LAUTECH Journal of Engineering and Technology 19 (3) 2025: 180-187
10.36108/laujet/5202.91.0371

Development of an Internet Of Things-Based Fingerprint Biometric Attendance System

[1]Olawole E. T., [1]Adebayo O. F., [1]Adeshina J. A., [2]Ariba F. O. and [1]Ajayi R. A.

[1]*Department of Computer Engineering, University of Ilorin, Kwara State, Nigeria.,*
[2]*Department of Electrical and Information Engineering. Landmark University, Kwara State, Nigeria.*

Article Info

Article history:

Received: June 19, 2025
Revised: July 26, 2025
Accepted: July 30, 2025

Keywords:

Internet-of-Things,
Web interface,
ESP 32 microcontroller,
Hypertext preprocessor (PHP)-based web interface

Corresponding Author:
olawole.et@unilorin.edu.ng

ABSTRACT

This research explores the design and implementation of an Internet of Things (IoT) based fingerprint biometric attendance system. The traditional methods of attendance tracking often suffer from inaccuracies, time fraud, and significant administrative burdens. In response to these challenges, biometric systems have gained popularity for their ability to uniquely identify individuals through their physical or behavioural characteristics, offering a more reliable and secure approach to attendance management. The system proposed in this research utilizes fingerprint recognition, one of the most widely adopted biometric modalities, due to its high accuracy, ease of use, and cost-effectiveness. Integrating this system with the Internet of Things (IoT) expands its capabilities. The system comprises an ESP32 microcontroller, a fingerprint module, an OLED display, and a locally hosted Hypertext preprocessor (PHP)-based web interface. The OLED display serves as an immediate feedback mechanism for users, confirming whether their attendance has been successfully recorded by displaying the appropriate message. The web interface is designed for administrative use, allowing for the management of attendance records, user enrollment, and data exportation for further analysis. The results of this research demonstrate that the proposed IoT-based fingerprint biometric attendance system is a feasible and efficient solution. It offers a user-friendly interface for both students and administrators, significantly improving the accuracy and security of attendance tracking, verifying identities quickly under 1-2 seconds, with high accuracy. The system's modular design and scalability also allow for future enhancements and adaptations to meet specific needs.

INTRODUCTION

Attendance is required at the majority of institutions, particularly those that are educational. In most educational institutions, the most common way to track attendance is for the instructor to call out each student's name or have them sign an attendance sheet that is distributed during class. This is an extra obligation for the lecturer/teacher to record attendance by summoning each student, which may take some minutes of the lecture, depending on the number of students (Bhagat, 2022).

Biometrics is an automated method of recognizing individuals based on physiological or behavioural characteristics. These technologies are being used to provide secure identification, verification solutions and offer a more secure and efficient way of validating identification, minimizing the possibility for fraud (Ch, 2017). By utilizing fingerprint biometrics, your system can accurately and automatically record attendance data, which is then stored in a centralized database. Biometric technology has advanced to the point that systems may now employ it without compromising mobility. With the recent development of several cloud-based computer and storage technologies, data may now be safely stored and accessed as needed. Images of the fingerprint and iris are thought to be the most reliable biometric data (Daugman, 2020). To ease concerns, a system that tracks attendance using biometric scanners and safely saves data in the cloud as a Google Spreadsheet may be useful. One component of the system that is utilized to confirm a student's identification is a fingerprint scanner. By using a Google Spreadsheet, the student may determine if they are allowed to attend if the fingerprint picture matches one of the database records (Patil et al., 2017). Biometric technology has revolutionized the way identity verification is conducted across various sectors, including security, healthcare, and education. Traditionally, attendance tracking in educational institutions has relied on manual methods such as sign-in sheets or ID card swiping (Wayman *et al.,* 2005). These methods, while effective to some extent, are prone to inaccuracies, fraud, and administrative burdens (Patil et al., 2020). As educational institutions continue to grow in size and complexity, there is an increasing need for more efficient, accurate, and secure attendance tracking systems (Parkhi *et* ., 2015). To address these challenges, biometric attendance systems have emerged as a viable solution, enabling the unique identification of individuals based on their physical or behavioural traits (Maltoni *et al.,* 2009). Among the various biometric modalities, fingerprint recognition has become particularly popular due to its high accuracy, ease of use, and cost-effectiveness (Jain, *et al.*, 2011). The integration of Internet of Things (IoT) technology further enhances the potential of biometric systems, allowing for real-time data collection, remote monitoring, and centralized management of attendance records. This integration significantly boosts the functionality and efficiency of biometric attendance systems (Faisal *et al.*, 2021). The current study aims to design and implement an IoT-based fingerprint biometric attendance system tailored for educational institutions. This system seeks to address the limitations of traditional methods and existing biometric solutions by providing a more reliable, user-friendly, and secure approach to attendance management. Through a review of relevant literature, this area explores the evolution of biometric technologies, the integration of IoT in attendance systems, and the limitations of existing approaches, thereby laying the groundwork for the development of the proposed system(Ratha *et al.,* 2004).

