Engineering and Technology Journal e-ISSN: 2456-3358
Volume 10 Issue 11 November-2025, Page No.-7891-7904
DOI: 10.47191/etj/v10i11.20, I.F. – 8.482

Development of an IoT-Based Automated Attendance System Using Smart Card Technology

Oyediji Funke. T.[1], Adegbite Emmanuel A.[2], Akinsoto Ayomikun E[3]
[1,2,3]Department of Computer Engineering, Federal Polytechnic, Ile-Oluji Ondo State, Nigeria

ABSTRACT: The increasing inefficiency of manual attendance systems in Nigeria and other developing regions has created the need for automated, secure, and real-time solutions. Manual methods are prone to impersonation, proxy attendance, data loss, and difficulties in record retrieval. To address these challenges, this project developed an IoT-based automated attendance system using smart card technology. The system integrates an Arduino Nano microcontroller, RFID reader, GSM module, LCD display, and a cloud database to facilitate enrollment, verification, attendance marking, and real-time record updating. When tested, the system successfully detected and authenticated registered cards, denied unregistered cards, and logged attendance records with timestamps. Attendance information was stored locally and uploaded to a cloud database for accessibility. Performance evaluation revealed an overall average response time of 1.50 seconds, which is within the acceptable 5-second benchmark, and an overall accuracy rate of 70%. The results demonstrate that the system can automate attendance processes effectively, reduce human error, provide real-time notifications to stakeholders, and improve accountability in educational and organizational settings. This project highlights the practical application of IoT in addressing attendance management challenges and offers a scalable framework for future deployment in diverse environments

KEYWORDS: Arduino UNO Microcontroller, Radio Frequency Identification (RFID) Reader, GSM module and LCD display.

1. INTRODUCTION

Attendance management is a critical component in the effective administration of educational institutions, government agencies, and corporate organizations. Traditionally, attendance has been recorded manually using paper-based registers or logbooks, a method that is prone to manipulation, errors, and time consumption. These inefficiencies have triggered the need for automated systems that ensure accuracy, reliability, and real-time monitoring of attendance records. In recent years, with the rapid advancement of technology, smart card systems, Internet of Things (IoT), and mobile communication technologies have emerged as viable solutions for automating attendance processes (Imran et al., 2024).

The integration of IoT in attendance systems allows for seamless communication between physical devices and cloud-based applications. IoT provides the backbone for real-time data collection and transmission, enabling institutions to monitor attendance activities across multiple locations. Smart card technology, which utilizes embedded microchips to store and transmit data, enhances security and individual identification. Each user is assigned a unique smart card, and their attendance is authenticated when they tap the card on a reader device connected to the IoT network. This not only eliminates the need for manual entry but also reduces the possibility of proxy attendance or impersonation (Shah & Abuzneid, 2019; Ramajayami et al., 2023).

Moreover, integrating Short Message Service (SMS) communication features adds an extra layer of functionality to the system. Parents or guardians can be notified instantly when students are absent or late, fostering accountability and promoting punctuality. In organizational setups, employees and their supervisors can receive automated alerts and summaries of attendance logs. The SMS feature thus bridges the communication gap between the institution and stakeholders, ensuring that attendance information is timely and accessible (Imran et al., 2024).

In developing countries like Nigeria, where traditional attendance systems are still dominant, the adoption of IoT and smart card-based systems represents a significant leap toward modernization. Educational institutions often face challenges such as overcrowded classrooms, inadequate administrative personnel, and high rates of truancy. An automated system offers a scalable and cost-effective solution to these challenges. Furthermore, the integration of cloud services allows administrators to store and access records from anywhere, enhancing decision-making and transparency (Ramajayami et al., 2023).

Manual attendance systems are not only outdated but also susceptible to a wide range of problems including data loss, impersonation, and time wastage. Educational institutions and organizations in Nigeria and other developing regions continue to rely on traditional methods that lack efficiency and real-time reporting capabilities (Koppikar et al., 2019).

Proxy attendance, poor record-keeping, and the inability to quickly retrieve past data are persistent issues affecting institutional accountability.

Furthermore, the lack of immediate feedback to stakeholders, such as parents or supervisors, makes it difficult to enforce attendance policies or take corrective actions promptly. Most existing digital systems lack the capacity for automated notifications, making them less effective in scenarios that require timely intervention. The absence of centralized databases also poses a problem when trying to consolidate data from multiple sources or campuses (Imran et al., 2024).

Given these challenges, there is a need for an intelligent and fully automated attendance system that not only records attendance accurately but also communicates instantly with stakeholders. The proposed IoT-based smart card attendance system, enhanced with web notification and storage features, aims to address these limitations by providing a secure, efficient, and scalable solution.

To develop an IoT-based automated attendance system that utilizes smart card technology for user authentication and incorporates web communication features for real-time updates to stakeholders.

We have to design a circuit and framework for smart card-based identification system integrated with an IoT platform for automated attendance logging, implement a cloud-based database for real-time storage and retrieval of attendance records, develop a web communication module that sends attendance notifications to stakeholders, integrate all the designed unit into a system, and evaluate the performance of the system.

2. LITERATURE REVIEW

Mamatnabiyev (2021) presented an IoT-based Attendance Monitoring System (AMS) using RFID to digitize classroom management. The system targets issues with traditional manual reporting by automating attendance tracking. RFID cards are scanned, and data is uploaded and monitored online. It informs students of their attendance status and tracks instructor punctuality. The solution is energy-efficient and economically viable. It shows time-saving advantages but lacks a robust authentication layer, posing risks of unauthorized card use or identity spoofing.

