Jewel Journal of Scientific Research (JJSR) 10(2): 260–270, 2025
©Federal University of Kashere-Nigeria (Print ISSN: 2384 – 6267, Online ISSN 2756-651X)
https://journals.fukashere.edu.ng/index.php/jjsr

Real-Time Access Control System Using Radio Frequency Identification with Android Application

***[1]Odeyemi, C. S.**
[1]Department of Computer Engineering, School of Electrical Systems Engineering, Federal University of Technology, P. M. B. 704 Akure Nigeria.
***Corresponding author**: charityodeyemi@gmail.com, csodeyemi@futa.edu.ng; +2348066439866

Abstract
Access control bothers on ensuring that only authorized persons are granted access into a facility. Close circuit television (CCTV) system and the artificial intelligence based facial recognition technology, which are widely employed in access control systems are expensive and complex to operate and maintain. This study developed a smart, less expensive and easy to maintain door access enable system based on the radio frequency identification (RFID) technology. The design also incorporates an android application (App) which monitors and controls the door status remotely. RFID reader, relay and other electronics components were interfaced with NodeMCU microcontroller. The android application was developed to communicate with the hardware through the wireless fidelity (Wi-Fi) network. When tested, the system identified registered RFID tag and decline the unregistered one, opened the door and sent information to the app immediately. Alternative control was also provided through the mobile app for an authorized person who does not have a tag. At every point of testing, information transmission and reception was less than 4 seconds. The overall performance evaluation of the developed non-contact door access control system for this study performs favourably well with a response time less than 2.5 sec. which is within the standard real-time of 10 sec.

Keywords: Radio Frequency Identification, Android, Access Control, Security, Smart, Microcontroller
Received: 11th Sept, 2025 *Accepted:* 21th Nov, 2025 *Published Online:* 26th Dec, 2025

Introduction

The evolution of technology has significantly transformed the way we interact with our environment which requires effective security systems. In Africa, and other parts of the world, the demand for enhanced security measures and smart home solutions has been on the increase. Traditional lock and key systems are giving way to more sophisticated, convenient, and secure access control methods, in which RFID technology has gained prominence. The world, with its diverse socio-economic landscape, experiences several security and access control challenges. Residential and commercial properties require dependable security systems that not only safeguard against unauthorized access but also offer user-friendly functionalities (Aluri, 2020; Danjuma and Nwaizugbo, 2022). The traditional door lock systems are gradually becoming outdated in the face of advancing technology, necessitating the development of innovative solutions such as the use of RFID in conjunction with other technologies to address these issues.

RFID technology is a potent and versatile tool that can be effectively employed for access control. It enables secure, contactless authentication (Hao *et al.*, 2025), making it well-suited for various applications, including smart door locks. RFID allows users to gain

access with a simple swipe of an RFID card or tag, eliminating the need for physical keys, which are subject to losses and unauthorized duplication (Kamel and Memari, 2019; Lee *et al*., 2021). The integration of an Android App further enhances the usability and functionality of an RFID-based smart door system. This innovation aligns with the global trend towards smart homes and Internet of Things (IoT), empowering users to control and monitor their facilities, regardless of their physical location. Developing countries' market, especially those in Africa, offers unique opportunities for the implementation of such technologies. However, factors such as power supply reliability, internet connectivity, and cultural norms must be considered when designing and deploying smart home solutions (Abubakar *et al*., 2022; Tao *et al*., 2025).

This study focuses on bridging the existing gap between traditional access control systems and complex and expensive, modern technologically advanced solutions, catering for the specific needs and conditions of resource constraint countries. It explores the development of an RFID-based smart door lock system with an Android App, which has the potential to revolutionize the way Africans approach home and property security. By investigating the feasibility and usability of this system in the Nigerian context, this research not only contributes to the local technological landscape but also opens up new possibilities for securing homes and businesses while simultaneously enhancing convenience and control for users in Nigeria. This study addresses primary challenges, including inadequate security with conventional locks, mitigating loss and inconvenience due to traditional key vulnerabilities, limited access control, and the absence of real-time monitoring, especially when users need to grant access remotely. The aim is to design and implement an RFID-based smart door lock system integrated with an Android App to enhance security.

There have been advancements in the design of RFID smart lock systems. A smart lock system research presents a smart locking and unlocking system for home door security. Tilala *et al.* (2017) proposed a system that controls the door lock through an Android app using Wi-Fi as the communication protocol that communicates with WeMos D1 Wi-Fi module embedded in the door lock and the Firebase cloud messaging service. The system operates with the user's smartphone and WeMos D1 Wi-Fi module connected to the network. The database server and the Firebase cloud messaging service (FCM) were connected to the Wi-Fi module using the internet. The problem with this design is the delay in receiving messages which can act as a constraint to the system.

