IoT BIOMETRIC ATTENDANCE SYSTEM NEXUS WITH AUTOMATED DATA STREAMLINING AND SOFTWARE ORCHESTRATION

1st N Mohammed Nowsath
Dept of CSE
Dr.MGR Educational and Research Institute
Chennai, India
nowsath2003@gmail.com

2nd SK Jhothish Kumar
Dept of CSE
Dr.MGR Educational and Research Institute
Chennai, India
skjhothish123@gmail.com

3rd M Gopala Krishnan
Dept of CSE
Dr.MGR Educational and Research Institute
Chennai, India
gopal.krishnan28102002@gmail.com

4th M Devika Asst.Prof
Dept of CSE
Dr.MGR Educational and Research Institute
Chennai, India
devika.cse@drmgrdu.ac.in

***Abstract*— Biometric technology involves the recognition and authentication of individuals by examining unique characteristics of the human body. In modern times, attendance is taken traditionally in educational institutions using paper and pen, it increases the workload for teachers and also takes time. The purpose of this design is to make a biometric system for students. As the world becomes modern and digitalized, so we need to make a portable system for attendance with an embedded software application. By this proposal, authorized access will be given to the teacher to activate the biometric for each period. After student attendance is recognized by a fingerprint sensor the required messages will be sent to their parents for every period and the data will be stored in the application. In addition, the proposed system could increase productivity and reduce the manual process, truancy, and lateness in educational institutions.**

***Keywords*-- IoT, Attendance, Fingerprint, Biometrics, Firebase, Android Application**

I. INTRODUCTION

The demand for efficient attendance management systems has intensified in the dynamic landscape of educational technology. This paper introduces a cutting-edge solution that leverages the power of Internet of Things (IoT) technology, biometric authentication, and embedded software to revolutionize the traditional attendance tracking process. Our proposed system not only ensures accurate and secure identification through students' biometrics but also seamlessly integrates with automatic data storage, offering educational institutions a comprehensive and streamlined approach to attendance monitoring. This innovative convergence of hardware and software promises to enhance efficiency, reduce administrative burden, and elevate the overall experience of attendance management in educational settings.

In this system, students' unique fingerprints serve as their digital signatures, eliminating the possibility of proxy attendance and ensuring the utmost data accuracy. The integration of IoT enables real-time data collection, transmission, and analysis, allowing educators and administrators to access attendance records instantaneously, regardless of their physical location. n. Beyond just automating attendance, this system offers a wealth of potential benefits, such as identifying patterns in attendance behavior, providing early intervention for students with irregular attendance, and enhancing campus security by restricting access to unauthorized individuals.

The importance of monitoring student attendance within the educational domain is well-established. It serves as a fundamental metric for assessing students' engagement and participation in the learning process. Traditionally, attendance was taken through manual roll calls, a time-consuming, error-prone, and archaic process. The advent of barcode scanners brought some automation but still fell short of addressing the need for a reliable, tamper-proof, and efficient attendance tracking system. The digital age has magnified the urgency of seeking advanced, automated solutions in educational institutions, pushing for innovation to keep pace with evolving demands. In response, IoT-based biometric attendance systems have emerged as a beacon of technological progress, offering a holistic and dependable solution for monitoring student presence.

As we delve deeper into the intricate workings of this IoT-based biometric attendance system, we will explore the technology's underlying principles, its advantages over conventional methods, and its potential impact on the educational landscape. Moreover, we will delve into the ethical considerations surrounding biometric data usage and the steps taken to ensure the security and privacy of students' personal information. Join us on this transformative journey as we unlock the

future of attendance tracking, where precision, efficiency, and security converge to create an educational experience like no other.

In conclusion, the integration of IoT technology with biometric fingerprint authentication in student attendance systems heralds a remarkable stride forward in educational technology. By automating attendance tracking and heightening its precision, these systems alleviate administrative burdens, empower educators with real-time insights, and contribute to a more efficient educational environment. As we delve deeper into the intricacies of IoT-based biometric attendance systems for students, this exploration will unveil not only their technical intricacies but also their profound impact on education, discussing the benefits, challenges, and wider implications for the future of learning.

II. RELATED WORKS

[7] Here in this paper the authors "L.S. Ezema, C.K.A. JoeUzuegbu, J. N. Eneh, and I. Amanze" have introduced and executed a dependable, secure, swift, and effective system as a substitute for a conventional and undependable manual system. The proposed system is adaptable for implementation in various organizations and institutions. Its deployment is anticipated to streamline processes, diminish the workload on administrators, and transition from traditional stationery to electronic devices. Although a system yielding the projected outcomes has been created, opportunities for enhancement persist.

