JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

STUDENT ATTENDANCE MANAGEMENT SYSTEM USING FINGERPRINT SENSOR

**SOURAV NANDI, **SOUMYADIPTA BANERJEE, **SOUMAJIT DHARA,
**SHUVAJIT GAYEN, **SUNNY RAJ **
DR. AMRITA NAMTIRTHA, **DR. PRANATI RAKSHIT
DEPT. OF COMPUTER SCIENCE ENGINEERING, JIS COLLEGE OF ENGINEERING,
KALYANI, NADIA-741235, WEST BENGAL, INDIA

ABSTRACT

In many Organizations keeps track of employee and students' attendance via attendance management system. It is used to developing student/employee gratification or sense of well-being and providing absolute benefits and resources. An advanced verification for employees, known as biometric technology, is utilized in many schools and companies. A proposal has been put forth to develop a prototype that aims to streamline the process of recording employees' attendance and automate payroll generation using biometric technology. The Adafruit Fingerprint Fuzzy Vault scheme algorithm has been used by this sample. A user interface module has been developed using Visual Basic, allowing for fingerprint and face registration during the login process with the prototype. The result was tested at JIS College of Engineering.

1. INTRODUCTION

In many higher education institutions, especially in India, proper attendance monitoring is considered a crucial criterion for ensuring quality and promoting student satisfaction. According to Acro print, accurately tracking employee attendance or time is essential for precise payroll computation and enforcing discipline regarding punctuality. While some companies and schools still rely on manual punchcards or logbooks to record employee attendance, there is a growing need for more advanced and efficient systems. There are two types of traditional methods which are token-based and knowledge-based identifications [1].

In the current practice of using a logbook, employees manually write down their names, time, and signature to log in and out of the office or school. Alternatively, employees can utilize a punch card machine by inserting their time card or punch card into a slot on the Bundy clock when logging in or out of the office. However, these methods have limitations. According to a study conducted by Harris Interactive Inc., it was revealed that 21 percent of hourly employees admit to engaging in time theft. These include the face, fingerprints, and iris. On the contrary, behavioral characteristics deal with features observed from human action. Examples of human action are gait, voice, and signature [2].

According to research, while only 5 percent of employees admitted to engaging in buddy punching, 69 percent acknowledged punching inand out earlier or later than scheduled, 22 percent reported adding additional time to their time sheets, and 14 percent did not punch out for unpaid lunches or breaks. Biometric technology provides an advanced verification system widely used in schools and companies. It employs programmed methods to identify or verify individuals based on their physiological or behavioral characteristics. Physiological characteristics include hand or finger images and facial features, while behavioral characteristics are acquired or learned traits. Examples of behavioral characteristics include dynamic signature authentication, speaker verification, and keystroke dynamics. Biometric verification involves comparing a registered or enrolled biometric sample, such as a fingerprint captured during login, with a newly captured biometric sample.

2. LITERATURE SURVEY

As will be seen below, there are numerous similar academic works that use technological devices to track student attendance. It was suggested in [3] to use an embedded computer system to track attendance during lectures. An electronic card reader serially connected to a personal computer made this method better, but it still has the drawback of allowing someone to take attendance for another individual if they have access to their electronic card. An iris-based wireless attendance management system was utilized by the authors of [4] to verify user identity. In order to capture images, extract detailed information from them, store them, and compare them to database entries, this system uses an off-line iris recognition management system. By using buddy punching or incorrect clocking in, this system prevents it. When one employee or student unreasonably clocks in for another, this is known as buddy punching. The only issue with this type of biometric technology is that people typically are hesitant to use it because they believe that having their iris scanned could eventually cause damage to their eyes. A system that authenticates users using passwords was created and implemented by the authors as referred in [5]. Since the password can be altered or shared, this solution could still not completely prevent impersonation. Frequently, users are unable to access systems because of lost passwords or computer hacks.

