

Development of an IoT-Based Biometric Attendance Management System

*¹Mary A. Adedoyin, ²Oluwagbemiga O. Shoewu, ³Abayomi I.O. Yussuff, ⁴Adetokumbo A. Adenowo, ⁵Ahmed Shitta and ⁶Olayinka Okedokun

¹Department of Electronic and Computer Engineering, Lagos State University, Nigeria

²Department of Computer Science, Lagos State University, Nigeria

mary.adedoyin@lasu.edu.ng | oluwagbemiga.shoewu@lasu.edu.com | abayomi.yussuff@lasu.edu.ng | adetokumbo.adenowo@lasu.edu.ng | ahmedshitta4@gmail.com | okedokunyinka@yahoo.com

Received: 15-JUNE-2024; Reviewed: 28-AUGUST-2024; Accepted: 09-SEP-2024

<https://dx.doi.org/10.4314/fuoyejet.v9i3.5>

ORIGINAL RESEARCH

Abstract— In educational institutions and business organizations, efficient attendance recording and monitoring are essential. Traditional manual methods are complex, time-consuming, and inaccurate, allowing impersonation and lacking data availability for analysis. IoT technology offers a solution through smart attendance systems, but most of the existing solutions are not scalable and cannot handle extensive data processing and storage requirements efficiently. Additionally, biometric accuracy and reliability need improvement. Hence, this work presents an IoT-based biometric attendance management system using a Node Microcontroller Unit (NodeMCU), an Inter-Integrated Circuit (I2C), a Liquid Crystal Display (LCD), a fingerprint sensor, and a power supply. It features an interactive graphical user interface (GUI) accessible via Android devices or laptops, enabling remote monitoring and reporting through a web application. Tested with multiple students, the system showed ease of implementation, high security, time savings, and improved accuracy and reliability over traditional methods. Key contributions include automatic attendance management and a comparative analysis against existing techniques using metrics such as power consumption, security, speed, cost, functionalities and portability. The system captures and verifies fingerprints in approximately 4 seconds, operates on minimal power (5V), and is cost-effective with locally sourced components. It ensures secure and reliable attendance tracking, eliminating proxy attendance and manual errors by storing data in the cloud.

Keywords— Database, Fingerprint sensor, Hardware, Smart attendance management system, Software.

1 INTRODUCTION

The traditional method of using paper and pen to take attendance has proven inefficient (Adejumobi *et al.*, 2022). For example, it is challenging to keep track of the attendance sheets, and a lack of complete backup is a serious risk. Natural disasters such as floods, fires, and other events can cause significant damage to the records. Also, it is time-consuming to keep such papers up to date. In addition, the traditional process allows impersonation, causing attendance to be unreliable. In the traditional process, recorded attendance may be unavailable for analysis when needed because the data is not stored in a database. An automatic attendance management solution is highly needed to address these problems. Recently, the technology of Internet-of-Things (IoT) and its diverse applications have enabled the development of smart systems such as attendance monitoring management systems, since automated processes are utilized to substitute manual efforts. IoT comprises devices connected to the Internet, facilitating direct device-to-device communication without human intervention, aimed at delivering smart services to users. These interconnected devices incorporate electronics, sensors, and software applications over wireless networks to provide enhanced services (Adedoyin & Falowo, 2020).

IoT is applied in healthcare (Braimoh & Daniel, 2023), automation, manufacturing, transportation, agriculture, education and many more (Raza, 2022).

Also, web-based applications are employed for data and record management. It has the ability to support multiusers and manage simultaneous access to records and report queries from different locations, thereby reducing time and costs (Othman *et al.*, 2012). Biometric authentication automatically identifies a person's identity based on their unique characteristics, which remain the same throughout his/her lifetime. The general architecture of a biometric system is presented in Figure 1.

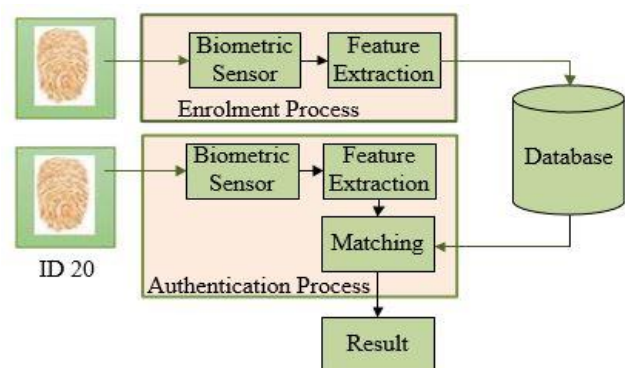


Fig. 1. General Architecture of a Biometric System.