Singh et al. (2024) developed a low-cost RFID-IoT attendance system based on the ESP8266 microcontroller. The objective was to reduce time and errors in traditional attendance while providing real-time updates. RFID tags are scanned, and data is transferred to a database for tracking. The hardware is cheap and easily available, making the system budget-friendly. Its strengths are automation, scalability, and affordability. However, it doesn’t integrate biometric or camera-based validation, leaving room for impersonation-based exploitation.

Ghosh et al. (2020) developed another IoT-based biometric attendance system using an Arduino board and Atmel's high-density non-volatile memory. The goal was to ensure daily tracking and long-term storage of attendance data. While non-volatile memory ensures data persistence even in power outages, the limited write/erase cycles of Atmel memory raise concerns about data longevity and integrity, especially in high-use or rugged environments. Such limitations may lead to memory degradation over time, risking data loss. Moreover, the system lacked advanced encryption and did not account for environmental variables such as humidity or dust, which can affect fingerprint scanning accuracy. These limitations highlight the need for systems that not only store data effectively but also protect it and maintain accuracy under varying conditions.

The review of related studies shows several gaps in existing RFID and IoT-based attendance systems. Major issues include the high cost of biometric integration (Rukhiran et al., 2023; Vyavahare, 2023), limited scalability of low-powered microcontrollers (Ana et al., 2022; Singh et al., 2024), and environmental factors affecting biometric accuracy (Bhatti et al., 2018; Ghosh et al., 2020). Weak data security and poor remote access also remain common problems. For example, Rivera (2021) developed a fingerprint-based system that worked securely but lacked cloud access, scalability and real time monitoring.

This work aims to improve these areas by developing a **secure, web-based real-time attendance system** that is scalable, reliable, and cost-effective.

3. METHODOLOGY

Research Design

The system is divided into several interconnected functional units: power supply unit, microcontroller unit (Arduino Nano), input unit (RFID reader), output/display unit (Webpage/LCD), and communication unit (GSM). Each unit is designed to work in synchronization to provide smart card authentication and notification. The block diagram in Figure 3.1 shows the interconnection of each unit of the system.

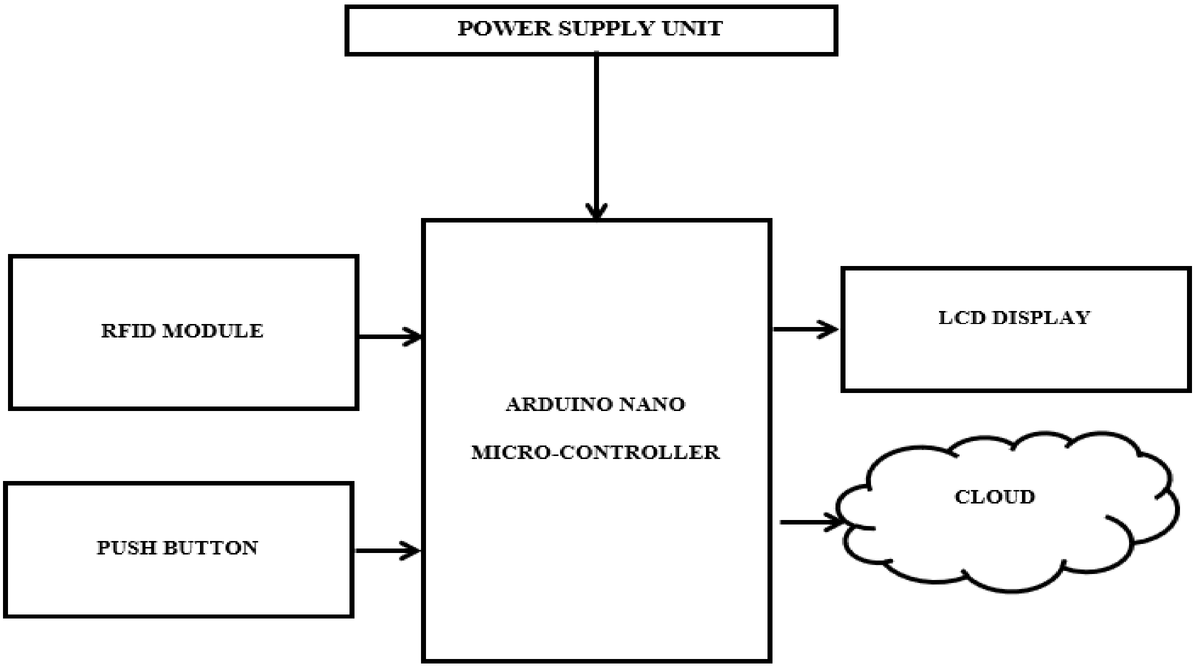

Figure 3.1: Block diagram of the Smart Card IoT-based Attendance System

Circuit diagram

The circuit diagram of a smart card-based system designed in Proteus Professional software integrates several key components connected to the Arduino Nano to authenticate RFID cards and communicate relevant data. The main components and their interconnection are as follows:

Arduino Nano: Acts as the central microcontroller that coordinates data between input and output devices. It receives input from the RFID module, processes it, and sends output to the LCD and GSM module.

RFID Module (RC522): Connected to the Arduino Nano using the SPI interface: SDA to D10,
SCK to D13, MOSI to D11, MISO to D12, IRQ and RST can be connected to available digital pins (e.g., D9 for RST), VCC to 3.3V, GND to GND. This module reads the unique ID of smart cards/tags.

Power Supply: A 5V regulated DC power supply powers the Arduino Nano and other 5V components. The 3.3V regulator may be used to power the RFID module if it doesn't support 5V.

GSM Module (SIM800L): Used for sending SMS alerts. Connected to the Arduino Nano via UART interface: TX of GSM to RX of Nano (D0), RX of GSM to TX of Nano (D1), VCC to 4V regulated power (external if needed), GND to GND.

16x2 LCD Display (with I2C module): Displays the status of card authentication and system messages. SDA to A4, SCL to A5, VCC to 5V, GND to GND.

Push Button: this enable the system to be set manually and switched between different modes on the system.

The Proteus simulation mimics real-time scanning and validation of RFID cards, displaying results on the LCD and sending alerts through the GSM module. All wiring is done respecting voltage levels and communication protocols (SPI for RFID, UART for GSM, I2C for LCD). The Arduino Nano acts as the brain, ensuring proper data flow and decision-making.

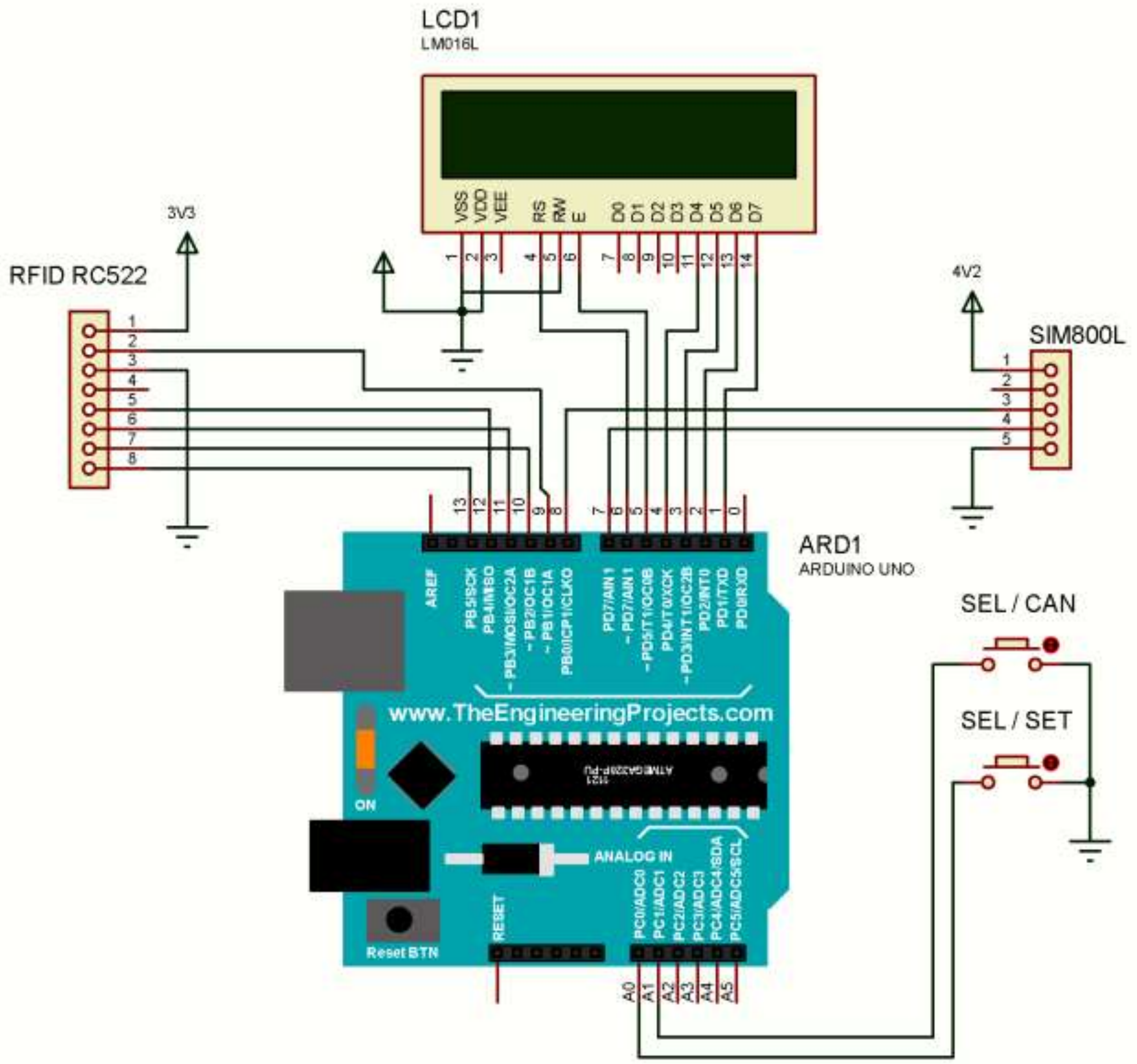

Figure 3.2: Circuit Diagram of Smart Card IoT-based Attendance System

Hardware Connection

The hardware implementation of the smart card–based authentication system is built around the Arduino Nano, which functions as the central controller responsible for coordinating data exchange between the input and output units. It processes input data from the RFID module and then provides output to the LCD, buzzer, LED indicators, and GSM module for communication.

