SAVONIA

University of Applied Sciences

THESIS – BACHELOR'S DEGREE PROGRAMME
TECHNOLOGY, COMMUNICATION AND TRANSPORT

# A WEB-BASED ATTENDANCE MANAGEMENT SYSTEM USING A MICROCONTOLLER

AUTHOR/S Alhassan Safianu

SAVONIA UNIVERSITY OF APPLIED SCIENCES

THESIS
Abstract

| | |
|---|---|
| Field of Study<br>Technology, Communication and Transport | |
| Degree Programme<br>Degree Programme in Information Technology, Internet of Things | |
| Author<br>Alhassan Safianu | |
| Title of Thesis<br>A WEB-BASED ATTENDANCE MANAGEMENT SYSTEM USING A MICROCONTROLLER | |
| Date 26/05/2024 | Pages/Number of appendices 30 |
| Client Organisation /Partners<br>Savonia University of Applied Sciences | |

Abstract:

This thesis presents the development of a web-based attendance management system that integrates a microcontroller and a fingerprint sensor. The goal was to improve the precision and effectiveness of conventional techniques employed for monitoring attendance. The system was intentionally created to tackle prevalent problems such as fraud and human error, providing a more dependable and user-friendly alternative for educational institutions.

The main element of the system consisted of a microcontroller connected to a fingerprint sensor, allowing students to verify their attendance via biometric identity. After the fingerprint scanning process was completed, the attendance data was sent to a web server and kept securely in a database. The data can be accessed through a web-based application that offers features such as live attendance tracking, report creation, and in-depth data analysis.

Throughout the development phase, a thorough evaluation was conducted on various microcontroller platforms and communication protocols to guarantee smooth integration and attain maximum performance.

The accuracy and reliability of the fingerprint sensor underwent thorough testing in various environments. The entire system passed thorough testing in a controlled setting, showcasing its exceptional accuracy and efficiency in comparison to manual methods of tracking attendance.

This strategy led to substantial reductions in administrative workload, decreased occurrences of attendance fraud, and enhanced overall management of student attendance information. This project demonstrated the capacity to combine microcontroller technology with biometric sensors and web-based applications, offering an innovative way to modernize attendance tracking in educational environments.

Keywords

A web-based attendance management system, Microcontroller, Fingerprint sensor, Biometric identity verification, Data security and Accuracy.

CONTENTS

List of figures

# INTRODUCTION

## 1.1 Motivation and Problem Statement

Every university, institution, or college has a uniform policy on attendance. Staff are required to keep accurate attendance records. As far as keeping daily attendance is concerned, the traditional process is inefficient and takes a long time to organize information and determine each student's mean presence. For instance, lecturers at Savonia University of Applied Sciences. check attendance by passing around a sheet of paper on which students are required to write their names and index numbers, along with their signatures. In this method of attendance monitoring, students provide the required information for their classmates who are absent. Taking student details is a time-consuming and distracting process because it happens while the lecturer is teaching. Creating a correlation between the current attendance record and the previous attendance record is another challenging task. Due to this, it is necessary to have a platform that can handle the organization of student data and the calculations of mean attendance. Students' educational excellence and their attendance are strongly correlated, according to observational evidence (Newman-Ford et al. 2008).

According to Patil and Shukla (2014), mentioning names every day by a lecturer is a common problem and a waste of time. It takes about five to ten minutes for a class of about 50 students just to record attendance, and it is suggested that the process should be automated to simplify things and to eliminate time wastage.

This project work is going to employ a more innovative attendance management system that utilizes sophisticated technology so that the complicated tasks of storing paper sheets and creating backups can be simplified and automated.

## 1.2 Aim

This project aims at developing a web-based attendance management system using a microcomputer.

## 1.3 Objectives:

- Examine related scholarly publications from the past few years.
- Document any general procedures or methods for managing attendance.
- Design and construction of an easy-to-implement biometric attendance register to record students' attendance at lectures.
- Build a web-based database to store user data for confirmation and use.

- The device is tested and trained to be used in organizations to take attendance.

## 1.4 Research Questions

- What microcontroller should be integrated into the attendance management system to ensure accurate and reliable data transfer?
- Can the attendance data collected be easily managed and analysed with the web-based platform?
- How can the web-based platform be secured and protected to ensure privacy and security?

# 2 LITERATURE SURVEY

Academic organizations must monitor attendance, but traditional methods of taking attendance using paper sheets are time-consuming, inaccurate, and problematic. Various technical solutions are implemented to reduce administrative burdens and partly automate this process. In most cases, Radio Frequency Identification (RFID) technology, biometric solutions such as fingerprint recognition and mobile devices are being used. (Smith 2020.)

Recent years have witnessed notable developments in web-based attendance management systems built on microcontrollers. Being flexible and reasonably priced, microcontrollers provide a good way to automatically record attendance. To maximize accuracy and reduce hand-off mistakes, an RFID-based attendance system running an Arduino microcontroller was developed. The system used an RFID reader linked to Arduino to store and control attendance records by means of web server connection. This arrangement clearly outperformed conventional attendance systems in allowing real-time processing and instantaneous data availability. (Kumar & Reddy 2020.)

The paper presents the results of the study and implementation of the JIC CMS (Jubail Industrial College Classroom Management System) pilot program. In this pilot project, the Android platform is used for the mobile app, which is written in Xamarin. This prototype of the proposed system combines face recognition and biometric verification with RFID for high levels of authentication. A key feature of the system is the ability to set the system up to work in a smart mode when it closes automatically after a predetermined amount of time. web-based system is presented by which utilizes the NFC tag's capability to initiate the web browser and
access the URL coded in the tag. (Takahashi et al. 2020.)

The NFC tag sticker pasted at a student's seat lets the web application know their seat and classroom IDs when they tap the sticker with their smartphone. Students are prompted to enter their student ID and password, and the web server acquires the lecture ID from the database. Student's web application registers the student's attendance in the database once all the session variables are filled for the session. In the teacher's web application, the seat maps of the classroom display the student IDs. This article describes an eLearning system that provides materials, tracks student attendance, and manages grades through the web. By using this system, a prototype is created that will be built in the future. In this e-learning system, value management is managed, attendance is managed, and curriculum is managed so that teachers, students, and parents can access and collaborate on student learning activities with ease and efficiency. (Takyudin et al. 2021.)

# 3 COMPARATIVE ANALYSIS OF ATTENDANCE TRACKING SYSTEM IN EDUCATION

Several strategies have been applied in the field of educational institution attendance systems to ensure exact monitoring of student attendance. While human roll-calling and sign-in forms have long been used, increasingly advanced technical solutions are progressively replacing these out-of-date methods. Among them, systems using fingerprint, face, and RFID card identification have grown to be the most often used ones. Although every one of these techniques have advantages and drawbacks of their own, fingerprint-based solutions stand out as being particularly helpful in several significant spheres. (Mijić et al. 2019.)

Manual attendance systems are quite prone to manipulation and mistakes even if they are simple to operate. Teachers may unintentionally note students as present or absent; students can choose to engage in proxy attendance by signing in for their colleagues. RFID-based solutions further this by automating the process but are not perfect. Under a technique sometimes referred to as "buddy punching," which alters attendance records, students may still swap cards. Moreover, RFID systems make students always remember to carry their cards; if they forget or misplace them, this could lead to issues. (Shivraj et al. 2020.)

Facial recognition technology, applied with artificial intelligence, is a more sophisticated approach of student identification. This approach, which is usually pragmatic and frictioless, can be influenced by changes in the lighting, camera angles, and student appearances—that is, by new hairstyles, glasses, etc. Apart from possible biases in the recognition algorithms, the usage and storage of face data raises major privacy questions. (Nguyen et al. 2021.)

Conversely, fingerprint-based attendance systems offer a good mix of convenience of use, safety, and accuracy. Every person has unique fingerprints, hence false attendance records is less likely. Unlike RFID cards, fingerprints cannot be lost or forgotten hence students may be confident they always have their "attendance marker". Since their dependability has considerably raised, fingertip injuries and filth are no more common issues for fingerprint scanners. Furthermore, constructed with robust encryption to protect biometric data and satisfy privacy concerns are modern fingerprint systems (Jain et al. 2019).

Ultimately, even if every attendance system approach has benefits and drawbacks, fingerprint-based systems provide a better option for educational institutions trying to raise attendance accuracy and lower fraudulent activities. Given their durability and uniqueness as well as advances in data security and scanner technology, fingerprints are an excellent choice. By use of fingerprint identification, schools may provide a more consistent, efficient, and safe attendance tracking system that enhances the quality of education. (Shivraj et al. 2020.)