*Corresponding Author

Section B- ELECTRICAL/COMPUTER ENGINEERING & RELATED SCIENCES

Can be cited as:

Adedoyin M.A., Shoewu O.O., Yussuff A.O., Adenowo A.A., Shitta A., and Ojedokun O (2023). Development of an IoT-Based Biometric Attendance Management System. FUOYE Journal of Engineering and Technology (FUOYEJET), 9(3), 397-405. <https://dx.doi.org/10.46792/fuoyejet.v9i3.5>

Biometrics include fingerprint, facial, retinal, laughter, voice and iris (Adedoyin *et al.*, 2020). Fingerprint-based biometric technology aids in eliminating the issue of impersonation because the fingerprint is unique to every individual (Al Amin *et al.*; Shoewu & Idowu, 2012). Among all the biological characteristics, the use of fingerprints is more widely adopted as a personal

identification technique. Biometric sensor is used for fingerprint scanning. The following are the problems that may occur during fingerprint scanning: finger misplacement, orientation, wet finger, dirty finger and skin problems (Jain *et al.*, 2012) as shown in Figure 2. In this work, an adaptive algorithm was developed that can adapt to various skin conditions and still recognise and adjust to different finger orientations.






Problems	Fingerprint Snapshot	Problems	Fingerprint Snapshot
Finger misplacement		Dirty finger	
Orientation		Skin problem	
Wet finger			

Fig. 2. Fingerprint Scanning Problems

2 RELATED WORKS

In the literature, a lot of research has been done to replace the old, inefficient, and ineffective attendance management systems with more efficient, automated, less cumbersome, and digital solutions. In addition, different technologies have been proposed to manage the attendance of students or employees. These technologies include Global System for Mobile Communications (GSM), Quick Response (QR) code, ZigBee (IEEE 802.15.4-based specification for a set of high-level communication protocols), Radio Frequency Identification (RFID), barcodes, General Packet Radio Server (GPRS), IoT and many more. However, most of the existing solutions are not scalable and cannot handle extensive data processing and storage requirements efficiently. Additionally, biometric accuracy and reliability need improvement. The authors in Dutta *et al.* (2020) used Arduino UNO microcontroller and GSM technology to develop a smart fingerprint attendance system. ZigBee technology was employed to develop a fingerprint attendance system in Rajasekar and Vivek (2012). A fingerprint-based attendance system using a microcontroller and LabView technique was developed by the authors in Yadav *et al.* (2015). The authors in Ahmed *et al.* (2016) developed a multifactor attendance system that utilised the RFID technology and fingerprint biometrics to track and manage students' attendance records. An attendance monitoring system using biometric fingerprint recognition module was developed in Revera, 2021. However, the major limitation of the above works is that IoT technology has not been employed to track the attendance report remotely anywhere, anytime. An IoT-based students' attendance monitoring system to monitor 75% attendance of every student was developed in Ezeofor and Georgewill, (2019). Similarly, the authors in Ana *et al.*, (2022) developed IoT-based biometric attendance system. However, the above works used ESP32 microcontroller, which has limited memory and may be insufficient for some IoT applications that require more memory and higher accuracy. In addition, it may not be suitable for some applications that require faster

and more stable connection. Also, an IoT-based biometric attendance system using Arduino has been proposed by Ghosh *et al.* (2020) to keep records of attendance and count the data for daily purposes. However, the authors used the Atmel high density non-volatile memory technology, which have a limited number of write/erase cycles. This means that after a certain number of cycles, the memory cells can wear out, leading to potential data loss or memory failure especially in harsh environmental conditions. The authors in Ramajayami *et al.* (2023) developed an IoT-based biometric attendance monitoring system but the system has limited functionalities and may struggle with scalability and data processing.

Different from the existing literature, the aim of this work is to develop an IoT-based biometric attendance management system that consists of both hardware and software that is scalable and can handle extensive data processing and storage requirements efficiently with high accuracy and reliability. The system features an interactive graphical user interface (GUI) accessible on an Android device or a laptop, which allows the user to view or download the attendance report remotely anywhere, anytime via a web-based application. The system was developed using the Node Microcontroller Unit (NodeMCU), Inter-Integrated Circuit (I2C) and Liquid Crystal Display (LCD) and power supply, along with a fingerprint scanner for biometrics to be recorded and stored in the database so that the attendance of pre-enrolled students or employees can be taken and verified. The NodeMCU is a popular open-source firmware and development kit that provides several advantages, particularly in the realm of IoT projects. It comes with integrated Wi-Fi (ESP8266), simplifying the process of connecting devices to the internet without needing additional modules. It has high accuracy in biometric recognition, and secure data transmission (Lohar *et al.*, 2023). The NodeMCU boards are very cost-effective compared to other microcontroller boards with a wide number of write/erase cycles. It can easily connect to various cloud services, allowing for data logging, remote monitoring, and control of devices over the internet. Also, an adaptive algorithm was integrated to cater for various skin conditions and address the problem that may arise during the fingerprint scanning. In addition, encryption protocols were implemented to safeguard sensitive biometric data.

3 METHODOLOGY

The IoT-Based biometric attendance management system involves system architecture, system flowchart and system process. The system process comprises two stages, which are enrolment and authentication with online web pages.

3.1 ARCHITECTURE OF IOT-BASED BIOMETRIC ATTENDANCE MANAGEMENT SYSTEM

The developed IoT-based biometric attendance management system architecture is divided into two parts, the fabrication of the physical (hardware) design and the development of the web-based application (software) design. The system architecture is shown in Figure 3. The hardware components are NodeMCU, I2C,

LCD, power supply and fingerprint sensor. The software includes HTML, CSS, JAVASCRIPT, MYSQL, PHP and embedded C/C++.