[8] The authors "Karthik Krishnamurthi, S.Irudhaya Mary, B.N Sumalatha, and Adler Pereira" introduces a biometric system centered around fingerprints for monitoring attendance. This system employs a handheld fingerprint sensor to accurately track individuals' attendance. Through experimentation, the research demonstrates that the implementation of such a fingerprint-based system effectively mitigates fraudulent activities, thereby enhancing the dependability of attendance records.

[6] In this paper, Yash Mittal, Aishwarya Varshney, Prachi Aggarwal, Kapil Matani, and V. K. Mittal have introduced a scalable solution designed for identification and authentication purposes, offering a viable alternative to RFID-based attendance management systems. Their implemented system has the flexibility to extend its functionality to multiple locations and adapt to various scenarios. Specifically tailored for educational institutions, the Classroom Attendance Management System serves as an effective tool for recording attendance during lectures and examinations. The system utilizes a fingerprint scanner to capture new fingerprints when a user places their finger on the device. Subsequently, the captured fingerprint image is compared with templates already stored in the database. Notably, the authors have expanded the system to include an online platform where users can generate attendance reports. The performance evaluation results for both the Authentication and Classroom Attendance Management Systems have yielded positive and promising outcomes.

[9] The authors Mohamed Basheer K P and Raghu C V have developed an innovative Fingerprint Attendance System designed for classrooms, aiming to automate the attendance process in educational institutions. The system consists of a portable hand-held device and a host computer equipped with a user-friendly graphical interface (GUI) application. The handheld device, powered by a rechargeable battery, integrates a fingerprint module, microcontroller, Real-Time Clock (RTC), buttons, and a Graphic Liquid Crystal Display (GLCD). By leveraging this system, students can effortlessly record their attendance during lectures by placing their finger on the sensor, eliminating the traditional manual attendance calls.
The GUI application on the host computer serves as a valuable tool for teachers, enabling them to efficiently manage the device, transfer student lists, and maintain comprehensive attendance records. Additionally, the system incorporates robust security features to thwart unauthorized access. The successful implementation and testing of the prototype underscore the system's potential in simplifying and enhancing attendance management within classroom settings.

[3] Here in this paper the authors "Jordi Sapes, and Francesc Solsona" the project named "FingerScanner" is presented as a security system implemented on a Raspberry Pi B+ with Node.js as its primary programming language. The system incorporates a Fingerprint Scanner GT(511C1R), a magnetic lock, and a switch to create a comprehensive solution for user validation and access control. Following a client-server model, the application utilizes Angular.js for the client and Node.js for the server. It provides administrators with a web interface for user management, allowing tasks such as user registration, deletion, and updating. The secure identification is achieved through the fingerprint scanner, which controls access by activating and deactivating a magnetic lock. The project details various functionalities, including fingerprint enrollment, identification, and deletion, highlighting its suitability for real-time applications and embedded systems.

III. SYSTEM METHODOLOGY

In our proposed system, we have given an access control to access the biometric system with an embedded application. Every period the status of the student's attendance information will be sent to their respective parents' mobile. Thus, the main objective is to make the regularity of the students and reduce the paper and logbook traditional method. All the data about the student's attendance will be stored in the given software and the attendance percentage will be calculated automatically so there will be no need for any separate application.