Sathya *et al*. (2020) provide a detailed examination of the implementation and benefits of biometric fingerprint systems in managing attendance. The authors emphasize that biometric systems, particularly those using fingerprint recognition, are superior to traditional attendance methods because they reduce the potential for fraud and enhance the accuracy of attendance records. This technology is particularly beneficial in environments where security and precise record-keeping are critical, such as educational institutions and workplaces. The system outlined in the article utilizes an Arduino microcontroller paired with fingerprint scanners to automate the attendance process. This combination of hardware and software offers a practical and reliable solution for tracking attendance. Additionally, the article explores the potential of multimodal biometric systems, which combine various biometric traits, like fingerprints and facial recognition, to further enhance accuracy and reduce false match rates. The authors discuss the challenges of fingerprint recognition, such as issues related to nonlinear distortion that can impact the system's performance, providing a foundation for future research in this area.

Faisal *et al* (2021) presents the "ONGULANKO" system, an IoT-based biometric attendance logger designed to improve the efficiency and accuracy of attendance management in educational settings. This system integrates biometric fingerprint recognition with IoT technology, offering a more automated and reliable method for recording student attendance. The authors highlight the system's capacity to reduce impersonation and streamline the attendance process, which is often cumbersome with traditional methods. The "ONGULANKO" system includes both an Android application and a web interface, facilitating user interaction and data management. This dual-platform approach is particularly useful for ensuring that the system is accessible and easy to use for both students and administrators. Despite its strengths, the paper notes areas for future development, including the potential for remote matching and database sharing across devices. These enhancements could significantly improve the system's scalability and usability. The authors also recommend upgrading the fingerprint sensor technology to reduce the false rejection rates, a common issue in biometric systems.

Patil *et al*. (2020) developed an IoT-based biometric and RFID attendance system that combines the advantages of both biometric fingerprint recognition and RFID technology to improve attendance tracking in educational institutions. The system addresses common issues such as time wastage and human error, offering a more accurate and efficient method for recording attendance. The biometric component of the system ensures precise identification of students, which improves attendance rates and accountability. The project's success is partly attributed to formative evaluations conducted during the development phase. Stakeholder feedback, gathered through surveys and interviews, was instrumental in refining the system to meet user needs. This iterative development process allowed for early detection of potential issues and the implementation of necessary adjustments to enhance functionality. Post-implementation support, including regular updates and maintenance of the system's hardware and software components, was also identified as crucial for the system's long-term success.

The "Students Monitor Fingerprint Biometric System" (SMFBS) by Oduah *et al.* (2018) represents a significant advancement in the application of biometric technology for student attendance monitoring. The system leverages fingerprint biometric recognition to automate the process of attendance tracking, offering a more secure and accurate alternative to traditional methods like paper-based registers or ID cards. A key strength of the SMFBS lies in its focus on security and accuracy. Traditional attendance methods are often prone to issues such as loss, theft, or fraud, where students can manipulate their attendance records. In contrast, biometric systems like SMFBS use unique physical traits, in this case, fingerprints, making it nearly impossible for students to falsify their presence. As reported by the authors, the SMFBS significantly reduces the chances of impersonation, ensuring that attendance records are both accurate and reliable (Oduah *et al*., 2018). The system's technical implementation also highlights its practicality and efficiency. The SMFBS uses an Arduino Uno microcontroller, a widely available and affordable piece of hardware, to manage the system's operations. The integration of a Liquid Crystal Display (LCD) further enhances the user experience by providing immediate feedback during the fingerprint enrollment and verification process. This makes the system user-friendly, allowing for quick enrollment, averaging 2 minutes per student and even faster attendance marking, with a verification time of approximately 5 seconds (Oduah et al., 2018). Moreover, the SMFBS is designed to be scalable, with the capability to manage up to 5,000 students. This makes it suitable for large educational institutions where managing attendance manually would be cumbersome and time-consuming. The system's scalability, combined with its accuracy and security, positions it as an effective solution for modernizing attendance management in schools and universities. Building upon the strengths of previous works while addressing their limitations, this study presents a robust and scalable IOT biometric attendance system that adjusts to users' routines.

METHODOLOGY

The design of the fingerprint model is divided into two modules, which are the hardware and the software modules. Figure 1 shows the block diagram of the model.

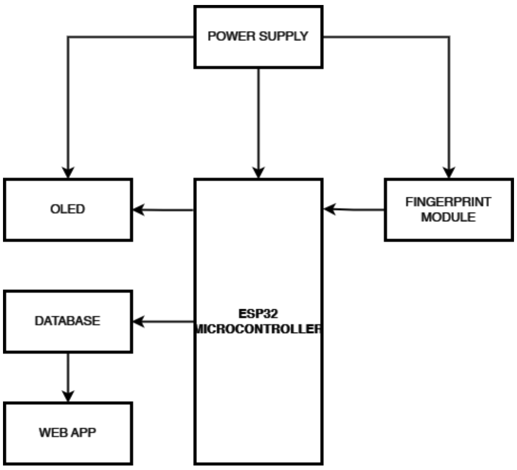

Figure 1: Block diagram of the model

Hardware description

The ESP32 microcontroller is the brain of the system, handling all major processing tasks. It is equipped with a dual-core processor, integrated Wi-Fi, and Bluetooth capabilities, making it well-suited for IoT applications. In this attendance system, the ESP32 receives the fingerprint data from the AS608 sensor, processes it, and checks it against the stored fingerprint templates to verify the user's identity. Once a match is found, or if there is no match, the ESP32 decides the next steps, such as updating the display or sending data to the server. The ESP32 is responsible for communicating with all other components of the system. It sends data to the OLED display to provide user feedback and uses its Wi-Fi module to transmit attendance data to a locally hosted website. The ESP32 makes real-time decisions based on the fingerprint data it receives. For example, if a fingerprint is recognized, the ESP32 will record the time and send this data to the server, updating the attendance log. If the fingerprint is not recognized, the microcontroller will prompt the user to try again. The Fingerprint sensor module is a key component in this system, responsible for capturing and processing biometric data. When a user places their finger on the sensor, it scans the fingerprint and converts the unique patterns of ridges and valleys into a digital image.

This image is then processed to create a fingerprint template, which is a mathematical representation of the fingerprint. The sensor ensures that only authorized individuals can record their attendance, providing a high level of security and preventing fraudulent check-ins. It is the primary interface through which the system authenticates users. The OLED display is the primary interface through which the system communicates with the user. It provides immediate visual feedback during the fingerprint scanning process. This feedback is crucial for guiding the user through the process and ensuring that they know the outcome of their interaction with the system.

The power supply is essential for ensuring that all components in the system have a stable and reliable source of energy. It typically consists of a regulated power source, such as a 5V DC adapter that provides the necessary voltage and current to the ESP32 microcontroller, fingerprint sensor, and OLED display. The power supply must be robust enough to handle the power demands of the system, particularly during data transmission and fingerprint scanning. The Wi-Fi module in the ESP32 enables the system to connect to a wireless network, allowing for real-time data transmission to a remote server or locally hosted website. This module plays a critical role in the IoT functionality of the system, as it allows attendance data to be uploaded instantly to a central database, where it can be monitored and managed by administrators.

