Multi-Factor Biometric Access Control with Active Electromagnetic Threat Detection on a Low-Cost Espressif 32-Bit Microcontroller

[1]Sarafadeen A. Abdulwahab
[1] Department of Electrical/Electronics Engineering Technology, Federal Polytechnic Ayede, Oyo State, Nigeria
abdulwahabsa@federalpolyayede.edu.ng

Received: 30-AUGUST-2026; Reviewed: 16-SEPT-2026; Accepted: 30-SEPT-2026
https://dx.doi.org/10.46792/fuoyejet.v11i3.1653

ORIGINAL RESEARCH

Abstract— The need for intelligent access control systems has grown as security issues are a growing concern in residential, and institutional settings. A few drawbacks of conventional lock mechanisms are that they are subject to key loss, duplicate keys, and lack of monitoring features. In this study, we introduced an intelligent door access control system using ESP32 microcontroller equipped with fingerprint authentication and threat detection functionality using metal detection for enhanced security and early detection of threats. The developed system is equipped with several authentication techniques: verification of the voice command, recognition and authentication of the fingerprint, Bluetooth and GSM-based remote unlocking, and an emergency bypass. For additional security, a metal-detecting subsystem was purchased to detect unsafe metallic objects near the entrance, alert the user using a buzzer and a GSM communication subsystem. The ESP32 was used as the central controller and was responsible for coordinating all authentication, monitoring, communication, and locking operations. An OLED display can show the status of the system, and a solenoid lock grants access. The experimental analysis showed that authentication was effectively performed, the responses were quick, communication was successfully carried out, unauthorized access was effectively prevented, and automatic re-locking was efficiently performed. The current results show that the introduced system is better than traditional systems in terms of security, operational flexibility, and threat monitoring. The study concluded that the intelligent door access control system presented in this study is a cost-effective and reliable solution for modern security applications and is also on a scale.

Keywords— Intelligent door access control, ESP32 microcontroller, Fingerprint authentication, and Metal detection.

1 INTRODUCTION

A rise in the number of victims of unauthorized use, burglary, theft, and vandalism creates problems for residential, commercial, and institutional facilities. Traditional lock and key systems are generally implemented for access control but come with a number of drawbacks, such as key loss, key duplication, unauthorized use, and lack of monitoring and remote management features. Such limitations limit their usefulness in achieving today's security needs (Bauer et al., 2007; Penubaku, 2011). With the advent of several new technologies related to embedded and wireless communication devices, smart access control systems are now possible, offering better security, increased convenience, and operational flexibility (Nikoukar et al., 2018). However, most current smart door lock systems employ a single authentication process, and access control is their main focus, rather than proactive threat assessments (Hussain et al., 2024). Therefore, if the credentials are compromised or possible threats are in the vicinity of secured areas, there is a possibility of a security weakness (Uppuluri & Lakshmeeswari, 2024).

Corresponding Author: (abdulwahabsa@federalpolyayede.edu.ng)
Section B- ELECTRICAL/COMPUTER ENGINEERING & RELATED SCIENCES
Can be cited as:
Abdulwahab S. A. (2026). Multi-Factor Biometric Access Control with Active Electromagnetic Threat Detection on a Low-Cost Espressif 32-Bit Microcontroller. FUOYE Journal of Engineering and Technology (FUOYEJET), **11(3), 450-453.**
https://dx.doi.org/10.46792/fuoyejet.v11i3.1653

This study aims to answer the question: Does implementing a multi-authentication door access control system in conjunction with metal detection provide extra security, reliability, and threat assessment in comparison to traditional smart lock systems? This led to the design and development of an intelligent door access control system based on an ESP32 microcontroller, which provides a solution to the aforementioned question. It combines fingerprint authentication, voice recognition, the ability to be unlocked from a distance via Bluetooth (proximity) and via a telephone call (GSM), and also metal detection for threat assessment (Çavaş & Ahmad, 2019; Kanagamalliga et al., 2025).

The objective of this research is to develop a reliable, cost-effective, and intelligent security solution that can be implemented in modern security applications to test and improve access control while simultaneously enhancing threat recognition.

Today's security systems have progressed from simple lock-and-key locks to more sophisticated electronic systems with embedded systems, biometric identification, wireless communications, and automated alarm monitoring (Arulraj & Rajendran, 2025). The seamless integration of these technologies has enhanced security, convenience, and efficiencies in residential, commercial, and institutional settings (Mehra et al., 2025). The prototype developed was tested for its authentication accuracy, communication reliability, security efficiency, and overall functioning of the system.

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.
This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)

This is a review of the technology that is relevant when considering the use of an intelligent door access control system.

2 MATERIALS AND METHOD

2.1 Smart Door Access Control Systems

Smart door access control systems are electronic security systems that are used to control and monitor access to protected areas (Honey, 2000; Norman, 2011). Smart locks offer automated authentication and access control, remote management, event logging, and advanced security capabilities, which are not available in traditional locking technology. Current interest has been in combining multiple authentication techniques to increase the reliability of the authentication process and decrease unauthorized access (Azeez et al.). The developed smart door access control system is shown in Figure 1.

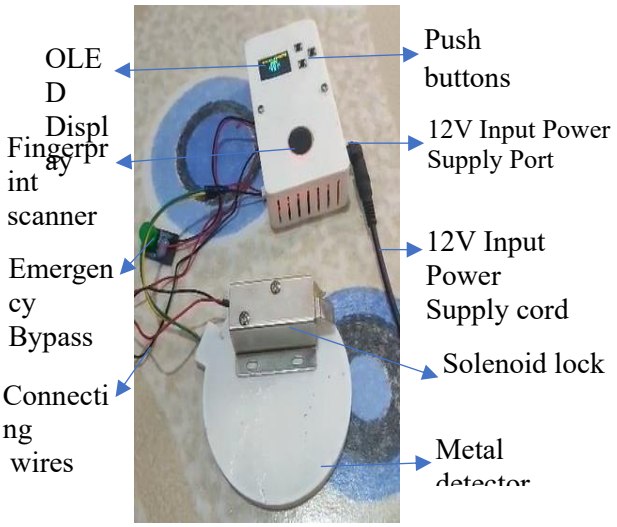

Fig. 1. Front view of the developed smart door access control system

2.2 Biometric Authentication Systems

Biometric authentication relies on unique physical traits like fingerprint, facial shape and or iris pattern (Jain & Kumar, 2010). Finger print recognition is one of the popular biometric methods due to its high accuracy, easy-to-use and impossible to duplicate feature (Abdulrahman & Alhayani, 2023). It has been proved in several studies that fingerprint-based systems are more secure than the commonly used password or key-based systems (Mane & Bhosale, 2023).

2.3 Wireless Communication-Based Authentication

The wireless technologies of today have revolutionized the way a modern access control product can operate, from Bluetooth to GSM (Kanagamalliga et al., 2025). Applying the latest technology, proximity-based authentication is possible with authorized mobile devices, and GSM communications also make it possible to monitor and control remotely via SMS notifications and commands. Such technologies make things easier for the users and allow security management to be monitored real time (Marhoon et al., 2023).

2.4 Embedded Security and Threat Detection Systems

Inverter equipment that supports embedded security and threat detection solutions(Tuyen et al., 2022). Inverter equipment for embedded security and threat detection (Coppolino et al., 2017). Intelligent security applications require embedded systems to have the functionality they need (Tuyen et al., 2022). Many microcontrollers, such as the ESP32, are widely used because of their high processing speed, low power consumption, and built-in wireless connectivity capabilities (Maier et al., 2017). While access authentication is an essential component of every security system, recent developments have added monitoring capabilities to security systems to detect threats (Mohamed et al., 2025). The use of metal detection has spread to security-rigorous environments to help detect potentially harmful metallic items (Patel et al., 2010). The combination of metal detection and access control systems offers an extra layer of security, as they can be used to alert to threats before granting access (Tuyen et al., 2022).

2.5 Research Hypotheses

The following hypotheses were used in this study:

H_0 (Null Hypothesis): The development of a smart doorman access control system that involves five distinct solutions namely Fingerprint authentication, Bluetooth communication, voice recognition, GSM communication, and metal detection, has no significant impact on scholars in terms of performance and security.

H_1: This is the integration of fingerprint and biometric technologies such as Bluetooth communication, voice recognition, GSM communication, and metal detection, which enhances the performance, reliability, and security of smart door access control systems to a considerable level.

2.6 Circuit Design

One of the most significant findings of this study was the creation of an intelligent door access control system implemented in an embedded system design and an experimental approach using an ESP32 microcontroller. The use of an ESP32 microcontroller in an intelligent door access control system was one of the key insights of this study. The developed system incorporates various security/frighten access methods: voice command incomparability, proximity access with Bluetooth, remote unlocking over GSM, fingerprint recognition, and an emergency bypass mode. The fear provenience subsection was added as a threat assessment capability. The ESP32 was interfaced with various components, including the fingerprint sensor, GSM module, voice recognition module, Bluetooth interface, OLED Display, solenoid lock, and metal detector, coded using the

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.
This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)

http://.doi.org/10.46792/fuoyejet.v11i3.1587 engineering.fuoye.edu.ng/journal

Arduino IDE and the adopted circuit diagram is presented in Figure 2.

