SvedbergOpen
DISSEMINATION OF KNOWLEDGE
International Journal of Artificial Intelligence and Machine Learning
Publisher's Home Page: https://www.svedbergopen.com/
Research Paper Open Access

Fingerprint Based Student Identification System For Secure Attendance Using Iot

[1*]S. Bharathi, [2]Deepali Prashant Pawar, [3]Dr Seshu Babu Pulagara, [4]Dr. Arijit Chakraborty [5]Manikandan Rajagopal, [6]Dr Sangeetha V

[1*]Associate professor, Department of Electronics and Communication Engineering, Dr. Mahalingam College of Engineering and Technology, Coimbatore, India https://orcid.org/0000-0001-9638-3779
bharathi_mani@yahoo.com
[2]Assistant Professor, Computer Department, SNJB's KBJ COE,Chandwad, 423101 https://orcid.org/0009-0008-6420-2839 pawar.dpcoe@snjb.org
[3]Assistant Professor, National Institute of Technical Teachers Training and Research Chennai, Tamil Nadu - 600 113 https://orcid.org/0000-0003-4410-2562 seshubabu@nitttrc.edu.in
[4]Assistant Professor, Department of Bachelor of Computer Applications, The Heritage Academy, Chowbaga Road, Anandapur, Kolkata: 700107, West Bengal https://orcid.org/0000-0002-7111-7711
arijitchakraborty.besu@gmail.com
[5]School of Business and management, Christ University, Bangalore https://orcid.org/0000-0001-7915-0180
Manikandan.rajagopal@christuniversity.in
[6]Associate Professor, Kristu Jayanti Institute of Technology (KJIT), School of Computational and Physical Science, Kristu Jayanti Deemed to be University, Bengaluru https://orcid.org/0000-0002-5768-9297
sangeetha.v@kristujayanti.com

Abstract: Traditional systems consume a lot of resources and are vulnerable to security issues such as proxy attendance, so a fingerprint-based student identification system integrated with IoT technology is proposed to address these challenges. This paper introduces an IoT-based Fingerprint Student Identification System for secure and efficient attendance management in educational institutions. The system is composed of IoT hardware, such as a fingerprint sensor, microcontroller, and IoT modules like ESP8266 for connectivity, and uses the Blynk platform to provide a user-friendly interface for real-time attendance tracking and task planning on the activity and task dashboard. This work includes selecting compatible hardware, using Blynk APIs for secure data communication, and designing a customizable app to improve the experience of managing attendance.

Keywords: Biometric, wifi module, IoT, Fingerprint Sensor, Attendance, Arduino UNO

1. Introduction

Education systems have been plagued by malpractice and the use of unauthorized proxies for taking attendance, and with the global growth of the education industry, a robust, efficient, and scalable attendance system has become increasingly necessary. There have been attempts at using various technologies to solve this problem, such as biometrics like finger print facial and iris recognition, all of which are advanced and effective, but with significant drawbacks; facial recognition systems, for example, may necessitate high-quality cameras, substantial processing power, and environmental factors like lighting. Similarly, iris recognition, while highly accurate, involves expensive hardware. However, Fingerprint-based biometric attendance system [1,2] is cost-effective and more efficient than other systems. Fingerprint technology is proven to be reliable, ubiquitous, and easy to implement with existing infrastructure. Unlike other biometric methods, fingerprint scanners are inexpensive and low maintenance. For the implementation of automatic attendance monitoring system based on finger print, the existing systems are based on RFID [3,4], GSM [5], and web-based [6] techniques.

In addition to streamlining attendance, these systems minimize the potential for malpractice, such as buddy punching or falsified records. This approach proposes to display finger print based attendance for a particular period and task/class assigned for the student while entering the attendance which makes it more accurate and accountable

for institutions of all sizes. The system comprises a fingerprint scanner, an Arduino Uno microcontroller, and an ESP8266 Wi-Fi module to capture a digital image, process the image to extract identifying features, and upload data to the cloud for real-time access to up-to-date attendance records, monitor trends, generate reports, and data-driven decision on curriculum and student performance. It uses a fingerprint scanner, an Arduino Uno microcontroller, and an ESP8266 Wi-Fi module that captures a digital image, processes it to extract identifying features, and uploads data to the cloud for real-time access to up-to-date attendance records, monitor trends, generate reports, and data-driven decision on curriculum and student performance.

The system also seamlessly integrates with educational management systems and uses APIs to communicate with hardware and the app, where data is displayed and managed securely, using the Blynk app interface to give real-time insights into activity and tasks, and monitoring the dashboard for higher authorities and parents. Cloud connectivity allows secure remote access to attendance data, facilitating administrative processes and increasing transparency for all stakeholders.

2. Literature Review

Aayushi Singh et al. [7] describe a mobile-based attendance system that uses fingerprint recognition and geo fencing to overcome the limitations of traditional attendance methods and reduce the burden on teachers and students by allowing them to record attendance through a smartphone application. Biometric authentication provides security and accuracy, while geo fencing ensures that attendance is marked only in designated areas, reducing the risk of abuse, making this approach particularly useful in resource-constrained environments such as government schools. Seng Chun Hoo and Haidi Ibrahim [8] review the hardware requirements for biometric-based attendance systems in education, including the increased application of biometric recognition technology, a process that uses physical or behavioral characteristics, such as fingerprints, face, iris, and voice, to verify a person's identity, which can replace manual attendance methods that are tedious, time-consuming, and susceptible to fraud. Over the past decade, the development of biometric-based attendance systems in educational settings has been enhanced by advancements in hardware requirements.

Ajibola Oyedeji et al. [9] developed a more secure student identification and authentication system that can prevent impersonation during examinations, a problem that plagues institutions in developing countries such as Nigeria, by using radio frequency identification (RFID) and biometric fingerprint technology. The system includes an Arduino microcontroller, a fingerprint reader, an RFID reader, and a desktop application for easy interface with a database to store student data such as fingerprints for verification. Fahmida Yesmin Chowdhury [10] suggests an automated attendance management system that uses fingerprint biometrics, QR code scanning, and GPS to automate attendance in educational institutions, improving the time and accuracy in large classrooms where manual methods are tedious and inaccurate, and it prevents fraudulent attendance by verifying the location of a student using GPS and identifying specific classes using QR codes. V Ruhitha et al. [11] describe an Internet of Things (IoT)-based attendance management system that uses facial recognition, which is deployed on Raspberry Pi 3B hardware.

In [9], Ajibola Oyedeji et al. proposed a student identification and authentication system to prevent impersonation during examination which occurs in every institution mostly in the developing countries like Nigeria. This system will make use of RFID and biometric fingerprint. The vital components consist of an Arduino microcontroller, fingerprint reader, RFID reader, and desktop application. The desktop application interfaces with the database to store student data which includes and can be used for fingerprint verification. An automated attendance management system for educational institutions that make use of fingerprint biometrics, GPS. And QR code scanning has been suggested by Fahmida Yesmin Chowdhury [10]. The authors have seen the time-consuming and inaccurate nature of manual attendance systems in large classrooms for engineering students. The possibilities of fraud are reduced by monitoring the GPS of a student to verify the attendance as well as identifying the specific class using QR codes. According to V Ruhitha and others [11], the attendance management system based on Internet of Things (IoT) that makes use of facial recognition deployed on Raspberry Pi 3B.

Several studies have highlighted the need for a comprehensive set of criteria and metrics to evaluate biometric systems thoroughly, but many of the systems currently evaluated are limited in the datasets and metrics used, which limits the scope for their discovery and exposes them to security and privacy issues. As biometric systems are used increasingly for protection of identity, addressing their security and privacy issues is essential for their wider use. Mohammad Nabati et al. [14] presented a new approach to tackle this problem in fingerprint-based positioning methods, especially regarding the effect of noise in RSS vectors. In these systems, RSS vectors from access points are measured at reference points and stored in a database for training pattern recognition algorithms. The RSS signals are often corrupted by various types of noise, which can degrade the accuracy of the positioning systems. The authors propose a fast and accurate positioning algorithm that uses a DNN to learn the distribution of available RSS samples in the offline phase, instead of using averaging.

