.

[3] P. Kocher, J. Jaffe, and B. Jun, "Differential power analysis," in Advances in Cryptology - CRYPTO 1999, vol. 1666, pp. 388-397, Aug. 1999.

[4] D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano, "Public key encryption with keyword search," in Proc. Eurocrypt 2004, Interlaken, Switzerland, pp. 506-522, 2004.

[5] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications of the ACM, vol. 21, no. 2, pp. 120-126, 1978.

[6] National Institute of Standards and Technology, "Advanced Encryption Standard (AES)," FIPS PUB 197, Nov. 2001. [Online]. Available: https://csrc.nist.gov/publications/detail/fips/197/final

[7] Raspberry Pi Foundation, "Raspberry Pi 5 - Complete Specifications," 2024. [Online]. Available: https://www.raspberrypi.com/products/raspberry-pi-5/

[8] Internet Engineering Task Force, "The Transport Layer Security (TLS) Protocol Version 1.3," RFC 8446, Aug. 2018.

[9] National Institute of Standards and Technology, "Digital Identity Guidelines," NIST SP 800-63-3, Jun. 2017.

[10]ISO/IEC 27040:2015, "Information Technology - Security Techniques - Storage Security," International Organization for Standardization, 2015.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com