Additionally, we provide various options like an RFID-based and a GSM-GPRS-based authentication system. With each of these device-based solutions, there are problems. The GSM-GPRS based systems employ the fixed location of the classroom for recording attendance; this position is not dynamic. As a result, if the location changes, the inaccurate attendance can be recorded. RFID [5]-based authentication solutions have the drawback that RFID cards can be misplaced or stolen and that RFID detectors must be installed. RFID cards also cannot stop impersonation. However, this fingerprint authentication technique provides a simple and affordable method of identifying. Each person's fingerprint is unique to them. Even identical twins do not have the same fingerprint characteristics, and unlike a password, a fingerprint cannot be copied, misplaced, or forgotten. Because the system generates exports at the conclusion of the semester, it enables students to easily register for lectures and eliminates mistakes that are related to attendance registers. The benefit of this system is that, in contrast to other fingerprint identification systems already in use, it may function as an independent system.

3. MATERIALS USED FOR PROPOSED METHOD

Fingerprint Sensor

For our project, we have utilized the R305 fingerprint sensor. The R305 biometric fingerprint module is equipped with a high-precision, high-performance matching algorithm, and a high-capacity flash chip. Its functionality is based on fingerprint image processing, matching, memory search, and performing desired functions. The module communicates with a microcontroller using serial communication. The default Baud Rate is set to 57600, and it cannot be changed. This fingerprint sensor module can store up to 980 fingerprints. It also includes a USB cable, enabling direct connection to a PC. Basically, a fingerprint is characterized by different patterns of ridge and valley features [3]. Both fingerprint scanners and readers serve as highly secure and suitable devices forenhancing security compared to using a traditional password. Passwords can be easily scanned or forgotten, making them less reliable. Usinga USB-based fingerprint reader or scanner with biometric software allows for verification, identification, and authentication, where your fingerprints act as digital passwords. Despite the benefits, the FTIR-based optical sensor is susceptible to a dry or wet finger that yields saturated or weak impression, respectively [4]. These fingerprints cannot be easily forgotten, lost, or stolen, providing enhanced security measures.

Node MCU:

It is firmware based on the open-source LUA programming language, specifically developed for the ESP8266 Wi-Fi chip. It offers a wide range of functionalities and is accompanied by the Node MCU Development board, which serves as a platform for utilizing the capabilities of the ESP8266 chip. The hardware design of Node MCU is open and can be customized or modified according to specific requirements. The Node MCU Development board consists of the ESP8266 Wi-Fi-enabled chip, which is a cost-effective solution developed by Espressif Systems. The chip supports the TCP/IP protocol, enabling seamless Wi-Fi connectivity. To learn more about the ESP8266 chip, you can refer to the ESP8266 Wi-Fi module. The Node MCU Dev Kit features Analog and Digital pins that resemble those found on Arduino boards, providing versatility in terms of connectivity and sensor integration. It also supports various serial communication protocols, allowing seamless integration with devices such as I2C-enabled LCDs, Magnetometer HMC5883, MPU-6050 Gyro meter + Accelerometer, RTC chips, GPS modules, touch screen displays, SD cards, and more. With the Node MCU Dev Kit, you can leverage the power of the ESP8266 chip, its extensive connectivity options, and the flexibility of the LUA programming language to create innovative projects and applications.

LCD

In our project, we have utilized an I2C module to drive a 16x2 (1602) alphanumeric LCD. The I2C module is equipped with an embedded PCF8574 I2C chip, which converts I2C serial data into parallel data for the LCD. To determine the specific version, you can examine the black I2C adapter board on the underside of the module. If you find three sets of pads labeled A0, A1, and A2, then the default address will be 0x3F. If there are no pads, the default address will be 0x27. The module also includes a contrast adjustment potentiometer located on the underside of the display. This potentiometer may need to be adjusted to ensure the text is displayed correctly on screen. When working with embedded systems, it is crucial to have a reliable output device that provides the necessary information. The 16x2 LCD fulfills this requirement by offering alphanumeric output and serving purposes such as information display and process status monitoring. It can be easily interfaced withvarious host controllers, including 8051 derivatives, PIC Series, AVR, and ARM series controllers, as well as development boards like Arduino or Raspberry Pi.

Breadboard:

A breadboard is a board used for prototyping or constructing circuits. It provides a convenient way to place components and establish connections without the need for soldering. The breadboard consists of a grid of holes where you can insert components and wires to create circuits. The holes in the breadboard securely hold the components and wires in place while also establishing electrical connections. Breadboards are particularly useful for learning purposes and rapid prototyping of simple circuits due to their ease of use and quick setup. However, they are less suitable for more complex circuits or circuits operating at high frequencies. Additionally, breadboard circuits are not recommended for long-term use compared to circuits built on protoboards or printed circuit boards (PCBs). While protoboards require soldering, PCBs involve design and manufacturing costs. Breadboards offer a cost-effective and solderless alternative for temporary circuit setups and experimentation.