# 4 THEORY AND DESIGN CONSIDERATION

## 4.1 Theory Consideration

This system will serve the main function of checking and monitoring student attendance at universities. Below are the theoretical concepts that were used in the implementation of this project.

Figure 1. Shows the basic architecture of the biometric attendance management system.

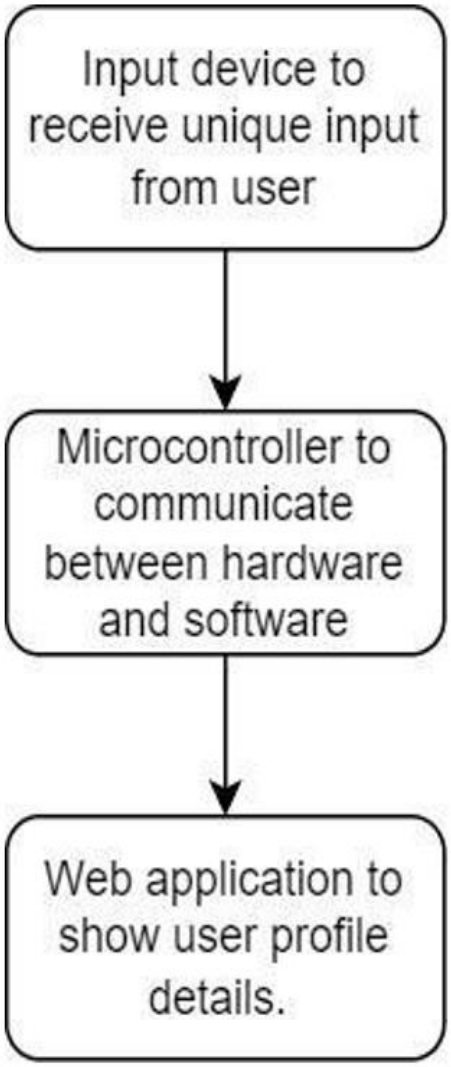



Figure 1. Basic Architecture of the attendance system (Springer 2011)

To successfully check the attendance of users, three basic components are required.

- An input device that receives information that is unique to each user. Uniqueness plays a significant role in determining the reliability of the attendance management system.

- Microcontrollers allow hardware and software to communicate. Hardware is the input device that receives data from user while software is the web application that provides a platform to explore more details.
- Enrollment and authentication are the two most important functions of a fingerprint sensor. The enrollment process is the first step in using the attendance management system.

### 4.1.1 Registration/Identification and Enrollment Stage

A biometric identification system's enrollment process involves capturing an individual's unique physiological characteristics and associating them with their personal information to create a comprehensive identity record. Because fingerprints are unique and permanent, they are frequently used in biometrics. Individuals begin the enrollment process by entering their personal information, such as their name, date of birth, and other relevant details. An individual's fingerprint is simultaneously scanned using a fingerprint sensor, which captures a high- resolution image of the fingertip.

Afterwards, the system searches for features in the fingerprint image and extracts minutiae. The feature finding process involves identifying prominent fingerprint characteristics or patterns, whereas the minutiae extraction process involves locating minute boundaries, bifurcations, and intersections. A fingerprint's uniqueness is derived from these minutiae points. A fingerprint template is created by combining the unique features of the fingerprint. The fingerprint template is a compact, encrypted representation of the fingerprint without any sensitive information. It serves as a reference point for future identification and verification processes.

In the enrollment process, every fingerprint is linked to a unique identification number, allowing for a direct link between biometric data and personal information. If the ID and fingerprint are paired in the future, the individual will be able to be recognized quickly and accurately.

Figure 2. Enrollment flowchart that shows the steps involved in an enrollment process.

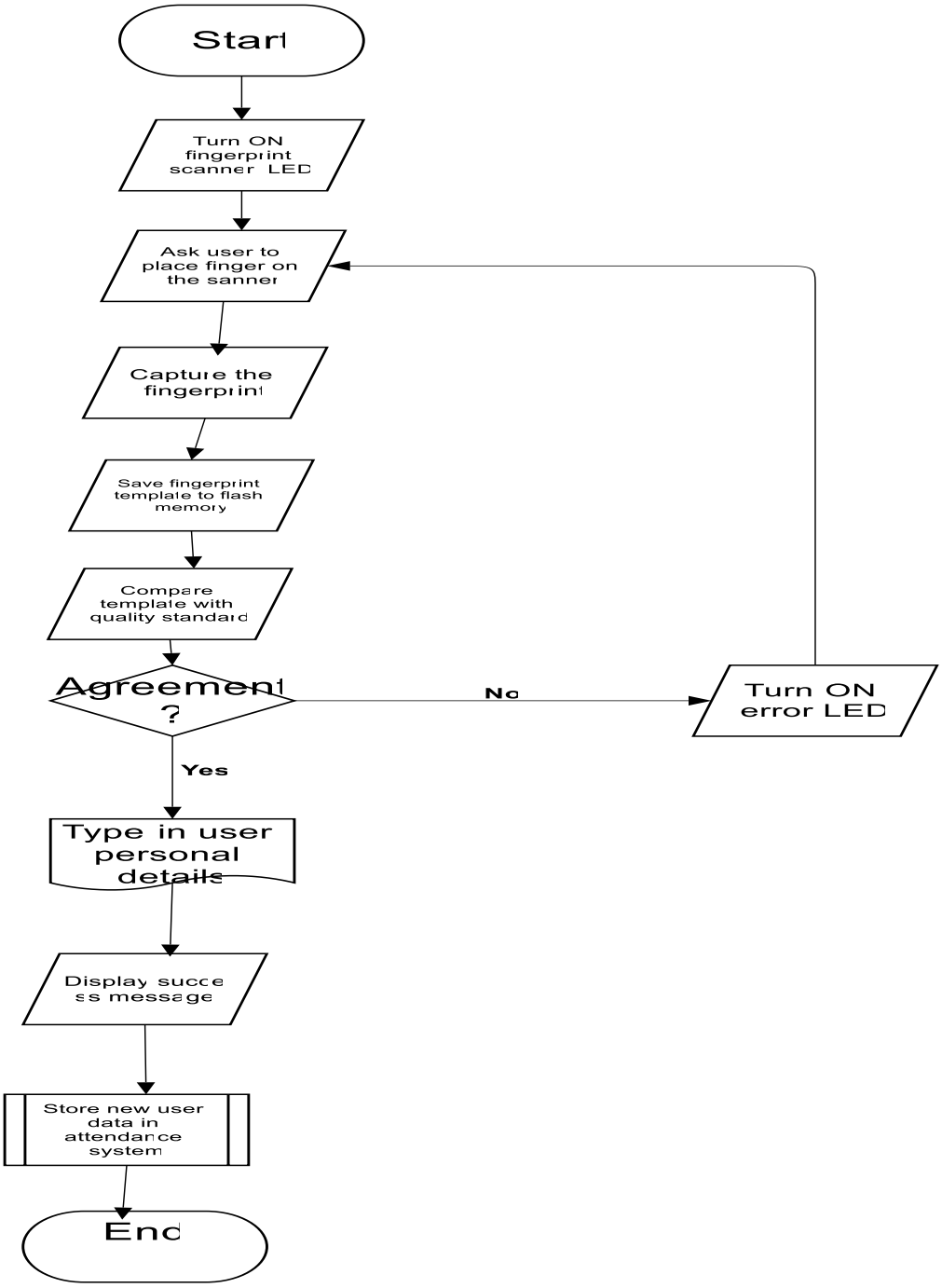



Figure 2. Enrollment Flowchart (Handbook of biometrics 2007)

### 4.1.2 Authentication Stage

Fingerprint authentication is a fundamental component of biometric systems for verifying identity. This involves capturing a unique fingerprint template and storing it, which is later used to verify a person's identity during subsequent authentications.

Figure 3. Shows the authentication flowchart process in the biometric attendance system.