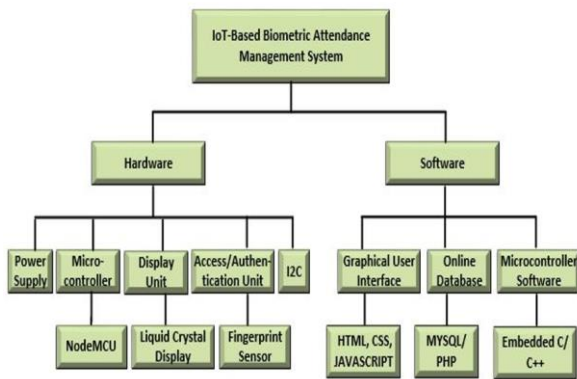


Fig. 3. IoT-Based Biometric Attendance Management System Architecture.

3.1.1 DESCRIPTION OF HARDWARE COMPONENTS

1) Power supply: The system needs +5 DC power to operate at its best. The +5 DC voltage is obtained by connecting a capacitor, regulator, step-down transformer, and bridge diodes together. Portable power supply enables the system to operate in remote or off-grid locations.

2) The NodeMCU is an ultra-low powered microcontroller that runs on ESP8266. It provides a connection interface between the sensors and the internet. It offers a combination of ease of use, affordability, compact size, versatility, built-in Wi-Fi, and energy efficiency. These advantages make it an excellent choice for developing a wide range of IoT applications.

3) 16x2 LCD is a type of LCD that displays images using the light-modulating properties of crystals.

4) Fingerprint Sensor: The use of a fingerprint sensor is the most popular method of biometric identification. R305 fingerprint sensor module with TTL UART interface is used since it is simple to operate and includes an intuitive Arduino library that enables its functionality and facilitates simple testing.

5) I2C: This is a serial communication bus that is used to interface the microcontroller with other peripheral devices. In this work, I2C interfaces the NodeMCU with LCD. I2C's simplicity, efficiency, flexibility in addressing multiple devices, support for multi-master configurations, low pin count and variable speeds make it a preferred choice in this work.

3.1.2 DESCRIPTION OF WEB-BASED APPLICATION SOFTWARE DESIGN

1) The user interfaces for web-based application development are what enable users to interact with the system to retrieve or store data. The system is scripted, which used CSS (for the webpage design), HTML (for the structure), and JavaScript (to add the webpage functionalities).

2) Data on student attendance can be stored in MySQL, a relational database management system (RDBMS) that is cloud-based. PHP is also a general-purpose programming language, which has been used to add user information, manipulate/modify data to be stored and transferred to MySQL database.

3) The microcontroller's control programs and online web-based applications were written in different programming languages. To guarantee that all hardware components function properly, the NodeMCU microcontroller was coded in embedded C/C++.

The circuit diagram of the system is displayed in Figure 4, which shows the connection of the hardware components. From Figure 4, information about any fingerprint captured by the fingerprint sensor is sent directly to the software that houses the online database through the help of the Wi-Fi module, ESP8266, which communicates wirelessly with the device (Android device or a laptop) on which the software runs. Figure 5 shows the internal part of the developed system.

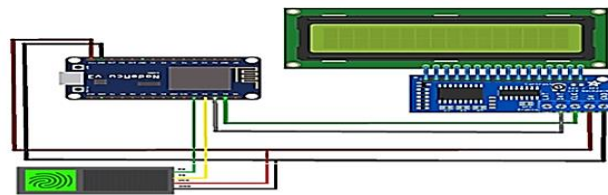


Fig. 4. Circuit diagram of the system.



Fig. 5. The internal part of the developed system.

3.2 SYSTEM FLOWCHART

The flow chart that shows the procedure of the system is presented in Figure 6.

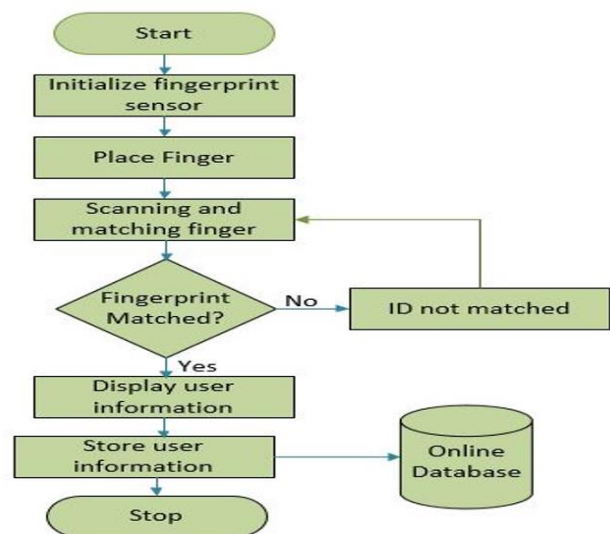


Fig. 6. Flowchart of the IoT-Based Biometric Attendance Management System.