Jumper Wires:

A jumper is a component made of conductive material, enclosed in a nonconductive plastic block to prevent unintended circuit shorts. It serves as a means of creating electrical connections between pins or terminals, similar to an on/off switch. By placing a jumper over two or more pins, specific configuration settings can be activated. Jumpers can be added or removed to enable different performance options for components. A group of pins with a small metal pin at the end, along with a sleeve or shunt that allows electric currents to flow across different circuit points, is referred to as a jumper block. In older PCs, jumpers were commonly used to set voltage levels, adjust the speed of the central processing unit (CPU), reset the basic input/output system (BIOS) configuration, and clear complementary metal oxide semiconductor (CMOS) information. Motherboards often featured multiple jumper pairs or banks of DIP (dual in-line package) switches. It was not uncommon to find 30 to 40 jumper pairs on a motherboard. However, due to inadequate documentation and the complexity of jumper settings, some systems were challenging to configure correctly. Over time, motherboard designs shifted towards fewer labeled and numbered jumper blocks to simplify setup and configuration**.**

4. METHODOLOGY:

The chosen methodology for this project is Evolutionary Prototyping, which is a type of prototyping methodology. Evolutionary prototyping involves developing an initial prototype and then refining it through multiple cycles until it reaches the final complete system (Sommerville, 2000). The reason for selecting this methodology is that it allows continuous feedback and suggestions from users to improve the prototype until the final system is delivered.

Evolutionary prototyping consists of four phases: initial concept, designing and implementing the initial prototype, refining the prototype, and delivering the complete system. There are several strengths associated with evolutionary prototyping. It helps speed up system development by allowing iterative improvements. The quality of the final product is enhanced as it goes through several prototype iterations, ensuring that all functionalities and requirements are met. Furthermore, user satisfaction is likely to be high since each prototype is based on user-specified requirements.

Overall, the evolutionary prototyping methodology offers advantages such as faster development, improved product quality, and increased user satisfaction. However, it also poses challenges regarding project predictability, developer frustration, and code maintainability.

4.1. FLOW CHART FOR PROPOSED SYSTEM

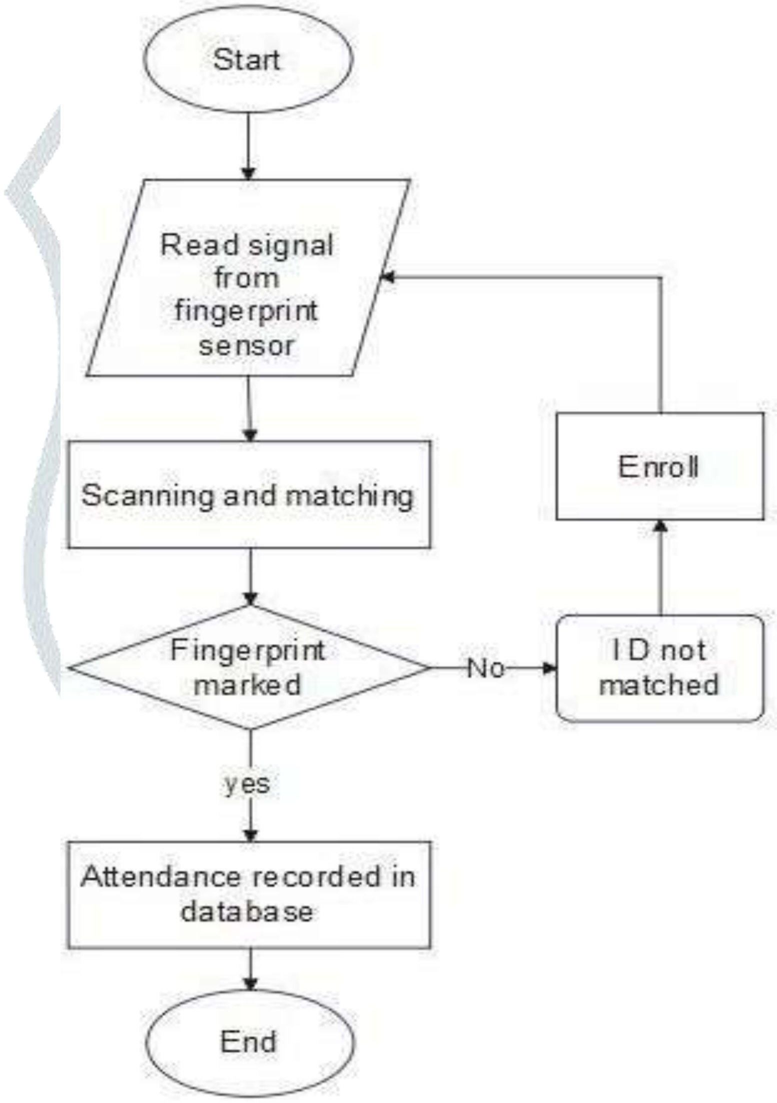


Fig 1. System flowchart

4.2 FINGERPRINT

Various types of sensors are used to capture the fingerprint image. Basically, the image sensor for fingerprint can be categorized into three types which are optical, solid state, and ultrasound[5]. A fingerprint is a unique pattern formed by the friction ridges on the surface of the finger. These ridges create dark lines in the fingerprint image, as shown in Figure 2. The white spaces between the ridges are known as valleys and represent the shallow parts of the skin. The presence of ridges and valleys allows us to grip objects firmly by creating friction. However, the uniqueness of a fingerprint is not solely determined by these ridges and valleys. The distinctiveness is primarily achieved through the presence of minutiae points. Minutiae points are specific pointswhere the ridges have characteristics such as endings, bifurcations, or other pattern variations. These minutiae points play a crucial role in fingerprint recognition. By comparing and matching the minutiae points of different fingers from the same individual, privacy protection and accurate identification can be achieved [11]. It is the combination of these minutiae points that provides the basis for the uniqueness and security of fingerprint-based biometric systems.

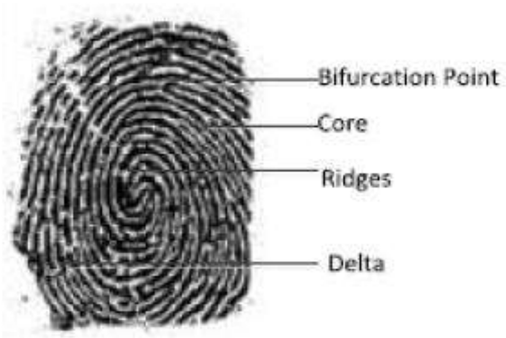


Fig 2. Fingerprint

Biometric Authentication and Processing

Biometric authentication encompasses six distinct phases, as depicted in Figure 3. The registration phase is the initial step, involving various processes such as pre-processing, region-of-interest detection, and feature extraction. During this phase, the biometric data of an individual is captured, and relevant features are extracted. These extracted features are then securely stored in a database for future reference. Moving to the recognition phase, it also comprises several steps. First, the captured biometric data is pre-processed to enhance its quality. Then, the region of interest (ROI) is detected to isolate the specific area containing the relevant biometric information. Next, feature extraction techniques are applied to extract distinctive features from the ROI. These features are then compared with the stored templates in the database using matching algorithms. Finally, a decision is made based on the similarity or dissimilarity between the captured biometric data and the templates to authenticate the individual. The recognition phase involves a comprehensive process of pre-processing, ROI detection, feature extraction, matching, and decision-making, all aimed at accurately verifying the identity of an individual using their biometric data.

4.3 SYSTEM DESIGN:

System design refers to the process of creating a detailed plan or blueprint for the architecture, components, and interactions of a system. It involves identifying system requirements, defining its structure, specifying the subsystems and modules, and determining how they will work together to achieve the desired functionality. The goal of system design is to ensure that the system meets its objectives, and is scalable, efficient, reliable, and maintainable. The below figure describes our system design.