The research, focusing on a centrally controlled and enhanced security system (ACCESS) was a system for enhancing accessibility and security. It also includes surveillance mechanisms to monitor intruders and any movement around the homes, and remotely control of appliances through a mobile App. People access their homes and workplaces frequently every day and there are many problems associated with security and accessibility. Elderly people may face difficulty in walking repeatedly to open doors. Also, when there is a security breach like a theft, it becomes difficult to trace the people who visited the property. In a proposed system, a centrally controlled and enhanced security system (ACCESS), a manual method employed in locking was replaced by a mobile App, users can lock or unlock their doors using a mobile App (Gadupu *et al*. 2021). Also related work like using RFID authentication has been used for access control, where the door is opened by recognizing the RFID tag.

The development of a smart lock system based on the IoT and Cloud Platform project consists of a cloud server, a mobile phone App and a smart lock. Smart lock mainly included STM32 main control chip, digital keyboard module and WIFI module. The digital keyboard module used an infrared light signal to communicate with STM32 and supported digital keyboard password unlocking. The module was connected to the cloud platform of the Internet. The App was connected with the cloud platform to realize the remote control and management of the smart lock. In other to improve the reliability of the intelligent lock system, the fault-tolerant

mechanism of hardware and the secure key scheme of software was designed. After a normal operation and abnormal tests, the system was safe and reliable, suitable for smart home door locks and related appliances (Yin *et al.*, 2021).

Methodology

This section discusses the design and implementation of the RFID based access control door lock system with Android applications. The design of the main hardware system and the software system for this study were systematically presented.

Hardware Design

Figure 1 shows the system block diagram. The device makes use of a NODEMCU, an RFID reader, a servo motor, a buzzer, and a mobile application designed by the MIT app inventor. The system is powered by a rechargeable 5 v lithium-ion battery, so the system does not run out of power. The RFID reader reads the card and compares it with the data already stored on the microcontroller. If the RFID card/tag number matches what is in the database, the system triggers the motor and the buzzer to open the door. However, if the card/tag number does not match, it triggers the buzzer which sounds as an alarm system. In both cases, the system sends the information about the activities to the mobile application.

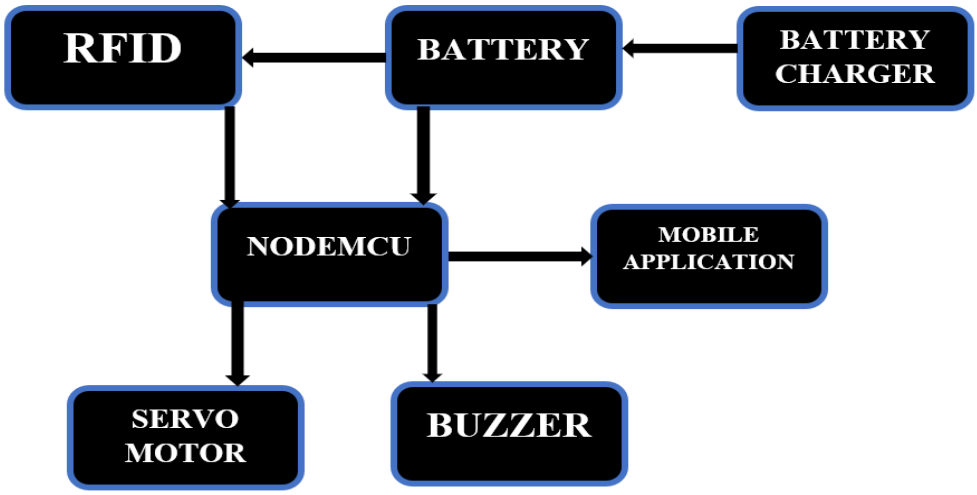

Figure 1: The System Block Diagram

Components and Connections

The RFID reader employed in this study has 8 pins (SDA, SCK, digital pin, MOSI, MISO, IRQ, GND, RST, 3.3V). The GND pin is connected to the GND of the NodeMCU, the 3.3V to the 3.3V pin, the SDA pin is connected to the D2 pin, SCK to pin D5, MOSI to pin D7, MISO to pin D6, RST to pin D1. The IRQ pin is not used for any connection. The RFID reader reads the RFID of the tag and sends it to the NodeMCU as shown in Figure 2

After the NodeMCU confirms that the RFID is on the database, it triggers the servo to turn. This allows the door to open. After ten seconds, the servo turns back in the reverse direction, thereby locks the door and prevents entrance without permission. The servo has three terminals (VCC, GND, and data). The VCC terminal is connected to the 3.3V pin of the NodeMCU, the GND to GND and the data terminal to the D3 pin of the NodeMCU as shown in Figure 2. The buzzer gives a sound to communicate the opening of the lock to the user. The buzzer has two terminals (positive and negative terminals). The negative terminal is connected to the ground (GND) and the positive terminal to the D4 terminal of the NodeMCU as shown in Figure 2.