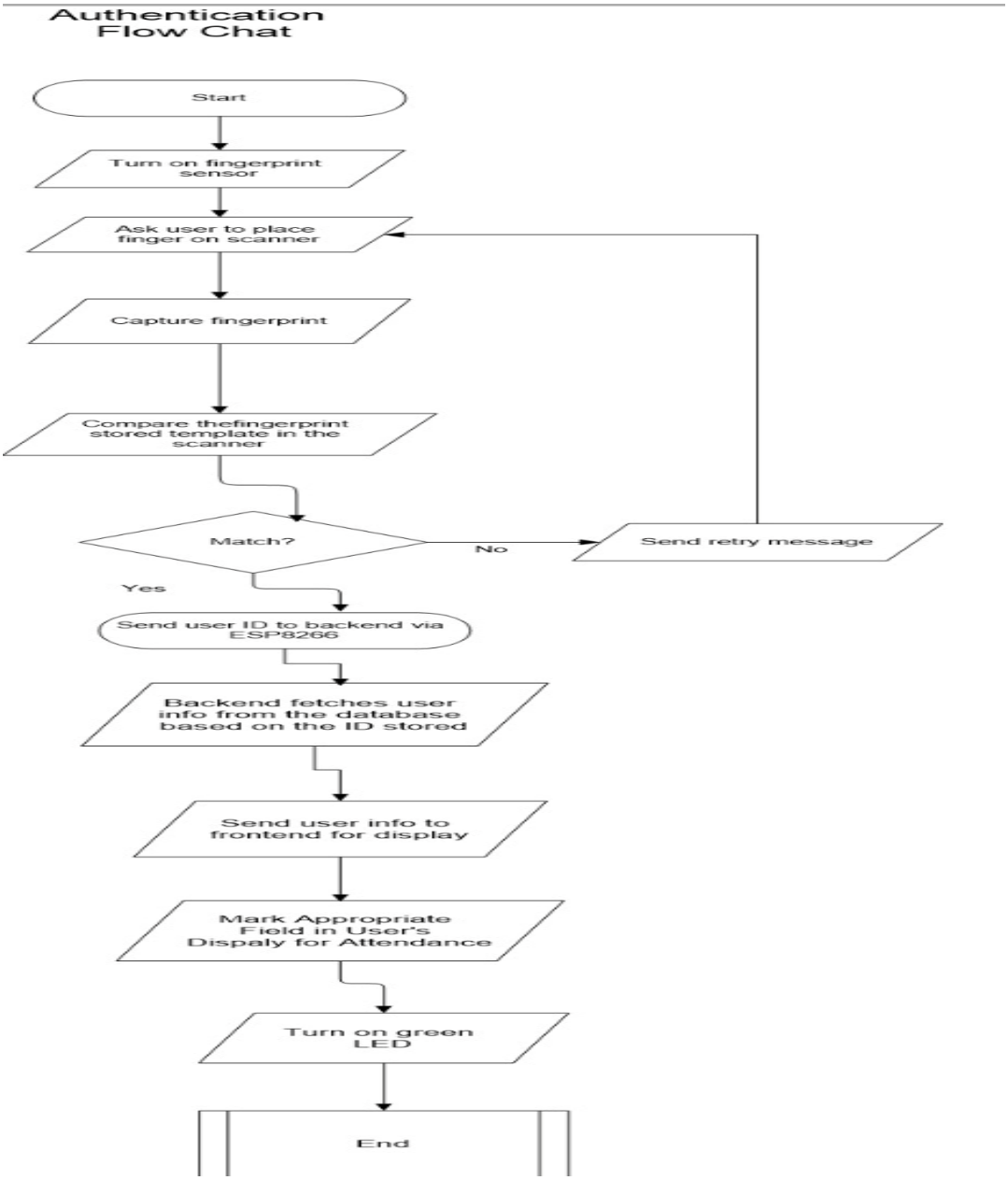



Figure 3. Authentication Flowchart (Handbook of biometrics 2007)

An authentication process is initiated by placing the user's finger on the fingerprint sensor. In the sensor, a fresh fingerprint image is captured, and features are extracted, and minutiae are identified. This is done by comparing the newly captured fingerprint against multiple fingerprint templates stored in its internal memory via a 1: N

search. The fingerprint sensor verifies the user's identity if the template matches the existing fingerprint's features. The ID associated with the matching template is sent to the microcontroller, and a field is marked in the user's personal details as an attendance record. When no matching template is found, the authentication is considered unsuccessful, and an alert is sent, notifying the user to attempt authentication again.

Figure 4. Shows the authentication process between fingerprint sensor and microcontroller.

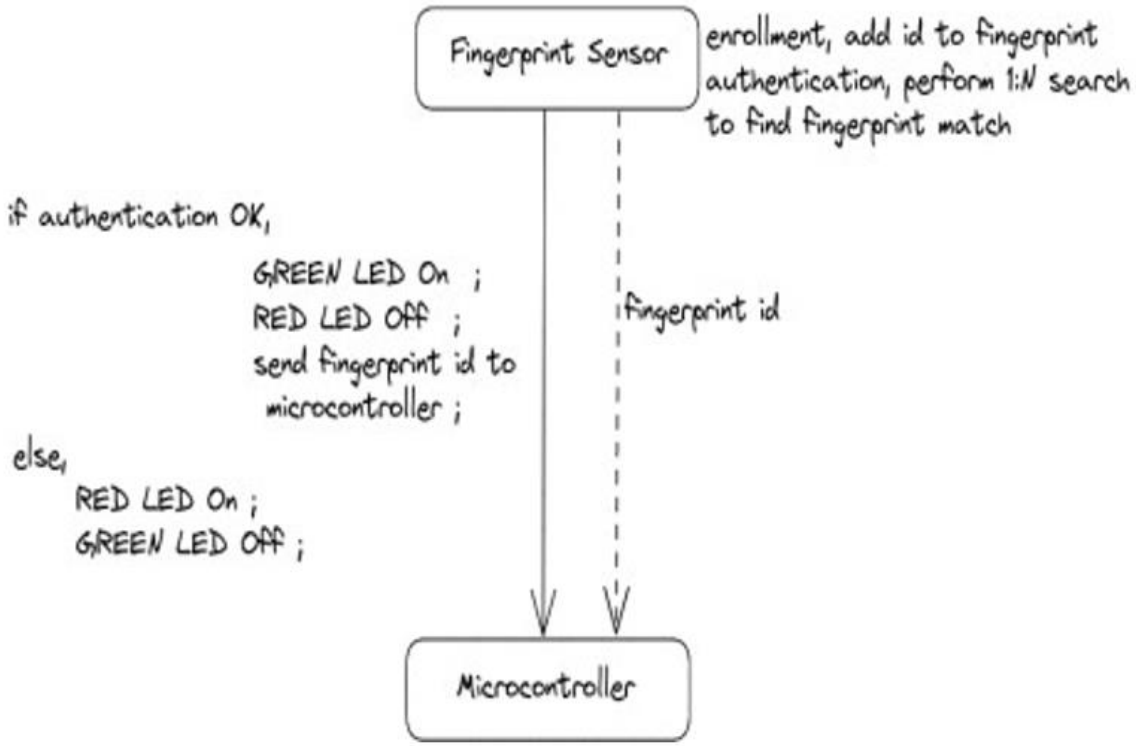



Figure 4. Authentication Process Between Fingerprint Sensor and Microcontroller

Fiqure 5. Shows the authentication process between microcontroller and the WebApp.

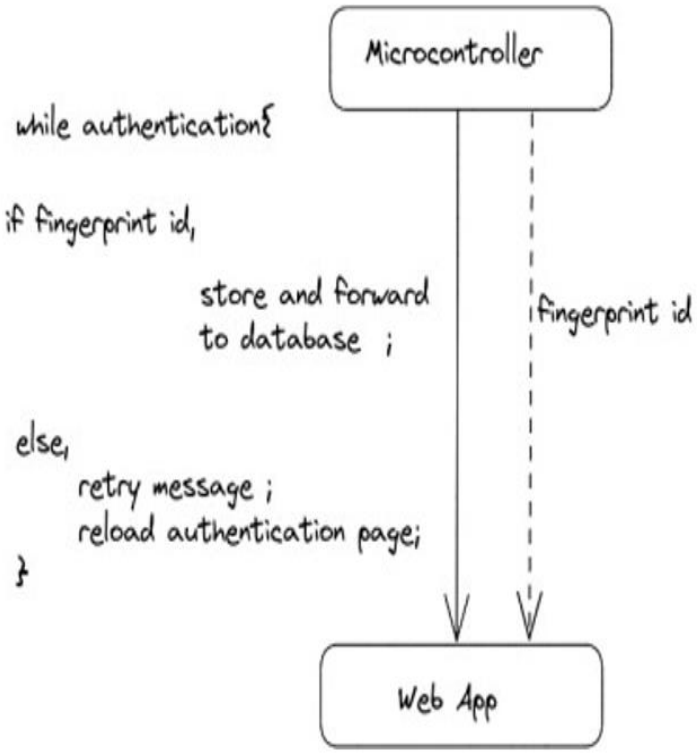



Figure 5. Authentication Process Between Microcontroller and WebApp

### 4.1.3 Software

This project primarily involves developing a web application as part of its software component. A web application serves as the user interface, enabling access and management of attendance records, as well as generating absentee lists. A web application facilitates user registration by providing dedicated fields for entering personal information, which plays an important role in the enrollment process. In addition, authorized personnel can delete users from the system by managing their data. Backends and frontends are the two fundamental components of web applications. The frontend is the part of the application that users directly interact with when accessing the website, representing the visual and interactive elements. The application incorporates various components to facilitate data input and display. Backends, or server-sides, manage data, process user requests, and execute business logic in the background. The backend is responsible for the core functionality that enables the frontend to operate effectively. As the engine behind the web application, the Backend supports its robust functionality and responsiveness.

### 4.1.4 Web-App: Frontend

Early web development relied on three key technologies to create the frontend of websites: HTML, CSS, and JavaScript. Hypertext Markup Language, or HTML, serves as a basis for the frontend, defining elements like headings, paragraphs, images, and links. With CSS, or Cascading Stylesheet, the design was enhanced with colors, fonts, layouts, and styles. The final component, JavaScript, provided the webpage with interactive features, animations, and form validation.

With rapid technological advancements, frontend development has evolved significantly, with new tools and frameworks that simplify and enhance design. React js and Solid js have revolutionized how frontend applications are developed, offering more efficient and scalable methods. There are also UI (User Interface) frameworks that offer pre-defined components for web pages, such as buttons, tables, and dialogs, allowing frontend programming to be streamlined and development to be sped up. Examples of these UI frameworks include TanStack Table and Shadcn, which enable developers to develop user-friendly web applications quickly. (Johnson 2023.)

### 4.1.5 Frontend-Framework: React

The React library is a powerful JavaScript UI library that uses reusable components to build dynamic user interfaces. The components are useful as building blocks that can be re-used across different web pages, enhancing reusability and maintainability. An important part of React's functionality is its implementation of the virtual DOM (Document Object Model). It is a programming interface that represents web pages as a tree of objects, each of which corresponds to a web element. When updating the content of a webpage, the programmer accesses and manipulates the DOM's objects, and the browser renders the new content. However, frequent changes can make this process computationally intensive and inefficient.

React optimizes re-rendering by using a virtual document object. React websites are loaded by the browser, which renders the actual DOM as well as a virtual DOM to track any changes. React first applies the changes to the virtual DOM instead of the actual DOM when modifying a webpage. Next, React compares the virtual and actual DOMs to identify the differences in positions and content. DOM variations are only updated when they are identified, which significantly reduces re-rendering costs and improves performance.

As a result of leveraging the virtual DOM, React minimizes overhead associated with DOM manipulation, resulting in a more responsive and smoother user interface. It is because of this optimization that React is a popular choice for building modern and dynamic web applications. (React Documentation 2023.)

### 4.1.6 User-Interface Framework

UI frameworks for web applications, also known as component libraries, provide pre-built sets of reusable components that enable developers to design consistent and visually pleasing user interfaces. Examples include Material UI, Shadcn, Tanstack Table.

### 4.1.7 Databases

Generally, a database is a structured collection of data. Using it, information can be stored, retrieved, updated, and manipulated efficiently. There are two major types of databases. Relational and Non- relational (NOSQL) databases. (Elmasri & Navathe 2016.)

In relational databases, data is stored and organized using a tabular structure (rows and columns). In this system, data is structured, and foreign keys are used to establish relationships between table The NoSQL database uses a variety of data models and storage mechanisms, allowing for more flexibility with unstructured or semi-structured data.

Often, they are used for large-scale applications or in scenarios where data structures can change over time. Examples: MongoDB (Document Store), Cassandra (Wide-Column Store), Ready (Key-Value store) and Neo4j (Graph Database). Examples include MySQL, PostgreSQL, Oracle, Microsoft SQL Server.

### 4.1.8 MangoDB

Considering factors like: Simplicity, Cost of usage and Ease of programmability. MangoDB was selected for the project. In MongoDB, the document model resembles JSON, and the query language is unique. The query language may require some adjustment for developers more familiar with SQL, but most consider it to be user-friendly.

Cost-effective solution offered by MongoDB Being an open-source database helps to eliminate the need for expensive licensing costs associated with private database systems. Furthermore, MongoDB's scalability helps the project to start with less infrastructure and readily grow as needed. This reduces first costs and best uses available resources. For educational institutions with limited finances especially, this flexible payment system is quite helpful. It presents a scalable solution free of significant initial outlay.

Fiqure 6. Shows the dashboard of MangoDB database for attendance cluster.

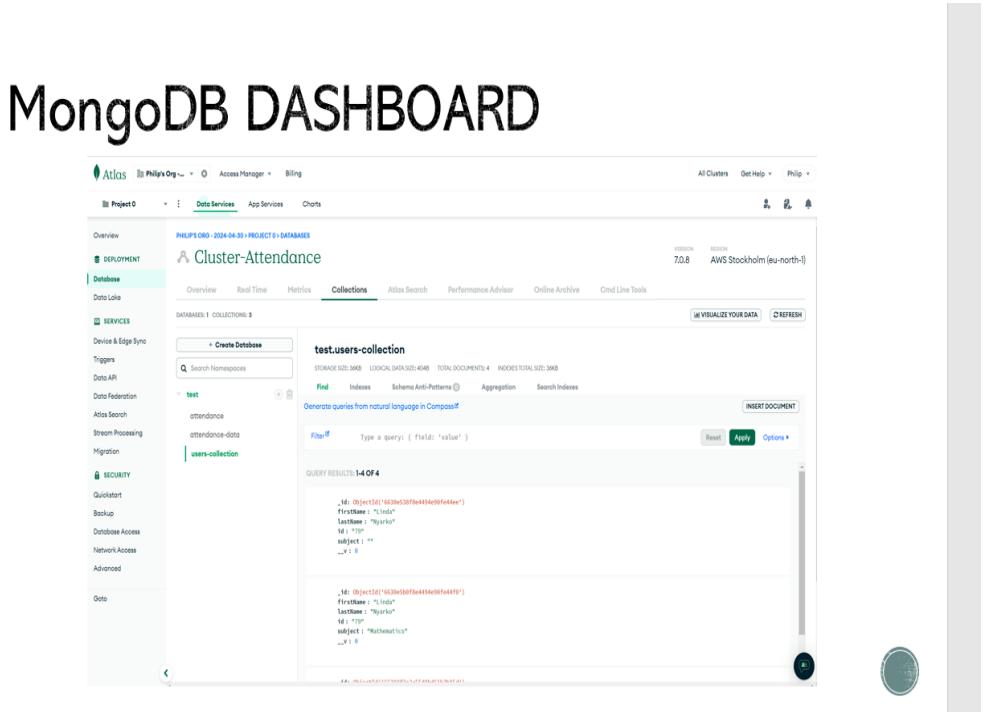



Figure 6. MangoDB Dashboard

Using JSON-like documents in MongoDB makes programming simple and fits rather nicely with contemporary methods. It also fits quite a spectrum of programming languages. Query language and aggregate structure are designed to rapidly access and control data. MongoDB offers excellent documentation and a beneficial community, so simplifying the learning and debugging process for developers and so the development experience. For MongoDB's committed community and user-friendly interface, fast and efficient project development and deployment would be perfect. (MongoDB 2023.)