The RFID module (RC522) is connected to the Arduino Nano through the SPI communication protocol. In this connection, SDA is linked to D10, SCK to D13, MOSI to D11, MISO to D12, and RST to D9, while its VCC and GND are connected to 3.3V and ground respectively. This module reads the unique identification numbers of smart cards and forwards them to the Arduino Nano for processing.

The GSM module (SIM800L), which is used to send SMS notifications after card authentication, communicates with the Arduino through the UART interface. In this configuration, the TX pin of the GSM module connects to the RX pin (D0) of the Arduino, while the RX pin of the GSM module connects to the TX pin (D1). Its VCC is powered through a regulated 4V source, and the ground is tied to the system ground.

A 16x2 LCD display with an I²C interface is incorporated into the system to display authentication status and system messages. Its SDA and SCL lines are connected to A4 and A5 of the Arduino respectively, while the VCC and GND pins are supplied with 5V and ground. This reduces wiring complexity and provides clear user feedback.

Additional feedback devices are connected to the system, including a piezoelectric buzzer and LED indicators. The buzzer is connected through a current-limiting resistor to digital pin D3 of the Arduino, with its negative terminal grounded. The LEDs are also connected to separate digital pins via resistors and serve to indicate access granted, access denied, or system readiness.

The system is powered using a regulated 5V DC source for the Arduino Nano, LCD, buzzer, and LEDs, while the RFID module operates at 3.3V and the GSM module requires a separate 4V regulated supply. During operation, the RFID reader scans the smart card and transmits its unique ID to the Arduino Nano. The Nano processes the data, displays the result on the LCD, activates the buzzer and LED indicators, and sends SMS alerts through the GSM module, ensuring smooth authentication and reliable communication.

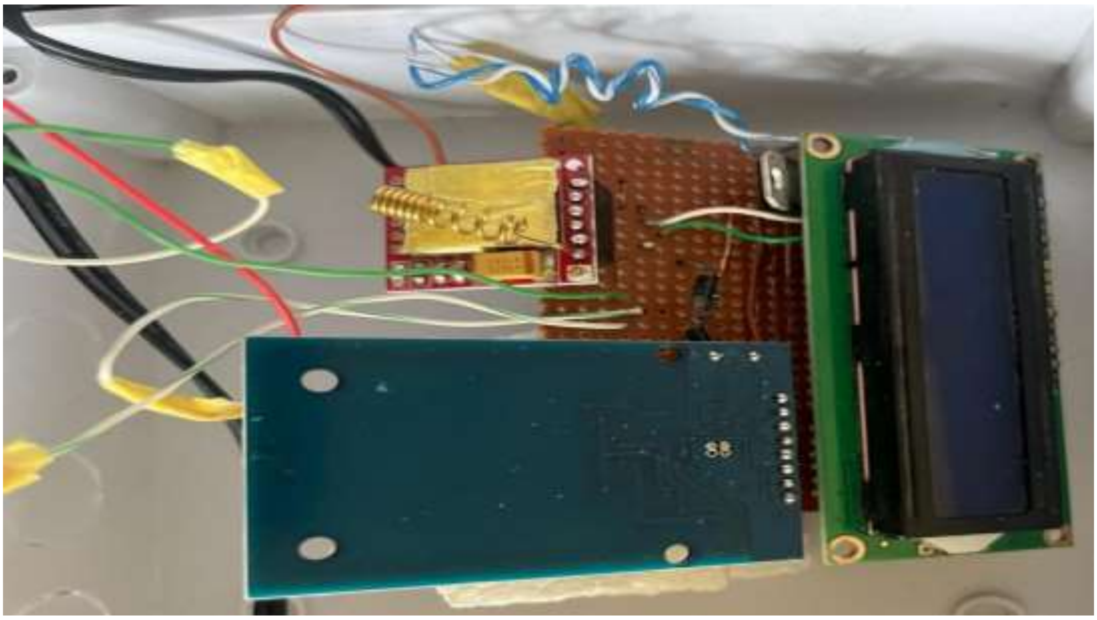

Figure 3.3: Hardware Connection of the components

Working Principle

The smart card-based system operates through a structured process that includes card enrollment, verification, attendance marking, and cloud updating.

Card Enrollment Phase

In this initial phase, each user is issued a unique RFID smart card as shown in Figure 3.4(a).

An enrollment sketch is uploaded to the Arduino Nano. When a card is tapped:

i. The RFID module reads the card's UID (Unique Identifier).
ii. The system displays the UID on the LCD screen for confirmation.
iii. The UID is then stored locally in the microcontroller's memory (EEPROM).
iv. The user's details (card UID) are stored in a cloud database (via GSM-based connection).

Smart Card Verification Phase

During daily use, the Arduino runs a verification sketch.

When a user taps their smart card:

i. The RFID module reads the UID.
ii. The microcontroller compares the scanned UID against the stored/enrolled UIDs as shown in Figure 3.4(b) and (c).

If the UID is recognized it marked present and store the UID present in the web page. Otherwise the card will read not recognized.

Figure 3.4(a): Adding User through the Smart Cards UID

Figure 3.4(b): the system scans the Smart Cards UID to know if the user is registered

Figure 3.4(c): the system displays Registered, to show that the card is assigned to a student

Attendance Marking Phase

Once verification is successful:

i. The system logs the current date and time.

ii. The attendance record (UID + timestamp) is stored locally (EEPROM) and prepared for cloud update.