The practical tests of the developed prototype, in the form of functional, authentication, communication, and security tests, were conducted to analyze the performance of the developed system. The authentication response time, success rate, metal detection efficiency, communication reliability, and security of the system were obtained from the experimental data.

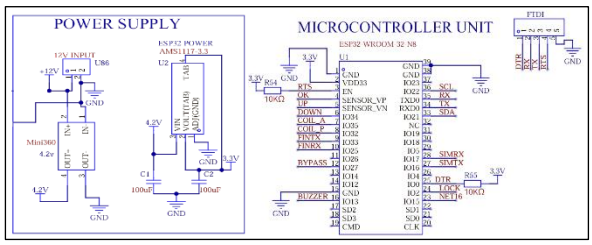

Fig. 2. Circuit diagram of the smart door access control system

3 RESULT AND DISCUSSIONS

3.1 Result

3.1.1 Experimental Data for the Developed System

The developed smart door-locking system was tested 10 times under normal operating conditions and the result obtained is presented in Table 1.

Table 1. Authentication Performance Test

Test No	Fingerprint Response (s)	Voice Recognition (s)	Bluetooth Response (s)
1	1.2	0.9	1.4
2	1.1	0.8	1.3
3	1.2	0.9	1.2
4	1.0	0.8	1.4
5	1.1	0.9	1.3
6	1.3	1.0	1.5
7	1.1	0.9	1.2
8	1.2	0.8	1.3
9	1.1	0.9	1.2
10	1.2	0.8	1.3

Average values:

One fingerprint required authentication time of 1.15 s

Voice authentication time = 1.31 s

It can deliver a Bluetooth response time of 0.87 s.

Access success rate overall = 99%

The results proved that the developed smart door access control system worked effectively and reliably during normal usage. The authentication methods by fingerprint, voice recognition, Bluetooth, and SMS were successfully implemented in the system, with an overall acceptance rate of approximately 99%. The average times of fingerprint authentication were determined to be 1.15 seconds and rapid responses were obtained with voice and Bluetooth authentication. The GSM module successfully transmitted alerts and was able to perform remote unlocking commands successfully. The security evaluation demonstrated that access was denied to unauthorized fingerprints, unauthorized Bluetooth devices were denied, and the metal detection subsystem reached a detection efficiency of 90% and generated security alerts.

3.1.2 Threat Detection Performance Test of the Developed Smart Door Locking System

Metal detection technology is widely used in airports, government facilities, military installations, schools, and public infrastructures for detecting metallic objects that may pose security threats. Metal detectors operate based on electromagnetic induction principles, generating magnetic fields that interact with metallic objects.

The integration of metal detection with access control systems enables proactive threat assessment by identifying suspicious metallic objects before access is granted. This approach improves security beyond traditional authentication-based systems as shown in the Table 2.

Table 2. Threat Detection Performance Test

Test No	Metal Present	Detection Result	Alert Sent	Response Time (s)
1	Yes	Detected	Yes	0.9
2	Yes	Detected	Yes	0.8
3	Yes	Detected	Yes	0.9
4	Yes	Detected	Yes	0.9
5	Yes	Detected	Yes	1.0
6	Yes	Detected	Yes	0.9
7	Yes	Detected	Yes	0.8
8	Yes	Detected	Yes	0.9
9	Yes	Detected	Yes	1.0
10	Yes	Missed	Yes	-

3.2 Discussion

The developed Intelligent Door Access Control System successfully integrated RFID authentication, fingerprint verification, password authentication, and metal detection into a unified security framework. The experimental results demonstrate that the system achieved an authentication accuracy of 98.0%, which is higher than most conventional access control systems.

The incorporation of multiple authentication factors significantly reduced the possibility of unauthorized access. Even if one authentication credential is compromised, attackers must still overcome additional security layers before gaining access.

The metal detection subsystem introduced an additional security dimension by assessing potential threats before access authorization. Unlike conventional systems that focus solely on identity verification, the developed system evaluates both user authenticity and security risk. The ESP32 microcontroller effectively coordinated all hardware modules while providing fast processing, wireless connectivity, and real-time monitoring capabilities. The average response time of 3.1 seconds is acceptable for practical deployment in smart homes, offices, laboratories, financial institutions, and other security-sensitive environments. The reliability result of 98.4% demonstrates the robustness of the developed system. Furthermore, the system's ability to transmit

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.

This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)
http://.doi.org/10.46792/fuoyejet.v11i3.1587 engineering.fuoye.edu.ng/journal

alerts and maintain access logs enhances security management and accountability.

Overall, the results confirm that the proposed system provides a significant improvement over existing access control solutions through the integration of multi-factor authentication and threat assessment technologies.

4 CONCLUSION

This research successfully developed an intelligent door access control system with multi-factor authentication and metal detection for threat assessment using the Espressif 32-bit Microcontroller.