## 4.2 Design Consideration

### 4.2.1 Hardware

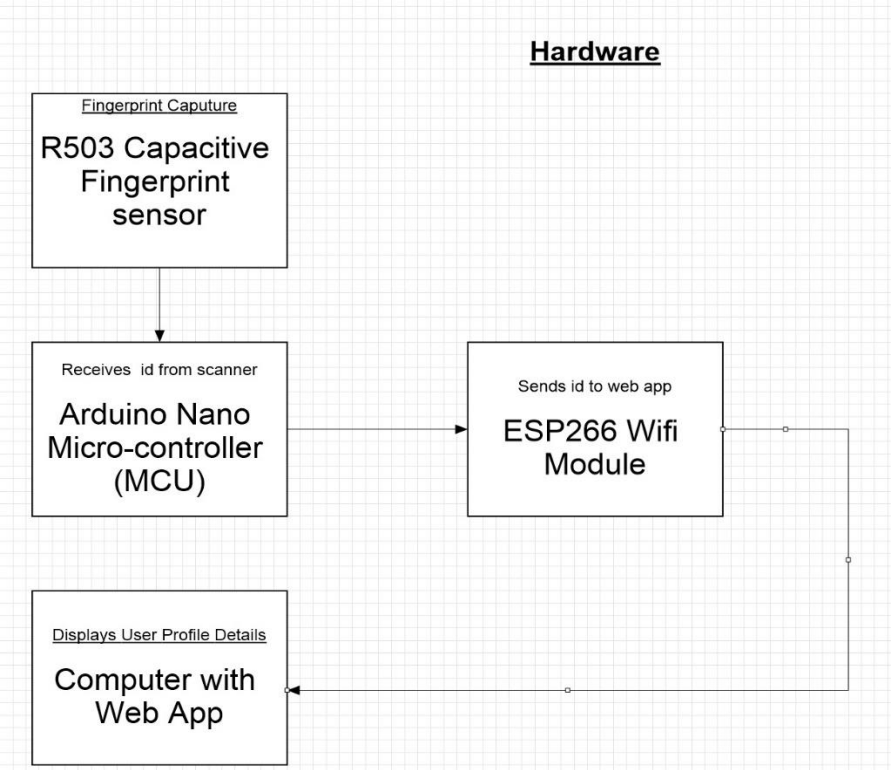



Figure 7. Hardware Architecture

The above figure 7 shows the general architecture of the system.

### 4.2.2 Components

The main components are: R503 capacitive fingerprint sensor, Arduino Nano, and ESP8266 Wifi Module.

R503 Capacitive Fingerprint Sensor

The R503 Capacitive Fingerprint Sensor is a biometric sensor module designed to capture and recognize fingerprint using capacitive touch technology and offer a reliable and accurate solution for fingerprint recognition, enabling a secure authentication in a wide range of electronic devices and systems. In applications where security is essential, capacitive fingerprint sensor provide a high accuracy and reliability, as seen in figure 8 below.

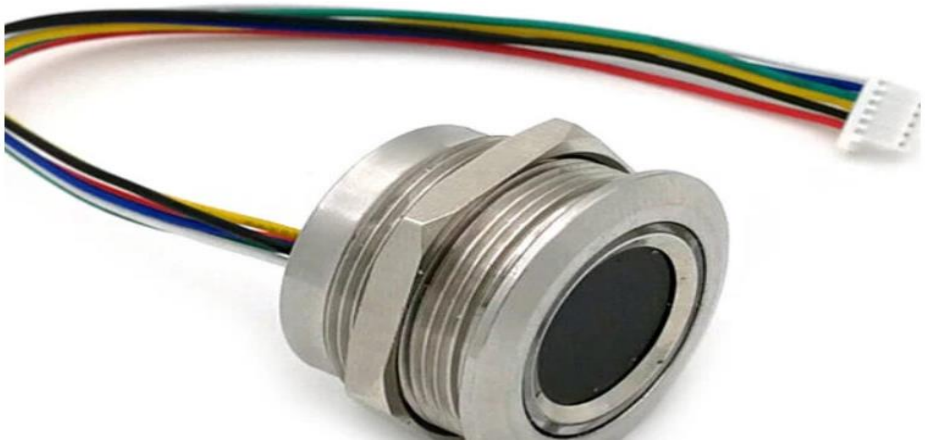


Figure 8. R03 Capacitive Fingerprint Sensor (Digikey.com)

The Arduino Nano

This is powerful and flexible microcontroller board that packs a lot of features into a small form factor, making it ideal for a wide range of projects and applications. The Arduino Nano is compatible with a large library of components, including fingerprint scanners, speakers, and humidity sensors, etc. As a result, it is easier and smoother to interface the board with the components required for this project, labelled in figure 9.

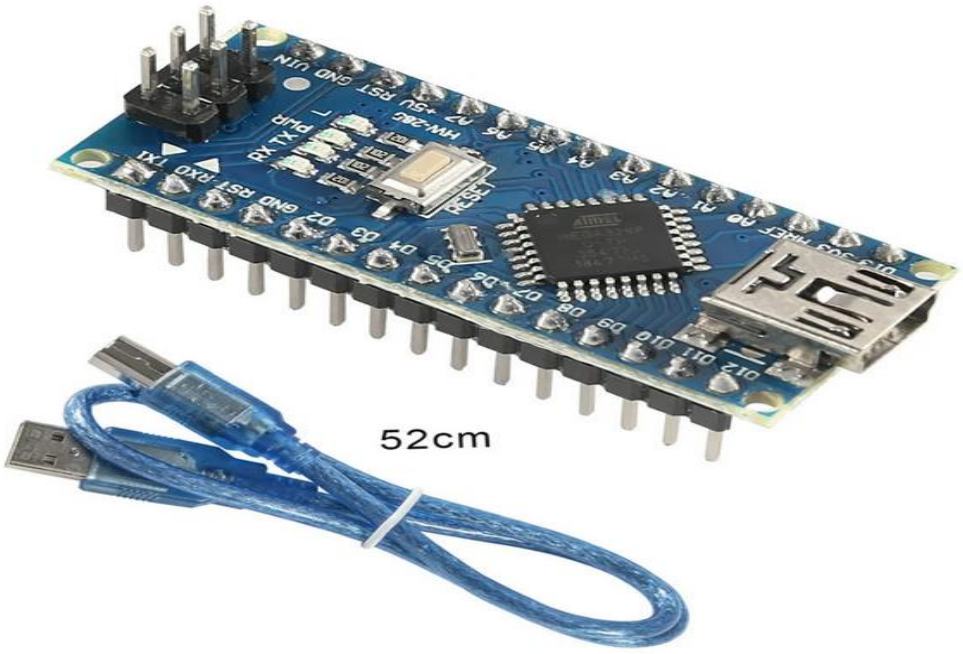



Figure 9.Arduino Nano

The ESP8266 Wifi Module

Fiqure 10. This the wifi moduleWith its low cost and flexibility, the ESP8266 Wifi module comes with an onboard Wifi module and is an ideal module for IoT devices and projects. This eliminates the need to purchase a Wifi module separately for the project.

The ESP8266 Wifi module can be programmed using the Arduino IDE, which simplifies the process for many developers.


Figure 10. ESP8266 Wifi Module (Digikey.com)

# 5 METHODOLOGY

## 5.1 Introduction

As we develop our attendance management system using the microcontroller, we examine the technical foundation. This methodology outlines the systematic approach we took to create a robust and efficient attendance management system. Furthermore, we introduce the use of a capacitive fingerprint scanner for secure user authentication, a feature that facilitates both accurate and secure attendance management. It serves as a technical roadmap, leading all readers through the elements, interactions, and processes that collectively form our system's backbone.

## 5.2 Hardware Setup

The prototype work is shown in the figure with jumper cables and breadboards used to connect the various components. They are connected to an Arduino Nano board that coordinates their functions. To complete the final

prototype connection, the individual components will be connected and tested using the same cables and Arduino IDE. These individual testing phases include locating and downloading the necessary libraries to integrate the various components onto the microcontroller board. To function, the components must be downloaded and installed. The Arduino code is written in C++ with some special methods and functions added.

Figure 11. and figure 12. Shows the circuit diagram and the setup of the project respectively.

