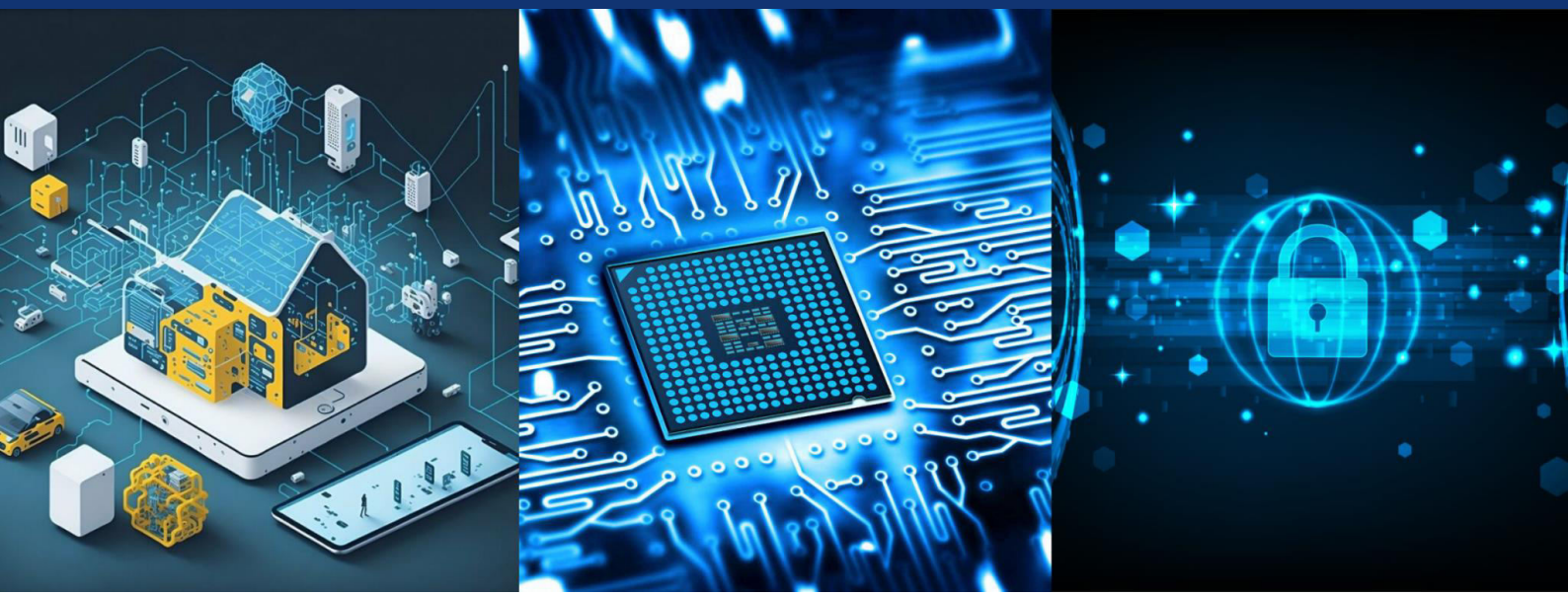
IJIRCCE

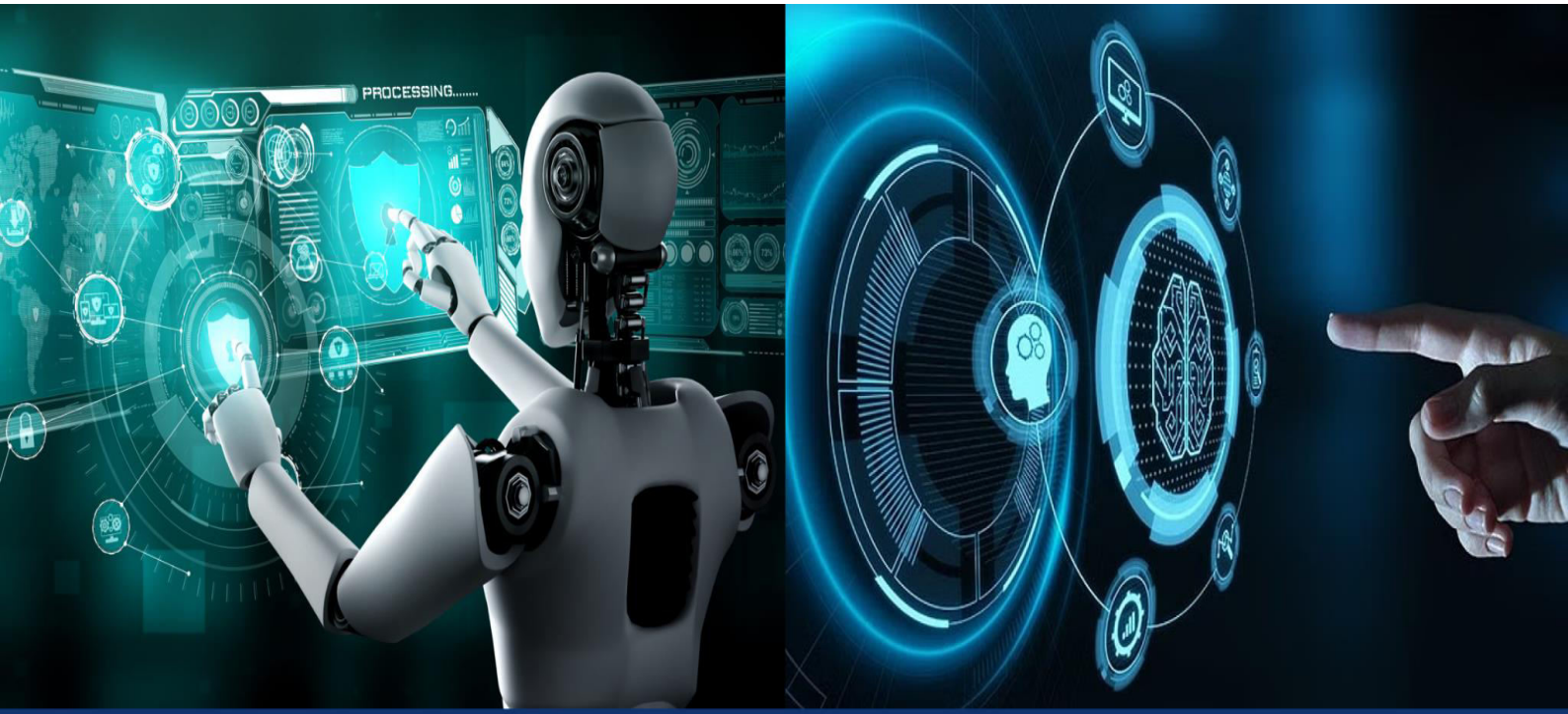
ISSN(O): 2320-9801

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: 9.927

Volume 14, Issue 5, May 2026

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405108

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| 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 Boot Authentication in Personal Computers Using Fingerprint Recognition and Hardware-Level Access Control

Sakthiganesh R, R. Marimuthu

M.Sc., Dept. of Cyber Forensic and Information Security, Dr. M.G.R. Educational and Research Institute, Maduravoyal, Chennai, Tamil Nadu, India

Faculty, Dept. of Centre for Cyber Forensics and Information Security, University of Madras, Chennai, Tamil Nadu, India

ABSTRACT: This paper proposes a hardware-level biometric authentication system that physically controls the boot process of personal computers. A Raspberry Pi 3B+ interfaces with an R307S fingerprint sensor via UART and controls a 5V relay connected to the ATX motherboard PWR_SW header, preventing boot without fingerprint verification. Fingerprint templates are stored on-device, access logs are encrypted using AES-128 Fernet, and the service auto-starts via systemd. Prototype validation confirms sub-second response times and successful authentication across all defined test cases.

KEYWORDS: Fingerprint Authentication; Secure Boot; Raspberry Pi; Hardware Access Control; IoT Security

I. INTRODUCTION

Unauthorized physical access to personal computers remains a persistent security concern in enterprise, academic, and government environments. Conventional security mechanisms such as BIOS passwords, full disk encryption, and operating system login screens are invoked after the system has already received power and begun the boot sequence. Consequently, these measures are susceptible to physical attacks including bootable USB-based OS bypass, hard disk removal and cloning, CMOS battery extraction to reset BIOS credentials, and pre-boot execution environment exploits.