The local server or website is where all attendance data is stored, managed, and accessed. The server is typically built using a combination of PHP for server-side scripting and My Stuctured Quaried Language (MySQL) for database management. When the ESP32 sends attendance data over Wi-Fi, this data is received by the server and stored in the MySQL database.

The database is the backbone of the system's data storage, organizing and maintaining all attendance records. Each record typically includes the user's ID, the timestamp of the check-in or check-out, and any other relevant data (such as the IP address of the device used to access the system). The database is structured to allow for efficient storage and retrieval of data, ensuring that even large datasets can be managed effectively. The web interface, built using PHP, is dynamic and interactive, allowing users to interact with the system in real time. PHP scripts handle user input, process it, and generate the corresponding output.

Software description

Arduino IDE

The Arduino IDE is used as an open-source integrated development environment tailored for programming the Arduino board. It offered a friendly platform where code, referred to as "sketches," is written and uploaded directly to Arduino hardware. The Arduino IDE was used to write and upload the code to the mocrocontroller (e,,g the Arduino board) that controls the biometric sensor (e,g the fingerprint scanner) and communicates with the IoT platform In the firmware development the Arduino IDE was used to develop the firmware that runs on the microcontroller, enabling it to read biometric data from sensor, process the data using biometric algorithms and sends attendance data to the IoT platform or backend server. Also, during interaction with sensors and modules, the Arduino IDE is used to integrate the biometric sensor with other modules, such as Wi-Fi or Ethernet modules, to enable IoT connectivity.

PHP Programming Language

PHP, or Hypertext Preprocessor, is an open-source, server-side scripting language that plays a crucial role in web development. PHP is used to create the server-side logic, database interactions and Application Programming Interface (API) integration for the attendance system. It was also used to interact with the database, such as MySQL, to store and retrieve attendance records, user data, and other relevant information. PHP was used to create web web-based interface for the administrators to manage the system, view attendance records and generate reports. It is used to integrate the fingerprint biometric device with a web application, allowing for seamless communication between the device and the system.

Visual Studio Code

Visual Studio Code (VS Code) is used primarily as the code editor for writing and debugging the code for the research software component. It was used in the debugging features used for troubleshooting the system software components, ensuring seamless interaction between the fingerprint sensor, IoT device and the backend server.

RESULTS

The IoT-based fingerprint biometric attendance system was successfully designed and developed. The system comprised several key components, including the ESP32 microcontroller, a fingerprint sensor module, an OLED display, and a web-based application hosted locally for managing attendance data. The entire system was packaged within an acrylic fiber housing to ensure durability and portability. The integration of hardware and software components was meticulously planned and executed to achieve seamless operation. The ESP32 microcontroller served as the core processing unit, interfacing with the fingerprint sensor to capture biometric data, which was then transmitted to the web application via Wi-Fi. The web application provided a user-friendly interface for administrators to enrol new users, update existing records, and generate attendance reports.

System Testing and Performance Evaluation

System testing was conducted in multiple phases, including pre-assembly testing, post-assembly testing, and real-world testing in an educational setting. The objective was to evaluate the system's performance in terms of accuracy, speed, reliability, and user satisfaction.

Pre-Assembly Testing

Before assembling the system, each component was individually tested to ensure functionality. The fingerprint module, OLED display, and ESP32 microcontroller were tested using sample codes and basic circuits to verify their operation. The fingerprint module's ability to capture and recognize fingerprints was tested using multiple samples from different individuals. The OLED display was evaluated for clarity and responsiveness, while the ESP32 was tested for its Wi-Fi connectivity and data processing capabilities. All components passed the pre-assembly tests, confirming their readiness for integration.

Post-Assembly Testing

After the system was fully assembled, post-assembly testing was conducted to identify any issues arising from the integration of components. The system was powered using a micro-USB cable, and its overall functionality was evaluated. The fingerprint module was tested for its ability to accurately capture and transmit data to the ESP32, which then displayed the results on the OLED screen. The web application was accessed via a local network to verify data transmission, user interface functionality, and data storage. The system performed as expected during post-assembly testing, with accurate data capture and seamless communication between hardware and software components. No significant issues were detected, indicating a successful integration process.