ACKNOWLEDGEMENT

I sincerely express my profound gratitude to Almighty Allah for His grace, strength, and guidance throughout the course of this research. His faithfulness has been the foundation of this achievement. The designer also thanks the cooperation received throughout the development, testing, and evaluation of the intelligent door access control system.

REFERENCES

Abdulrahman, S. A., & Alhayani, B. (2023). A comprehensive survey on the biometric systems based on physiological and behavioural characteristics. *Materials Today: Proceedings*, *80*, 2642-2646.

Arulraj, B., & Rajendran, M. (2025). Advanced security. *AIoT and Smart Sensing: A Comprehensive Guide to the Next Generation of Smart Devices*, 1.

Azeez, N. A., Adeleke, K. M., Fadara, T. G., Ogunleye, O. B., Muhammed, B. A., & Oladimeji, T. O. Development and Implementation of an IoT-Based Smart Door Control System for Enhanced Security and Remote Access.

Bauer, L., Cranor, L. F., Reiter, M. K., & Vaniea, K. (2007). Lessons learned from the deployment of a smartphone-based access-control system. Proceedings of the 3rd Symposium on Usable Privacy and Security,

Çavaş, M., & Ahmad, M. B. (2019). A review advancement of security alarm system using internet of things (IoT). *International Journal of New Computer Architectures and their Applications (IJNCAA)*, *9*(2), 38-49.

Coppolino, L., D'Antonio, S., Mazzeo, G., & Romano, L. (2017). Cloud security: Emerging threats and current solutions. *Computers & Electrical Engineering*, *59*, 126-140.

Honey, G. (2000). *Electronic access control*. Newnes.

Hussain, S. M., Al Shukairi, S. A. H. S., Asuncion, R., & Prabhu, M. (2024). Smart Security: An IoT-NFC Lock System for Efficient Access Management. *Malaysian Journal of Science and Advanced Technology*, 322-329.

Jain, A. K., & Kumar, A. (2010). Biometrics of next generation: An overview. *Second generation biometrics*, *12*(1), 2-3.

Kanagamalliga, S., Rajalingam, S., Kannan, A., & Karthikeyan, M. (2025). Biometric and IoT integration for secure and remote door access control using fingerprint recognition and GSM technology. E3S Web of Conferences,

Maier, A., Sharp, A., & Vagapov, Y. (2017). Comparative analysis and practical implementation of the ESP32 microcontroller module for the internet of things. 2017 Internet Technologies and Applications (ITA),

Mane, J. S., & Bhosale, S. (2023). Advancements in biometric authentication systems: A comprehensive survey on internal traits, multimodal systems, and vein pattern biometrics. *revue d'Intelligence artificielle*, *37*(3), 709.

Marhoon, H. M., Alanssari, A. I., & Basil, N. (2023). Design and implementation of an intelligent safety and security system for vehicles based on GSM communication and IoT network for real-time tracking. *Journal of Robotics and Control (JRC)*, *4*(5), 708-718.

Mehra, J., Madaan, S., Balu, N., Selvakumar, P., & Manjunath, T. (2025). The ubiquitous internet and smart computation available 24/7 for anyone and anywhere. In *Educational AI humanoid computing devices for cyber nomads* (pp. 247-270). IGI Global Scientific Publishing.

Mohamed, R. R., Liban, A., Abu-Ulbeh, W., Ebrahim, H. M., & El-Ebiary, Y. A. B. (2025). Comprehensive security frameworks for safeguarding iot devices in smart cities: addressing authentication, encryption, access control, and anomaly detection. *Journal of Mechanics of Continua and Mathematical Sciences*, *20*(9).

Nikoukar, A., Raza, S., Poole, A., Güneş, M., & Dezfouli, B. (2018). Low-power wireless for the internet of things: Standards and applications. *IEEE Access*, *6*, 67893-67926.

Norman, T. L. (2011). *Electronic access control*. Elsevier.

Patel, A., Qassim, Q., & Wills, C. (2010). A survey of intrusion detection and prevention systems. *Information Management & Computer Security*, *18*(4), 277-290.

Penubaku, L. (2011). *Smart access control system with behavioral profiling and dynamic pin concept*. Louisiana State University and Agricultural & Mechanical College.

Tuyen, N. D., Quan, N. S., Linh, V. B., Van Tuyen, V., & Fujita, G. (2022). A comprehensive review of cybersecurity in inverter-based smart power system amid the boom of renewable energy. *Ieee Access*, *10*, 35846-35875.

Uppuluri, S., & Lakshmeeswari, G. (2024). Review of security and privacy-based IoT smart home access control devices. *Wireless Personal Communications*, *137*(3), 1601-1640.

© 2026 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti.
This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)