

An Electronic and Web-Based Authentication, Identification, and Logging Management System

Augustus E. Ibhaze^{1,*}, Onyekachukwu A. Aribeara²

Department of Electrical and Electronics Engineering, University of Lagos, Akoka, Lagos, Nigeria.

eibhaze@unilag.edu.ng¹, oaribeana@gmail.com²

ABSTRACT

The need for participants' performance assessments in academia and industry has been a growing concern. It has attendance, among other metrics, is a key factor in engendering a holistic approach to decision-making. For institutions or organizations where managing people is an important yet challenging task, attendance tracking and management could be employed to improve this seemingly time-consuming process while keeping an accurate attendance record. The manual/quasi-analog approach of taking attendance in some institutions could be unreliable and inefficient, leading to inaccurate computation of attendance rates and data loss. This work, therefore, proposes a system that employs embedded technology and a biometric/ web-based application to enhance attendance management. The hardware encompasses the integration of an ESP8266 NodeMCU and the biometric AS608 fingerprint sensor interfaced with the database for which the front-end and back-end integration was through the React framework. The system uses a web application that displays the attendance results and scheduled course data from its database, provides feedback to lecturers on which student missed classes and calculates a student's average attendance for the semester. By implementing this system, the accuracy of student attendance is expected to experience an appreciable improvement, eliminate proxy signing, provide a more secure alternative for attendance recording, curtail tardiness to classes, and ultimately improve student productivity on execution.

Keywords: Attendance, Biometric, Database, Enrollment, Internet-Of-Things, OLED.

*Corresponding author

Peer review under the responsibility of University of Baghdad.

<https://doi.org/10.31026/j.eng.2024.01.01>

This is an open access article under the CC BY 4 license (<http://creativecommons.org/licenses/by/4.0/>).

Article received: 01/07/2023

Article accepted: 30/12/2023

Article published: 01/01/2024



نظام إدارة التصديق والتعريف والولوج الإلكتروني باعتماد الويب

اوغسطس اي ابهيز^{1*}، اونيكوجوكاو أي اربينا²

قسم الهندسة الكهربائية والالكترونيك، جامعة لاكوس، اكوكا، لاكوس، نيجيريا

الخلاصة

كانت الحاجة إلى تقييم أداء المشاركين في الأوساط الأكاديمية والصناعية مصدر قلق متزايد وجعلت الحضور من بين مقاييس أخرى عاملاً رئيسياً في إيجاد نهج شامل في صنع القرار. بالنسبة للمؤسسات أو المنظمات التي تكون فيها إدارة الأشخاص مهمة ولكنها مهمة صعبة ، يمكن استخدام وسائل تتبع الحضور وإدارته لتحسين هذه العملية التي تبدو مستهلكة للوقت مع الاحتفاظ بسجل حضور دقيق. قد يكون النهج اليدوي / شبه التناظري لأخذ الحضور في بعض المؤسسات غير موثوق به وغير فعال ، مما يؤدي إلى حساب غير دقيق لمعدل الحضور وفقدان البيانات. لذلك يقترح هذا العمل نظاماً يستخدم التكنولوجيا المضمنة وتطبيقاً قائماً على المقاييس الحيوية / الويب لتعزيز إدارة الحضور. يشتمل الجهاز على تكامل ESP8266 NodeMCU ومستشعر بصمة الإصبع المقاييس الحيوية AS608 المتصل بقاعدة البيانات التي تم دمج الواجهة الأمامية والخلفية من خلال واجهة عمل React . يتضمن النظام استخدام تطبيق ويب يعرض نتائج الحضور وبيانات الدورات المجدولة من قاعدة بياناته ، ويقدم ملاحظات للمحاضرين عن أي طالب غاب عن الفصول الدراسية ويحسب متوسط حضور الطالب للفصل الدراسي . من خلال تنفيذ هذا النظام ، من المتوقع أن تشهد دقة حضور الطلاب تحسناً ملموساً ، والقضاء على توقيع الوكيل ، وتوفير بديل أكثر أماناً لتسجيل الحضور ، وتقليل التأخير في الفصول الدراسية وتحسين إنتاجية الطالب في نهاية المطاف عند التنفيذ.

الكلمات المفتاحية: الحضور، القياسات الحيوية، قاعدة البيانات، التسجيل، إنترنت الأشياء، OLED.

1. INTRODUCTION

Electronic communication systems have experienced a paradigm shift in terms of integration in recent years following the emergence of smart solutions, the Internet of Things (IoT), web and cloud computing, among others (Mahmood et al., 2013; Younis, 2014; Younis et al., 2015; Idachaba et al., 2017; Younis and Hussein, 2018; Ibhaze et al., 2018; Ibhaze et al., 2019; Ajiroghene et al., 2020; Fadhil et al., 2020; Ibhaze et al., 2020; Younis and Alwan, 2021). Skillful implementation of electronic devices such as sensors, microcontrollers, and cloud computing solutions (storage and servers) has made IoT deployment seamless (Ibhaze et al., 2016; Idachaba and Ibhaze, 2016; Younis and Muhammad, 2018).

The attendance management system is one application where the ingenuity in electronic communication devices has attracted research attention and innovation. Attendance systems involve the processes, methods, and technologies used in managing and tracking the presence or absence of people in a particular setting and various sectors such as health care, education, events, workplace, and government institutions for identification, security, and administrative purposes (Kizza, 2023). The processes take various forms, from paper-based traditional methods to more modern approaches. These technologies provide



accurate, secure, and more efficient ways of attendance management for streamlined operations and attendance data-driven recommendations. Attendance management in educational institutions can be quite challenging due to the limitation of paper and file-based methods. Each institution has its standards regarding a student's attendance, which highlights the importance of keeping an accurate attendance record (Younis et al., 2012). The current system of taking attendance has many restrictions, such as difficulties in computing percentage attendance due to inaccuracies and the tedious and time-consuming process (Seelam et al., 2021; Keerthi et al., 2022). A biometric approach can be adopted (Dastidar et al., 2017; Esttaifan, 2023; Joodi et al., 2023). A well-validated method adopted in research makes use of the fingerprint biometrics method of human identification (Galbally et al., 2012; Mohamed and Raghu, 2012; Yuan et al., 2023) since its unique data cannot be forgotten, replicated, or stolen (Thales, 2021) and it helps to decrease student absenteeism (Amor et al., 2019) and improve student productivity.

For a biometric system to perform optimally, the morphological characteristics used in determining a person's identity must satisfy a set of requirements. The characteristic targeted must be universal to every human being, meaning it should be versatile in all aspects. It has to have a certain degree of uniqueness for the system to be secure and accurately collect data. The said feature should be a more permanent characteristic. It should not change so much over time because the system counts on the data to be the same and always gives the same outcome. Lastly, the characteristics should be quantitative and easy to collect and process (Lin et al., 1997).

The main focus of creating a system that collects biometric data is that the data should be collected easily. Otherwise, the system will fail to perform its functions. As given in Table 1, the performances of various biometric technologies in meeting the requirements of biometric identification are compared to show how each characteristic measured meets the requirement. In addition to accuracy, biometric features must be evaluated based on their ability to prevent circumvention and fraudulent activities (which can impact false acceptance rates) and their overall acceptability by users. However, accuracy is the most important factor to consider when designing a reliable biometric system

Table 1. Performance of various biometric technologies on various properties of biometric features (Lin et al., 1997)

Biometric	Universality	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	High	Low	Medium	High	Low	High	Low
Fingerprint	Medium	High	High	Medium	High	Medium	High
Hand Geometry	Medium	Medium	Medium	High	Medium	Medium	Medium
Hand Vein	Medium	Medium	Medium	Medium	Medium	Medium	High
Iris	High	High	High	Medium	High	Low	High
Retinal Scan	High	High	Medium	Low	High	Low	High
Signature	Low	Low	Low	High	Low	High	Low
Voice Print	High	High	Low	High	Medium	High	High



To build a successful biometric system, the following components would be required: a scanner to record the identifier, assess its quality, and generate a compact representation of the biometric identifier; software to control scanner modes and measure observed and stored data; and a database to store biometric information for future comparison **(Alexander, 2021)**

In recent times, fingerprint biometrics has been recognized to be one of the most prevalent forms of automatic identification used in biometrics. It is cost-efficient, easy to use, accessible, widely distributed, and hard to defraud, making it a convenient and functional tool for identity verification and authentication. This biometric system uses an identifier that you possess (fingerprints), and its advantage is that every person would always have their fingerprints on them, belonging to them alone **(Okta, 2023)**.