3.2.1 INITIALIZATION PROCEDURES

The complete constructed system is powered on as shown

in Figure 7(a). Then, the system will search for the available Wi-Fi connection. Figure 7(b) shows the connection status of the system through the LCD. Immediately after the connection is successful, the IoT-based biometric attendance management system is activated as shown in Figure 7(c). Next, the system will check for the readiness of the fingerprint sensor to scan the finger as depicted in Figure 7(d). A red Light Emitting Diode (LED) blinks if the sensor is found and this is also displayed on the LCD as shown in Figure 7(e). Figure 7(f) shows that the system is ready to accept the finger for scanning. It takes about 3-4 seconds to complete the initialization procedures under robust internet connection.



Fig. 7(a). System is powered on.



Fig. 7(b). System's connection status.



Fig. 7(c). System's activation status.

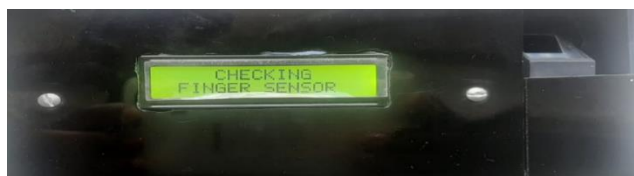


Fig. 7(d). System checking for fingerprint sensor.

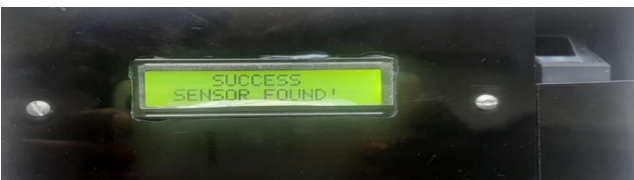


Fig. 7(e). Fingerprint sensor found.



Fig. 7(f). Fingerprint sensor ready for scanning.

Fig. 7. Initialization Procedures of the System.

3.2.2 PLACING OF FINGER PROCEDURES

As shown in Figure 8(a), when the fingerprint sensor is ready for scanning, it will ask the user to place a finger on the fingerprint sensor. Then, the user places his/her finger on the fingerprint scanner and the sensor scans the finger as shown in Figure 8(b). Hence, the buzzer gets activated, whereas the red LED blinks upon taking any records.



Fig. 8(a). Sensor interface to place finger.



Fig. 8(b). Sensor with scanned finger.

The system generates a unique identification (ID) number for the user and displays the user information, if the scanning and matching are done successfully. The fingerprint ID is saved in the system. Then, the system looks for a match in the database. Then, the information of the user is saved in the online database, if there is a match.

3.2.3 ONLINE DATABASE ALGORITHM

The online database algorithm is shown below:

1. Start
2. Access the website by logging in.
3. Is the Administrator (Admin)/Lecturer officially registered? No, go to the Admin/Lecturer registration interface and register;
4. Yes, data would be saved in a database.
5. Is the user (student or employee) registered? No, go to the user registration interface and register;
6. Yes, save student's information to the database.
7. If you are an Admin/Lecturer and have already registered, click login.
8. Enter the login information and click the login button.
9. View or download attendance for any course of interest.
10. Stop

3.3 IOT-BASED BIOMETRIC ATTENDANCE MANAGEMENT

SYSTEM PROCESS

The system process involves enrolment (registration of user) and verification (fingerprint recognition and matching)

3.3.1 Enrolment Process

Enrolment is the process of collecting an individual's information into the system's database for recognition and verification to be done (Adejumobi *et al.*, 2022). To begin, an admin needs to log in to the web portal as shown in Figures 9(a) and 9(b) to enrol users by capturing each individual's fingerprint. A sample of fingerprint capturing for model creation is shown in Figure 10. The template for the input of student information such as user's full name, matriculation/serial number, email address and gender is shown in Figure 11. The fingerprints of individuals are captured on the fingerprint sensor and stored in a database with a unique ID number. This activity is carried out once, or when a new entry is to be inserted into the database. Enrolment Procedures (Registration) are as follows:

1. Start enrolment by placing the finger on the fingerprint sensor for scanning.
2. Capture the fingerprint from the sensor.
3. Enrol, the first user by creating a model of the user with a unique ID number assigned.
4. Remove the finger and,
5. Repeat steps 1-4 to enrol the next user.
6. Stop

The enrolment interface is shown in Figure 10, which is used to capture the information of each user to be enrolled. The details of that particular person are saved in the database. If any alteration is detected in the specific finger currently being captured once or twice, capturing will proceed to a third attempt; otherwise, the capturing process will terminate. This is necessary in order to minimise the time it takes for the verification of an individual.

3.3.1 VERIFICATION PROCESS

Verification involves fingerprint recognition and matching. Once the enrolment is successful, the next step is the verification process which is the recognition and one-to-one matching of fingerprints.

Fingerprint recognition involves capturing an image of a person's fingerprint and recording its characteristics, such as arches, whorls, loops, minutiae, furrows, and edge outlines. Matching the fingerprint can be achieved through three methods: minutiae matching, correlation, and ridge matching (Asabere *et al.*, 2019). The verification is done by placing the finger on the fingerprint sensor. The procedure of verification is shown below:

1. Start the verification process by placing a finger on the fingerprint sensor
2. Verify and store the information of a particular user.