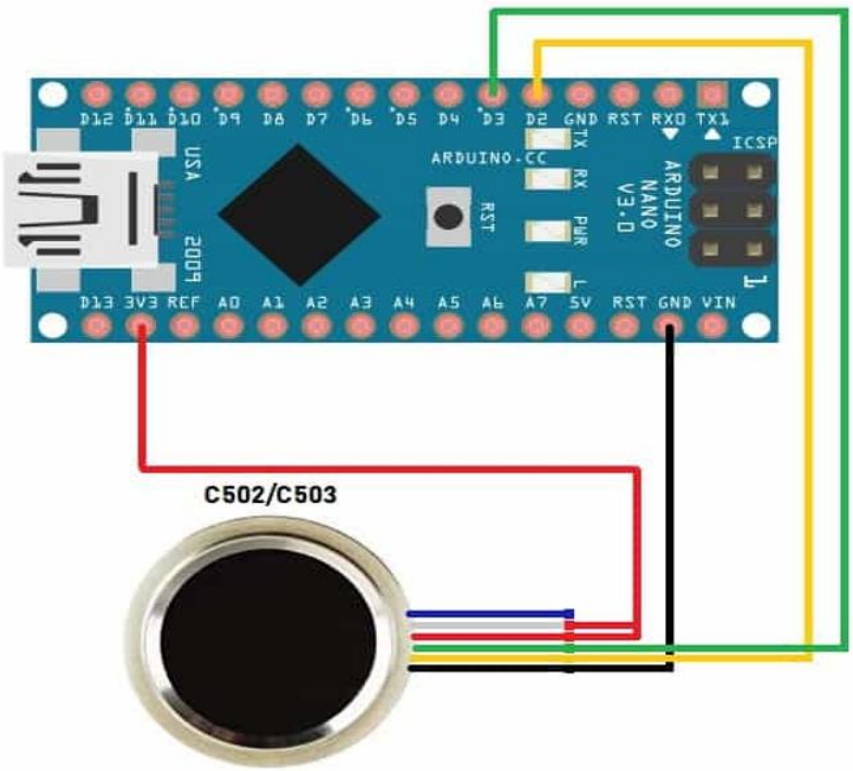



Figure 11. Circuit Diagram Between Sensor and Arduino Nano

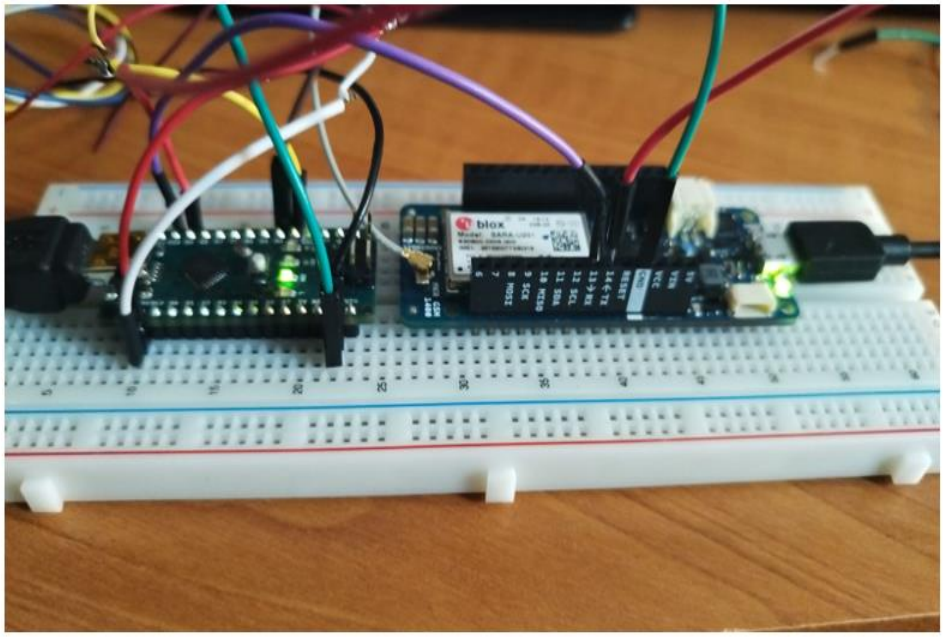


Figure 12. Setup of the Project

## 5.3 Fingerprint Data Processing

First, the R503 capacitive fingerprint sensor is properly initialized and configured by setting up communication between the sensor and microcontroller. The fingerprint sensors use an array of tiny capacitors to capture fingerprint images. A user places their finger on the sensor surface, and its system captures ridges and valleys on their fingerprint. Sensor software includes algorithms to enhance captured images, remove noise, and enhance fingerprint patterns.

Next is, Minutiae extraction and these are distinct features on a fingerprint, such as bifurcation points and ridge endings. An algorithm in the sensor analyses the enhanced fingerprint image to identify these minutiae. A fingerprint pattern template is created from these points.

### 5.3.1 Creating Template, Storage and Matching

The sensor's software generates a template based on the extracted minutiae points. This template is a condensed representation of the fingerprint's unique features. The template does not hold the entire fingerprint image, but rather a mathematical representation of key minutiae.

A template generated by the sensor is stored in its memory or database. To authenticate, it is necessary to capture a user's fingerprint to create a new template, which is then compared with the existing templates. The matching algorithm assesses the likeness between the recently generated template and the stored templates to ascertain if there's a match.

Figure 13. Shows the general overview of the biometric system.

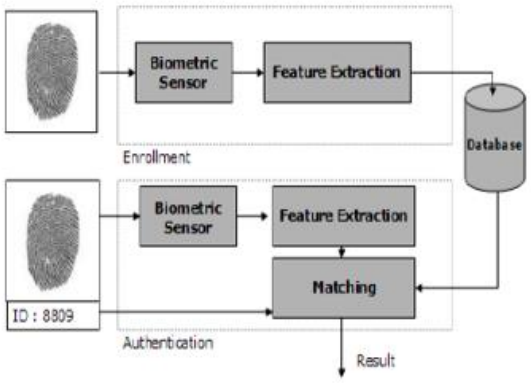



Figure 13. Overview of the Biometric System (M. James 2011)

### 5.3.2 Some Challenges and Solution Associated with Data Processing

Processing fingerprint data can face difficulties due to inconsistencies in finger placement, image quality, and sensor performance. Some typical challenges and their solutions are:

- Noise and Inconsistencies: There are several factors that can influence fingerprint images, including moisture, dirt, and uneven pressure.
- Solution: The fingerprint sensor uses image enhancement techniques to remove noise and improve image quality.
- Variation in template matching: Matching templates can be affected by variations in finger placement during enrolment and authentication.
- Solution: Tolerance mechanisms are likely included in the algorithm to accommodate slight variations in fingerprint placement.
- Security: Keeping templates secure to prevent unauthorized access.
- Solution: To guard against potential breaches, the fingerprint sensor may utilize encryption techniques.

# 6 SOFTWARE INTEGRATION

A server functions as a middleman between the backend and frontend. From a technical standpoint, it is also considered a component of the backend.

The front end of the website includes the homepage and all other related web pages that are visible to the user upon entering the website. The frontend pages are capable of functioning by utilizing data obtained from the backend. Our frontend pages will retrieve attendance data from the backend's SQL database and present it. The frontend will send a request to a connected server, specifically asking for certain defined pieces of data. The server, in addition to connecting to the backend, will retrieve this information from the built database and return it to the frontend for usage or display.

The backend performs several services behind the scenes, including recording attendance and fetching data from the database, as shown in figure 14.

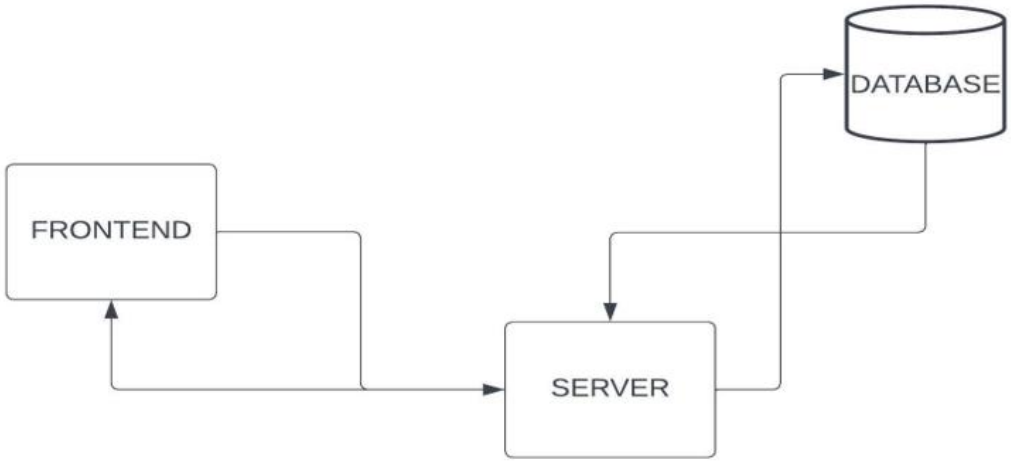



Figure 14. Website's General Architecture

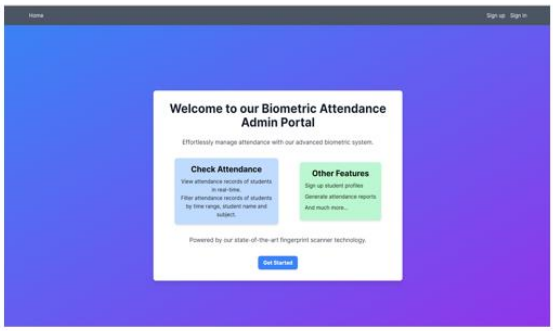
## 6.1 Display of Attendance on Frontend

Once the process of enrollment and authentication is completed, a student will be able to access their attendance history, including the specific periods of attendance, on the designated website. This occurs after his authentication.