Outputs

The system features two primary outputs:

- The hardware output (the OLED display)
- The software output (the web interface)

The Hardware Output

The OLED display serves as an immediate feedback mechanism for the user, indicating whether their attendance has been successfully recorded. It displays an appropriate message confirming the success or failure of the attendance capture process. This feature is crucial in providing real-time feedback to users, ensuring they are informed about the status of their attendance.

Figure 2: The hardware output

The Software Output

The web interface is designed for administrative use. It allows administrators to access attendance records, manage user information, and export attendance data if needed. The interface is connected to the system's database, which stores the attendance logs captured by the fingerprint module. The ability to export data in spreadsheet format is particularly useful for further analysis or reporting purposes.

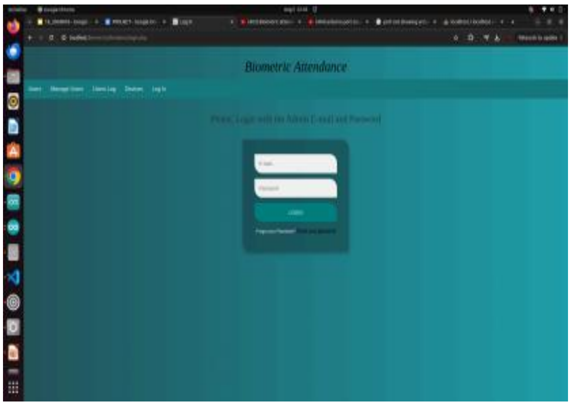

Figure 3: Web interface - Admin login page

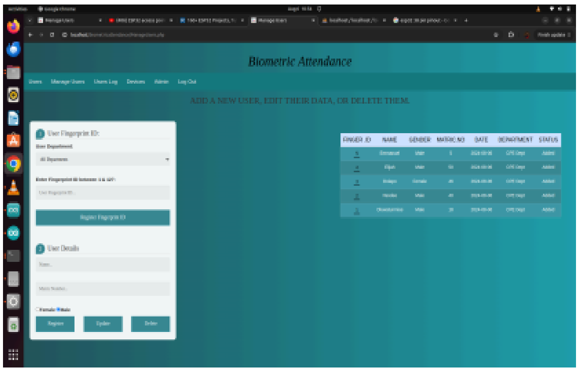

Figure 4: Web interface - Manage Users page

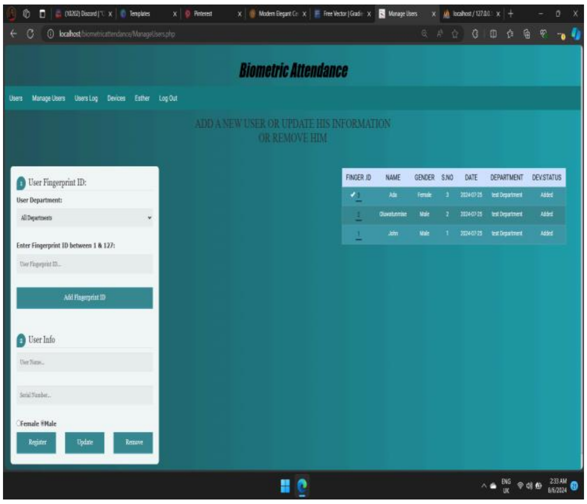

Figure 5: Web Interface - User log

The results from the testing phase demonstrate that the IoT-based fingerprint biometric attendance system meets the primary objectives of the study. The system effectively addresses the limitations of traditional attendance tracking methods by providing a more accurate, efficient, and secure solution. While the system performed well in the testing environment, challenges related to network connectivity and scalability highlight the need for further research and development. Nonetheless, the system's positive impact on user experience and administrative efficiency underscores its potential as a transformative solution for attendance tracking.

Packaging

The project's packaging was crafted from acrylic fiber, providing a durable and protective enclosure for the system's components. The packaging securely houses the circuit board, fingerprint module, OLED display, and ESP32 microcontroller, ensuring all parts are well-organised and shielded from external factors. As illustrated in Figure 6, the integration of these components into the packaging box is clearly demonstrated. Additionally, the packaging is designed with portability in mind, making it convenient for users to carry the system with ease.