The results show that the algorithm proposed outperforms traditional regression algorithms, such as deep

neural network regression, Gaussian process regression, random forest, and weighted KNN, in a single RSS sample and multiple RSS samples. According to Reena Garg [15], fingerprint recognition systems, known for their invariance and consistency, can be improved via deep learning techniques. The classification performance of a fingerprint recognition system greatly relies on the feature extraction. Recently, deep learning models have been used to extract fingerprint features. As per earlier research, a big challenge which can impact such systems is a small sample size used. With this in mind Garg has proposed two novel techniques – inversion and multi- augmentation that generate new images for each feature maps to enrich the sample size. It is clear from the literature survey that the existing systems do not have cross functional capabilities and are functionally overhead to implement. The current work propose an alternate methodology which address the critical issue in the faucets of attendance management system.

3. Proposed Methodology

An IoT based Fingerprint Attendance System is proposed which can eliminate the traditional manual roll calls or sign in sheets method prone to error, time-consuming and fraudulent practice like proxy attendance by integrating hardware components such as fingerprint sensors, Wi-Fi modules and LCD displays with cloud-based software for real-time data management and analytics providing a secure automated user friendly solution leading to improved accountability and reduced human intervention.

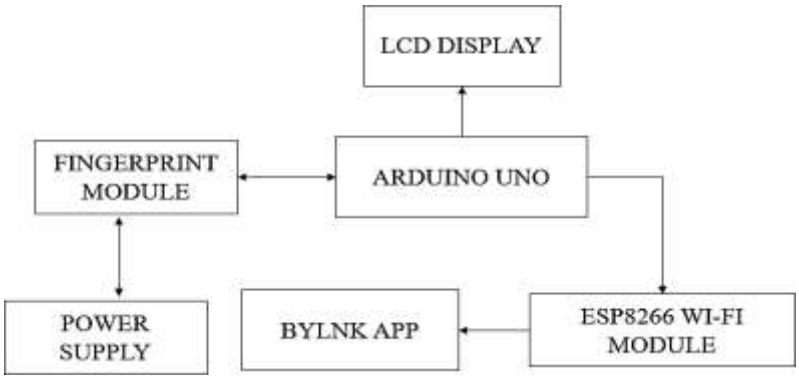

Figure 1. Block diagram of the proposed system

The hardware and software components of the proposed system are integrated as a block diagram shown in fig.1, where the Arduino Uno microcontroller manages data flow between the fingerprint module, the ESP8266 Wi-Fi module, the LCD display, and the Blynk app. The fingerprint module captures the unique biometric data of the students, which is processed by the Arduino Uno before being sent via the ESP8266 Wi-Fi module to a cloud server for secure storage and comparison. The LCD display, located at the user interface, provides real-time feedback to students, confirming attendance or alerting them to errors in the scanning process. The system uses a dedicated power supply to ensure consistent performance in areas where electricity is unreliable. The system also has an enrollment and authentication process including activity and task dashboard, which is the heart of the system.

Fingerprint registration of students is done every academic term during the enrollment process. The fingerprint sensor is able to scan the fingerprint of each student multiple times to make a complete biometric template. The document is stored as Encrypted in cloud database for Access. To mark their daily attendance, students must place their finger on the scanner. This data is captured and sent to the cloud server for authentication. The scanned fingerprint is compared with stored templates using a strong matching algorithm on the server. When a match is detected, the student's attendance is automatically taken and a display on LCD confirms it. The system uses advanced encryption protocols to protect biometric data from unauthorized access, ensuring the security of the data. To prevent sniffing attacks in transit, all communications between the system starvation hardware and the cloud server are encrypted with TLS/SSL. Along with that, the biometric data which is stored in the cloud is AES-256, an encryption standard. The user data of the system is further arranged in accordance with the data protection law including the General Data Protection Regulation or GDPR. The protective arrangements keep biometric data confidential and the measures guarding the biometric system against unauthorized usage or damage.

The system has been made scalable and maintainable to be suitable for small school to large university level. The system's cloud-based system design makes it scalable as new fingerprint scanners or additional server capacity

can simply be added without the need for any major hardware changes. The system is monitored in real-time. Software updates take place in order to enhance usability and respond to new security threats. Backups are automated. A disaster recovery plan is prepared to prevent a system failure and allow the working and data availability. By maintaining the system at a low code, it would be easy and less-painful to scale and maintain it. The system also gives great importance to user experience and accessibility. This makes sure that all stakeholders including students, teachers, and administrators can use it. Web and mobile applications' user interfaces are designed to be intuitive and easy to use, requiring little or no training. Users can register their fingerprints, view attendance history and manage data through these interfaces.