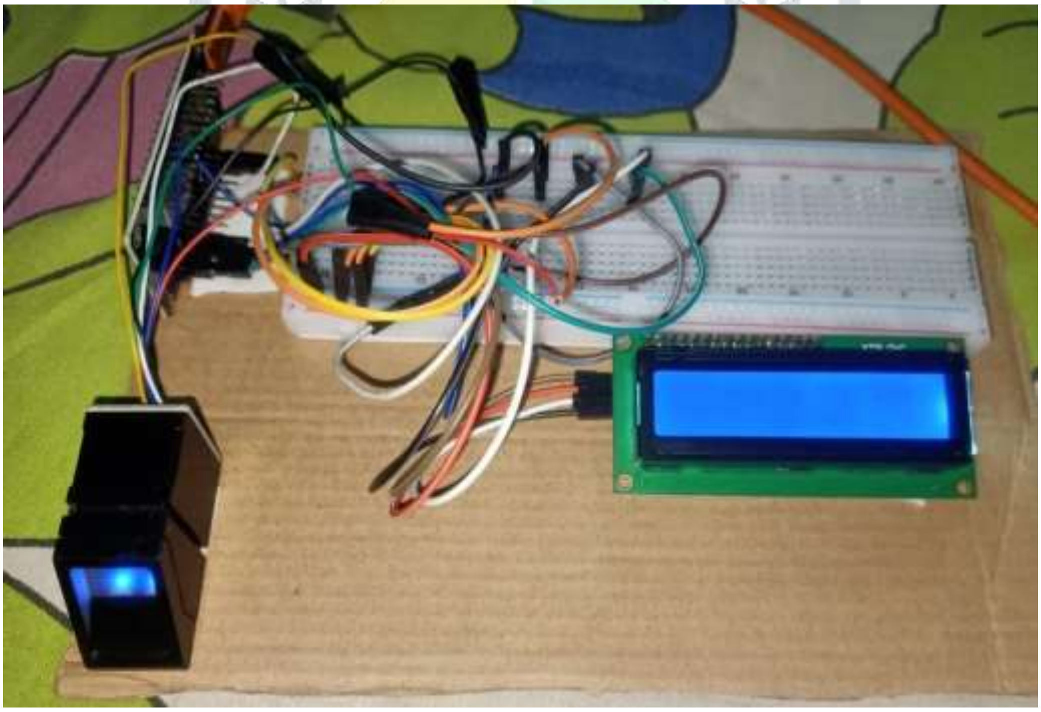
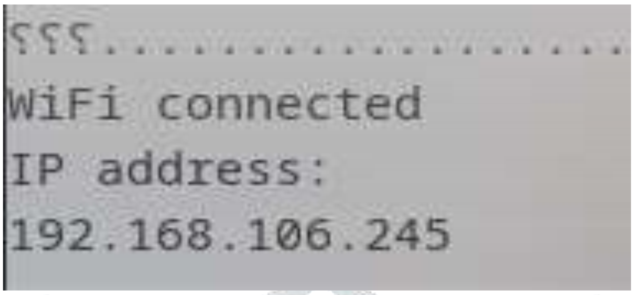


Fig 3. Model

The above model includes the hardware tools such as Breadboard, I2C Module for 16x2 (1602) Alphanumeric LCD, R305 Fingerprint Sensor, Node MCU, and Jumpers.
And all these hardware tools combine to make an attendance management system that could be used in institutions like schools, colleges, and in many more workplaces.

4.4 OPERATION:
The system contains node MCU. The internet through which the node MCU is connected, display shows Wi-Fi is connected and the IP address of that same internet is shown. After showing the above messages and IP address the display shows 'Sensor Found'.



```
ςςς....................
WiFi connected
IP address:
192.168.106.245
```

Fig 4. Wi-Fi connection

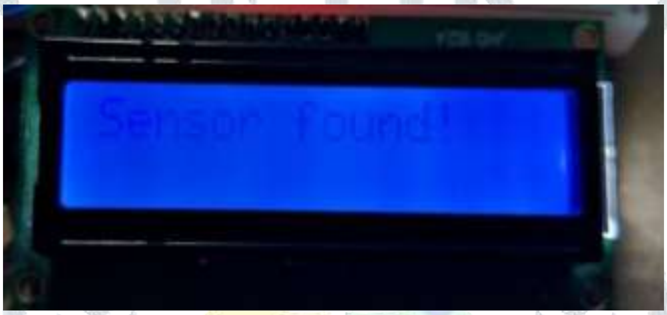


Fig 5. Sensor found

The operation of the system for attendance reporting starts with a message showing on the display as waiting for a sensor that indicates to give a valid fingerprint. As shown below the sensor is waiting for fingerprint detection.