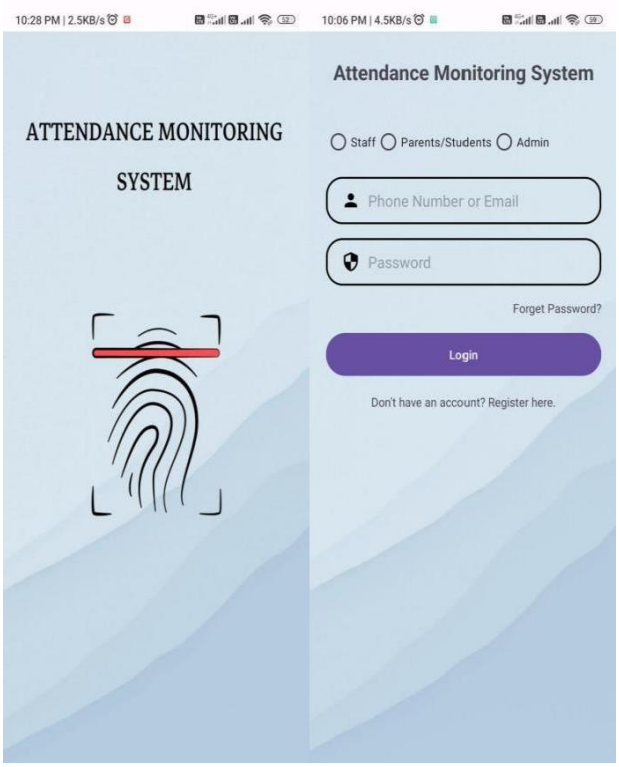

Figure 1. First & Login Page of Embedded Software

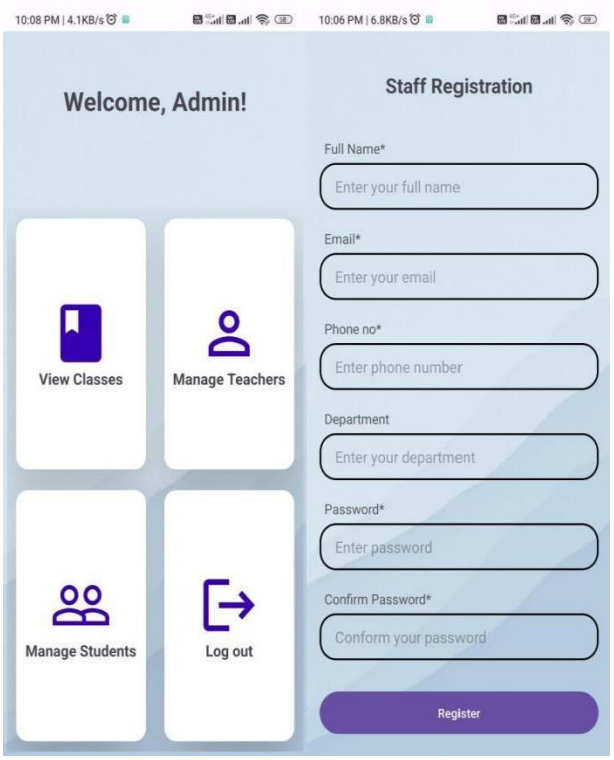

Figure 2. Admin Page & Staff Registration

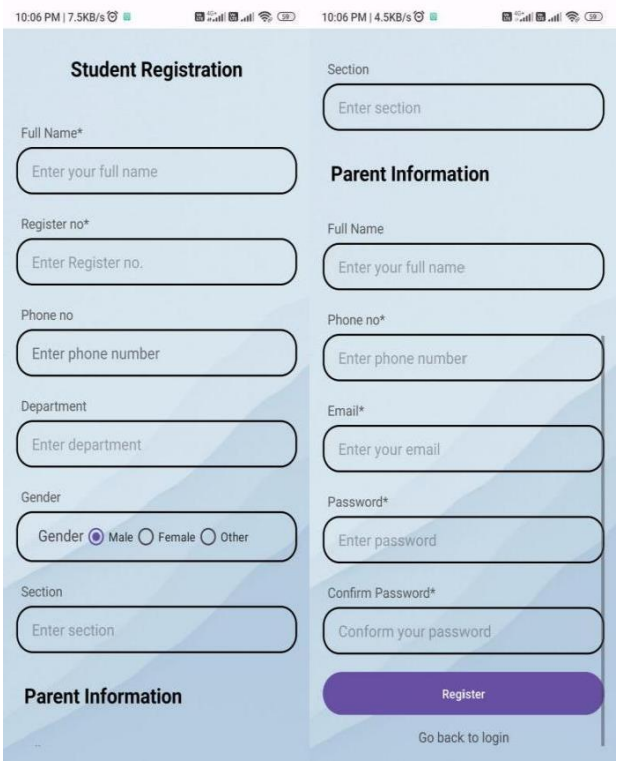

Figure 3. Student Registration

IV. SYSTEM ARCHITECTURE

A. FINGERPRINT MODULE:

This is the hardware component responsible for capturing fingerprint data. It typically consists of a fingerprint sensor, processing unit, and storage for

fingerprint templates. When an individual places their finger on the sensor, it captures the fingerprint image and processes it to extract unique features that can be used for identification or verification.

B. ESP32:

The ESP32 acts as the microcontroller that interfaces with the fingerprint module. It reads data from the fingerprint module, processes it, and then communicates with external services MQTT. These boards are often used for their connectivity and processing capabilities.