3. Send the details to the database.
4. Keep a record of the fingerprints successfully verified that can be downloaded online anywhere, anytime.
5. Repeat steps 1-4 to verify the next user.
6. Stop

The fingerprints are compared to the images in the database. If the finger is not adequately held or the fingerprint is not accurately recognised, attendance will not be recorded. The attendance will only be recorded if the current scanned fingerprint matches any previously recorded fingerprint in the database. If any fingerprint matches, the microcontroller will print the information of the user saved for that fingerprint on the LCD.

3.4 ONLINE WEBPAGE

The online webpages consist of an Admin/Lecturer login page, fingerprint capturing for students taking the course page, registered users' page, course selection page, users' daily logs page, and attendance report exported to Microsoft Excel.

3.4.1 ADMIN/LECTURER LOGIN PAGE

The central Admin of the proposed system has to create a profile for lecturers who want to use the fingerprint biometric attendance system for taking attendance during the semester course. If the profile has been created for every lecturer by using their relevant courses then, they can have the ability to access the biometric system and start the attendance session for their intended courses and also export it to Microsoft Excel format from the system.

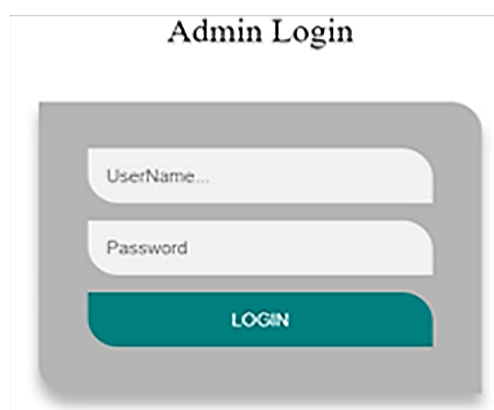
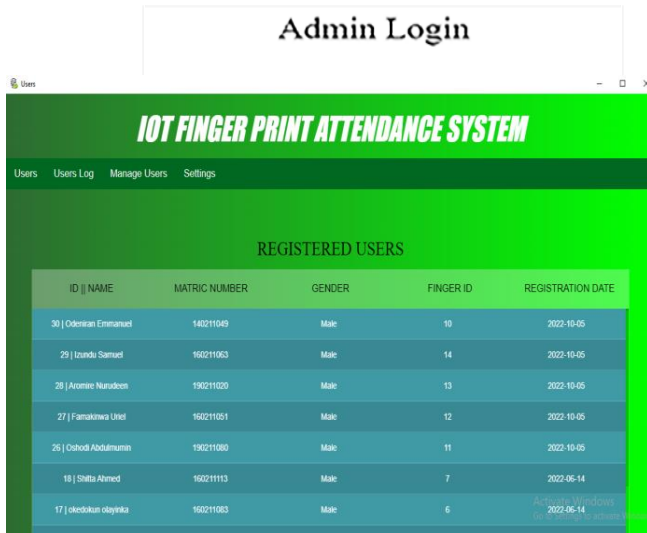


Fig. 9(a). Admin/Lecturer Login



interface to modify the information of users such as updating user information, deleting users, etc.
Fig. 12. Total registered users count page.

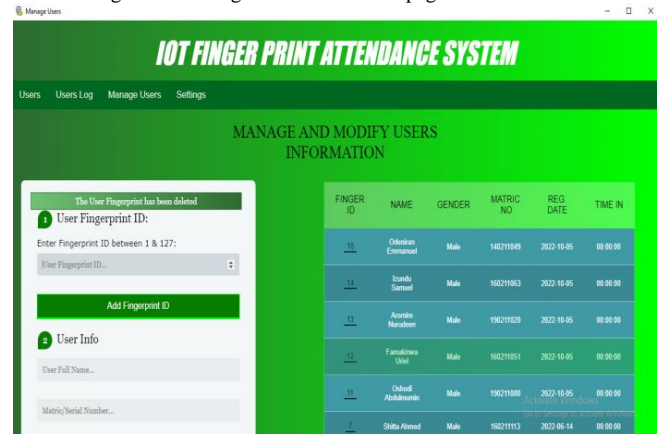


Fig. 13. Manage and Modify user's information.

It follows that lecturers must be registered into the system to have control over students' enrolment, verification and attendance management. Lecturers must login to the system to proceed with the enrolment of students for a particular course. Figure 10 shows how student biometrics are captured and sent to the database for model creation.



Fig. 10. Fingerprint capturing for model.

3.4.4 COURSE SELECTION PAGE

The course selection page is the page to select a course before taking the attendance of the user. The template is shown in Figure 14.

3.4.5 USERS' DAILY LOGS PAGE

The users' daily logs page is the page on which the lecturer can view the total number of students that attended a particular course lecture. The time the student signs in and signs out of the lecture and also the lecturer can export this daily log to excel format to provide a handy output if printed. Attendance taken for any day can always be accessed through this page. Users can select a previous lecture date to generate attendance for it because all lecture attendance is saved in the database and can be retrieved at any time. The users' daily logs page is shown in Figure 15.