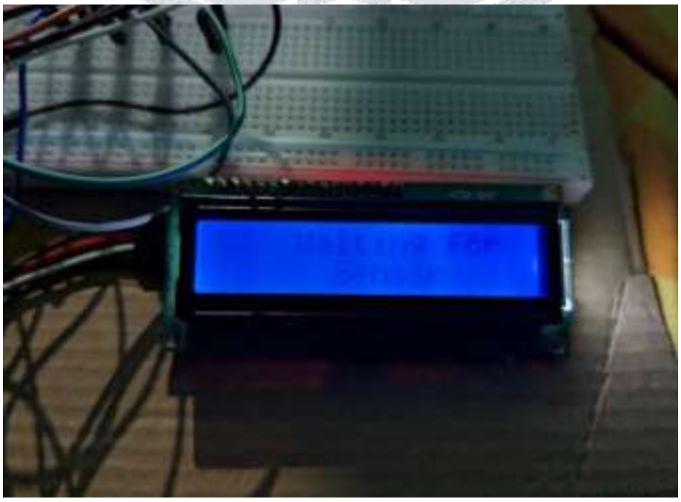


Fig 6. waiting for sensor

When someone provides a fingerprint at the fingerprint sensor, if the fingerprint is not detected properly the sensor shows the message as 'Place a Valid Finger'. Also, if a fingerprint is not registered in the database, the sensor throws the same message as the sensor could not find the fingerprint in the database.

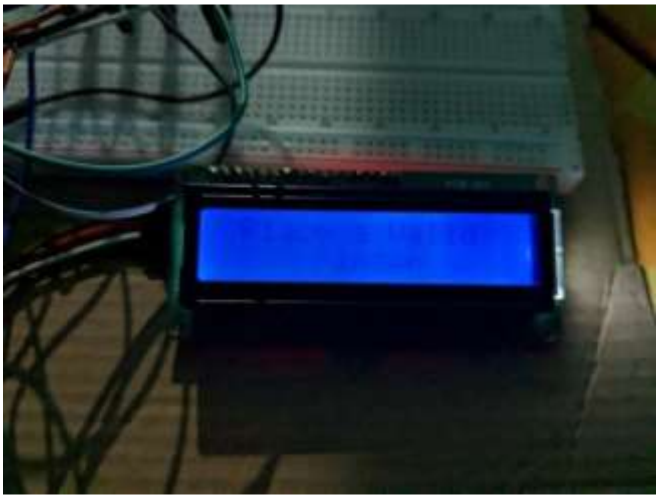


Fig 7. Place a valid finger

If the sensor founds a valid finger that is a fingerprint that is registered already and the same fingerprint is detected as input then the sensor throws a message with the registered fingerprint name e.g., 'Welcome Sourav', here Sourav is a user whose fingerprint was registered already and when his fingerprint is given as input the sensor detects and confirms the fingerprint as valid and throws the message.

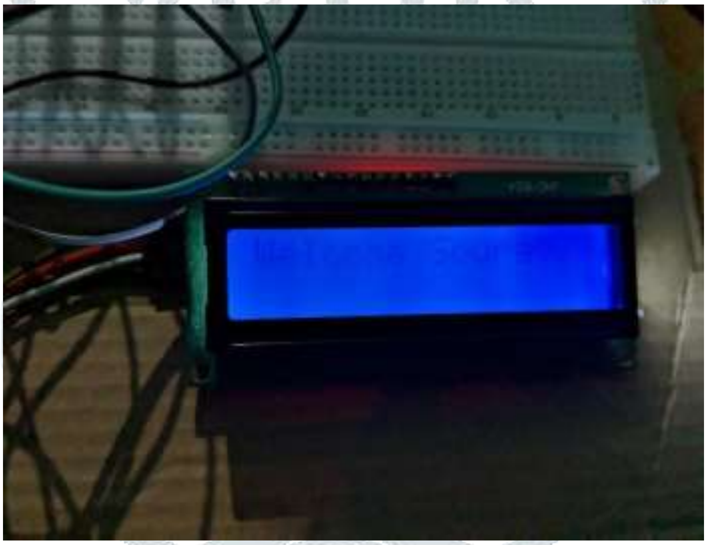


Fig 8. Welcome

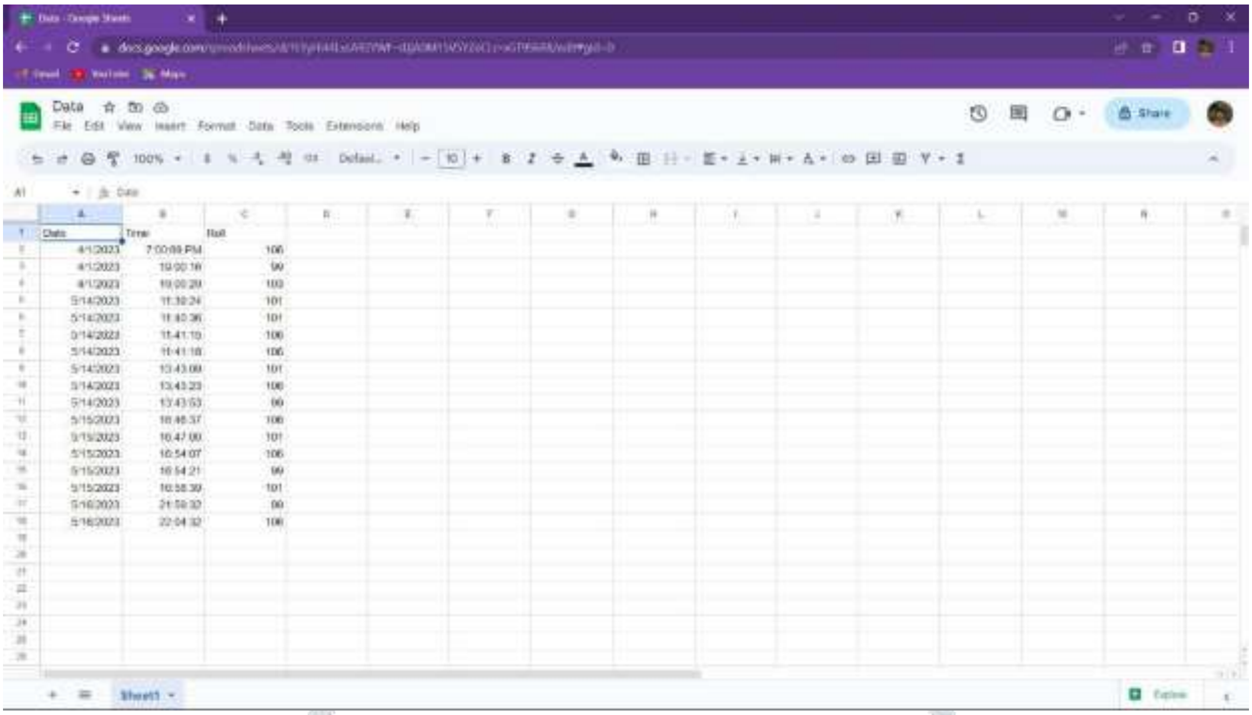
5. RESULT AND DISCUSSION

When a new user or student comes to give attendance, they place their finger in the fingerprint scanner then after scanning it matches the fingerprint with the respective fingerprint stored in the database and if the fingerprint is not stored in the database, then he /she has to place their finger in the fingerprint sensor to get their fingerprint store in the database and then they have to repeat the same to mark their attendance successfully.

When the user or student successfully attends the following data would be saved in the database in the form of an Excel sheet.

As we can see from the above, the data of the students or users have been successfully marked with log-in date, time, and ID (their respective roll number).

The other data can be added according to the intuitions or the organization's needs.



Date	Time	Roll
4/1/2023	7:00:09 PM	106
4/1/2023	19:00:16	99
4/1/2023	19:00:20	100
5/14/2023	11:30:24	101
5/14/2023	11:40:36	101
5/14/2023	11:41:10	106
5/14/2023	11:41:18	106
5/14/2023	13:43:08	101
5/14/2023	13:43:23	106
5/14/2023	13:43:53	99
5/15/2023	16:46:37	106
5/15/2023	16:47:00	101
5/15/2023	16:54:07	106
5/15/2023	16:54:21	99
5/15/2023	16:58:39	101
5/16/2023	21:59:32	99
5/16/2023	22:04:32	106

Fig 9. Database

As we can see from the above, the data of the students or users have been successfully marked with log-in date, time, and ID (their respective roll number). The other data can be added according to the intuitions or the organization's needs.