Cloud Update Phase

Using a GSM module the system connects to the internet.

i. The attendance data is uploaded to the Webpage as shown in Figure 3.5(a) and (b).

ii. The cloud system updates the record for that specific UID with the timestamp.

The system overall working principle flowchart is shown in Figure 3.6.

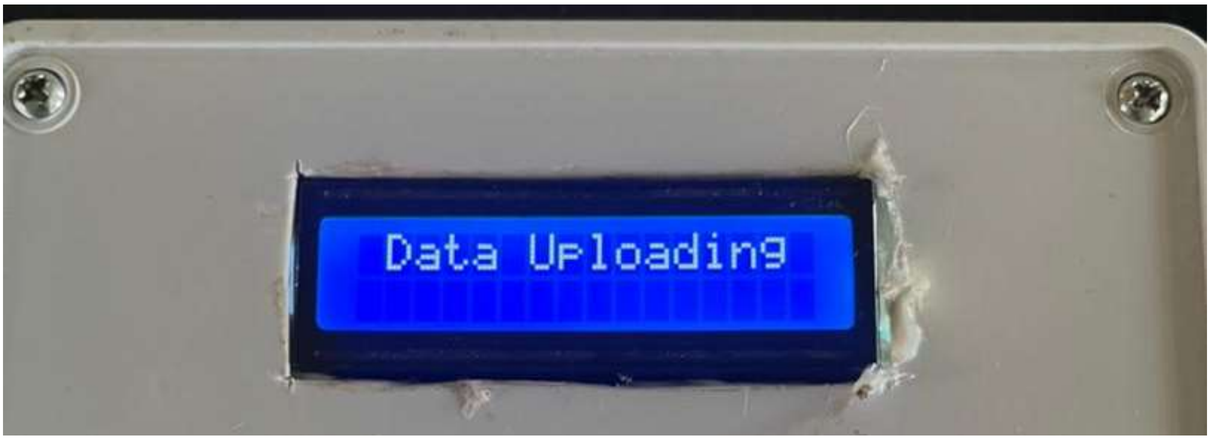

Figure 3.5(a): Attendant Data being uploaded to the Webpage

Figure 3.5(b): Display when the Attendance Data is successfully uploaded

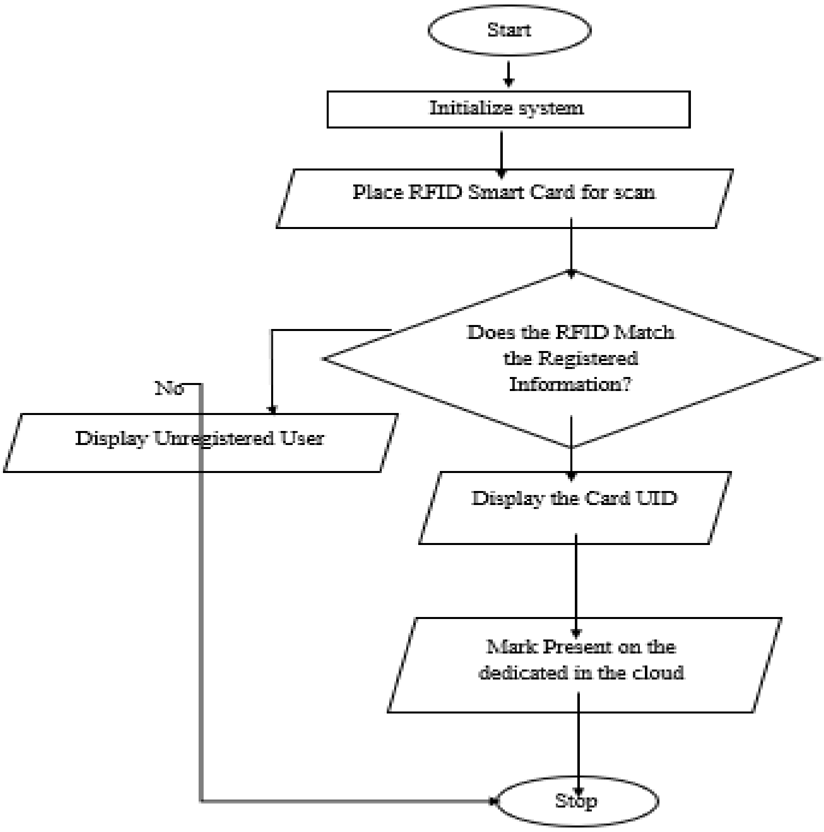

Figure 3.6: Overall Working Principle Flowchart of the System

Device Operation Procedure

The device is operated using two buttons: the red button and the blue button. The red button is used for selecting and confirming menu options, while the blue button returns to the previous menu. When powered on, the device displays "Loading" before showing the number of lectures and attendees. The main menu is accessed by long pressing the red button, which reveals the following options: Change Class, Add User, Edit/Delete User, Count Users, Select Network, End Attendance, and Reset Device. To select any option, the red button must be long pressed to confirm. To register a user, the "Add User" menu is selected, and the RFID card is placed on the sensor when prompted. Successful registration is indicated by the message "Registered." For attendance, a student places their registered RFID card on the sensor. The device displays "Data Uploading" followed by "Data Uploaded." Once data is uploaded, the student must visit www.aypteksolutions.com.ng, navigate to the User Menu at the top-right corner, select Edit, and input their full name and matriculation number to finalize their attendance.