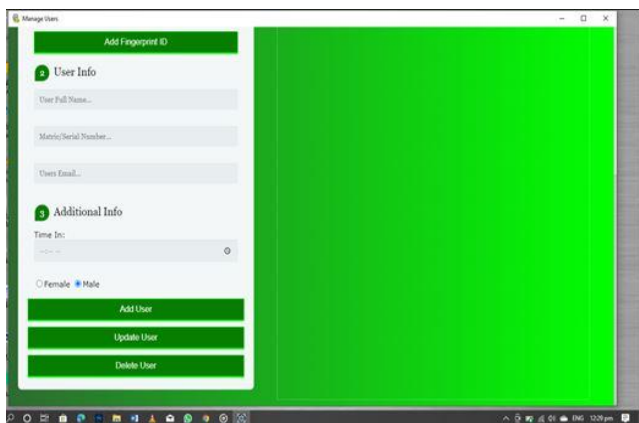


Fig. 11. Template for saving student Information creation.

3.4.3 Registered Users' Page

This is the page on which all students enrolled in a course can be viewed at once. The information displayed is the user ID, full name, matric number, gender, finger ID and registration date. Figure 12 shows the total number of users that have registered while Figure 13 shows the

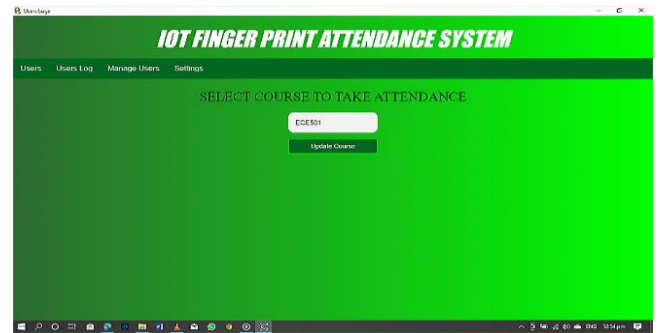


Fig. 14. Course selection page.

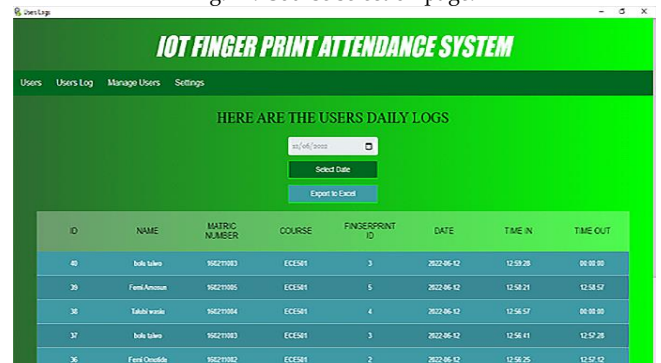


Fig. 15. Users' daily logs page.

Attendance report exported to Microsoft Excel. The sample of the students' report output during the testing of the system is shown in Figure 16, which was later exported to datasheet format.

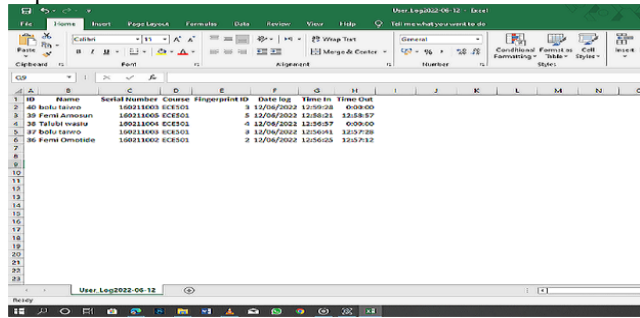


Fig. 16. Report output on Microsoft Excel.

The developed system is displayed in Figure 17, which can be placed at the entrance of a lecture theatre so that student attendance in lectures can be taken. Each

student's record will be updated in a database, and data will be sent via Wi-Fi to the server.



Fig. 17. Developed system.

4. RESULT AND DISCUSSION

Extensive testing and verification were performed on many students to evaluate the system's performance and functionalities under different network conditions and assessing its scalability for a growing number of users. Security measures, including encryption protocols and user authentication, were implemented. The software application was tested in terms of user authentication and reporting. The IoT functionality was tested in terms of remote monitoring, data collection and connectivity. The biometric functionality was tested in terms of identity matching and verification, data storage, access control and real-time processing. The results provided two major contributions which are automatic attendance management of the students and comparative analysis of the developed system with the existing techniques of attendance

management systems. The metrics for the comparative analysis are power consumption, security, speed, cost, functionalities and portability. The power consumption is very low. It takes only 5V for the microcontroller to operate maximally. The system is highly secured because fingerprint, which is unique to an individual was used. The developed system has a fast-processing speed. It takes an average of 4 seconds for a fingerprint to be captured and verified. Also, the system is cost-effective because all the components used are locally sourced. The system has wide functionalities due to the numerous functions of the microcontroller used and intelligent algorithms integrated into the system as compared to the existing works that used the IoT technologies with different microcontrollers and algorithms. The system is wireless and portable. The technologies chosen for the analysis are IoT, ZigBee and GSM, Android and RFID, LabVIEW. The summary of the comparative analysis is presented in Table 1.