Fingerprints are unique patterns of ridges and valleys on the human fingers formed by the flow-like ridges on the skin's surface. These ridges, also known as single curved segments and valleys, the spaces between two ridges, are determined by the initial state of the embryonic mesoderm during development. The uniqueness of the human fingerprint can be summarized by three principles: namely, each finger has unique epidermal ridges and valleys, fingerprints vary within limits that allow for classification, and the ridges and valleys are permanent and unchanging for a given finger **(Lin et al., 1997)**. In the design of a fingerprint verification system, all these characteristics must be catered for with no room for error. Therefore, a fingerprint verification system must have the following essential design components: acquisition, representation (template) and preprocessing, feature extraction, and minutiae matching.

In acquiring fingerprint data, one (more or less) has two options. It could be used to obtain the impression of a fingerprint on paper and scan the fingerprint on paper with a scanner in a retrograde manner. Another method would be to use a live scanner that detects and creates the fingerprint image by determining the light and dark areas created by the fingerprint ridges. The former is a bit cumbersome in real applications and may sometimes be inaccurate. The latter case is the more acceptable data acquisition method **(Socheat and Wang, 2020)**. The technique used by these live scanners (also known as optical scanners) is called Optical Frustrated Total Internal Reflection, and this technique uses a glass prism/platen, LED light source, and charge-couple device (CCD) camera for producing fingerprint images. When the fingers are placed on the prism/platen, the ridges are in contact with the glass platen, while the valleys are not. The CCD and a light-sensitive microchip are placed on the other side of the glass platen. The microchip creates a digital image of the ridges and valleys of the fingerprint, resulting in a corresponding fingerprint image on the CCD **(Miguel, 2018)**. In a fingerprint image, ridges and valleys often run in parallel. When analyzed globally, fingerprint patterns exhibit one or more regions where the ridges and valleys create a pattern of distinct shapes. These regions may be classified into three topologies: loop, arch, and whorl.

Fig. 1 depicts the three basic fingerprint ridge patterns: loops (radial loop pattern), whorls (whirlpool pattern), and arches (wave-like pattern). The scanner's processor typically checks for clear image capture and various values, such as pixel darkness and overall values, when representing acquired data in templates. Because these detectors are sensitive to low-light levels, they are known to produce excellent grayscale images. The grayscale images of the fingerprint produced by the detector represent the original fingerprint and template matching during verification. After obtaining an image template, the template is rarely of good quality to begin feature extraction, and this is often due to a couple of factors during acquisition. Therefore, the image must be enhanced to provide a more accurate image and

maintain a moderate false rejection/acceptance rate. This process of image enhancement for feature extraction is called pre-processing.



Figure 1. The different types of fingerprint topologies

According to (Abbood et al., 2014), the pre-processing of a fingerprint image may be categorized into Image binarization, Ridge thinning, Ridge orientation estimation and location, Image enhancement, and spurious minutiae removal. Image binarization can be defined as the process of converting the fingerprint image into a binary image. How binarization works is that it tests each pixel in the image based on a reference threshold value based on average brightness. A pixel below the threshold value would be converted to black, and a pixel above the threshold value would be converted to white. After binarization, ridge thinning is applied to the image to reduce the ridgeline of the fingerprint from thick lines to thinner lines or pixels. This makes minutiae point extraction easier because ridge ending or bifurcation points can be determined from the image. Following this step is the location and estimation of ridge orientation (types) (Socheat and Wang, 2020). **Fig. 2** depicts the different results of the original fingerprint obtained after binarization and thinning.

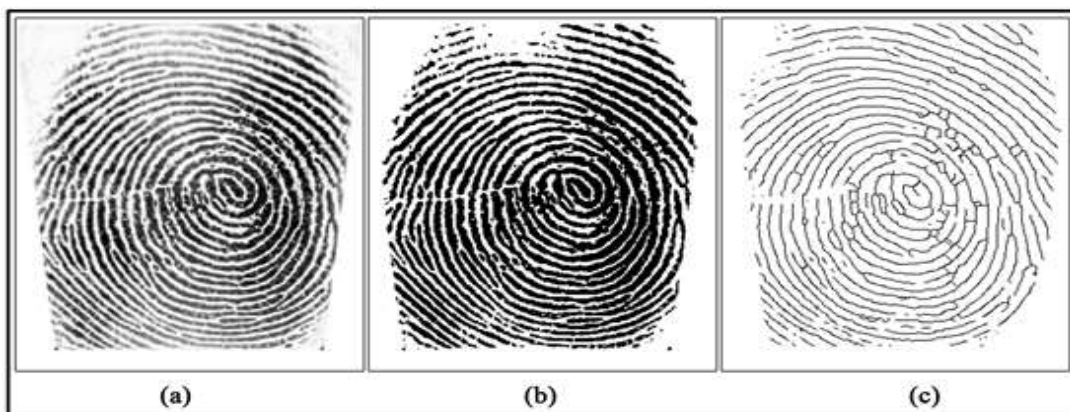


Figure 2. a) Original fingerprint, b) Fingerprint after binarization, c) Fingerprint after ridge thinning

The orientation of a ridge in a grid of n by m pixels can be estimated using the process of ridge orientation estimation. This method uses a matrix formula to compare the central pixel to its neighboring pixels. It is important to note that this approach is specific to the

algorithmic method described in the article by (Lin et al., 1997). This is performed to determine the location and key features of each type of minutiae in the fingerprint image template. After this stage, image enhancement algorithms are used to improve the quality of the image, especially in noisy areas. Additional enhancements called spurious minutiae removal can also be performed to remove spurious minutiae due to excess noise not filtered out (Peralta et al., 2014).

During feature extraction, the main focus is being able to extract minutiae points. Fig. 3 identifies the ridge orientation types, minutiae points known as ridge discontinuities, and are of two main types: ridge ending and ridge bifurcation (Socheat and Wang, 2020). The average amount of minutiae for a good fingerprint is 40 – 100 points. It is these points that are used for evaluating the uniqueness of a person's fingerprint. A feature extractor finds the ridge endings and ridge bifurcation in the fingerprint image.

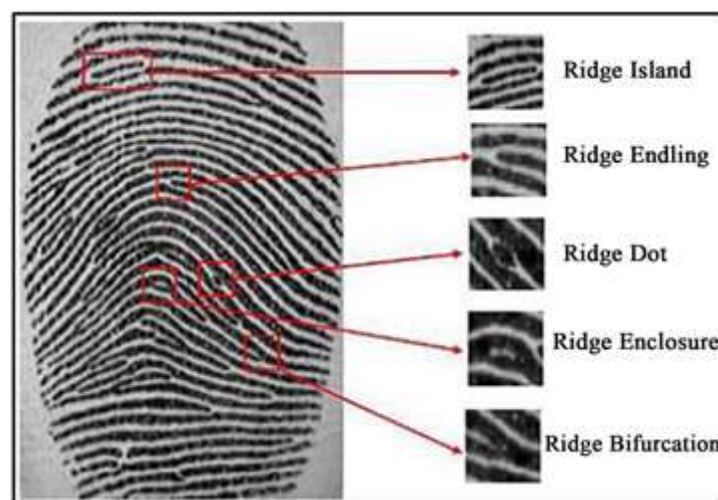


Figure 3. Different types of ridge orientation

If the ridges are perfectly identified in the image, then minutiae extraction of the focal point on the image will be trivial. The quality of the fingerprint print image is very important at this stage because the performance of minutiae extracting algorithms depends heavily on the image quality (Cao and Wang, 2016).

Fig. 4 identifies minutiae points for ridge bifurcations and ridge endings using a 3 x 3 matrix formula. Once all minutiae points have been identified, the template for the corresponding image can be created. The factors determining how minutiae are identified include Location, which is the x and y of the minutiae point concerning the origin. Direction is often determined by its orientation type, which describes the shape and type of fingerprint. Curvature is the curvature of the ridge at that point (Socheat and Wang, 2020). It is very important to note that templates may vary in size, allowing all minutiae points to be included. During the enrollment phase of the biometric system, all these stages of fingerprint image enhancement and noise removal will play a significant role in identifying a valid user, improving the confidence level of the print, and preventing the occurrence of a false negative. There has been an upsurge in the development of attendance systems to cater to several sectors' requirements, including education. These systems include the basic components of attendance systems, such as collecting required data, means of identification, communication technology, and data storage patterns (Rivera, 2021; Jayakumar et al., 2023; Younis and Abdulkareem, 2020).



excel exportation. Improvements were suggested by using info-graphics to display attendance information and adding a feedback response system for students to check attendance rates. In a similar study with **(Mishra et al., 2020)**, a battery-powered device employed a fingerprint sensor, a micro-controller, an RFID module for extra security, and an SD card module to store attendance data. This offered an alternative form of data storage and multi-factor authentication. The authors proposed designing a case to make the system more compact and protect its hardware components as an improvement to their work. This research aims to develop and implement a compact electronic and web-based fingerprint attendance system for students and lecturers that will improve student attendance performance and work performance for lecturers. This work also strives to improve the accuracy of attendance and eliminate proxy signing. Using a fingerprint, students can easily be authenticated and identified, enabling the institution to save time on manual data entry and keep accurate records of student performance to analyze, draw insight, and identify.

2. METHODOLOGY

To build the authentication, identification, and logging (AIL) management system, the fingerprint scanner, among other devices, was used to record the identifier and assess its quality, an application to control scanner modes and measure stored data, and a database to store information for future comparison.

The components used are the NodeMCU ESP8266 micro-controller board, Fingerprint sensor (AS608), 0.96in OLED display module, 3.7 V TP4056 lithium-ion battery/ charging module, and the MT3608 voltage booster. The NodeMCU ESP8266 micro-controller is an IoT development board responsible for executing code and controlling other components. It acts as the management system's central processing unit and controls the fingerprint sensor and OLED display through its general-purpose input and output pins. It has a WiFi module which allows the board to communicate to servers over the Internet. It communicates with the database using its API endpoint to get data related to the website through a series of timed HTTP requests made continuously.

The microcontroller sends information to the OLED display (an energy-efficient display module that utilizes OLED technology to showcase information and graphics) to indicate instructions for enrollment and attendance. The AS608 fingerprint sensor is a compact optical biometric sensor that captures and analyzes fingerprint patterns. It acts as an input and storage device, stores the enrolled fingerprint in its database, and supports real-time verification with high accuracy. The microcontroller is powered by the power management circuit, which includes the 3.7 V battery, lithium-ion battery charger, and voltage booster. The charging module ensures the battery is charged within specified voltage limits to prevent overcharging and damage. Because the micro-controller needs to be powered within specified voltage limits, that is, 3.6 V to 6 V, a voltage booster with an adjustable voltage range (2 V to 28 V) has been used to step up the output voltage of the battery to 5 V which was sufficient to power the microcontroller. **Figs. 5 and 6** depict the block diagram and the bread-boarding of the management system.

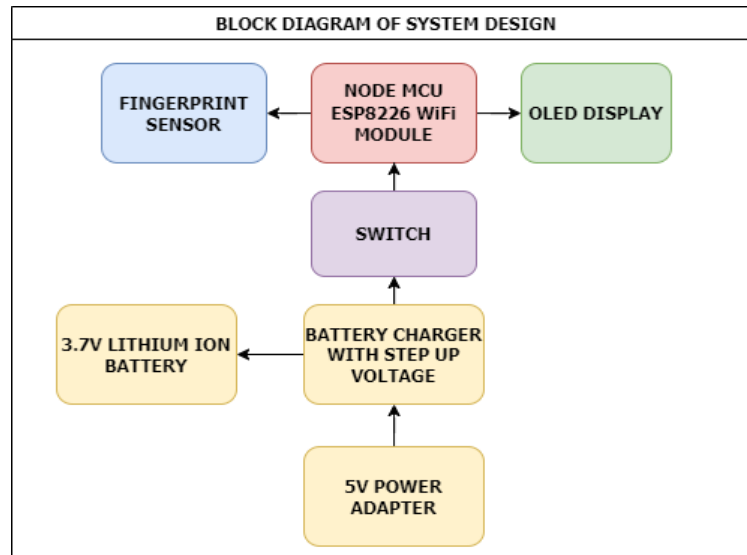


Figure 5. Block diagram of Fingerprint node

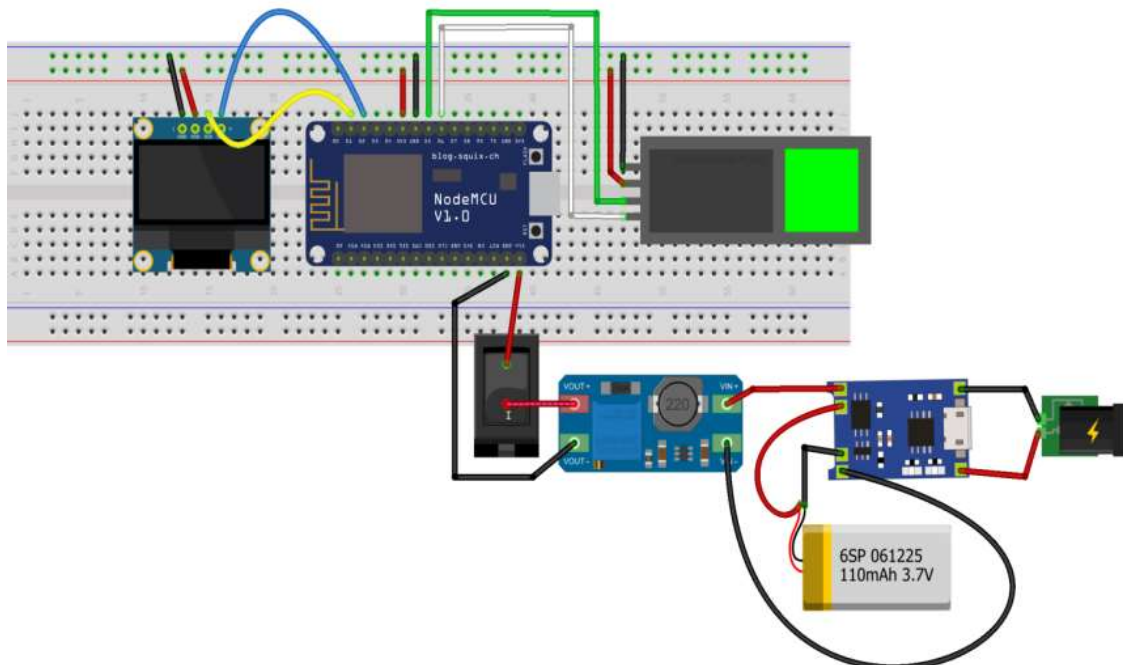


Figure 6. Fingerprint node design

The biometric attendance device is uniquely identified with an ID, which is used to request device-specific information from the website. With this ID, properties such as device mode flags for adding and deleting a user's fingerprint can be accessed and used in device operations. For enrollment mode, information on students such as name, email, matriculation number, and department could be collated beforehand to ensure detailed reports. Next, the mode of the device is to be set to enrollment mode to initiate scanning of the student's fingerprint. In the enrollment mode, the students' finger is scanned twice to ensure a higher confidence level, and a model is created for this fingerprint. This model is converted to a character file and stored in the fingerprint sensor's database. The sensor stores each fingerprint with an ID generated in code by the microcontroller. After the character file is stored in the database, the ID of the fingerprint is sent back to the website

via HTTP request. This ID is stored and used when recording student attendance, as depicted in **Fig. 7**. Fingerprints can also be updated for students scanned incorrectly. In this case, the microcontroller reuses the student's fingerprint ID to store a new fingerprint.

In attendance mode, the biometrics of the student are captured again, and the prints are compared with those stored in the database. If a reasonable confidence level match is found, the student's details and the time and the date the print was matched are stored on the attendance log. Also, in the case of a mismatch, they are given visual feedback to meet the admin and register. During attendance mode, the addition and deletion of fingerprints are not allowed to prevent conflicts in attendance. Fingerprints can only be deleted or added during enrollment mode. The software platform of this work is a website built and designed to efficiently and accurately manage student attendance in a classroom or educational setting. The software is designed to automate the process of recording and tracking student attendance, making it easier to manage student data and course scheduling. The website architecture has three parts: front-end design, back-end model, and front-end to back-end integration. For the front-end design of this website, several JavaScript libraries were used to create the view and interactivity of the website, the core being React.js. React.js is an open-source JavaScript library that allows developers to build interfaces using reusable UI components and update the data efficiently as it changes over time.

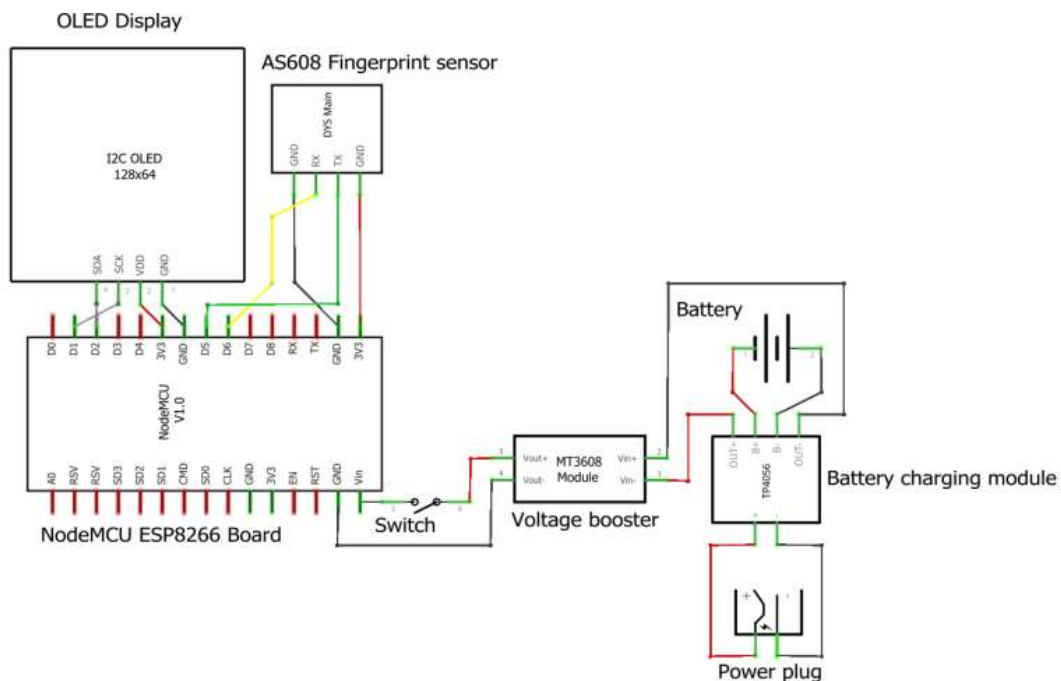


Figure 7. Fingerprint node schematic

React.js is based on the principle of component-based architecture is that the interface is broken down into small isolated components that are reused throughout the application. **Figs. 8 and 9** depict the components-based architecture of the website with React.js. With component-based architecture, each page can be easily broken down into smaller blocks of reusable components.

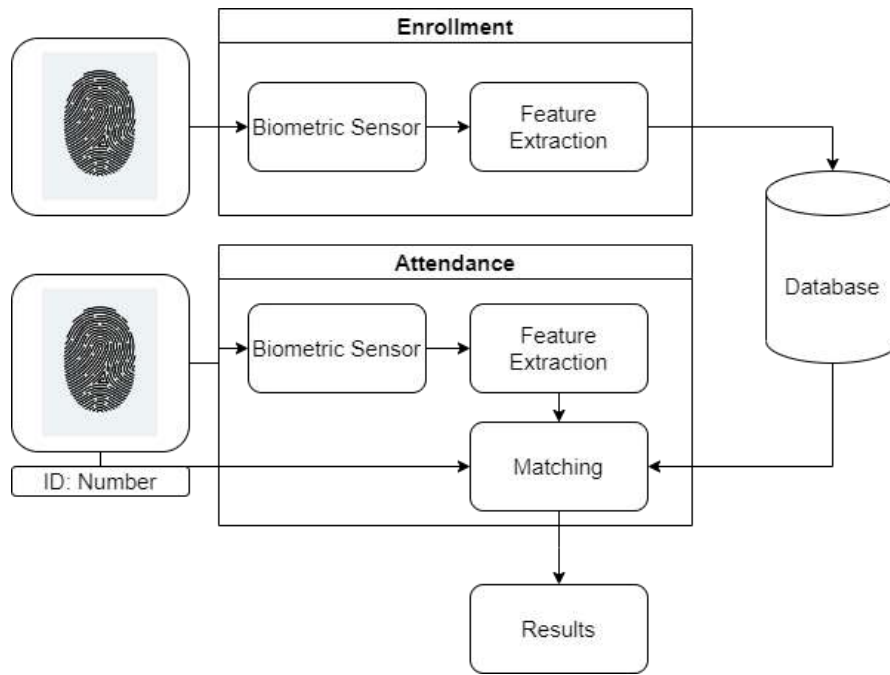


Figure 8. Workings of the device

```
<>
<Meta
  title="Manage System"
  desc="Manage Attendance, Devices, Courses, and Enrollments"
/>
<Layout>
  <Devices />
  <Courses />
  <Calendar />
</Layout>
</>
```

Figure 9. Code structure in React.js

Fig. 10 depicts the website layout, and the UI components used in this website are from a React UI library called Next-UI. The components offered by Next-UI include buttons, tables, form inputs, etc., as seen in Fig. 9, and these components come in customizable styles and adapt to different screen sizes. ApexCharts, another React library, was used for data visualizations and interpretations (charting). Finally, all these components and principles are tied together by a React framework called Next.js. It renders the components on the server and automatically handles routing due to its file-based routing functionality.

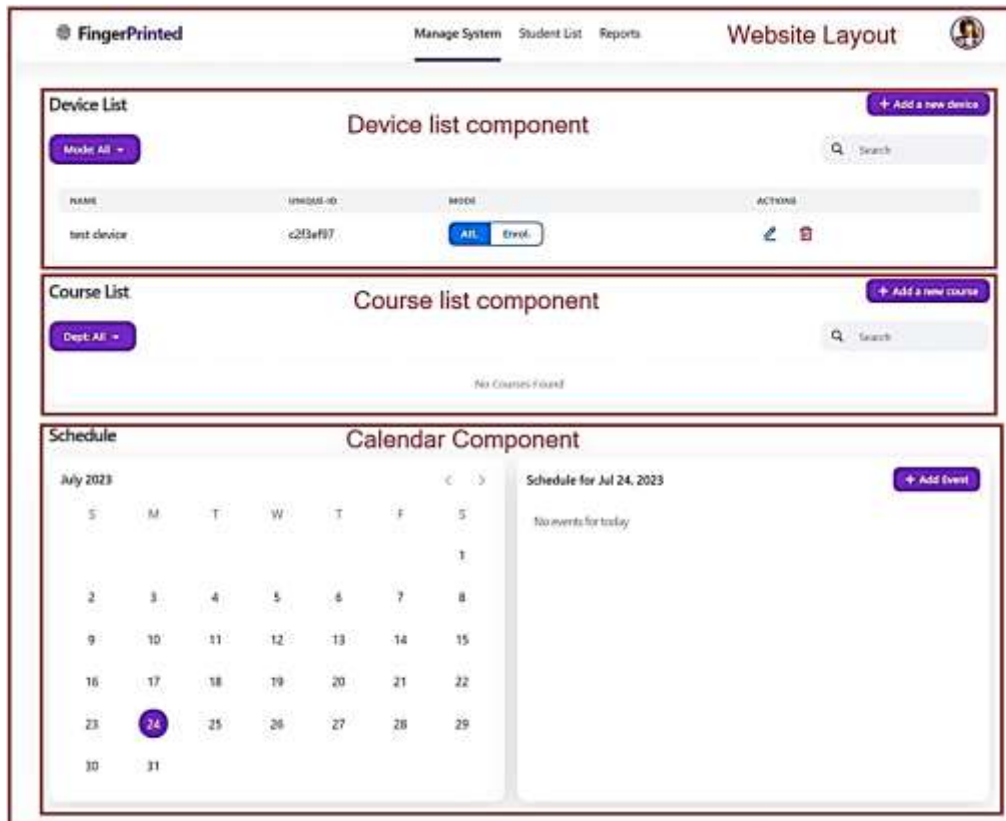


Figure 10. Manage System web page with each component highlighted

The back-end model is written in PHP (Hypertext Processor) and SQL (Structured Query Language). PHP is a scripting language that handles data processing and manipulation before sending it to the client (browser) or the database. PHP scripts are used in this website to perform actions such as adding, modifying, and deleting courses, students, events, and devices and retrieving attendance log information for the database. SQL is a programming language used within PHP script to query and manipulate information from the database. It is used to create, read, update, and delete data from the database and manipulate data on database tables. The database is the mode of storage primarily used in this project. The database created was compatible with SQL, allowing easy access to stored information. The database contains interrelated tables with information such as students' details, courses, devices, attendance logs, events, and other important information. **Fig. 11** shows the entity relationship diagram for the database tables used for the fingerprinted website with connectors indicating where the tables are linked.

The website was divided into three pages: Manage System, Student List, and Report. The Manage System consists of three parts: the Device list, where the device's status is managed. The course list where courses taken by students can be added and managed and the Schedule where lectures could be attended one-time or weekly for attendance purposes. In the Student List the student's information can be managed and updated occasionally. The fingerprint enrollment can also be initiated on this page, while in the Report, attendance reports are displayed and generated by date and course. It also displays recent attendances, and generated reports are downloaded in excel format. **Fig. 12** depicts the web application architecture for which the interface between the front-end and back-end has been detailed.

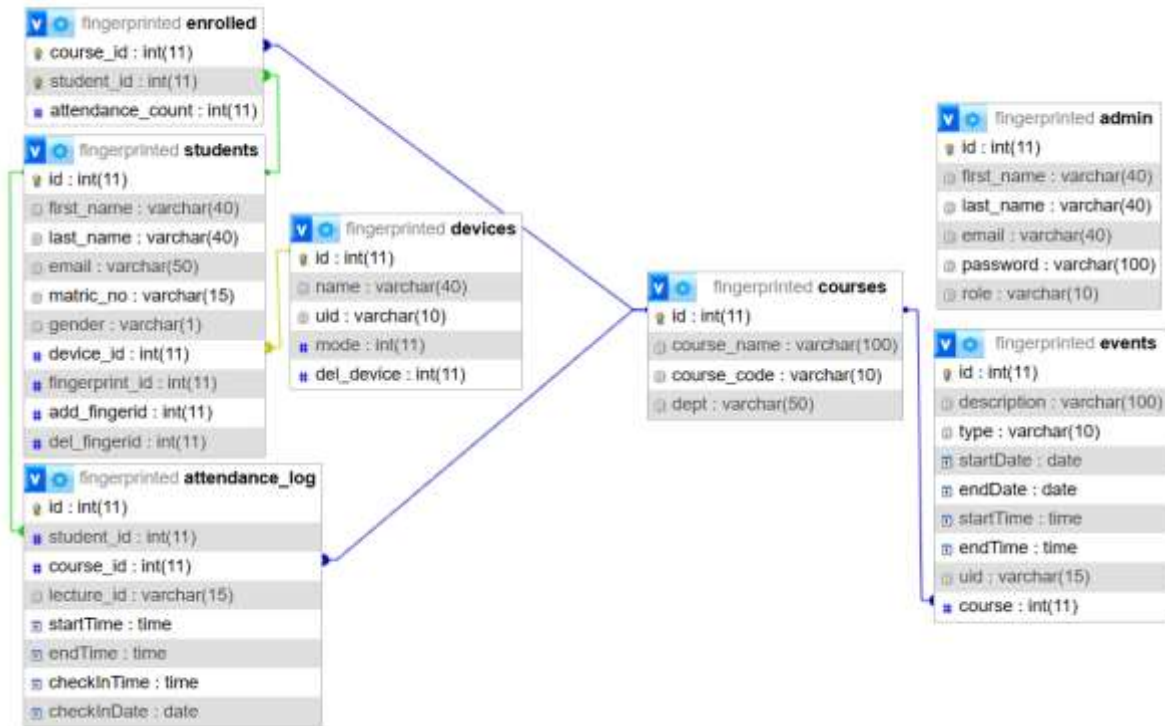


Figure 11. Entity relationship diagram for the fingerprinted database

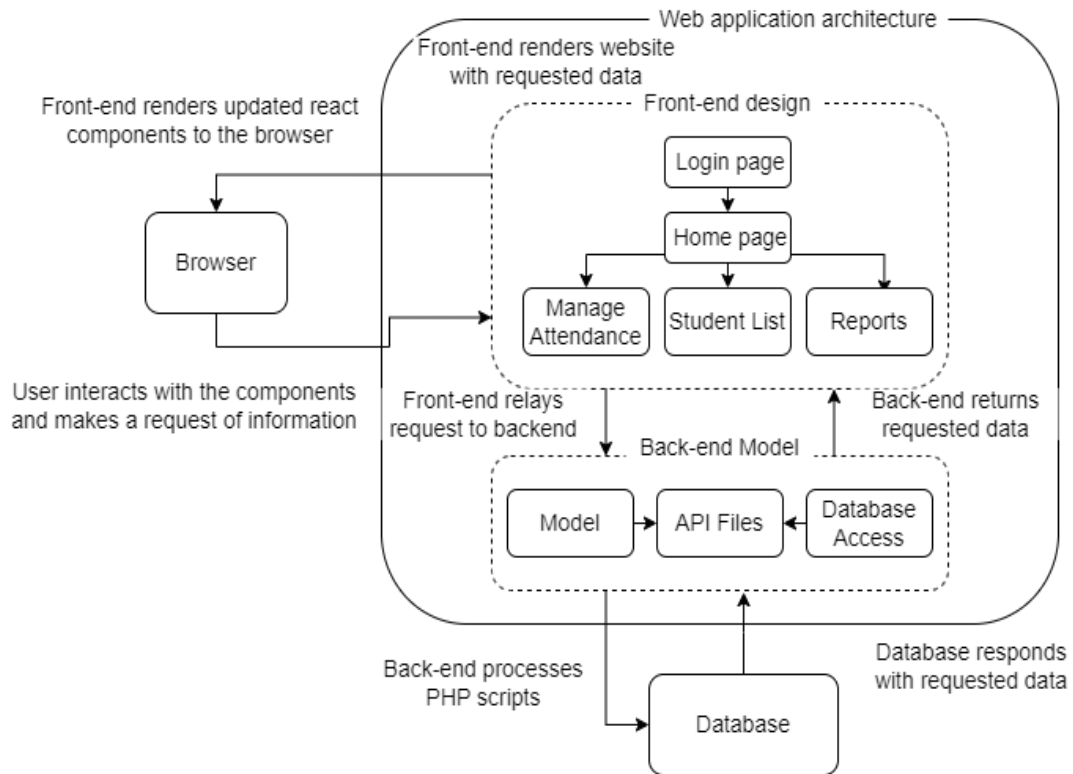


Figure 12. Web application architecture

The back-end model and front-end design are connected using API calls to receive and send data between API endpoints, which are routes on a web server/back-end designed to handle

incoming requests and provide access to database data, as shown in **Fig. 13**. In the front end, a fetch API command makes API calls to the defined endpoints on the back end. The back-end model locates the endpoint file in its server, processes the script, retrieves the required data, and sends a response back to the back end. This process, described as the request-response cycle, integrates the front-end and back-end of the website.

Knowing that two different servers render the front-end design and the back-end model is important. The front-end server is rendered by a server that supports Next.js/React.js applications (Vercel), while the back-end model is hosted by a web server that supports PHP scripts and SQL databases (000webhost). The front-end server communicates with the back-end server to send and receive information from the database.

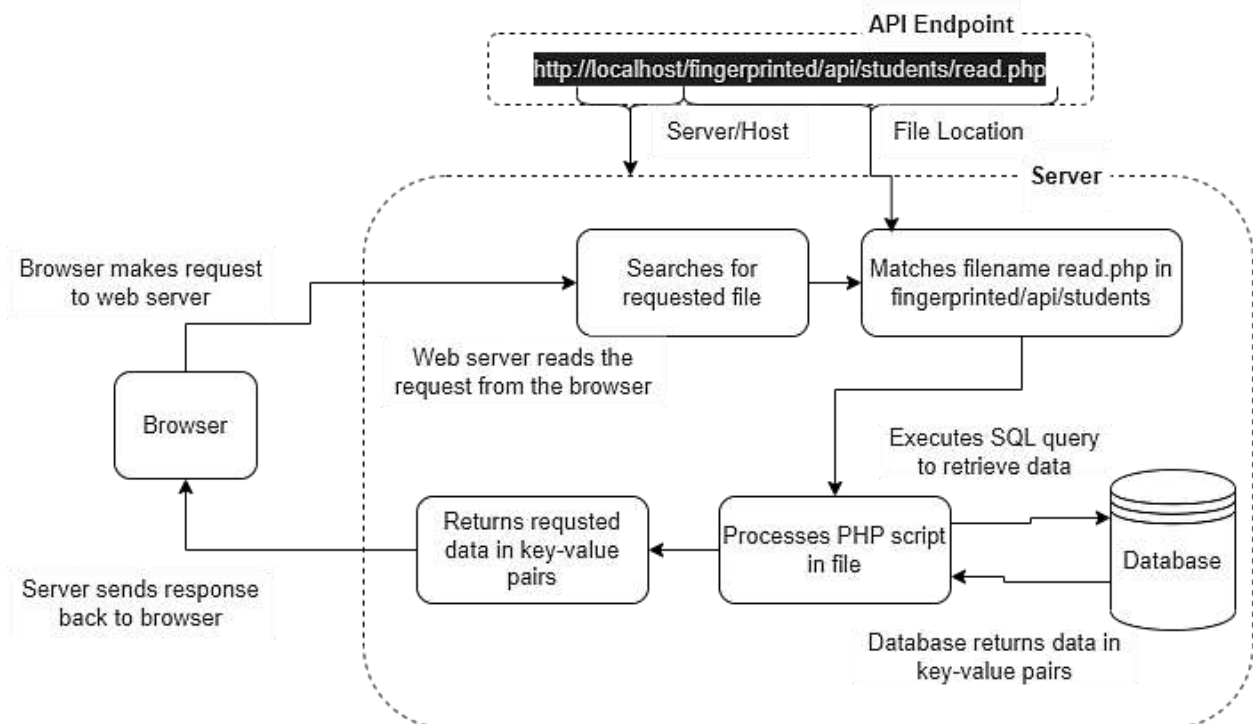


Figure 13. The front-end to back-end integration (also known as request-response cycle)

3. RESULTS AND DISCUSSION

The AIL management system was tested in all instances, from enrollment of students to attendance logging to deletion of existing fingerprints, among others. The AIL device can work in two forms. One way is to load the website and use a local database server connected to the same network as the device. This is faster regarding response time, and data is loaded and reloaded to the website efficiently. The downside, however, is that if the device or the computer is disconnected, data will not be recorded to the local database, defeating the purpose. The other alternative was to host the website online (using Vercel for the front-end and 000webhost for the back-end), making it readily available anytime, anywhere, as long as the device is connected to the Internet. This method was tested on mobile phones and computers, as shown in **Fig. 14** and **Figs. 22 to 29**. The downside of this method is that the device speed of performance at requesting information depends on the speed of the communication network.

Compared with existing attendance systems, this work proposes an enhanced attendance system that authenticates, identifies, and logs students' attendance, provides students with



feedback, and manages the scheduled courses to enable decision-making to improve students' performance. Also, an online real-time attendance management system coupled with course scheduling to enable efficient curriculum delivery has been proposed, where the front-end and back-end integration of the attendance/ course management system was deployed using the React framework coupled with the PHP and SQL implementation. Further to the software deployment in this research work, the hardware was integrated using embedded technology, where an ESP8266 NodeMCU microcontroller was utilized to eliminate the separate microcontroller and Wi-Fi/GSM shield in prior designs, thereby enabling a more compact design and easy-to-manage electronic integration.

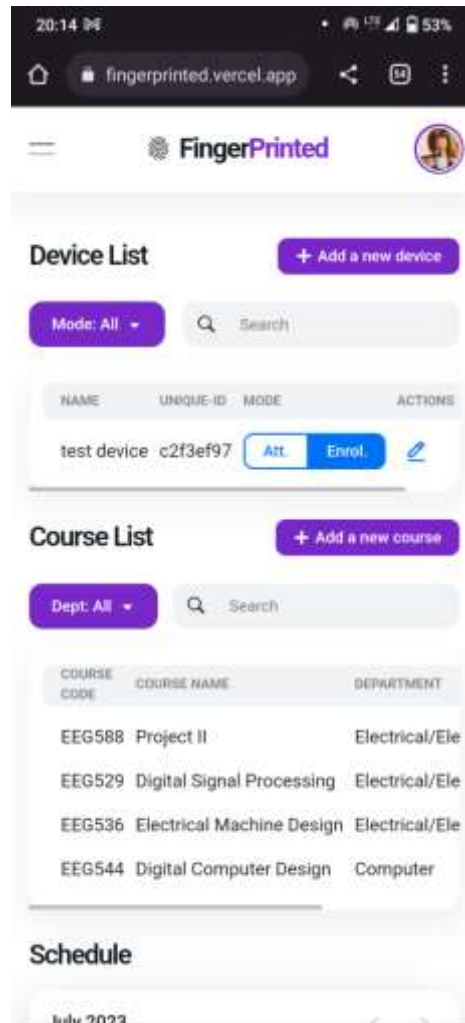


Figure 14. Mobile phone test of website

The main purpose of the AIL device is to be able to enrol and identify students' fingerprints, as shown in Figs. 16 and 17. Therefore, observing the behavior behind the mode changes is key. As described in the flowchart of Fig. 18, the enrollment mode involves more than adding new students. It also includes deleting student ID when they are not used anymore. This makes the switch to enrollment a little slower than the switch to attendance.



Figure 15. Device attempting connection to the Wi-Fi



Figure 16. Device indicating mode change to attendance



Figure 17. Device indicating mode change to enrollment

Here, the addition and deletion of fingerprints were carried out. As described in the methodology, adding a new fingerprint includes scanning the fingerprint placed on the sensor twice to obtain a good confidence level of the fingerprint. The fingerprint ID of the new user is also sent back to the database for storage and future identification, as shown in **Fig. 19**. The deletion of fingerprints is carried out on the website's interface, deleting the students' data and the fingerprint stored by the fingerprint sensor, as depicted in **Fig. 20**.

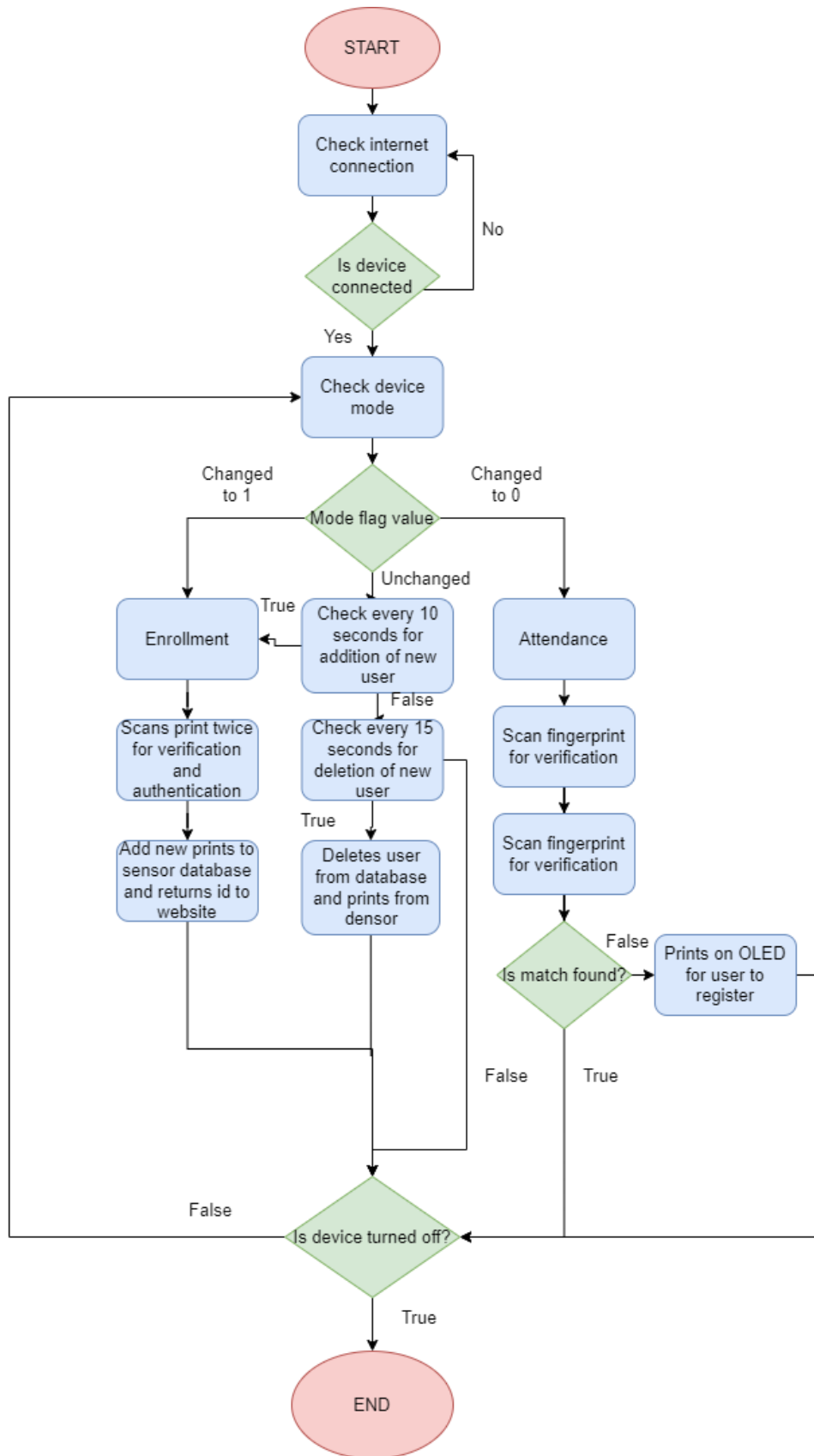


Figure 18. Flowchart of the workings of the attendance device



Figure 19. Device indicating and executing the addition of fingerprints



Figure 20. Device indicating and executing the deletion of fingerprints

In this aspect of the device's design, attendance management and similar scenarios surrounding attendance tracking were tested. When switched to the attendance mode, if a person places their fingerprint on the scanner, it is scanned, and the sensor searches for a match with high confidence. If a match is not found, the device prints a fingerprint is not enrolled message, as shown in **Fig. 21**. If a match is found, the device checks if an event or lecture is ongoing. If there is, the device checks if the student is enrolled in the course. If enrolled, attendance is taken for the student, and if not enrolled for the course, the device indicates that message. If no lecture is ongoing, the device will also show.

Since the research project is based on an AIL system modeled for classroom usage, it has been divided into two core parts: designing and testing the web application/software and constructing the hardware. **Fig. 22** depicts the app design interface for the AIL tracking. The image features a table of devices, showing details such as device name, ID, device mode, and action buttons (delete and edit). This allows users to add new devices by providing a name and generates a unique hexadecimal ID for the device to request information. This application can use multiple devices, as each would be identified with an ID. Users can also modify device modes for attendance or enrollment, edit device names, or delete device databases.



Figure 21. Device indicating that the student is not enrolled for the course.

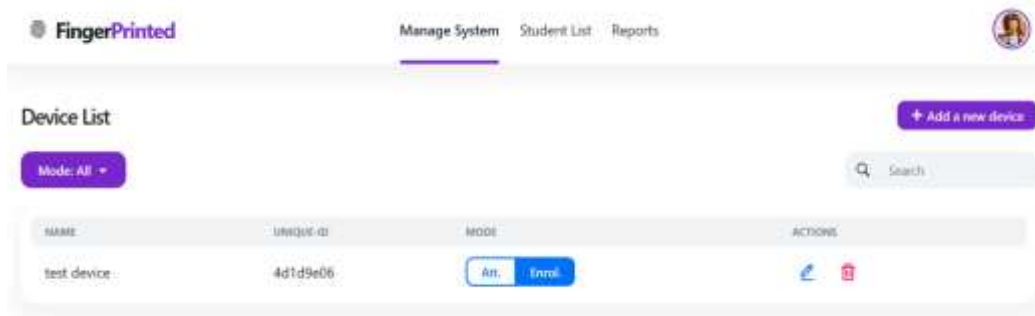


Figure 22. Screenshot of device list on Computer

Fig. 23 shows the management of the course interface. Here, courses the students are taking can be added to the database by course code, course name, and department. They can also be updated and deleted. Deleting a course would also delete all schedules related to it.



Figure 23. Screenshot of course list on PC

Using this calendar in the interface depicted in Fig. 24, the administrator can add events to manage scheduling, such as lectures, which could be weekly or one-time (for impromptu and extra lectures). These events could be associated with a course or not. If associated with a course, the attendance system would log attendance associated with the lecture within the time limit (mode has to be set to attendance). These events can be updated or deleted.

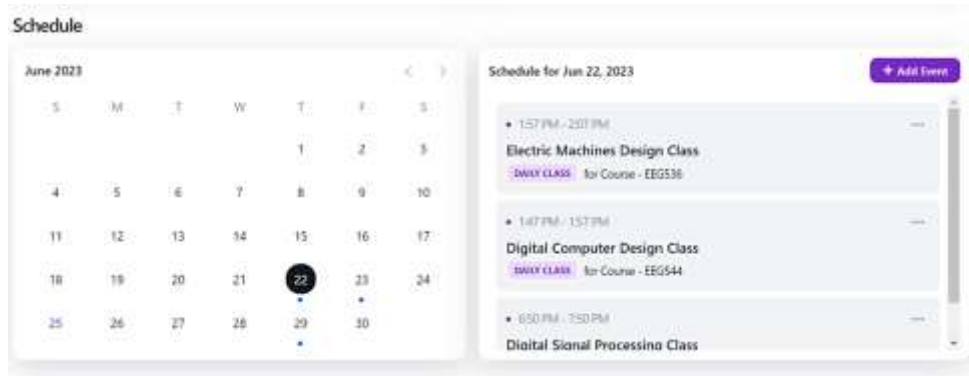


Figure 24. Screenshot of calendar schedule on PC

The enrollment phase involves the registration of students. The student’s name, email, matriculation number, gender, and other criteria, such as the device used, are added in this section, which could be used later in the enrollment phase of the system.

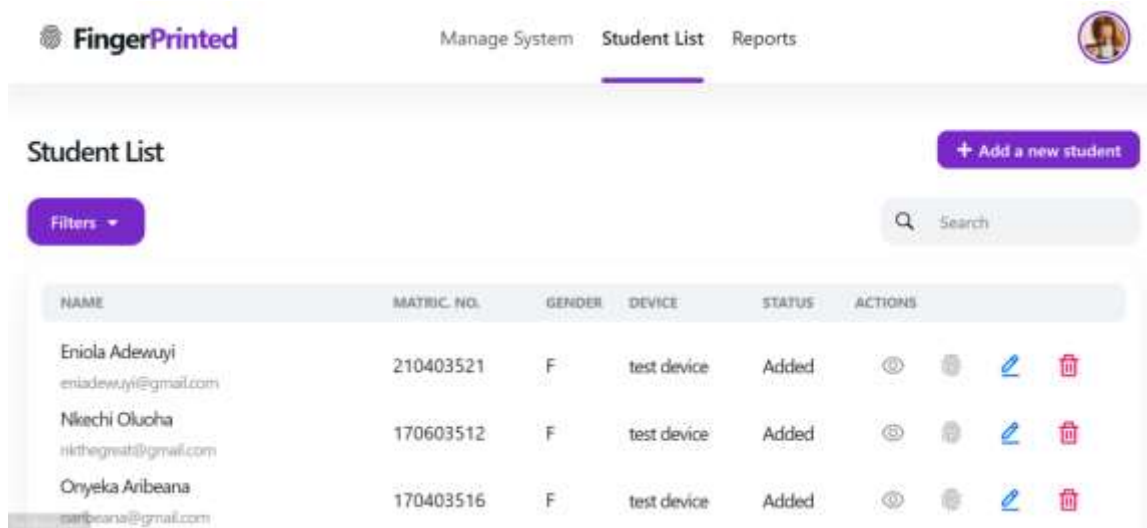


Figure 25. Screenshot of student list on PC

Fig. 25 provides the students list on the application. This table contains the collated information and other information, such as the status of fingerprint addition. Action buttons are also responsible for initiating enrollment and updating and deleting students’ information. Individual students could be scanned using their name, email, or matriculation number at the search bar. The attendance phase shown in Fig. 26 involves the logging of check in times of the students. By placing their finger on the sensor, the sensor retrieves the fingerprint ID from its database when a match is found and then sends it to the server. The server then uses the fingerprint ID to pull information from the student list and adds the data obtained to the attendance log along with the check-in time and date. On average, it takes five seconds to scan a student’s fingerprint and nine seconds if the first scan is processed incorrectly.



Figure 26. Screenshot of attendance report of the day on PC

Reports can also be generated and downloaded in excel format by course, date, and attendance rate. Figs. 27 and 28 depict the data visualization tools, such as a line chart and a bar chart, which would graphically represent attendance data and show data representations on different levels.

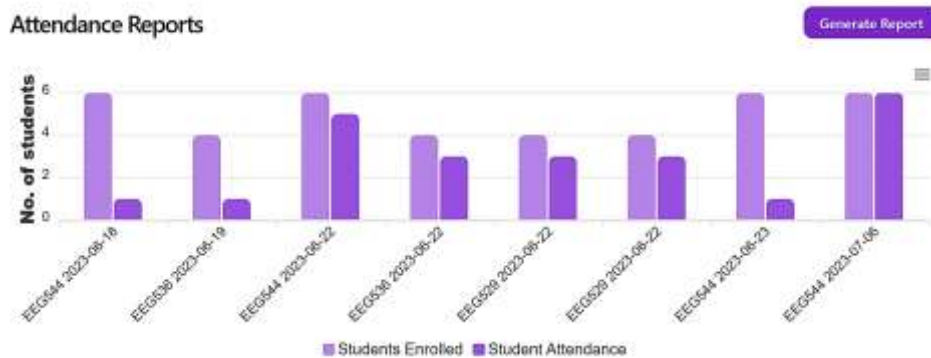


Figure 27. Screenshot of a bar chart showing the relationship between students enrolled and students attending

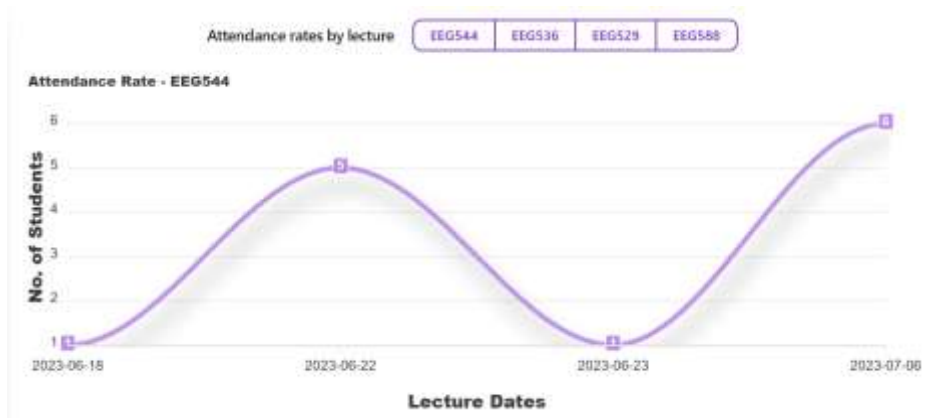


Figure 28. Screenshot of line chart describing the number of student attendees per lecture

Student attendance rates for all courses can also be generated and used for decision-making, such as filtering out the students who made the attendance requirement for the course for tests, exams, labs, and other mandatory functions. Students can check their biodata and enrolled courses using their matric no. All they need to do is go to the URL link/matric no.



and append their matric no, which displays all their information, even the courses they are enrolled in and their attendance rates, as shown in **Fig. 29**.

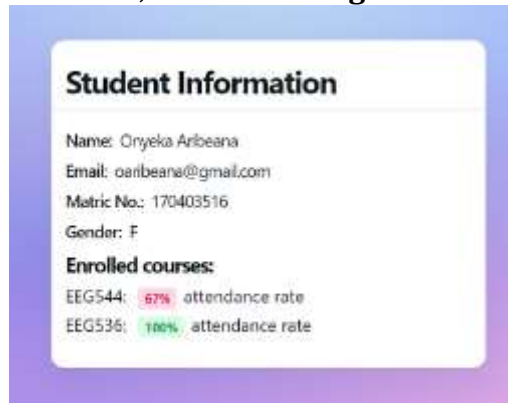


Figure 29. Screenshot displaying student information

4. CONCLUSIONS

The method of validating users using biometrics assists greatly in personal identification, authentication, and protection against impostors. The proposed system utilizes this validation method and aims to prove that fingerprint biometry is a worthwhile form of identification and will drastically improve the way attendance is taken in schools and other applicable areas of life where a person's presence needs to be accountable. The method employed in this system ensures real-time verification of students and utilizes an easy-to-use web application with secure data handling, automated reporting, and record keeping, and creates opportunities for easy access with mobile compatibility, all done with energy-saving and cost-efficient components. Implementing this technique would support organizations or institutions in managing attendance data and ensure timely computation of attendance rates so that improvements can be made in class settings and workspaces based on the deductions made. This, in turn, will improve the attendance rates and overall productivity of the users in any organization or institution.

One of the observed limitations of this proposed design is that the device relies heavily on Internet connectivity. Thus, the device could not operate perfectly in areas without connectivity. The device experienced delays when making requests to the network and occasional inaccuracies when matching fingerprints, possibly reducing its efficiency. An alternative identification mode, such as facial recognition, could be included in future work to make the attendance system more diverse. Machine learning algorithms such as fingerprint segmentation and feature selection can also be included to train fingerprints multimodal biometric techniques to improve their accuracy for a more efficient system.

REFERENCES

- Abbood, A.A., Sulong, G., and Peters, S.U., 2014. A review of fingerprint image pre-processing. *Journal Teknologi*, 69(2), pp. 79–84. [Doi:10.11113/jt.v69.3111](https://doi.org/10.11113/jt.v69.3111).
- Ajiroghene, O.S., Ekoko, E.C., Abuh, A., Ibhaze, A.E., and Orukpe, P.E., 2020. A dual channel home automation and security system using finite state machine. *Journal of Computer Science and Control Systems*, 13(2), pp. 5–10.



Alexander, G., 2021. What is biometrics?
<https://www.techtarget.com/searchsecurity/definition/biometrics>.

Amor, B.Y., Dowden, J., Borh, J.K., Castro, E., and Goel, N., 2020. The chronic absenteeism assessment project: Using biometrics to evaluate the magnitude of and reasons for chronic absenteeism in rural India. *International Journal of Educational Development*, 72, P. 102140. [Doi:10.1016/j.ijedudev.2019.102140](https://doi.org/10.1016/j.ijedudev.2019.102140)

BalaMurali, A., Sravanthi, P.S., and Rupa, B., 2020. Smart and secure voting machine using biometrics. In *2020 Fourth International Conference on Inventive Systems and Control (ICISC)* (pp. 127-132). IEEE. [Doi:10.1109/ICISC47916.2020.9171135](https://doi.org/10.1109/ICISC47916.2020.9171135)

Benyo, B., Sodor, B., Doktor, T., and Fördös, G., 2012. Student attendance monitoring at the university using NFC. In *Wireless Telecommunications Symposium, April 2012* (pp. 1-5). IEEE. [Doi:10.1109/WTS.2012.6266137](https://doi.org/10.1109/WTS.2012.6266137)

Cao L., and Wang, Y., 2016. *Fingerprint image enhancement and minutiae extraction algorithm*. MSc. Thesis at Linnaeus University Sweden. <https://www.diva-portal.org/smash/get/diva2:1105720/FULLTEXT01.pdf>.

Chennattu, S., Kelkar, A., Anthony, A., and Nagdeote, S., 2019. Portable biometric attendance system using IoT. In *2019 4th International Conference on Information Systems and Computer Networks (ISCON)*, November, (pp. 245-249). IEEE. [Doi:10.1109/ISCON47742.2019.9036275](https://doi.org/10.1109/ISCON47742.2019.9036275)

Dastidar, U.G., Jogi, N., Bansod, M., Madamwar, P., and Jalan, P., 2017. Fingerprint sensor based attendance system using atmega 328 and ESP8266. *International Journal of Research in Science & Engineering*, 3(2), pp. 471-475.

Esttaifan, B.A., 2023. A modified Vigenère Cipher based on time and Biometrics features. *Journal of Engineering*, 29(6), pp. 128–139. [Doi:10.31026/j.eng.2023.06.10](https://doi.org/10.31026/j.eng.2023.06.10)

Fadhil, H.M., Younis, M.I., Alsewari, A.A., Abd-Alrazzaq, M., Mahdi, A.T., and Alomoush, A.A., 2020. An open cloud-based platform for the creation and delivery of smart applications and services. The 6th International Conference on Software Engineering & Computer Systems, pp. 1–13. [Doi:10.1088/1757-899X/769/1/012067](https://doi.org/10.1088/1757-899X/769/1/012067)

Galbally, J., Alonso-Fernandez, F., Fierrez, J., Ortega-Garcia, J., 2012. A high performance fingerprint liveness detection method based on quality related features. *Future Generation Computer Systems*. 28, pp. 311–321. [Doi:10.1016/j.future.2010.11.024](https://doi.org/10.1016/j.future.2010.11.024)

Ibhaze, A.E., Akpabio, M.U., and Atayero, A.A.A., 2018. Smart meter solution for developing and emerging economies. *International Journal of Automation and Smart Technology*, 8(3), pp. 119 – 126. [Doi:10.5875/ausmt.v8i3.1529](https://doi.org/10.5875/ausmt.v8i3.1529)

Ibhaze, A.E., Eleanor, E.C., and Idachaba, F.E., 2016. E-health monitoring system for the aged. IEEE International Conference on Emerging Technologies and Innovative Business Practices for the Transformation of Societies (EmergiTech). [Doi: 10.1109/EmergiTech.2016.7737355](https://doi.org/10.1109/EmergiTech.2016.7737355)

Ibhaze, A.E., Okakwu, I.K., Akinrelere, A.T., and Imoize A.L., 2019. An intelligent dispatch system operating in a partially closed environment. *Network and Communication Technologies*, 4(1), pp. 26 – 35. [Doi:10.5539/nct.v4n1p26](https://doi.org/10.5539/nct.v4n1p26)

Ibhaze, A.E., Orukpe, P.E., and Edeko, F.O., 2020. High capacity data rate system: review of visible light communications technology. *Journal of Electronic Science and Technology*, 18(3), P. 100055. [Doi:10.1016/j.jnlest.2020.100055](https://doi.org/10.1016/j.jnlest.2020.100055)



Idachaba, F.E., and Ibhaze, A.E., 2016. Development of a real time road accident location and emergency alert system. *International Journal of Applied Engineering Research*, 11(23), pp. 11110 – 11113.

Idachaba, F.E., Olowoleni, J.O., Ibhaze A.E., and Oni, O.O., 2017. IoT enabled real-time fishpond management system. *Proceedings of the World Congress on Engineering and Computer Science*, 1, pp. 1 – 5.

Jayakumar, K., Surendar, V., Sheela, a., Javagar, P., Riyas, K., and Dhanush, K., 2022. Internet of Things based Biometric smart attendance system. *International Conference on Sustainable Computing and Data Communication Systems*. pp. 1492-1497. [Doi:10.1109/ICSCDS53736.2022.9761045](https://doi.org/10.1109/ICSCDS53736.2022.9761045)

Joodi, M.A., Saleh, M.H., and Kadhim, D.J., 2023. Proposed face detection classification model based on Amazon Web Services cloud (AWS). *Journal of Engineering*, 29(4), pp. 176 – 206. [Doi:10.31026/j.eng.2023.04.12](https://doi.org/10.31026/j.eng.2023.04.12)

Keerthi, Y., Sneha, A., Manasa, P.V. and Neelima, N., 2022. Enhanced Biometric Attendance Management System using IoT & Cloud. In *2022 International Conference on Electronics and Renewable Systems (ICEARS)*, March, (pp. 1-7). IEEE. [Doi:10.1109/ICEARS53579.2022.9751960](https://doi.org/10.1109/ICEARS53579.2022.9751960)

Kizza, J.M., 2023. Biometric technologies and ethics. In *Ethical and Social Issues in the Information Age*. (pp. 365-378). