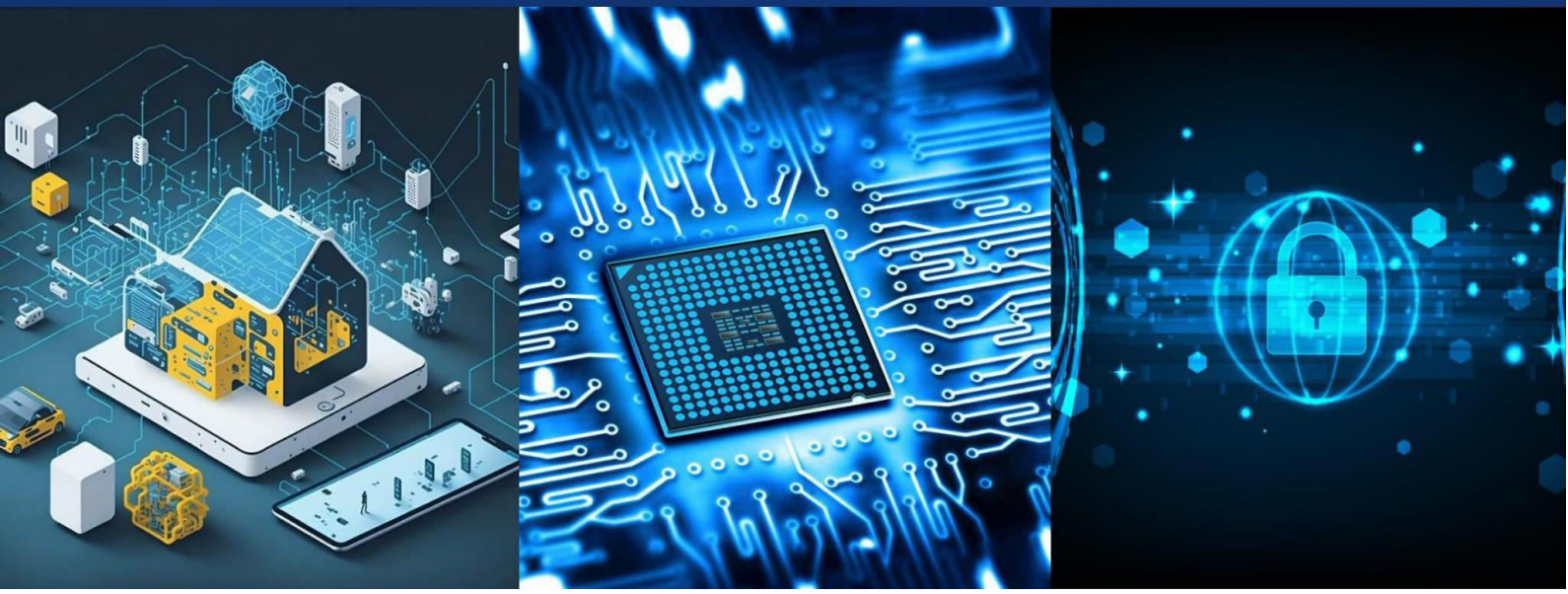
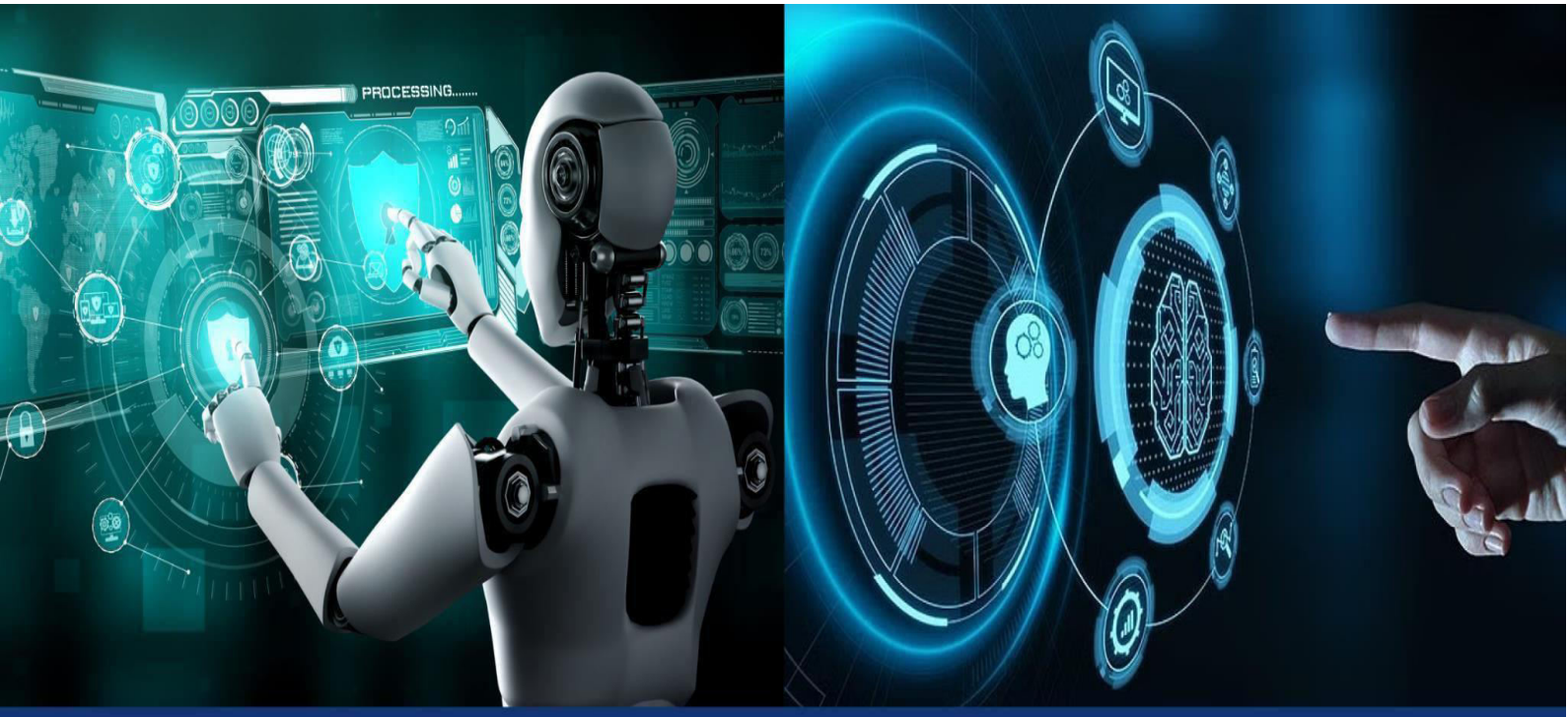
ISSN(O): 2320-9801
ISSN(P): 2320-9798