Table 1: Comparative Analysis of the IoT-Based System with other Technologies and Techniques

Technologies/Technique	Power Consumption	Security	Speed	Cost	Functionalities	Portability
IoT (This work)	Low	High	High	Low	Wide	Yes
IoT (Ramajayami <i>et al.</i> , 2023)	Low	High	High	Low	Limited	Yes
IoT (IoT (Ghosh <i>et al.</i> , 2020)	Low	High	High	Low	Limited	Yes
IoT (Ezeofor & Georgewill, 2019)	Low	High	High	Low	Limited	Yes
ZigBee, GSM (Dutta <i>et al.</i> , 2020)	Low	Moderate	Moderate	High	Limited	Yes
Android, RFID (Ahmed <i>et al.</i> , 2016)	Moderate	High	High	High	Limited	No
LabVIEW (Yadav <i>et al.</i> , 2015)	Moderate	Moderate	High	High	Limited	No

In addition, the response time analysis was carried out for the developed system and the traditional method of using paper and pen. It was observed that the average response time for the fingerprint sensor to identify a fingerprint stored in the database is about 4 seconds while the average response time for the traditional method was 13 seconds as depicted in Figure 18.

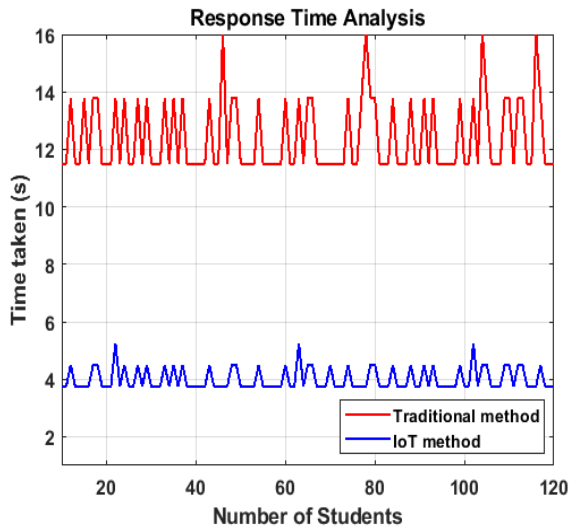


Fig 18: Time Response Analysis.

Also, the process of fingerprint scanning status and database match status was categorised as recognised

and found respectively for 6 tests (The process was carried out for 6 different courses on 100 students). The summary of the comparison of success rate (fingerprint scanning status displays recognised and database match status displays found on LCD) and failure rate (fingerprint scanning status displays not recognised and database match status displays not found on LCD) is presented in Table 2. Figure 19 shows the comparison of success rate and failure rate while Table 3 illustrated fingerprint scanning and matching analysis status for the first 20 students.

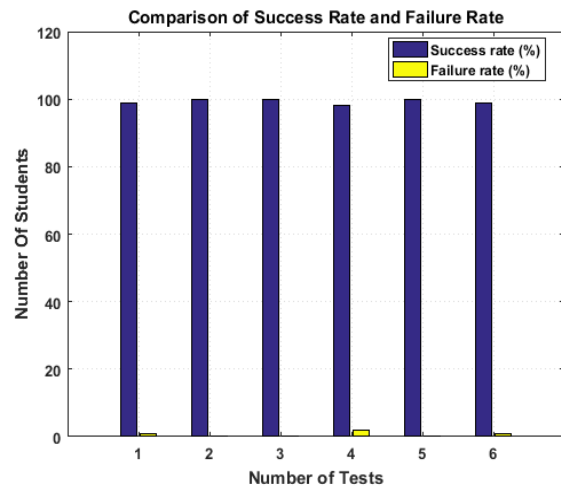


Fig 19: Comparison of Success and Failure Rate.

Table 2: Comparison of Success Rate and Failure Rate

Test/Rate	1	2	3	4	5	6
Success Rate (%)	99	100	100	98	100	99
Failure Rate (%)	1	0	0	2	0	1

Table 3: Fingerprint Scanning and Matching Analysis Status

S/N	Fingerprint ID	Biometric scanning status	Database match status	S/N	Finger print ID	Biometric scanning status	Database match status
1	001	Recognised	Found	11	011	Recognised	Found
2	002	Recognised	Found	12	012	Recognised	Found
3	003	Recognised	Found	13	013	Recognised	Found
4	004	Recognised	Found	14	014	Recognised	Found
5	005	Recognised	Found	15	015	Recognised	Found
6	006	Recognised	Found	16	016	Recognised	Found
7	007	Recognised	Found	17	017	Recognised	Found
8	008	Recognised	Found	18	018	Recognised	Found
9	009	Recognised	Found	19	019	Recognised	Found
10	010	Recognised	Found	20	020	Recognised	Found