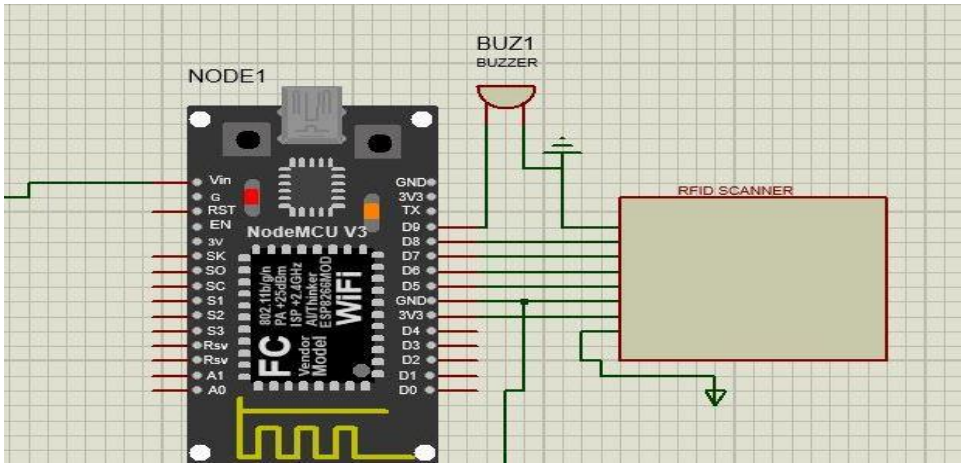

Figure 2: Layout Diagram of NodeMCU and RFID Reader with Buzzer

The system uses a 5 v lithium-ion battery. All the sensors are connected to the power and the ground of the battery to achieve a centralized power source, so all the devices have common ground and VCC. The schematic diagram of the system is shown in Figure 3.

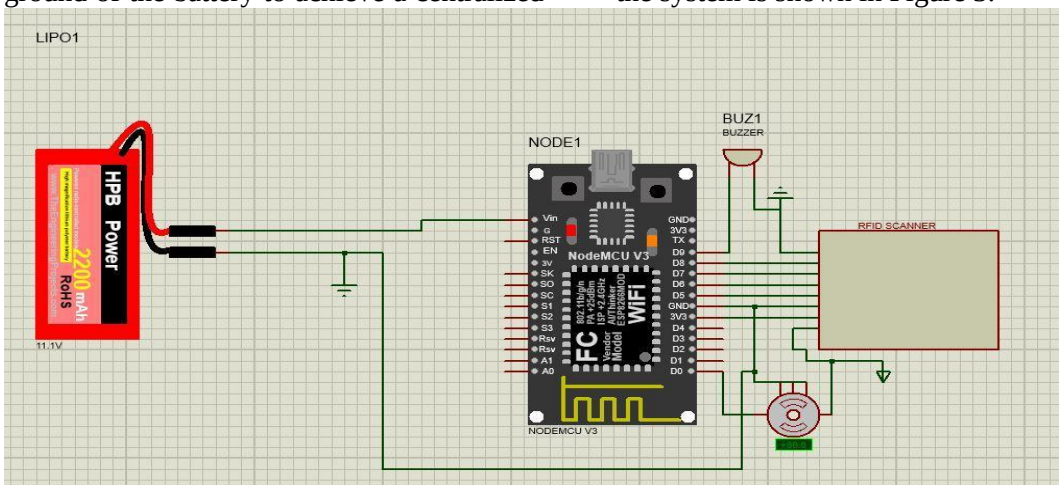

Figure 3: Full Circuit Diagram

The physical image of the internal section of the system showing the electronics components is as shown in Figure 4.

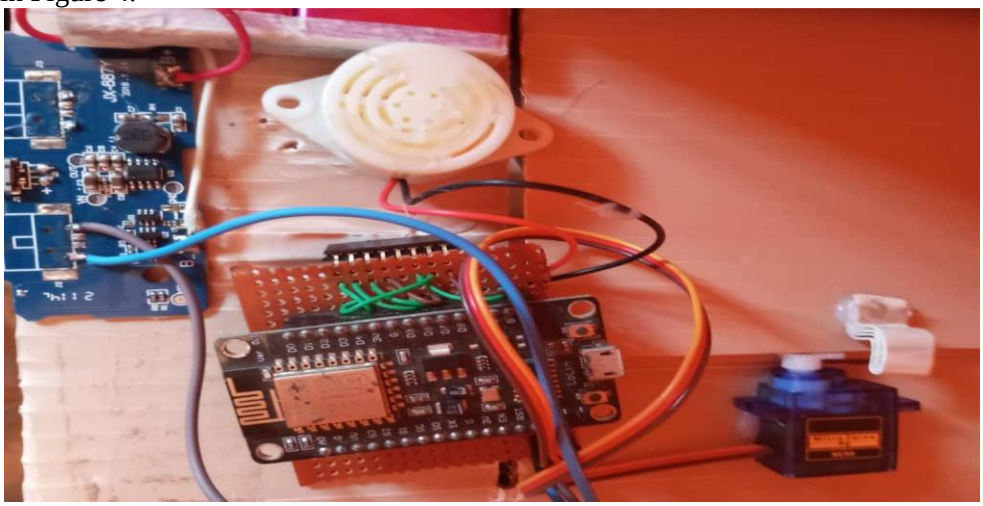

Figure 4: Internal part of the system

Software Development

The flowchart employed in developing the software aspect of the automatic access control system for this study is as shown in Figure 5.