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 1, January 2026**

© 2026 IJIRCCE | Volume 14, Issue 1, January 2026| DOI:10.15680/IJIRCCE.2026.1401051

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)

Design and Implementation of Three Level Security

Gella Uday Kumar[1], KP Jyothi Bhuvan[2], Nithish Gowda H[3], Puvi Krishna K[4], Malatesh S H[5]

Student, Dept. of Computer Science and Engineering, MS Engineering College, Bengaluru, Karnataka, India[1-4]

HOD, Dept. of Computer Science and Engineering, MS Engineering College, Bengaluru, Karnataka, India[5]

ABSTRACT: The advancement of embedded systems and security technologies has created new possibilities in the field of access control and safety. Traditional mechanical locks and single-factor authentication systems often lack adequate protection, traceability, and resistance to unauthorized access. This paper presents a Three-Level Door Security System using RFID, Fingerprint Authentication, and GSM-Based OTP Verification, designed to provide robust and reliable access control. The system verifies users through RFID identification, biometric fingerprint matching, and one-time password validation sent via GSM communication. It ensures that access is granted only when all authentication levels are successfully verified, significantly enhancing security. The system is implemented using an Arduino microcontroller with integrated sensors, a GSM module, relay-based door control, and an LCD interface, operating in a standalone embedded environment. Performance evaluation shows fast authentication response, high verification accuracy, stable operation, and reliable GSM communication. The proposed system demonstrates an effective and cost-efficient approach to implementing secure, multi-factor access control for residential and institutional applications.

KEYWORDS: Embedded Systems, Door Security System, RFID Authentication, Fingerprint Recognition, OTP Verification, GSM Module, Access Control, Microcontroller-Based Security

I. INTRODUCTION

Security is undergoing rapid transformation with the integration of embedded systems, biometric technologies, and wireless communication. Modern security requirements demand reliable, automated, and multi-layered protection mechanisms rather than traditional mechanical locking systems. Access control in residential, commercial, and institutional environments requires high accuracy, fast response, and strong resistance to unauthorized entry, which is often difficult to achieve using single-factor authentication methods alone.

Multi-factor security systems provide a robust and user-friendly approach to access control by combining multiple authentication techniques. Although several electronic locking systems exist, many rely on a single verification method and lack enhanced protection against theft, duplication, or impersonation. To address these limitations, this paper proposes a Three-Level Door Security System using RFID, fingerprint authentication, and GSMbased OTP verification that operates as a standalone embedded solution and provides secure, automated, and reliable access control through layered authentication.