Hardware-level access control fundamentally addresses this attack surface by enforcing authentication before any power is delivered to the system. This significantly reduces exposure to software-level bypass techniques, as the system cannot initiate any boot sequence without prior biometric verification. This paper presents a proof-of-concept prototype of a pre-OS authentication system built on the IoT paradigm using a Raspberry Pi 3B+ that physically gates the PC power button circuit via a 5V relay module.

The proposed system uses an R307S optical fingerprint sensor for biometric verification, stores templates on-device within the sensor's onboard flash memory, encrypts all access logs using AES-128 Fernet symmetric encryption, and operates entirely offline without any network dependency. It is designed for compatibility with ATX-compliant desktop computers without permanent modification to the target hardware.

The key contributions are: (1) hardware-level PC boot authentication operating entirely pre-OS; (2) complete offline operation with no network dependency; (3) on-device biometric template storage ensuring fingerprint data never leaves the sensor; (4) AES-128 Fernet encrypted audit logging; and (5) autonomous systemd service management for zero-intervention deployment. Full end-to-end PC boot validation is identified as future deployment work.

II. LITERATURE SURVEY

Karthik et al. [1] implemented a fingerprint authentication system on Raspberry Pi integrated with IoT sensors and cloud backend for remote device authentication. While UART-based fingerprint interfacing was demonstrated, the system

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405108

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

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

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

targeted cloud-connected IoT devices rather than local hardware power control, introducing network dependency unsuitable for offline environments.

Arunkumar and Arun Raja [2] developed a Raspberry Pi-based biometric authentication system with PostgreSQL database backend and PHP web interface. Their architecture requires persistent web server infrastructure and stores fingerprint templates on a remote database, both absent in the proposed offline design.

Heamalatha et al. [3] presented an IoT-based biometric attendance management system using ATmega328 microcontroller with cloud integration. This work focuses exclusively on attendance tracking and does not address hardware-level power control or pre-OS authentication.

An IEEE conference publication [4] demonstrated fingerprint authentication on Raspberry Pi using 1:N minutiae matching with remote cloud template storage, introducing authentication latency and remote data exposure risk, both eliminated in the proposed system through on-device sensor flash memory.

A review of the literature examined in this study did not identify prior work combining a Raspberry Pi, fingerprint sensor, and relay module to physically control an ATX PWR_SW header as a hardware-level pre-OS boot authentication gate. This constitutes the primary research gap addressed by this paper.

III. METHODOLOGY

A. System Architecture

The system consists of two principal components: the Raspberry Pi 3B+ as the authentication controller and the R307S optical fingerprint sensor as the biometric input device. A 5V single-channel relay module controlled via GPIO BCM pin 7 (physical Pin 26) serves as the physical power gate. Fig. 1 illustrates the complete system architecture including data flow, component interactions, and key architectural characteristics.