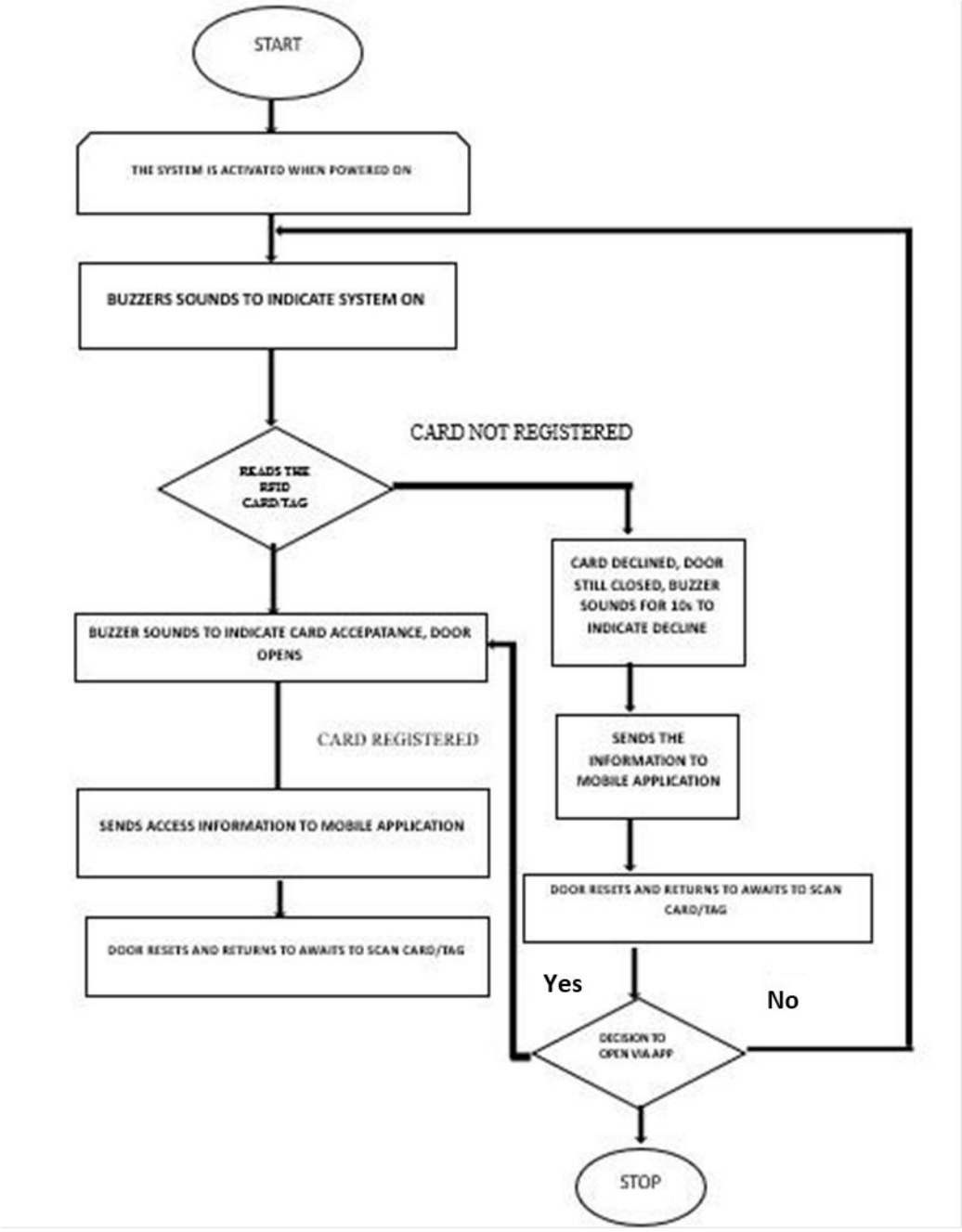

Figure 5: System Flowchart

Programming the microcontroller to communicate with the RFID module, servo, buzzer, and the MIT App Inventor server was carried out in the Arduino Integrated Development Environment (IDE). According to Theodoropoulos (2022), Arduino is an open-source platform for project development. Arduino is made up of a physical

programmable circuit board, this study employed NodeMCU as the microcontroller, which was powered from a computer using a USB cable. The code was built, debugged and compiled, then loaded to the NodeMCU. The software also includes the libraries for the sensors.