The system is built to support the visually impaired and those with other disabilities with screen reader and voice command functionalities. Students can easily use a fingerprint scanner since it provides clear visual feedback while performing the scanning operation. By focusing on accessibility and usability, the system will be increasingly adapted by the stakeholders for efficient management of attendance.

4. Results and Discussion

The fingerprint-based attendance system works in a systematic manner along with proper functioning to track attendance of students. The steps are various.

Step 1: Connect the fingerprint sensor and Arduino.
Step 2: install the fingerprint sensor library.
Step 3: Fingerprint Registration
Step 4: Fingerprint Confirmation.
Step 5: Linking Mobile to ESP8266 Wi-Fi Module.

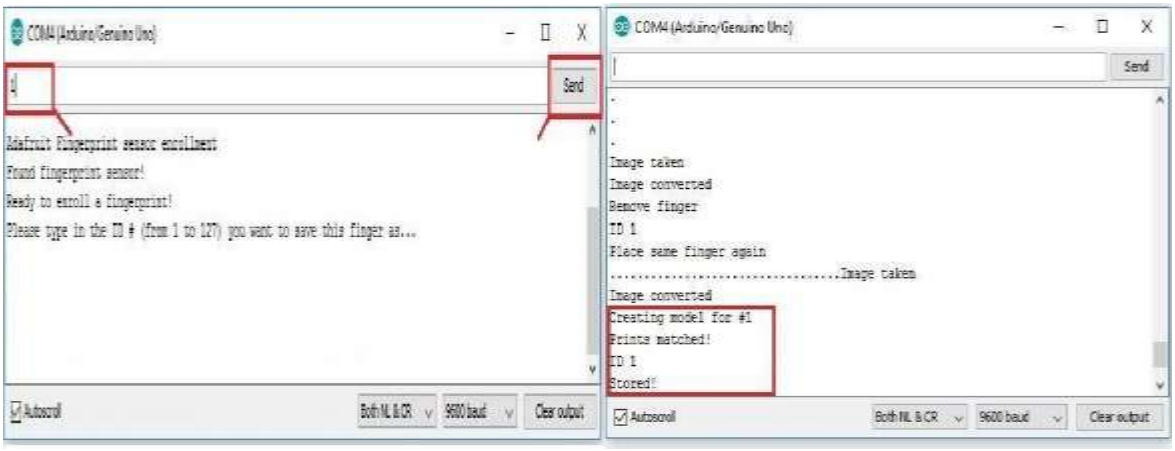

Figure.2 (a) Finger print enrollment process (b) Finger print verification process

When the fingerprint sensor module is connected to the Arduino, a new fingerprint can be added according to the interface. Figure 2 displays a screenshot of the enrollment and verification phases of the programme. You will need to press the same tip of the finger on the scanner twice. As shown in figure 2, the “Prints matched!” message will successfully save the fingerprint to the system. If the desired outcome is not achieved, the process must continue until that occurs. In order to facilitate the correct verification of features, it is necessary for the fingerprint to be taken properly during enrollment. In order to do this, we have to trace the scanner twice with the same finger. This double-scanning procedure is performed to check the accuracy of fingerprint image and other details. Following the initial scan, the system processes and stores the primary fingerprint data. To ensure the accuracy of the fingerprint the second scan is then done to confirm that the acquired image matches what is previously captured or stored. This technique lessens errors in the process of identity verification The effectiveness of any biometric system is dependent on proper enrollment because it reduces the chances of false rejections or unauthorised access in case of miscaptured biometric data.

Once the fingerprint is scanned, the candidate’s name and roll number should be revised. The attendance system updates the student attendance immediately when he/she scans the fingerprint by linking the scanned fingerprint to the student database. In particular, the system picks up the roll number and the name of the student from the database and displays it. The attendance record is automatically updated in real time. This process involves matching the scanned fingerprint with the template stored in the database. If a match occurs, the system updates to

validate the student's presence and all related information at that specific time. Every time a new fingerprint is enrolled, the name and roll number of the student must be entered. Need to update information of all students in the class similarly. The students' enrollment in various courses is shown in figure 3.