5 CONCLUSION

In this paper, a more efficient and effective way of

improving an attendance management system has been presented. This portable smart device offers more reliability and accuracy and enhances the overall efficiency of the operation process for which it is

designed. It does not only make the management of the attendance system easier but also helps to prevent the existence of issues related to impersonation. The developed system offers a dashboard that enables lecturers to navigate and control attendance activities. The captured data is stored in the cloud ensuring that the data stored is well secured. The biometric fingerprint system is based on the combination of several electronic components such as a fingerprint sensor which is meant to read fingerprints, and an LCD to display the student information (ID, Matric number, name, date and time of taking the record, etc.). The NodeMCU (ESP8266) facilitates communication with the fingerprint module based on pre-set commands. A buzzer gets activated, while the red LED blinks upon taking any records. A copy of a record is stored in the database as soon as it is recorded. One of the benefits of the system is that proxy attendance, which allows impersonation is eliminated. Also, errors due to manual methods of taking attendance by calling names or roll numbers are also eliminated. Additionally, students can check their attendance. An Admin can log into the system with his/her username and password. No other person could access the platform without permission. The major limitation of this current system is the issue of network failures, which can disrupt the system's functionalities, affecting attendance tracking. Future work could integrate Artificial Intelligence (AI) technology to IoT to analyse attendance data to provide insights into student performance or employee, correlating attendance with academic success or productivity. Overall, the developed system solves all the complexities associated with the traditional attendance management system.

REFERENCES

- Adedoyin, M. A., & Falowo, O. E. (2020). Combination of ultra-dense network and other 5G enabling technologies: A survey. *IEEE Access*, 8, 22893-22932. doi: 10.1109/ACCESS.2020.2969980
- Adedoyin, M. A., Shoewu, O. O., Adenowo, A. A., Yussuff, A. I. O. & Senapon, M. F. (2020). Development of a smart IoT-based home automation system. *Engineering and Technology Research Journal*, 5(2), 25-37. doi.org/1047545/etrj.2020.5.2.062
- Adedoyin, M. A., Adenowo, A. A., Shoewu, O. O., and Yussuff A. I. O. (2022). Development of a fingerprint-based attendance notification system using simple mail transfer protocol. *Engineering and Technology Research Journal*, 6(1), 39-49. doi.org/10.47545/etrj.2021.6.1.076
- 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.
- Al Amin, S., Islam, M. A., & Islam, M. S. (2021). A fingerprint based smart attendance and security system using IoT and Ultrasonic sensor. *International Conference on Automation, Control and Mechatronics for Industry 4.0 (ACMI)*, 1-5. doi: 10.1109/ACMI53878.2021.9528092.
- 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.
- Asabere, P., Sekyere F., & Ofosu W. K. (2019). Wireless biometric fingerprint attendance system using arduino and MYSQL database. *International Journal of Computer Science, Engineering and Applications*, 9(4), 1-10.
- 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. doi.org/10.46792/fuoyejet.v8i4.1099
- Dutta, R., Tamang T. and Pranoy P., (2020). Smart and secure fingerprint attendance system using arduino UNO with GSM alert. *3rd International Conference on Intelligent Sustainable Systems* 67-79. doi: 10.1109/ICISS49785.2020.9316127
- 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.
- Ghosh, S. S., Moni S., Gangopadhyay U., & Das M. (2020). IoT Based Biometric Attendance System using Arduino. *Thesis submitted to Department of Electrical Engineering, RCC Institute of Information Technology*, 1-103.
- Jain, T., Tomar U., Arora U., Jain S. (2012). IoT Based Biometric Attendance System. *International Journal of Electrical Engineering & Technology*, 11(2), 156-161.
- Lohar, A. S., Lohar O. S., Rokade Y.S., & Shinde M. (2023). IoT Based Biometric Attendance System Using ESP8266. *International Research Journal of Modernization in Engineering Technology and Science* 5(11), 982-985.
- Othman, M., Ismail S. N., & Noradzan H. (2012). An adaptation of the web-based system architecture in the development of the online attendance system. *IEEE Conference on Open Systems*, 1-6. doi: 10.1109/ICOS.2012.6417619
- Rajasekar, I., & Vivek, S. (2012). Wireless fingerprint attendance system using ZigBee technology. *International Journal of Power Control Signal and Computation*. 3(1), 118-121.
- 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.
- Rivera, R. B. (2021). Enhanced Attendance Monitoring System using Biometric Fingerprint Recognition, *International Journal of Recent Technology and Engineering* 9(5) 1-4, doi:10.35940/ijrte.E5070.019521
- Shoewu, O. O., & Idowu, A. O. (2012). Development of attendance management system using biometrics. *The Pacific Journal of Science and Technology*, 13(11), 300-307.
- Raza, H. W. (2022). IoT-Based Automatic Attendance System using Middleware. *Malaysian Institute of Information Technology, Universiti, Kuala Lumpur*, 1-6.
- Yadav, D. K., Singh, S., Pujari S., and Mishra, P. (2015). Fingerprint based attendance system using microcontroller and labView. *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, 4(6), 5111-5121.