II. RELATED WORK

Several research studies have focused on electronic access control systems, biometric authentication, and RFID-based security mechanisms. RFID-based door security systems provide fast and contactless identification, but they are vulnerable to card loss, duplication, or unauthorized use. Biometric-based systems such as fingerprint recognition enhance security by verifying user identity; however, they may suffer from false rejections due to sensor limitations or environmental conditions.

Multi-factor authentication systems combine two or more verification methods to improve security and reliability. GSM-based OTP systems add an additional layer of protection by validating user possession of a registered mobile device, but they depend on network availability. The proposed system integrates the advantages of RFID authentication,

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)

biometric fingerprint verification, and GSMbased OTP validation into a single embedded platform, providing a more secure, reliable, and cost-effective access control solution.

SYSTEM ARCHITECTURE

The proposed system follows a modular architecture consisting of five main layers:

- **Input Layer:** Captures user credentials through RFID card scanning and fingerprint sensing.
- **Verification Layer:** Validates RFID UID, fingerprint templates, and OTP entered via keypad.
- **Communication Layer:** Handles OTP transmission using GSM module for mobile verification.
- **Control Layer:** Manages authentication decisions and controls the relay-based door lock.
- **Display & Logging Layer:** Displays system status on LCD and records access attempts.

This layered architecture ensures high security, scalability, easy maintenance, and efficient system performance.

III. METHODOLOGY

The system workflow begins with capturing user credentials through RFID card scanning. The scanned card UID is verified against the authorized database, followed by biometric fingerprint authentication to confirm the user's identity. Upon successful verification, a one-time password (OTP) is generated and sent to the registered mobile number using the GSM module. The entered OTP is validated to ensure final authentication. Based on the verification results, the relay-controlled door lock is activated to grant or deny access. System status messages and authentication feedback are displayed on the LCD, and access attempts are recorded for monitoring and analysis.

SYSTEM IMPLEMENTATION

The system is implemented using Embedded C programming on an Arduino microcontroller platform. RFID authentication, fingerprint verification, and GSM-based OTP communication are handled using dedicated hardware modules and Arduino libraries. The LCD display is controlled through I²C communication for real-time status updates. The modular implementation includes separate modules for RFID scanning, fingerprint matching, OTP generation and verification, relay-based door control, display handling, and access logging. This approach simplifies testing, improves reliability, and allows easy future enhancements.

PERFORMANCE EVALUATION

Performance evaluation was conducted to assess system efficiency, accuracy, and stability. The system demonstrated quick response time during RFID detection, fingerprint verification, and OTP validation under normal operating conditions. Authentication operations were reliable, and the system remained stable during repeated access attempts. The evaluation confirms that the system performs effectively on embedded hardware for real-time access control and security applications.

IV. RESULTS AND DISCUSSION

The system successfully verified user access through RFID authentication, fingerprint verification, and GSM-based OTP validation. The layered authentication approach effectively prevented unauthorized access while ensuring smooth and quick operation for authorized users. The results show that the proposed security system provides reliable access control, enhances safety, and improves overall system security.

V. CONCLUSION AND FUTURE SCOPE

The Three-Level Door Security System using RFID, Fingerprint Authentication, and GSM-Based OTP Verification successfully demonstrates how embedded systems and security technologies can be combined to create a reliable and robust access control solution. The system provides secure authentication, stable performance, and improved protection against unauthorized access for residential and institutional environments.

Future enhancements may include integration of advanced biometric methods such as facial recognition, mobile application-based monitoring, cloud storage for access logs, AI-based intrusion detection, and smart home or building automation integration to further enhance security and usability.

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)

REFERENCES

[1] Stallings, W., Cryptography and Network Security: Principles and Practice, 7th Edition, Pearson Education, New Jersey, 2017.
[2] Arduino Documentation, Arduino Uno and Embedded C Programming, Available: https://www.arduino.cc
[3] Want, R., "An Introduction to RFID Technology," IEEE Pervasive Computing, vol. 5, no. 1, pp. 25–33, 2006.
[4] Maltoni, D., Maio, D., Jain, A. K., and Prabhakar, S., Handbook of Fingerprint Recognition, 2nd Edition, Springer, New York, 2009.
[5] SIMCom Wireless Solutions, SIM800 GSM/GPRS Module Hardware Design, Technical Documentation, 2015.
[6] Dr. Malatesh S. H., S. Kattimani, P. Pallabavi, V. A. P., and D. M. G., "Intruder Detection and Protection System," International Journal of Innovative Research in Technology (IJIRT), vol. 11, no. 12, p. 6287, May 2025, ISSN: 23496002.

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