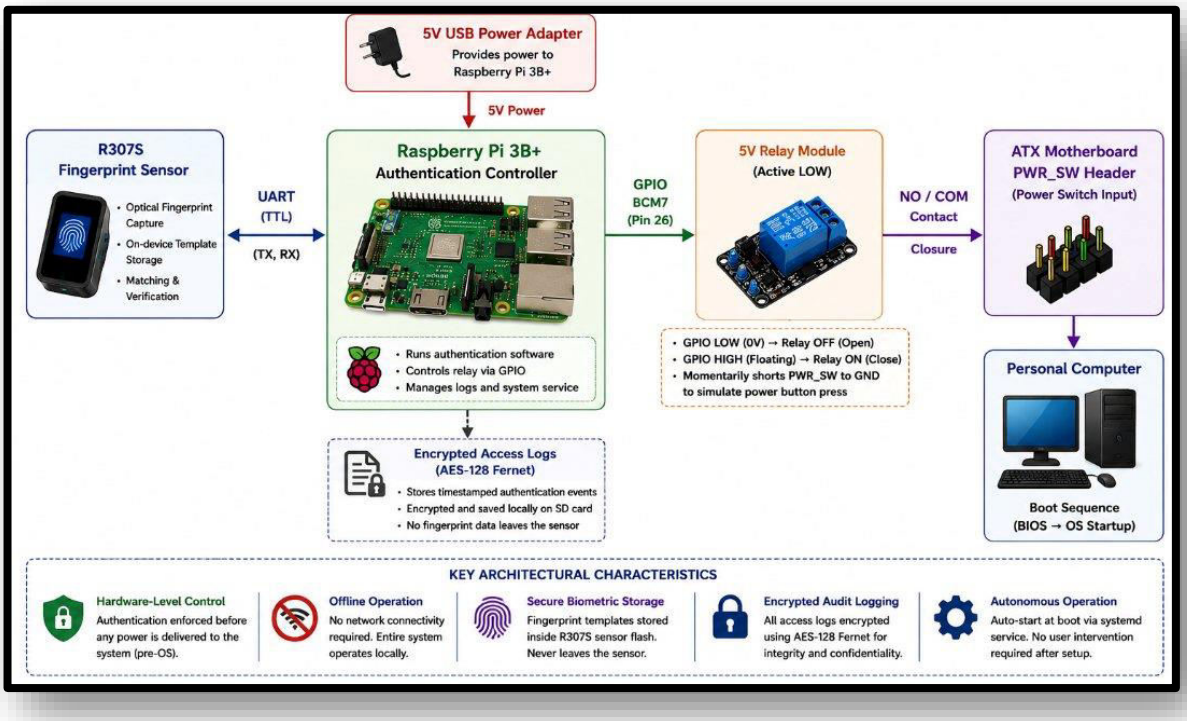


Fig. 1. System Architecture Diagram

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405108

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

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

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

B. Hardware Components and Wiring

Table I presents the hardware components. The R307S connects via UART: VCC (3.3V) to Pin 1, GND to Pin 6, sensor TX to RPi RXD (Pin 8, BCM GPIO15), and sensor RX to RPi TXD (Pin 10, BCM GPIO16). Bluetooth was disabled using dtoverlay=disable-bt to remap the hardware UART (ttyAMA0) to the GPIO header. The relay VCC connects to Pin 2 (5V), GND to Pin 14, and IN signal to Pin 26 (BCM GPIO7). Fig. 2 shows the complete wiring diagram with pin reference tables.

TABLE I. HARDWARE COMPONENTS

Component	Specification	Role in System
Raspberry Pi 3B+	1.4GHz Quad-Core, 1GB RAM, 40-pin GPIO, RPi OS 64-bit	Authentication controller
R307S Fingerprint Sensor	Optical UART TTL, 162 templates, FAR 0.001%, FRR 0.1%	Biometric input and 1:N matching
5V Relay Module	CYX RG GYX-3FC, Active LOW, NO/COM/NC terminals	Physical PWR_SW circuit gate
SanDisk MicroSD 32GB	Class 10, UHS-I	OS, code and encrypted log storage
5V USB Power Adapter	Micro USB, up to 3A output	Independent Raspberry Pi power supply

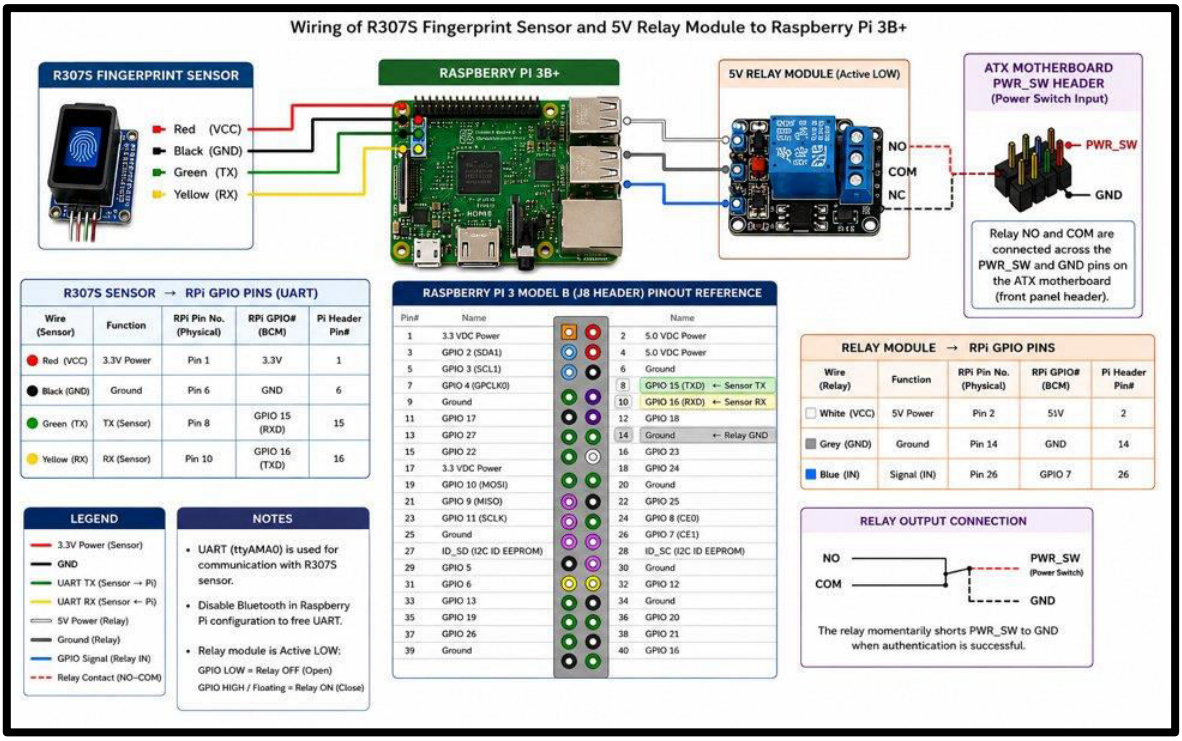


Fig. 2. Hardware Wiring Diagram with Pin Mapping Reference

C. Authentication Workflow

On power-up, systemd automatically launches start_auth.sh via fingerprint.service. The script introduces a startup delay to ensure UART availability, terminates any conflicting serial port process, then executes auth.py as root. GPIO pin 7 is initialized to OUTPUT LOW (relay standby), the Fernet key is loaded, and UART communication is established with the R307S at 57600 baud. The system polls readImage() continuously. On finger detection, convertImage() extracts a

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405108

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

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

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

minutiae template and searchTemplate() performs 1:N matching. Matches with score >= 50 trigger activate_relay(): GPIO is set to INPUT (floating) for one second, causing the Active LOW relay to close its NO-COM terminals and momentarily short the PWR_SW header. Fig. 3 illustrates the complete authentication flowchart and Fig. 4 shows the relay activation logic in detail.

Fig. 3. Authentication Workflow

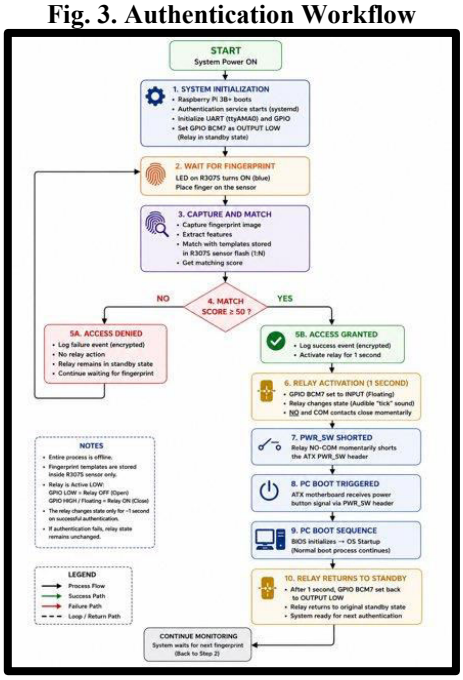
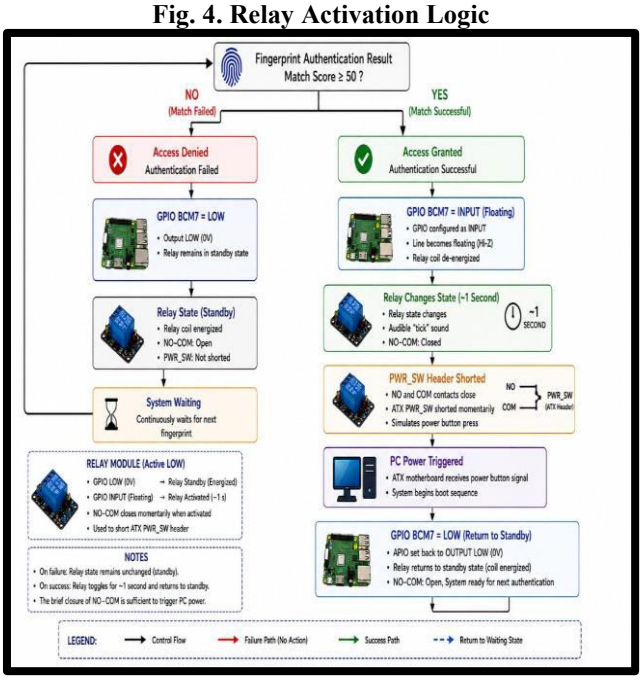


Fig. 4. Relay Activation Logic



D. Software Stack and Encryption

Table II presents the software components. Python 3.13 on Raspberry Pi OS (64-bit) serves as the runtime. Every authentication event is encrypted using Fernet symmetric encryption (AES-128-CBC with HMAC-SHA256) and appended to access_log.enc. The 32-byte key is stored separately in secret.key. The systemd fingerprint.service is configured with Restart=always and RestartSec=3, providing automatic recovery within 30 to 45 seconds after power interruption.

TABLE II. SOFTWARE STACK

Library / Component	Version	Purpose
Python	3.13	Core programming language
pyfingerprint	1.5	R307S UART communication and template matching
RPi.GPIO	0.7.1	GPIO relay control
cryptography (Fernet)	43.0.0	AES-128-CBC log encryption with HMAC-SHA256
pyserial	3.5	Low-level UART serial interface
systemd	—	Auto-start service and process management

IV. RESULTS AND DISCUSSION

A. Authentication Session Results

The prototype was validated through 15 defined test cases covering all functional and non-functional requirements including authorized authentication, unauthorized rejection, low accuracy score filtering, relay hardware trigger, UART communication stability, systemd auto-start, reboot persistence, sensor disconnection handling, and power interruption

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

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

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

recovery. All 15 test cases passed. Fig. 5 shows the actual terminal output from authentication sessions during prototype testing.

```
2026-05-06 19:45:12 | System started – Waiting for fingerprint...
2026-05-06 19:45:26 | GRANTED | User: Sakthiganesh | Finger: Right Thumb | Score: 174
2026-05-06 19:45:29 | GRANTED | User: Sakthiganesh | Finger: Right Thumb | Score: 176
2026-05-06 19:45:33 | GRANTED | User: Sakthiganesh | Finger: Right Thumb | Score: 109
2026-05-06 19:46:26 | GRANTED | User: sakthi | Finger: Right Thumb | Score: 131
2026-05-06 19:46:29 | GRANTED | User: Sakthiganesh | Finger: Right Thumb | Score: 261
2026-05-06 19:55:15 | System started – Waiting for fingerprint...
2026-05-06 19:55:21 | ERROR | The image contains too few feature points
2026-05-06 19:55:23 | GRANTED | User: Sakthiganesh | Finger: Right Thumb | Score: 84
2026-05-06 19:55:27 | GRANTED | User: sakthi | Finger: Right Thumb | Score: 97
2026-05-06 19:55:30 | GRANTED | User: Sakthiganesh | Finger: Right Thumb | Score: 160
2026-05-06 19:55:35 | DENIED | Unknown finger | Access refused
2026-05-06 19:55:38 | GRANTED | User: Sakthiganesh | Finger: Right Thumb | Score: 270
ganesh@Rasberrypi:~ $
```

Fig. 5. Terminal Output Showing Authentication Session Results (Decrypted Log)

B. Performance Metrics

Table III summarizes the key performance metrics observed during prototype evaluation. Authentication response time was measured from finger placement to relay activation using Python datetime timestamps. FAR and FRR values are cited from the R307S sensor datasheet and were not independently measured in this prototype study.

TABLE III. SYSTEM PERFORMANCE METRICS

Metric	Value / Notes
Authentication Response Time	< 1 second (finger placement to relay activation)
Accuracy Score Range Observed	52 — 270 (average ~170)
Minimum Accepted Score (MIN_SCORE)	50 — determined empirically through iterative testing
False Acceptance Rate (FAR)	0.001% (R307S sensor datasheet specification)
False Rejection Rate (FRR)	0.1% (R307S sensor datasheet specification)
Maximum Template Storage	162 fingerprints (onboard R307S sensor flash)
System Startup Time	30 – 45 seconds after power-on (includes UART stabilization)
Power Interruption Recovery	30 – 45 seconds (automatic via systemd Restart=always)
Prototype Test Cases Passed	15 / 15 (100% of defined functional test cases)

C. Comparison with Existing Systems

Table IV compares the proposed prototype with related prior work across key features.

TABLE IV. COMPARISON WITH EXISTING SYSTEMS

Feature	Karthik [1]	Arunkumar [2]	Heamalatha [3]	Proposed
Security Level	Application	Application	Application	Hardware (Pre-OS)
Cloud / Network	Required	Required	Required	Not required

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

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

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

Feature	Karthik [1]	Arunkumar [2]	Heamalatha [3]	Proposed
Template Storage	Cloud server	Remote DB	Local uC	On-device sensor flash
Log Encryption	No	No	No	AES-128-CBC Fernet
PC Boot Control	No	No	No	Yes (relay prototype)
Auto-Start Service	No	No	No	systemd daemon
Offline Operation	No	No	Partial	Fully offline

V. CONCLUSION AND FUTURE WORK

This paper presented a proof-of-concept prototype of a hardware-level PC boot authentication system using fingerprint biometrics on a Raspberry Pi 3B+. The prototype demonstrates that intercepting the ATX PWR_SW header through an Active LOW relay module is a viable approach to enforce pre-OS biometric verification, eliminating the software-bypass vulnerabilities inherent in conventional authentication schemes. The prototype achieves sub-second authentication response times, complete offline operation, on-device fingerprint template storage, AES-128 Fernet encrypted audit logging, and autonomous systemd service management — with all 15 defined functional test cases passing successfully.

The proposed system offers a cost-effective, hardware-agnostic solution designed for ATX-compliant desktop computers without permanent modification. Future work includes full end-to-end validation with an ATX desktop PC PWR_SW header connection, the integration of a manual bypass switch to facilitate maintenance operations and emergency access scenarios, TPM integration for complementary post-boot OS integrity verification, multi-factor authentication combining fingerprint with PIN, wireless enrollment and remote log monitoring, and extension to support multiple PC units through relay multiplexing.

REFERENCES

[1] S. V. Karthik, J. Subhash, N. K. Baskaran, and P. Suresh, "Fingerprint Authentication using Raspberry Pi based on IoT," Int. J. Novel Res. Dev., vol. 8, no. 1, 2023.
[2] L. Arunkumar and A. Arun Raja, "Biometrics Authentication Using Raspberry Pi," Int. J. Trends Eng. Technol., vol. 5, no. 2, pp. 25–28, May 2015, ISSN: 2349-9303.
[3] I. Heamalatha et al., "IoT based Biometric Student Access Control and Attendance Management," IJRASET, vol. 11, 2023. doi: 10.22214/ijraset.2023.50783.
[4] N. Jain, A. Sharma, and R. Kumar, "Fingerprint Based Authentication System Using Raspberry Pi," in Proc. IEEE Int. Conf. Computing, Communication and Automation (ICCCA), Greater Noida, India, 2017, pp. 1-5. doi: 10.1109/CCAA.2017.8229986.
[5] R. Bhagat, S. Patil, and M. Desai, "IoT based Smart Attendance System using Fingerprint and NodeMCU," IJRASET, vol. 10, 2022.
[6] Raspberry Pi Foundation, "Raspberry Pi 3 Model B+ Product Brief," 2018. [Online]. Available: https://www.raspberrypi.com. [Accessed: May 2026].
[7] GROW Technology, "R307 Optical Fingerprint Module User Manual," Ver. 1.2, 2020. [Online]. Available: https://www.openhacks.com/uploadsproductos/r307_fingerprint_module.pdf.
[8] Python Cryptography Project, "Fernet Symmetric Encryption Documentation," Ver. 43.0, 2024. [Online]. Available: https://cryptography.io. [Accessed: May 2026].

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