The screenshot of the MIT app inventor page which was used to develop the mobile application is as shown in Figure 6. Through the embedded program, the mobile application developed connects to the system and sends and receives data. The code was developed for the NodeMCU to get the RFID value of the RFID tag that comes in contact with the RFID reader. The RFID reader is connected to the microcontroller which helps in identifying the tag from the database. If the RFID tag is registered, the door is opened and the signal is sent to the database that the lock has opened.

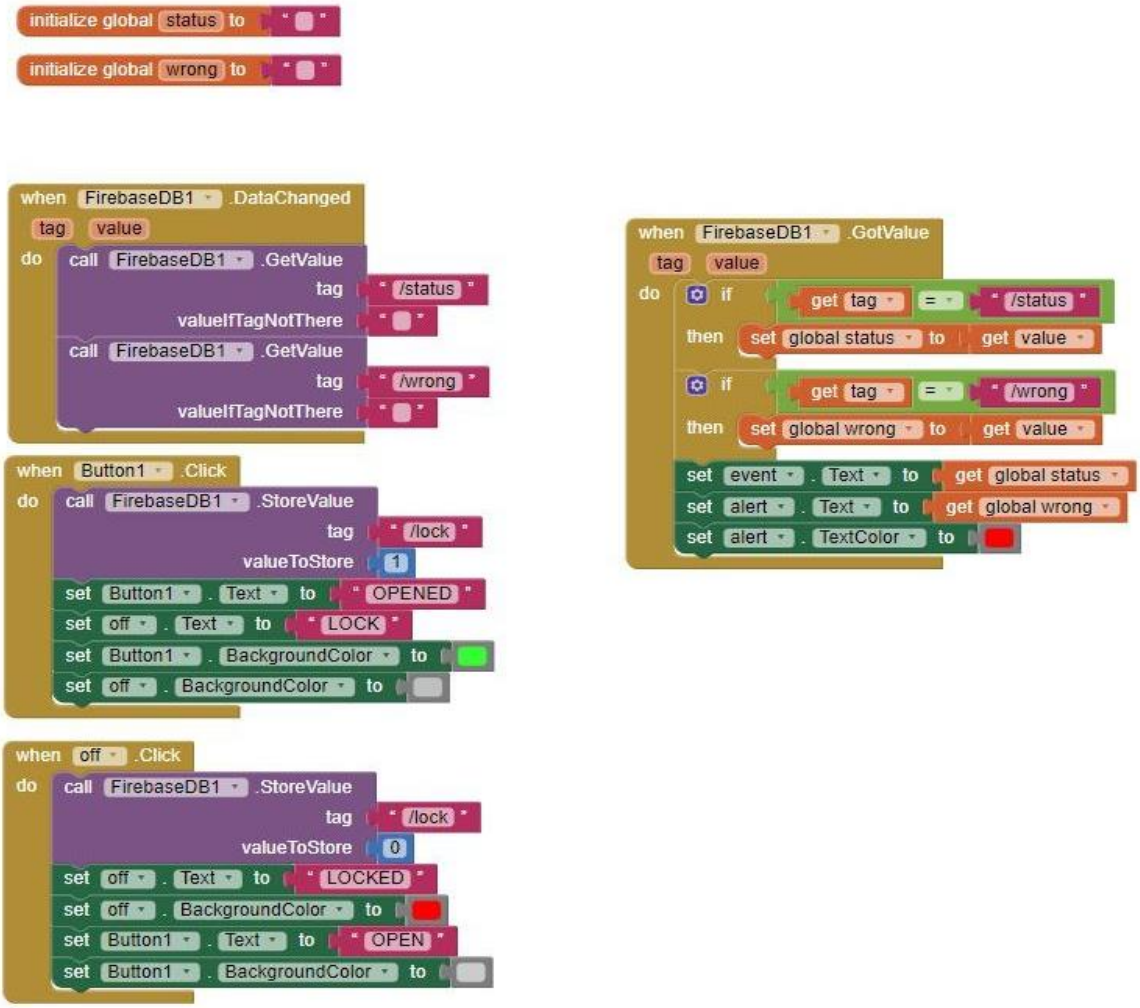

Figure 6: MIT App Inventor Code Developed

Integration and Fabrication

Integration focuses on combining different elements into a functioning whole, while fabrication involves the physical construction or manufacturing of components and systems. The RFID smart door lock system with Android App was housed in a plastic (PVC) enclosure that has an in-built battery and a charging port. Finally, this study employs the use of NodeMCU microcontroller, RFID reader, the servo, and MIT App Inventor to build a non-contact smart door system. The system can read the RFID tag, check if it is registered and open the door. This system also sends data to the web and takes instruction from the web increasing

the level of security it provides even from a remote area.

Performance Evaluation

The system underwent several rounds of testing to evaluate performance. The system functioned as expected, and all joints and connections were securely fastened. The sensors, modules, and displays all function accurately on real-time. Details of the observations during system testing are presented in this section.