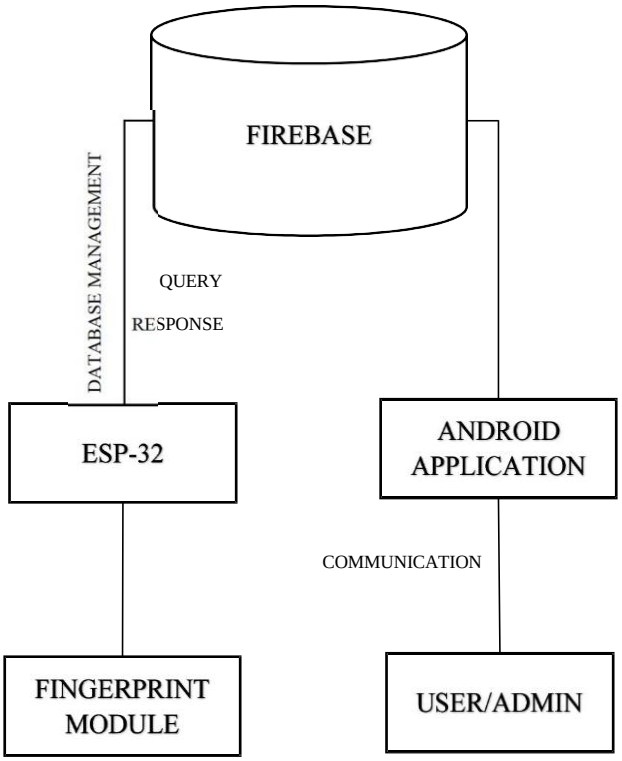

Figure 4. Architecture of the proposed system

B. ESP32:

The ESP32 acts as the microcontroller that interfaces with the fingerprint module. It reads data from the fingerprint module, processes it, and then communicates with external services MQTT. These boards are often used for their connectivity and processing capabilities.

C. FIREBASE:

Firebase is a popular mobile and web application development platform offered by Google. It includes various services, including a real-time database, authentication, and cloud functions. Firebase can be used to securely store and manage attendance data in real-time, making it accessible to applications and users.

Firebase includes a real-time NoSQL database where attendance data can be stored. This database is accessible from various platforms, and it ensures data synchronization in real-time. Firebase also provides data security and user authentication features.

D. APPLICATION:

This is the user-facing component of the attendance system. It can be a mobile app, web app, or desktop application that allows users to interact with the attendance data stored in the cloud database. Users can view attendance records, generate reports, and perform other tasks related to attendance management.

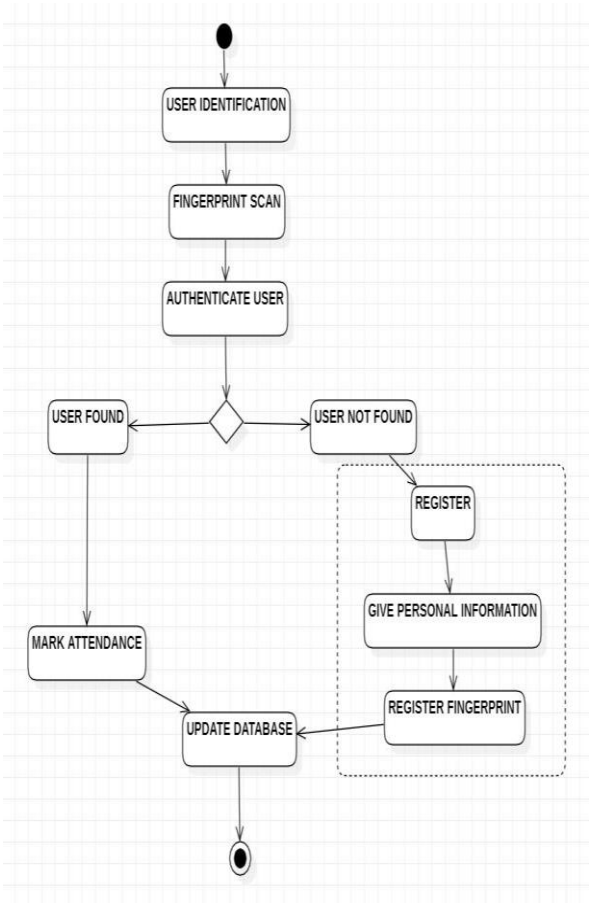

Figure 5. Process of Attendance Marking

V. RESULT AND DISCUSSION

Obtain the necessary hardware components like fingerprint modules, ESP32 microcontrollers, and other required sensors or devices. Set up software tools, including the ESP32, and Firebase for cloud_based storage and development environment for the application.

Connect the fingerprint module to the ESP32 and ensure proper wiring and communication between

the two components. Develop the interface code to capture and process fingerprint data, allowing for functions like enrollment and identity verification.

Implement code on the ESP32 for processing fingerprint data, implement logic for attendance tracking, including identifying unique fingerprints and sending data to the firebase, and enable MQTT connection on ESP32 to facilitate communication with other components.