Accuracy:

We have tested our attendance management model using fingerprint system with a dataset having 50 different fingerprints, for testing and have received the following accuracy

There was a accuracy of 80% that is out 50 different fingerprints 40 fingerprints were taken as a valid fingerprints by our model.

6. CONCLUSION

This paper introduces a fingerprint-based attendance management system that utilizes a minutiae-based fingerprint recognition/authentication system. The developed system is an embedded system designed to extract and analyze the local characteristics of fingerprints, specifically focusing on minutiae points. During the registration and verification processes, the system employs template-matching techniques. Templates containing minutiae points are compared to determine the authenticity of the fingerprint. Overall, the proposed system offers an efficient and reliable approach to attendance management using fingerprint recognition, specifically focusing on minutiae-based analysis and score-matching techniques.

7. FUTURE SCOPE

- Our next step would be to make the model more simplified and user-friendly.
- We want to add more data to reduce data redundancy if occurs.
- To introduce a message system, a message would be sent whenever someone gives attendance.
- Using more advanced technology and tools to make the system faster and more convenient.

8. ACKNOWLEDGEMENT

We would like to extend our heartfelt gratitude to all the faculty members who have provided us with their invaluable guidance and support throughout this project. Your expertise, encouragement, and willingness to assist us have been instrumental in our success. We are truly grateful for your time, knowledge, and dedication in helping us navigate through the challenges and complexities of this endeavor. Thank you for being a constant source of inspiration and for your unwavering commitment to our academic and personal growth.

9. REFERENCES

[1] A. Jain, L. Hong, and S. Pankanti, "Biometric identification," Communications of the ACM, vol. 43, no. 2, pp. 91–98, 2000.

[2] L. M. Dinca and G. P. Hancke, "The fall of one, the rise of many: a survey on multi-biometric fusion methods," IEEE Access, vol. 5, pp. 6247–6289, 2017.

[3] D. Maltoni, "A tutorial on fingerprint recognition," in Advanced Studies in Biometrics, M. Tistarelli, J. Bigun, and E. Grosso, Eds., pp. 43–68, Berlin Heidelberg, Springer-Verlag, 2005.

[4] N. K. Ratha, A. Senior, and R. M. Bolle, "Automated biometrics," in Advances in Pattern Recognition—ICAPR 2001, vol. 2013, S. Singh, N. Murshed, and W. Kropatsch, Eds., pp. 447–455, Springer-Verlag, Berlin Heidelberg, 2001.

[5] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition, Second edi, Springer-Verlag London Limited, 2009.

[6] Oloyede MO, Adedoyin AO, Adewole KS (2013) Fingerprint Biometric Authentication for Enhancing Staff Attendance System. International Journal of Applied Information System 5: 19-24.

[7] Punitha, K. 2017. Enactment of Face Recognition Algorithm for Attendance System. International Journal of Applied Engineering Research. Vol 12, Issue. 4.

[8] Patil, P., Khachane, A and Purohit, V. 2016. A Wireless Fingerprint Attendance System. International Journal of Security, Privacy and Trust Management. Vol 5, Issue 4

[9] Chandramohan, J, Nagarajan R., Kumar, M., Dineshkumar, T., Kannan, G., and Prakash, R. International Journal of Advanced Engineering,Management and Science, Vol 3, Issues 3

[10] Mathana Gopala Krishnan, Balaji, Shyam Babu 2015. Implementation of an Automated Attendance System using Face Recognition. International Journal of Scientific & Engineering Research. Volume 6, Issue 3

[11] S. B. Dabhade, Y. S. Rode, M. M. Kazi, R. R. Manza and K. V. Kale 2013. Face Recognition using Principal Component Analysis and Linear Discriminant Analysis

[12] Comparative Study. 2nd National Conference on Advancements in the Era of Multi-Disciplinary Systems

[13] S. Li and A. C. Kot 2013. Fingerprint Combination for Privacy Protection. IEEE Transactions on Information Forensics and Security, Vol. 8, No. 2, 350- 360