For every attempt whether successful or not, the microcontroller sends a message to the database. The interface of the mobile App changes appearance based on the status of the door as shown in the screenshots in Figure 7 and 8. When the door is locked but can be opened by the use of an RFID tag, the upper part of the screen (CLOSED Door Status) indicates that the door is currently closed and it requires a registered RFID to open it. The 'opened' tab at the middle of the screen indicates that the door can be opened by a tag with a registered RFID. When the 'LOCK' tab is toggled, no RFID rag will open the door, not even a registered tag will be able to open it. This is to ensure that the security is not easily compromised. Therefore if the RFID tag is stolen or missing, the admin can prevent entrance by unauthorized persons directly from the app.

As shown in the screenshots in figures 7 and 8, when a registered tag is brought close to the RFID reader, the door opens and the user of the mobile app is informed of the entrance. The door status **c**hanges from 'CLOSED' to 'OPENED' as shown in figure 7.

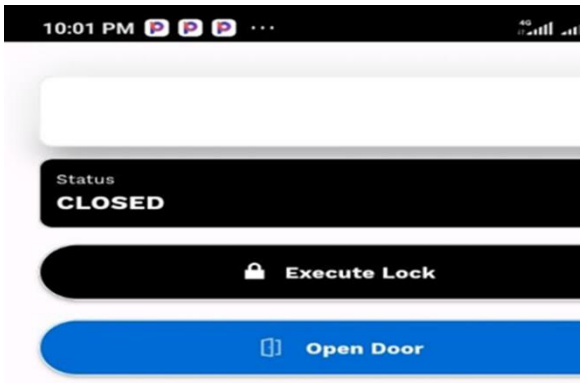

Figure 7: Screenshot showing the App in Closed Door Mode

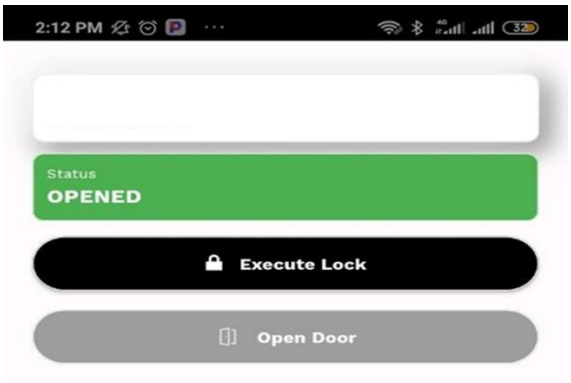

Figure 8: Screenshot showing the App in Opened Door Mode

On any attempt made by an unregistered tag, the user is notified through the app that an unidentified tag is attempting to open the door. Beneath the 'LOCK' and 'OPENED' tab, 'ATTENTION' is displayed in red for the attention of the app user to the failed attempt. This is shown in Figure 9.

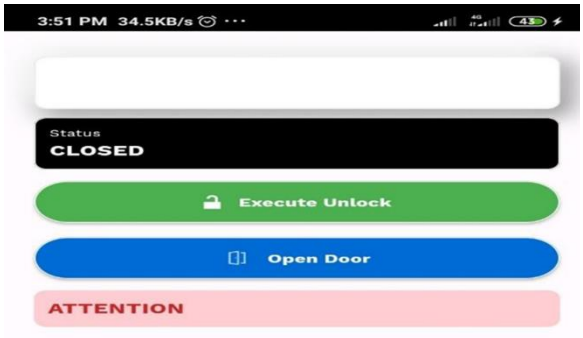

Figure 9: The screenshot of a failed attempt by an unidentified tag

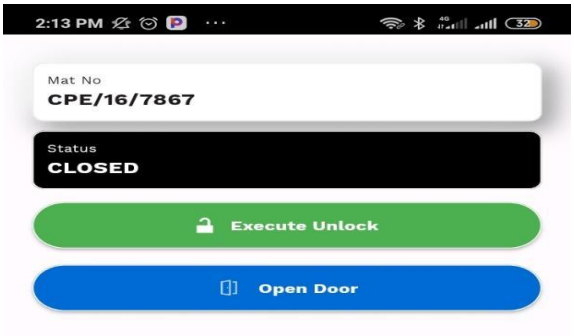

Figure 10: Screenshot showing the App in Execute Lock Mode

When the app user notices this failed attempt which is a security threat, especially when the tag is lost or has been stolen, the user can lock the door through the mobile app so that the door will not respond to any tag, not even the registered tag. This is achieved by simply toggling the 'Execute Unlock' tab at the middle of the app interface as shown in Figure 10:

In the attempt to open the door from the App as shown in the image of the screenshot in figure 11, the microcontroller communicates with the Android App and the smart lock system for on-App door control.