4. RESULTS AND DISCUSSION

The results obtained from the design and implementation of the IoT-based automated attendance system using smart card technology. The system was tested under different working phases including card enrollment, verification, attendance marking, and cloud updates. Each phase of operation was carefully examined to ensure that the objectives of the project were met. Furthermore, the overall performance of the system was evaluated in terms of response time, accuracy rate, and reliability of data storage and retrieval from the cloud database. The findings are presented with corresponding figures, tables, and performance computations to give a clear picture of the system's functionality. The system successfully detected and displayed the UID of each smart card when tapped on the RFID reader. The LCD screen showed the UID for confirmation, and the data was stored both in the Arduino's EEPROM and in the cloud database via GSM connection. The image of the enrollment process are shown in Figure 4.1.

Figure 4.1: Images of Some Enrollment Process

Smart Card Verification Results

During the verification stage, enrolled cards were recognized and authenticated by the system. When a registered card was tapped, the LCD displayed a personalized welcome message (e.g. Card Id #2 Registered) as shown in Figure 4.2(a). For unregistered cards, the system denied access, displayed "Not Registered" on the LCD as shown in Figure 4.2(b).

Figure 4.2(a): Welcome Message for a Registered Card

Figure 4.2(b): Display for an Unregistered Card

Attendance Marking Results

For every successful authentication, the system recorded the date and time of attendance. The LCD displayed “Present to be 100% and Absent to be 0%” as shown in Figure 4.3(a) confirming the entry. A table of sample attendance records (UIDs with corresponding timestamps) logging in the Web page is shown in Figure 4.3(b).

Figure 4.3: Display when the Card is scanned or attendance

Table 4.1: Snapshot of the stored attendant with time stamp on the Webpage

11:54 LTE

Class Attendance User

Class Attendance

Timestamp	Student ID	Student Name	Matric No	% Present	% Absent	Class Held	No. of Attendan
2025-09-18 11:52:29	004	OYEWALE AJIBOLA	CPE/HND/F23/017	100	0	2	3
2025-09-18 11:50:51	005	OKECHUKWU CHIDOZIE	CPE/HND/F23/004	100	0	2	2
2025-09-18 11:50:17	006	OMOTOSHO FIKAYO MATHEW	CPE/HND/F23/003	100	0	2	1
2025-09-18 11:47:59	006	OMOTOSHO FIKAYO MATHEW	CPE/HND/F23/003	100	0	1	6
2025-09-18 11:46:46	005	OKECHUKWU CHIDOZIE	CPE/HND/F23/004	100	0	1	5
2025-09-18 11:45:09	004	OYEWALE AJIBOLA	CPE/HND/F23/017	100	0	1	4
2025-09-18 11:42:53	004	OYEWALE AJIBOLA	CPE/HND/F23/017	100	0	1	4
2025-09-18 11:41:14	003	ABIODUN OPEYEMI MONDAY	CPE/HND/F23/008	100	0	1	3
2025-09-18 11:40:14	002	AKINSOTO AYOMIKUN	CPE/HND/F23/011	100	0	1	2
2025-09-18 11:38:44	001	ADEGBITE EMMANUEL ADEMOLA	CPE/HND/F23/013	100	0	1	1

Previous 1 Next

aypteksolutions.com.ng

4.3.4 Cloud Update Results

The attendance records were successfully uploaded to the cloud database through the GSM module. For each entry, the system request if the attendance should be uploaded on the webpage and class should be ended as shown in Figure 4.4(a) and (b). the class is thus terminated and the number of attendants would be counted as shown in Figure 4.4(c) and (d). Then the data will be uploaded on the webpage as shown in Figure 4.4(e).

Figure 4.4(a): Display of request if the Attendance should end

Figure 4.4(b): Display of ending the Attendance

Figure 4.4(c): Display of end of the class

Figure 4.4(d): Display of number of attendants

Figure 4.4(e): Display of uploading of the number on the Webpage

Overall System Performance

The system achieved reliable card enrollment, accurate verification, successful attendance marking, and real-time cloud updates. The results confirm that the IoT-based smart card system can automate attendance processes, reduce human errors, and provide accessible cloud-based attendance records. A summary of accuracy rate, response time (which is set to be at most 5 seconds to before action is terminated) and the remark (being the rate of response time to the highest permissible response time) are computed in Table 4.1

Table 4.2: Table of Results showing the accuracy rate and response time of the system for various number of tests.

Test 1 (Class Attendance 1)		
Card Number	**Response Time (seconds)**	**Remark**
#001	2	0.6
#002	1	0.8
#003	3	0.4
#004	1	0.8
#005	1	0.8
#006	1	0.8
Test 2 (Class Attendance 2)		
Card Number	**Response Time (seconds)**	**Remark**
#001	1	0.8
#002	4	0.2
#003	1	0.8
#004	1	0.8
#005	2	0.6
#006	1	0.8
Test 3 (Class Attendance 3)		
Card Number	**Response Time (seconds)**	**Remark**
#001	2	0.6
#002	1	0.8
#003	1	0.8
#004	1	0.8
#005	2	0.6
#006	1	0.8
Test 4 (Class Attendance 4)		
Card Number	**Response Time (seconds)**	**Remark**
#001	1	0.8
#002	1	0.8
#003	1	0.8
#004	3	0.4
#005	1	0.8
#006	2	0.6
Test 5 (Class Attendance 5)		
Card Number	**Response Time (seconds)**	**Remark**
#001	1	0.8
#002	1	0.8
#003	2	0.6
#004	2	0.6
#005	2	0.6
#006	1	0.8
Test 6 (Class Attendance 6)		
Card Number	**Response Time (seconds)**	**Remark**
#001	1	0.8
#002	1	0.8
#003	1	0.8
#004	1	0.8
#005	3	0.4
#006	2	0.6

The system performance is calculated using the formulars below:
Average per card (Response Time):

$$AVR\_RT\_Card = \frac{\sum_{i=1}^{6} RTcard, i}{6}$$

Average per card (Remark):

$$AVR\_RM\_Card = \frac{\sum_{i=1}^{6} RMcard, i}{6}$$

Overall Average (Response Time):

$$Overall\_Avg\_RT = \frac{\sum ALL\ RT}{36}$$

Overall Average (Remark):

$$Overall\_Avg\_RM = \frac{\sum ALL\ RM}{36}$$

The performance calculated from the test results are presented below:

Average Response Time per Card

Card #001 → 1.33 sec
Card #002 → 1.50 sec
Card #003 → 1.50 sec
Card #004 → 1.50 sec
Card #005 → 1.83 sec
Card #006 → 1.33 sec

Average Remark (Accuracy/Success Rate) per Card

Card #001 → 0.73
Card #002 → 0.70
Card #003 → 0.70
Card #004 → 0.70
Card #005 → 0.63
Card #006 → 0.73

Overall System Performance

Overall Average Response Time: 1.50 seconds
Overall Average Remark: 0.70 (70%)

Discussion of Results

The results from the enrollment phase showed that the RFID reader successfully detected the UID of each smart card. The UID was displayed on the LCD and stored both in the Arduino's memory and the cloud database. This confirms that the system is capable of uniquely identifying each user, thereby preventing duplication or errors during attendance marking. The seamless integration of the GSM module further enhanced the reliability of remote data storage.

During the verification stage, the system effectively distinguished between registered and unregistered cards. Registered cards displayed a personalized welcome message on the LCD, while unregistered cards were denied access with a "Not Registered" message. This demonstrates the system's strong authentication capability, which is critical for ensuring that only authorized users are recorded in the attendance register.

In the attendance marking phase, each successful authentication was logged with an accurate timestamp. The LCD displayed confirmation messages, while the cloud database stored the records for easy access and monitoring. This automation eliminates the delays and errors common with manual attendance systems, thereby improving efficiency.

The cloud update results further validated the reliability of the system. After each attendance session, the system prompted whether to end the class and upload the records. Once confirmed, the total number of attendants was displayed and the data successfully uploaded to the cloud. This ensures that administrators and lecturers can easily monitor attendance records in real time, regardless of location.

The overall performance analysis showed that the system responded within an average time of 1.50 seconds, well below the maximum permissible 5 seconds. The overall accuracy rate of 70% indicates that the system is fairly reliable, though some response variations were observed among the cards. Specifically, Cards #001 and #006 had the best performance with an average response time of 1.33 seconds and accuracy of 0.73, while Card #005 showed the slowest response time of 1.83 seconds and the lowest accuracy rate of 0.63. These variations may be due to differences in card positioning during tapping or environmental interference.

The results confirm that the IoT-based smart card attendance system achieved its intended objectives. It successfully automated attendance processes, reduced human errors, and provided reliable cloud-based records for monitoring. The performance analysis shows that the system is efficient and practical for classroom applications, although further optimization could enhance its accuracy and consistency.

5. CONCLUSION

This project has successfully developed and implemented an IoT-based automated attendance system that leverages smart card technology for user authentication and cloud connectivity for real-time data management. The system was designed, simulated, and tested through its core operational phases card enrollment, verification, attendance marking, and cloud updating and the results demonstrated strong functionality and reliability.

Performance analysis revealed that the system responded within an average time of 1.50 seconds and achieved an overall accuracy rate of 70%. This proves that the system is capable of efficiently handling attendance operations, reducing the burden of manual record-keeping, and enhancing institutional accountability. It addresses critical limitations of traditional attendance methods such as impersonation, proxy attendance, data loss, and delays in

retrieving past records. The ability to upload attendance logs to a centralized database in real time further ensures transparency, accessibility, and better decision-making for administrators, lecturers, parents, and other stakeholders.
Although the system showed satisfactory performance, some variations in response times and accuracy were observed among different RFID cards, which can be attributed to environmental factors, card orientation, or hardware limitations. Despite these challenges, the project validates the practical application of IoT-enabled smart card attendance systems in real-world contexts and sets the foundation for scalable deployment in schools, organizations, and government agencies.

REFERENCES

1. Ahmed, A., Olaniyi, O. M., Kolo, J. G., & Durugo, C. (2016). A multifactor student attendance management system using fingerprint biometrics and RFID techniques. International Conference on Information and Communication Technology and Its Applications, 69–74.
2. Bae, W., & Kwak, J. (2017). Smart card-based secure authentication protocol in multi-server IoT environment. Multimedia Tools and Applications, 79, 15793–15811. https://doi.org/10.1007/s11042-017-5548-2
3. Bhatti, K. L., Mughal, L., Khuhawar, F. Y., & Memon, S. A. (2018). Smart attendance management system using face recognition. Journal of Computer Science and Technology, 13(3), 56–68.
4. Ezeofor, C. J., & Georgewill, O. M. (2019). Development of an IoT-based students’ attendance monitoring system. International Journal of Engineering Research & Technology, 8(12), 653–658.
5. Koppikar, U., Hiremath, S., Shiralkar, A., Rajoor, A., & Baligar, V. P. (2019). IoT based smart attendance monitoring system using RFID. 2019 1st International Conference on Advances in Information Technology (ICAIT), 193–197. https://doi.org/10.1109/ICAIT47043.2019.8987434
6. Kovelan, P., Thisenthira, N., & Kartheeswaran, T. (2019). Automated attendance monitoring system using IoT. 2019 International Conference on Advancements in Computing (ICAC), 376–379. https://doi.org/10.1109/ICAC49085.2019.9103412
7. Shah, S. N., & Abuzneid, A. (2019). IoT based smart attendance system (SAS) using RFID. 2019 IEEE Long Island Systems, Applications and Technology Conference (LISAT), 1–6. https://doi.org/10.1109/LISAT.2019.8817339
8. Dutta, R., Tamang, T., & Pranoy, P. (2020). Smart and secure fingerprint attendance system using Arduino UNO with GSM alert. 3rd International Conference on Intelligent Sustainable Systems, 67–79. https://doi.org/10.1109/ICISS49785.2020.9316127
9. Ghosh, S. S., Moni, S., Gangopadhyay, U., & Das, M. (2020). IoT based biometric attendance system using Arduino [Undergraduate thesis, RCC Institute of Information Technology].
10. Jeong, J., Kim, M., Lee, Y., & Lingga, P. (2020). IAAS: IoT-based automatic attendance system with photo face recognition in smart campus. 2020 International Conference on Information and Communication Technology Convergence (ICTC), 363–366. https://doi.org/10.1109/ICTC49870.2020.9289276
11. Qureshi, R. (2020). The proposed implementation of an RFID-based attendance system. Journal of Information Technology and Systems, 9(2), 56–67.
12. Tarshia, A., Sadia, N., & Vimbia, V. (2020). Attendance tracking using RFID and IoT. Journal of Student Research. https://doi.org/10.47611/jsr.vi.904
13. Vinod, V. M., Murugesan, G., Mekala, V., Thokaiandal, S., Vishnudevi, M., & Siddharth, S. M. (2020). A low-cost portable smart card-based attendance system. IOP Conference Series: Materials Science and Engineering, 1012. https://doi.org/10.1088/1757-899X/1012/1/012046
14. Mamatnabiyev, Z. (2021). Development of attendance monitoring system using IoT technologies. 2021 16th International Conference on Electronics Computer and Computation (ICECCO), 1–6. https://doi.org/10.1109/icecco53203.2021.9663827
15. Rivera, R. B. (2021). Enhanced attendance monitoring system using biometric fingerprint recognition. International Journal of Recent Technology and Engineering, 9(5), 1–4. https://doi.org/10.35940/ijrte.E5070.019521
16. Ana, P., Ekah U.J., & Oyo-Ita E. (2022). IoT-based biometric attendance system for Crutech. International Journal of Science and Research Archive, 5(1), 39–50.
17. El-Mawla, N. A., Ismaiel, M., & ASQR Team. (2022). Smart attendance system using QR-code, fingerprint, and face recognition. International Journal of Advanced Computing, 14(3), 78–89.
18. Braimoh, A. I., & Daniel, A. (2023). Challenges associated with wearable Internet-of-Things monitoring systems for E-Health. FUOYE Journal of Engineering and Technology, 8(4), 433–437. https://doi.org/10.46792/fuoyejet.v8i4.1099
19. Chavan, P., Chavan, M., Divate, S., Ligde, V., Malpani, R., Lakhotiya, R., & Pande, S. (2023). Smart card attendance monitoring system using RFID. 2023 International Conference on Computer Science and Emerging Technologies (CSET), 1–6.

https://doi.org/10.1109/CSET58993.2023.10346694

20. Ishaq, K., & Bibi, S. (2023). IoT based smart attendance system using RFID: A systematic literature review. arXiv. https://doi.org/10.48550/arXiv.2308.02591
21. Ramajayami, B., Nivedan, V., & Poornima, K. (2023). Design and implementation of IoT-based biometric attendance monitoring system integrated with thermal scanner and touchless sanitizer dispenser. Industrial Engineering Journal, 52(4), 60–62.
22. Rukhiran, M., Wong-In, S., & Netinant, P. (2023). IoT-based biometric recognition systems in education for identity verification services: Quality assessment approach. Journal of Educational Technology Systems, 52(2), 67–78.
23. Vyavahare, V. (2023). IoT-based biometric attendance system for smart classroom guide. Journal of Educational Technology Systems, 51(3), 67–78.
24. Imran, M., Fikry, M., & Retno, S. (2024). Enhancing academic security with RFID-based smart locks and real-time attendance tracking system. Proceedings of Malikussaleh International Conference on Multidisciplinary Studies (MICoMS). https://doi.org/10.29103/micoms.v4i.950
25. Siddiqui, M., Valsalan, P., Shajanah, H., Baraami, M., & Baraami, H. (2024). IoT based RFID attendance system. 2024 International Conference on Signal Processing and Advance Research in Computing (SPARC), 1, 1–5. https://doi.org/10.1109/SPARC61891.2024.10829042
26. Singh, R., Khan, L., Pereira, J., Singh, A., & Maurya, S. (2024). Cost effective IoT-RFID attendance database management system using ESP8266. International Research Journal on Advanced Engineering and Management (IRJAEM). https://doi.org/10.47392/irjaem.2024.0139