When the fingerprint of that particular student is scanned, attendance of that student will be marked automatically for that period. In addition, the task given for that period will show with the roll number. The system recognizes the learner once they scan their fingerprint at the machine assigned to them. This is done by comparing the fingerprint to pre-registered templates stored in the data base The student attendance at the moment is recorded once the match is verified by the system instantly. This process ensures a more effective and impervious record than the usual roll call method. Simultaneously, the system digs into its database to discover new facts that are unique to the times. This consists of the homework or assignment set in connection with the student's course or syllabus for the period. Because the tasks displayed are connected to the roll number, each student gets customized information to their academic schedule.

Figure.3 Sample List of Students Enrollment

In a fingerprint-based attendance system, when a student scans the fingerprint at the designated sensor, the system processes the biometric data to confirm the identity of the student and records the attendance for the class period after the identity is confirmed. At the same time, the system displays the specific assignments or tasks associated with curriculum that must be completed during that period. The system shown in Figure 4 allows the student to know what is required of him or her for the day immediately, so there is less transition time to class activities, and academic productivity and organization remain high. The figure.4 shows the student with Roll number who successfully marked her attendance for the class period using a fingerprint-based method. There is an additional component that displays the project work for the same time frame as a proof of attendance.

In case any change occurs in the attendance policies, then again when the fingerprint is scanned within an hour of first scanning, this triggers a warning that acts both as deterrence and monitoring tool (Figure 5). The system allows for three warnings to be issued over time; however, if more than three are given to one student, it will inform the class coordinator who can take action because either there may have been user error or an intentional change in attendance records.

Figure.4 Illustration of system operation

Figure.5 Warning notification for multiple scan

Once the case reaches the three-warning limit, the system automatically escalates the case for administrative review, with a direct report to the class coordinator for further investigation. The class coordinator can review the details of the re-scans, speak with the student about the problem, and determine what action to take. These procedures ensure that the process of recording attendance is accurate and fair and that the educational institution maintains the integrity of its attendance data and exercises strict control over it. The hardware connections and its arrangement of the proposed IoT based finger print identification system is shown in Fig.6.

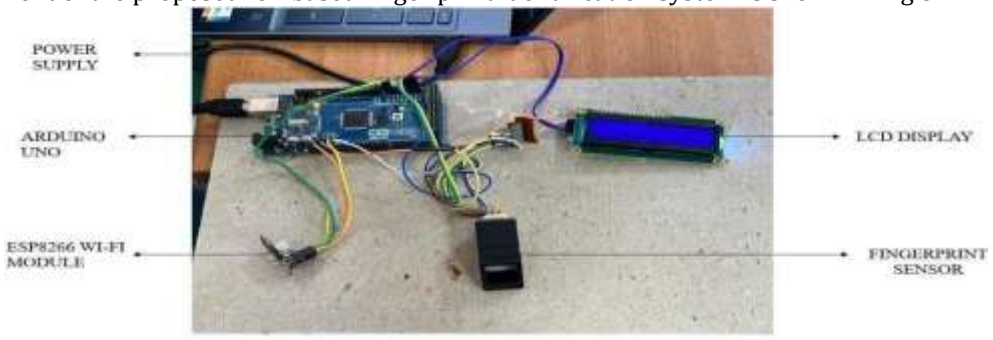

Figure.6 Hardware setup of the proposed system

5. Conclusion

Thus, the IoT-based fingerprint attendance system provides secure, scalable solutions in educational institutions with biometric verification integrated into the IoT and cloud data management technologies, which can overcome the limitation of traditional attendance. An app to monitor students' attendance will allow you to save a lot of time in the classroom as well as enhance the accountability of both students and staff. In addition, the activity and task dashboard provides a thorough understanding of the assignments and tasks related to that specific period after successful attendance capture. With the potential to transform how attendances are recorded, this solution is efficient, safe as well as very much accessible. Through IOT technology and Blynk user can get information on real time monitoring. The Blynk app integration provides a simple interface for both the teacher and the student. The app generates attendance reports and trends that teachers can easily access. Students enjoy a smooth and swift attendance process, enhancing their overall experience. For educational institutions, Blynk app has options to modify it as per their needs; thus, they can have an improved attendance management.