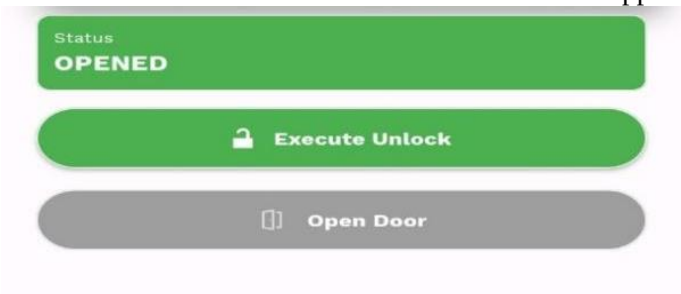

Figure 11: Opened Door from the Application

Results and Discussion

The RFID scanner reads and identifies RFID tags to start the authentication process, and if reliably detects tags, unique identifiers are provided for user authentication. The buzzer sounds when a valid RFID tag is presented, confirming successful authentication. The microcontroller manages RFID authentication, communicates with the Android app, and controls the servo motor. The charger circuit maintains stable battery charging, and the battery powers the system without an external source. The servo motor smoothly locks and unlocks the door after RFID authentication. The Android app seamlessly interacts with the system, allowing users to control access.

During testing as shown in Figure 12, efforts were made to ensure that the RFID scanner reads tags accurately to start authentication. The buzzer is checked to confirm it makes a sound when a valid tag is presented, signaling successful authentication. The NodeMCU testing focuses on seeing if it manages RFID authentication, communicates with the Android app, and controls the servo motor as the system processor. The charger circuit is observed to ensure it effectively charges the battery, maintaining a stable current and showing charging status. Battery testing ensures it reliably powers the system, even without an external source. The servo motor was tested to ensure it smoothly operates, turning and locking or unlocking the door after RFID authentication. Finally, the Android app was checked for a seamless interface, allowing users to control access. These tests aim to confirm each component works correctly, ensuring reliable performance in real-world situations.

Figure 12: The image of the completed system during testing

The system was intended to read the RFID if the tag comes in contact with it, check the database to confirm if the RFID is registered and open the lock, if it is. The lock can also be controlled over the internet through the app. The system worked and the outcome was accurate, and all sensors and components functioned flawlessly, with no lags or errors in the system. The tags were accurately read and door statuses were accurately sent to the app in real time as shown in Table 1. The internet connection was also flawless.

Table 1: The result when been tested with RFID tag and android application

Cases	Test name	Authorization			Expected output	Actual output
		Auto	App	Denied		
1	Unrecognised person	No	No	Yes	Door locked	Door locked
2	Unrecognised person	No	Yes	No	Door opened	Door opened
3	Recognised person	yes	No	No	Door opened	Door opened

Timing is an essential factor in a security system. Therefore, the system performance in real-time was evaluated under different lighting conditions, the observations are as presented in Table 2 and Figure 13. A variable intensity lamp was employed to vary the illumination between the tag and the reader. A digital lux meter was used to measure the intensity of the light, and vary the illumination from 50 to 500 lux. Employing a digital stop clock, the response time was recorded for each lighting condition as presented in Table 2 and Figure 13. It was observed that the response time decreases with increase in light intensity until 300 lux. The response time remain constant from 300 lux to 350 lux, then began to increase. The shortest response time of 0.4 sec. was observed from 300 to 350 lux, while the longest response time of 2.253 sec. was at 50 lux. The system's response time at 190 lux was the same as that observed at 500 lux. This results show that different light intensity affect the response time of RFID, which may be as a result of electromagnetic interference according to Yau and Yinshan, (2020) and Bukova *et al.*, (2023).

Table 2: Evaluation of the performance of the RFID tag under different lighting conditions

S/N	Light Intensity (Lux)	Response Time (Sec)
1	50	2.250
2	100	1.900
3	150	1.240
4	200	0.860
5	250	0.575
6	300	0.400
7	350	0.400
8	400	0.420
9	450	0.550
10	500	0.825

However, the response time was generally found to be less than 2.5 sec. Since any system involving user's interface is expected to have a response time not more than 10 sec. for a real time operation (Adams, 2021), it shows that the developed non-contact access control system using RFID with android application perform favourably well with similar studies in literature.