Create a Firebase account, set up a new project, and obtain the necessary credentials. Develop code to interact with Firebase real-time database, defining the structure for storing attendance records and student information.

We develop the mobile application for user-facing applications. Develop the application code, enabling users(teachers, administrators, students, or parents) to interact with attendance data, generate reports, and manage student information.

Conduct unit tests for each component to ensure they function correctly. Perform system integration testing to verify seamless communication and accurate attendance tracking.

Deploy the system component in the educational institution. Provide training for end-users on how to use the system effectively.

VI. CONCLUSION

The proposed IoT-based attendance system presents a promising solution to be challenges associated with traditional attendance management methods. By leveraging biometric authentication and IoT technology, this system aims to enhance accuracy, reduce administrative workload, and provide real-time attendance data for educational institutes.

The functionalities of the system can be further enhanced through the following recommendations:

- A future enhancement may explore additional security measures, scalability for larger institutions, and integration with academic platforms for comprehensive student data management.
- Investigate advanced biometric technologies beyond fingerprints, such as facial recognition or iris scanning, to offer a broader range of options for user identification.
- Implement a multi-modal biometric system that combines multiple biometric authentication methods for increased accuracy and security.
- Expand the use of IoT sensors beyond attendance tracking. For example, incorporate sensors to monitor classroom conditions, ensuring an optimal learning environment.
- Continuously improve the mobile application's user interface and functionality based on user feedback. Consider additional features such as real-time notifications, in-app analytics, and personalized dashboards.
- Implement automated reporting features that generate detailed attendance reports for administrators, teachers, and parents. Set up customizable notifications for specific attendance events.
- Integrate geolocation tracking to verify the physical presence of students, especially in scenarios where remote or off-site learning is prevalent.
- Research and implement energy-efficient IoT devices to minimize power consumption and contribute to sustainability efforts.

REFERENCES

[1] Nandini, S., & Sasikala, M. (2019). Fingerprint-based attendance system with automatic door unlocking system. International Journal of Recent Technology and Engineering, 8(2).

[2] Rathgeb, C., & Busch, C. (2017). How to break fingerprint template protection: A practical attack on Vkansee's vector field-based fingerprint template protection. IEEE Transactions on Information Forensics and Security, 12(5),

[3] Jordi Sapes, Francesc Solsona “FingerScanner: Embedding a Fingerprint Scanner in a Raspberry Pi”, Published on 6 February 2016

[4] Kaur, H., & Kaur, A. (2016). A Review on Fingerprint Biometric Authentication Systems. Procedia Computer Science, 85, 893-900.

[5] Rattani, A., Ross, A., & Jain, A. K. (2015). Fingerprint liveness detection: Past, present, and future. In Biometric Security and Privacy (pp. 219-254). Springer.

[6] Yash Mittal, Aishwary Varshney, Prachi Aggarwal, Kapil Matani and V. K. Mittal, "Fingerprint Biometric based Access Control and Classroom Attendance Management System," IEEE Transl. New Delhi, India, 17-20 Dec. 2015

[7] L.S. Ezema, C.K.A. Joe-Uzuegbu, J. N. Eneh and I. Amanze, "Fingerprint Based Attendance Management System," International Journal of Scientific & Engineering Research, Volume 6, Issue 7, July-2015

[8] Karthik Krishnamurthi, S.Irudaya Mary, B.N.Sumalatha, Adler Pereira, "Fingerprint Based Attendance System", IJARCCE , Vol. 4, Issue 3, March 2015

[9] K.P.Mohamed Basheer, C.V.Raghu, "Fingerprint attendance system for classroom needs," in 2012 IEEE India Conference (INDICON), 2012

[10] Rathgeb, C., & Uhl, A. (2011). A survey on biometric cryptosystems and cancelable biometrics. EURASIP Journal on Information Security, 2011(1), 3.

[11] Maltoni, D., Maio, D., Jain, A. K., & Prabhakar, S. (2009). Handbook of Fingerprint Recognition. Springer Science & Business Media.

[12] Fierrez, J., Ortega-Garcia, J., Gonzalez-Rodriguez, J., Bigun, J., & Akarun, L. (2006). Recent advances in fingerprint recognition. Handbook of Biometrics, 2.

[13] Jain, A. K., Ross, A., & Prabhakar, S. (2004). An Introduction to Biometric Recognition. IEEE Transactions on Circuits and Systems for Video Technology, 14(1), 4-20.

[14] Zhang, D., & Jain, A. K. (2002). A hierarchical approach to human face verification. In Proceedings of the 2002 International Conference on Image Processing (Vol. 3, pp. III-37). IEEE.