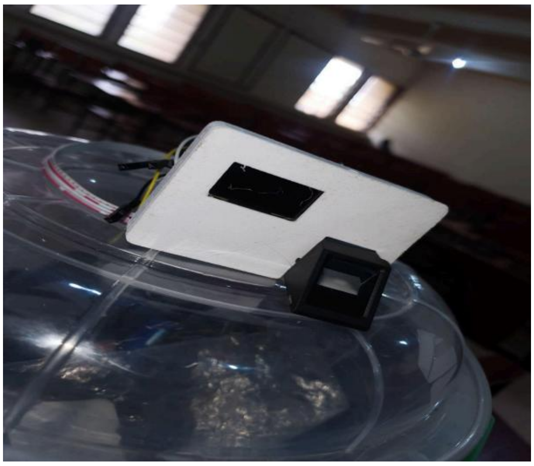

Figure 6: Integration of Components into packaging box

CONCLUSION

In conclusion, the development of an IoT-based fingerprint biometric attendance system has successfully addressed the limitations of traditional attendance methods in educational institutions. The system's design, which combines the accuracy of biometric technology with the advanced capabilities of IoT, offers a modern, efficient, and reliable solution for attendance management. The findings from this research demonstrate the system's effectiveness in improving accuracy, enhancing user experience, and providing administrators with greater control over attendance data. The attendance system verifies identities quickly under 1-2 seconds, with high accuracy, while the dual output configuration, an OLED display for immediate feedback and a web interface for remote data management, proved to be a critical feature that contributed to the system's overall success.

REFERENCES

Bhagat, S. (2022). Face recognition attendance system. *International Journal for Research in Applied Science and Engineering Technology, 10*(1), 280–283. https://doi.org/10.22214/ijraset.2022.39702

Ch, K. (2017). Various biometric authentication techniques: A review. *Journal of Biometrics & Biostatistics, 8*(5). https://doi.org/10.4172/2155-6180.1000371

Daugman, J. (2020). *How iris recognition works*. Springer.

Faisal, F., Hossain, S. A., & Sattar, A. (2021). ONGULANKO: An IoT based biometric attendance logger. In *Proceedings of the 2021 International Conference on Intelligent Computing and Control Systems (ICICCS)* (pp. 1-6). IEEE. https://doi.org/10.1109/ICICCS51141.2021.9432113

Jain, A. K., Ross, A., & Nandakumar, K. (2011). *Introduction to biometrics.* Springer.

Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). *Handbook of fingerprint recognition.* Springer.

Oduah, U. I., Nwaekwu, V. N., & Anyadubalu, F. O. (2018). Students monitor fingerprint biometric system. *FUW Trends in Science & Technology Journal, 3*(1), 252-256. Retrieved from http://www.ftstjournal.com

Parkhi, O. M., Vedaldi, A., & Zisserman, A. (2015). Deep face recognition. In *British Machine Vision Conference* (pp. 41.1-41.12).

Patil, A., Mahla, A., & Sonawane, S. (2017). IoT based attendance system. *International Research Journal of Engineering and Technology (IRJET), 4*(2), 2395-0056.

Patil, S., Bhosale, A., Bagade, M., Khopade, S., & Joshi, S. (2020). IoT-based biometric and RFID attendance system. *International Journal of Advance Research and Innovative Ideas in Education, 6*(2), 518-522. Retrieved from https://www.ijariie.com

Ratha, N. K., & Bolle, R. M. (2004). *Automatic fingerprint recognition systems.* Springer.

Sathya, D., Vallarasu, R., Gomathi Sankar, A., Habeeb Rahman, & Guru Sarathy. (2020). Biometric fingerprint for attendance system. *Sadakath: A Research Bulletin, 7*(2), 1-5.

Wayman, J. L., Jain, A. K., Maltoni, D., & Maio, D. (2005). *Biometric systems: Technology, design, and performance evaluation.* Springer.