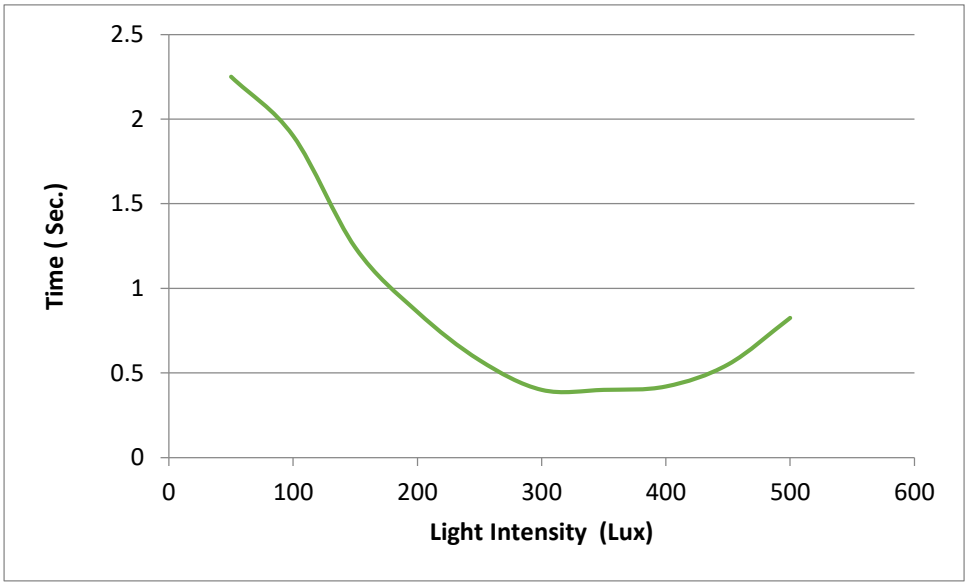

Figure 13: The plot of the system performance under different light intensity

Conclusion

The development of the non-contact access control system using RFID with an Android application, which employed NodeMCU as the microcontroller for this study has addressed critical challenges in access control technology especially in the resource contraints sub-Saharan African countries. Leveraging NodeMCU's capabilities to interface with RFID readers, seamless communication between hardware components and the Android interface was achieved. NodeMCU's reliability in maintaining consistent connectivity and efficient data transmission was demonstrated during testing. While the system benefited from NodeMCU's capabilities, areas for improvement include optimizing power consumption and refining data encryption protocols. Overall, NodeMCU's role in enabling seamless communication and control underscores its significance in access control technology, addressing the project's objectives and paving the way for future enhancements.

References

Abubakar, I., Dalglish, S. L., Angell, B., Sanuade, O., Abimbola, S., Adamu, A. L. and Zanna, F. H. (2022). The Lancet Nigeria Commission: investing in health and the future of the nation. *The Lancet*, 399(10330): 1155-1200.

Adams G. (2021): Real-Time performance and response latency measurements of Linux Kernels on single-board computers, *Computers* 10(5): 64; https://doi.org/10.3390/computers10050064

Aluri, D. C. (2020). Smart lock systems: An overview. *International Journal of Computer Applications*, 177(37): 40-43.

Bukova B., Tengler J., Brumercikova E., Brumercik F. and Kissova O. (2023): Environmental burden, case study of RFID technology in logistics centre. *Sensors (Basel)* 23(3): 1268, DOI:10.3390/323031268.

Danjuma, P. U., & Nwaizugbo, I. C. (2022). Drivers and Inhibitors of Online Shopping in Kogi State. *Nnadiebube Journal of Social Sciences*, 3(2): 1-25.

Gadupu, H., Mokharji, O., Kankaria, R., Kumar, S., & Jayavel, K. (2021). ACCESS-IoT enabled smart lock. *International Journal of Reconfigurable and Embedded Systems*, 10(3): 176.

Hao W., Zuozheng D., Xingping W., Zaihan Z., Run Z., Yunda C., Xiaochan W. and Guo Z. (2025): A wireless and passive RFID tag sensor for the detection of Pb2+ in soil combining chemiresistive sensing and impedance mismatch; A new method for onsite detection of hazardous

metals. *Journal of Hazardous Materials* 494(15): 138763 doi.org/10.1016/j.jhazmat.2025.138763

Kamel, E., & Memari, A. M. (2019). State-of-the-Art review of energy smart homes. *Journal of Architectural Engineering*, 25(1): 03118001.

Lee, H., Fridlind, A. M., & Ackerman, A. S. (2021). An evaluation of size-resolved cloud microphysics scheme numeric for use with radar observations. Part II: Condensation and evaporation. *Journal of the Atmospheric Sciences*, 78(5): 1629-1645.

Tao B., Dong L., Miao F., Liang X. and Chu P. K., (2025): Passive RFID Multi-Dimensional sensor for monitoring Light, Humidity, and ethanol. *Materials Science and Engineering* 313(2): 117908.https://doi.org/10.1016/j.mseb.117908.

Theodoropoulos, A. (2022). Participatory design and participatory debugging: Listening to students to improve computational thinking by creating games. *International Journal of Child-Computer Interaction*, 34: 100525.

Tilala, P., Roy, A. K., and Das, M. L. (2017). Home access control through a smart digital locking-unlocking system. In *TENCON 2017 IEEE Region 10 Conference*, 1409-1414

Yan Q. and Yinshan Y. (2020): Research on environmental factors affecting RFID reader performance, 2020 IEEE 5th information technology and mechatronics engineering conference (ITOEC);DOI:10.1109/ITOEC49072.2020.9141889

Yin, M., Huang, J., & Chen, H. (2021). Development of A Smart Lock System Based on the Internet of Things and Cloud Platform. *2021 IEEE International Conference on Artificial Intelligence and Industrial Design (AIID)*, 477-481.