With IoT based fingerprint identification for students, patterns of those who require additional support may also become evident through machine learning analysis. Other potential features might include health conditions (a vital feature in pandemic and other public health crises), the collection of highly sensitive data that will demand enhanced security measures to ensure privacy as well as compliance with international standards, and finally its integration into smart campus initiatives so it interacts with additional school management systems and environmental goals using green technologies while utilizing block chain technology for trustworthiness globally.

References

1. Aayushi Singh, Tanya Goel, Deepali Srivastava, Astha Singh,Ms. Shivani Agarwal, "Location Based Attendance Monitoring System", International Journal of Engineering Applied Sciences and Technology,Vol. 5, No.1, pp. 517-521, 2020.
2. Abhinav Dube, Dhruwaman Singh, Rajesh Kumar Asthana, Gurjit Singh Walia, "A Framework for Evaluation of Biometric Based Authentication System", Proceedings of the 3rd International Conference on Intelligent Sustainable Systems, pp.925-932, December 2020.
3. Ajibola Oyedeji, Ignatius Okakwu, Olatilewa Abolade, "Development of an enhanced student identification system", Firat University Journal of Experimental and Computational Engineering, Vol.2, No.2, pp.80-86, 2023.
4. Ansari A.N., Navada A., Agarwal S., Patel S. and Sonkamble B. "Automation of Attendance system using RFID Biometrics GSM modem with .Net framework", IEEE International conference on multimedia technology, pp. 2976-2979, July 26-28,2011.
5. Arulogun MO, Olatunbosun OT, Fakolujo A, Olaniyi OA. "RFID-based student's attendance management system", International journal of scientific Engineering and Research, Vol.4, No.2, 2013.
6. Fahmida Yesmin Chowdhury,"Implementation of Attendance Management System Utilizing Fingerprint, QR Code, and GPS Technology in Educational Institutions", International Journal of Science and Research,Vol.12, No.9, pp.2016-2019, 2023.
7. J.ChandraMohan, R Nagarajan, M Ashok kumar , T Dineshkumar, G Kannan, R Prakash, "Attendance Monitoring System of Students Based on Biometric and GPS Tracking System",International Journal of Advanced Engineering, Management and Science,Vol.3, No.3, 2017.
8. M. Kassim, H. Mazlan, N. Zaini and M. K. Salleh, "Web-based student attendance system using RFID technology", IEEE Control and System Graduate Research Colloquium, Malaysia, pp. 213-218, 2012.
9. Mohammad Nabati, Seyed Ali Ghorashi, "A real-time Fingerprint-based indoor positioning using Deep learning and preceding states", Expert Systems with Applications, Vol.213, 2023.
10. Reena Garg, Gunjan Singh, Aditya Singh, Manu Pratap Singh, "Fingerprint Recognition using Convolution neural network with inversion and Augmented techniques", Systems and Soft Computing, Vol.6, 2024.
11. Seng Chun Hoo, Haidi Ibrahim, "Biometric-Based Attendance Tracking System for Education Sectors: A Literature Survey on Hardware Requirements", Journal of Sensors, Vol. 2019, pp.1-25, 2019.
12. Talaviya G., Ramteke R. &Shete A.K. "Wireless Fingerprint Based College Attendance System Using Zigbee Technology", International Journal of Engineering and Advanced Technology , Vol. 2, No. 3, pp. 201-203, 2013.
13. V.Ruhitha,V N Prudhvi Raj,G Geetha,"Implementation of IOT based Attendance Management System on Raspberry Pi", IEEE International Conference on Intelligent Sustainable Systems, pp.584 - 587, 2019.
14. Verma P. & Gupta N., "Fingerprint Based Student Attendance System Using GSM", International Journal of Science and Research, Vol. 2, No.10, pp. 128-131, 2013.
15. Zainal N.I., Sidek K.A., Gunawan T.S. &Martini H.M.M, "Design and development of portable classroom attendance system based on Arduino and fingerprint Biometric", IEEE International conference on information and communication Technology, November 17-18, 2014.