In addition, lecturers have access to a comprehensive record of all students who have previously attended the class, including the specific periods of their attendance.

Figures 15-17. Shows user interface with admin portal ,adding and delete student and student attendance display.

GETTING STARTED




SIGN IN PAGE

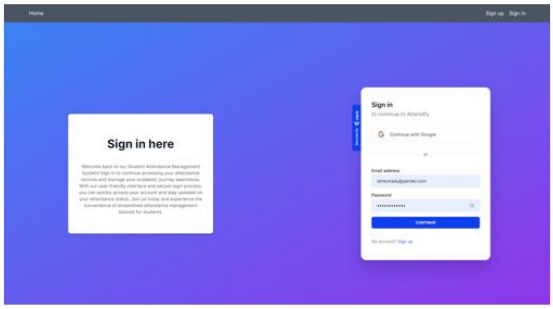
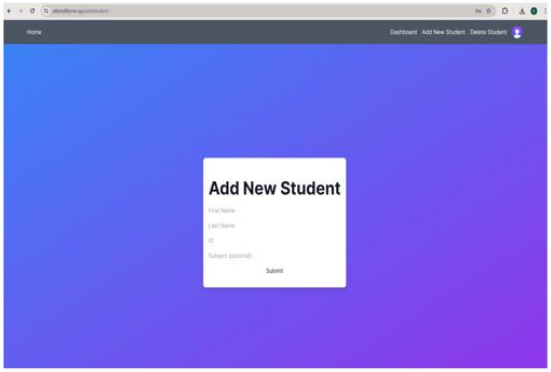



Figure 15. Admin Portal



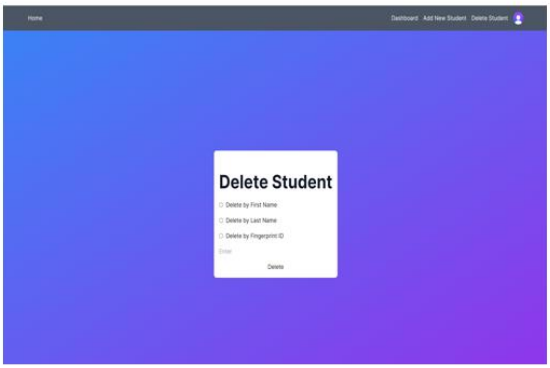




Figure 16. Adding and Deleting Student (Identifyme.xyz)

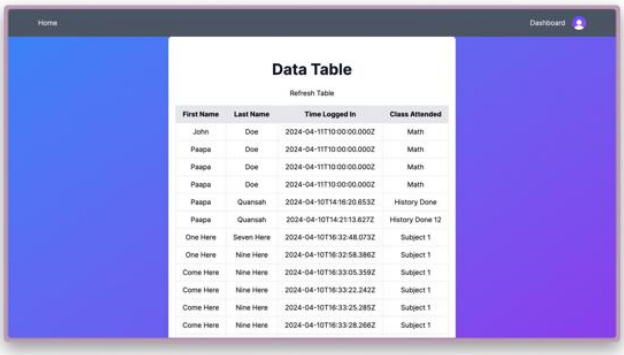



Figure 17. Show Attendance

# 7 RESULTS AND ANALYSIS

The project performed satisfactorily according to expectations following a series of tests. There was a total of 5 fingerprints that were registered in the system for the purpose of testing. No instances of False Acceptance or False Rejection were recorded during the testing. The scanning duration was often brief, typically lasting no more than one second.

Due to limited usage during testing, the efficacy and durability of the product in high volume applications remain uncertain. Under the assumption that all other factors remain constant, the system should have the capability to manage the identification numbers of a minimum of 200 individuals without encountering any issues.

In order to accommodate more than 200 fingerprints, the terminal will require the addition of an SD card to augment its capacity, hence boosting its onboard storage capacity.

# 8 CONCLUSION AND RECOMMENDATION

The design of the project which employs the use of biometric data in authentication was successful with an easy-to-use manner, improving the accuracy of attendance records, minimizing instances of fraudulent attendance markings, and capturing and storing attendance data with reliability. Admins can also access attendance records remotely through the system.

Nevertheless, the initiative encountered challenges. At times, the work was hindered by technical obstacles, such as the need to confirm the compatibility of hardware components and resolve software issues. Furthermore, conducting more comprehensive initial testing could have identified compatibility issues earlier, facilitating more efficient problem-solving.

Improving the fingerprint recognition technology would increase the user experience by enabling faster and more accurate processing. Exploring cloud-based alternatives for data access and storage could enhance the system's scalability and accessibility. In addition to enhancing the existing system, these modifications would facilitate broader use in other educational environments.

# 9 REFERENCES

ChatGPT 2023. OpenAI. GPT-3.5. Accessed for language check, May 2024. https://chat.openai.com

Al Hajri, E., Hafeez, F., & NV, A. A. 2019. Fully Automated Classroom Attendance System. Int. J. Interact. Mob. Technol., 13(8), 95-106.

Deshpande, V., Bhujade, R., Amin, S., Agarwal, R., & Untawale, S. 2021. Development of employee performance management system using web-based application. In 2021 International Conference on Intelligent Technologies (CONIT) (pp. 1-5). IEEE.

Erfan, M. 2021. Aplikasi Laporan Kehadiran Dosen dan Karyawan STMIK Palangkaraya. Jurnal Saintekom: Sains, Teknologi, Komputer dan Manajemen, 11(1), 52-61.

Fulton, E., Newby, K., Gokal, K., Kwah, K., Schumacher, L., Jackson, L. J., ... & Brown, K. 2019. Tailored digital behaviour change intervention with e-referral system to increase attendance at NHS stop smoking services (the MyWay project): study protocol for a randomised controlled feasibility trial. BMJ open, 9(4), e028721.

Kakarla, S., Gangula, P., Rahul, M. S., Singh, C. S. C., & Sarma, T. H. 2020. Smart attendance management system based on face recognition using CNN. In 2020 IEEE-HYDCON (pp. 1-5). IEEE.

Mijić, D., Bjelica, O., Durutović, J., & Ljubojević, M. 2019. An improved version of student at-tend-ance management system based on RFID. In 2019 18th International Symposium INFOTEH-JA-HORINA (INFOTEH) (pp. 1-5). IEEE.

Newman-Ford, L., Fitzgibbon, K., Lloyd, S., & Thomas, S. 2008. A large-scale investigation into the relationship between attendance and attainment: a study using an innovative, electronic attend-ance monitoring system. Studies in Higher Education, 33(6), 699-717

Nurjaman, A. S., & Yasin, V. 2020. Konsep desain aplikasi sistem manajemen kepegawaian ber-basis web pada PT. bintang komunikasi utama (Application design concept of web-based staffing management system at PT Bintang Komunikasi Utama). JISICOM (Journal of Information System, Informatics and Computing), 4(2), 143-174.

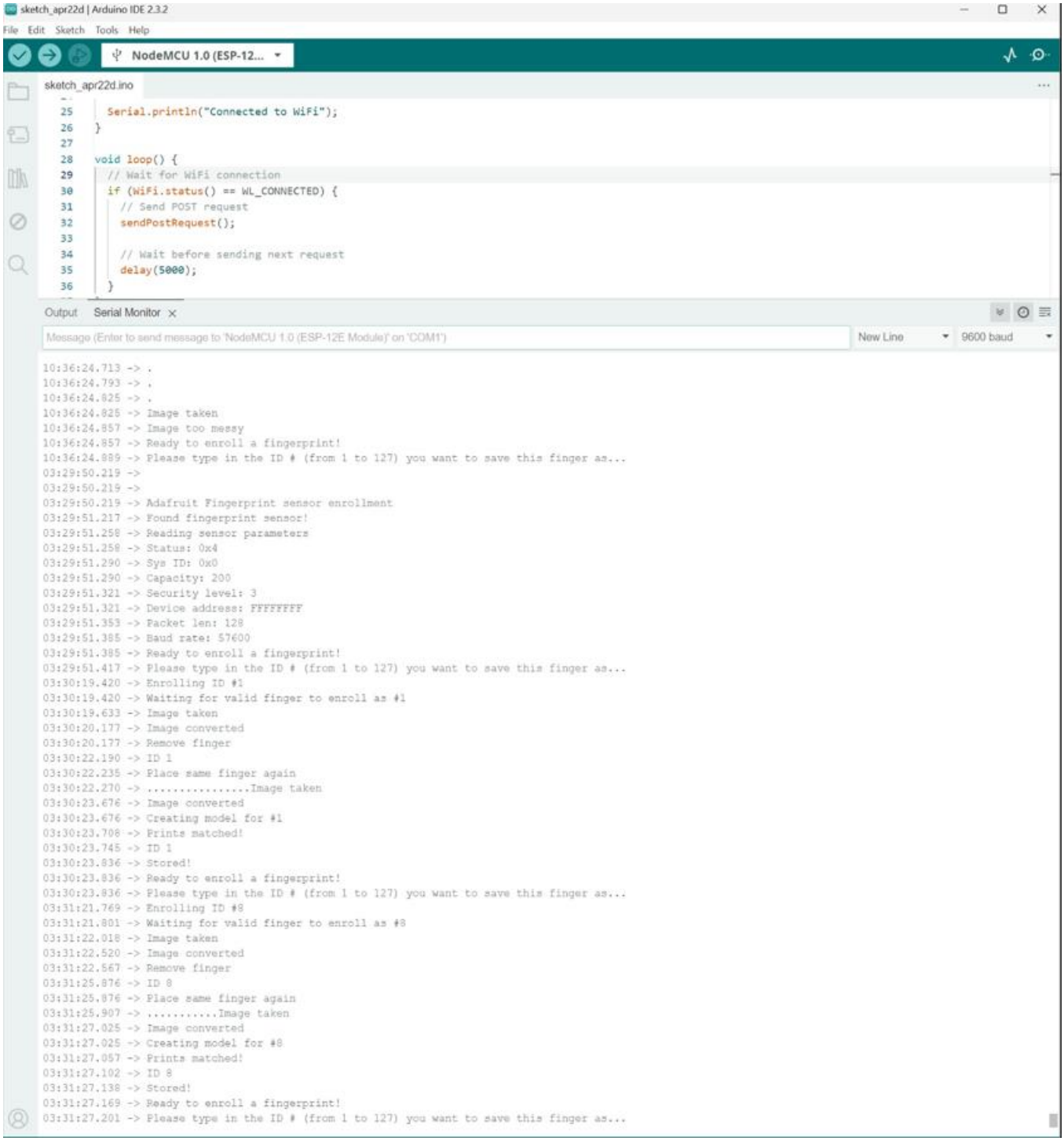
Rahmatulloh, A., Gunawan, R., & Darmawan, I. 2019. Web services to overcome in-teroperability in fingerprint-based attendance system. In 2018 International Conference on Industrial Enterprise and System Engineering (IcoIESE 2018) (pp. 277-282). Atlantis Press.

Takyudin, A., Faturrahman, H., Juwono, J., Julianto, M. R., & Yulianti, Y. 2021. Analisa dan Perancangan Sistem Informasi Elearning Berbasis Web untuk Memantau Aktivitas Belajar Peserta Didik di SMP Fioretti Tigaraksa. Jurnal Teknologi Sistem Informasi dan Aplikasi, 4(2), 110-118.

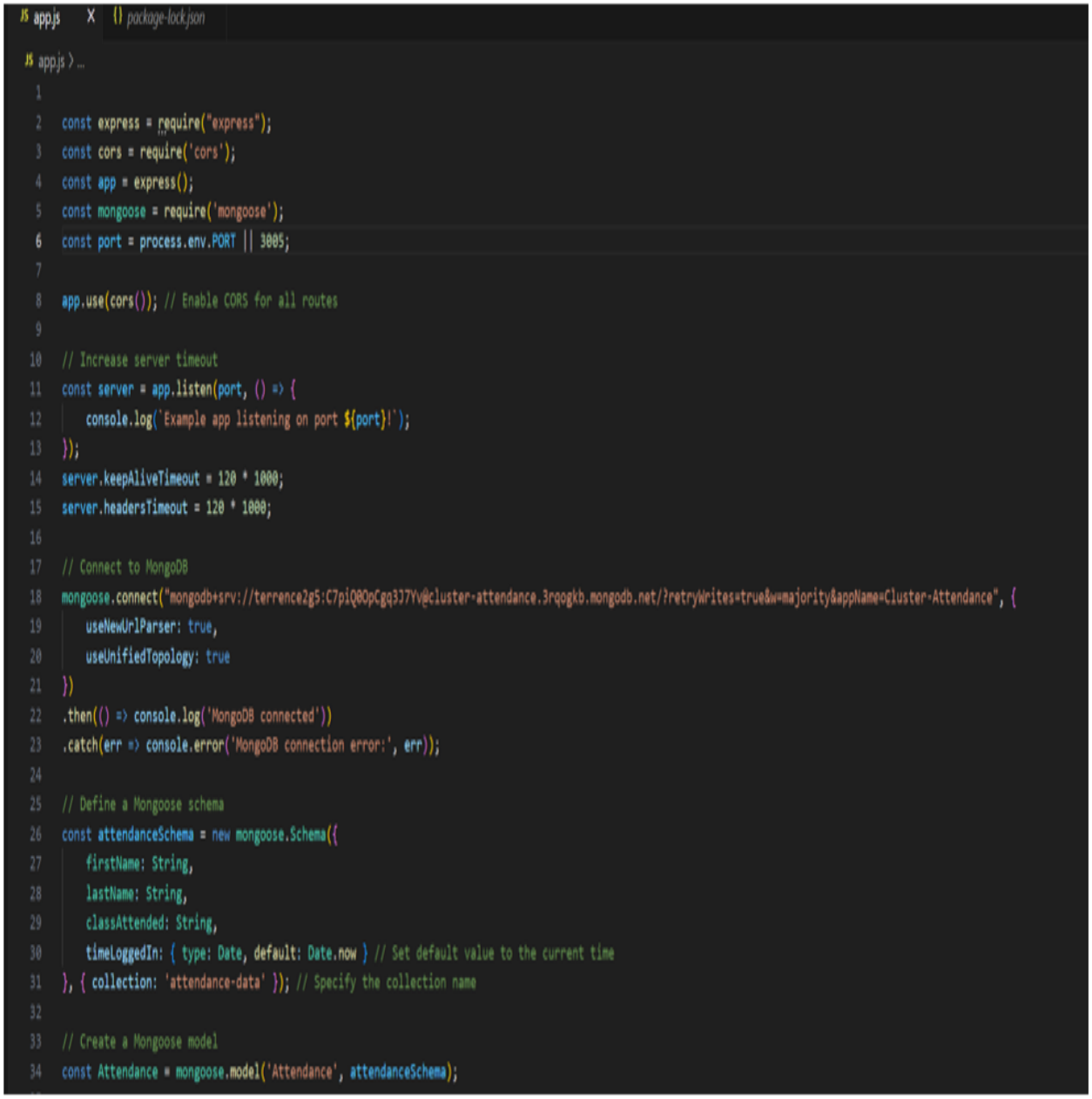
Walia, H., & Jain, N. 2016. Fingerprint based attendance systems-a review. International Re-search Journal of Engineering and Technology, 3(5), 1166-1171.

# 10 APPENDIX

Arduino Code for Fingerprint Capturing and Enrolment



Backend Code Connection String to MangoDB



```
app.js   X   {} package-lock.json

app.js > ...

1
2   const express = require("express");
3   const cors = require('cors');
4   const app = express();
5   const mongoose = require('mongoose');
6   const port = process.env.PORT || 3005;
7
8   app.use(cors()); // Enable CORS for all routes
9
10  // Increase server timeout
11  const server = app.listen(port, () => {
12      console.log(`Example app listening on port ${port}!`);
13  });
14  server.keepAliveTimeout = 120 * 1000;
15  server.headersTimeout = 120 * 1000;
16
17  // Connect to MongoDB
18  mongoose.connect("mongodb+srv://terrence2g5:C7piQ8OpCgq3J7Yv@cluster-attendance.3rqogkb.mongodb.net/?retryWrites=true&w=majority&appName=Cluster-Attendance", {
19      useNewUrlParser: true,
20      useUnifiedTopology: true
21  })
22  .then(() => console.log('MongoDB connected'))
23  .catch(err => console.error('MongoDB connection error:', err));
24
25  // Define a Mongoose schema
26  const attendanceSchema = new mongoose.Schema({
27      firstName: String,
28      lastName: String,
29      classAttended: String,
30      timeLoggedIn: { type: Date, default: Date.now } // Set default value to the current time
31  }, { collection: 'attendance-data' }); // Specify the collection name
32
33  // Create a Mongoose model
34  const Attendance = mongoose.model('Attendance', attendanceSchema);
```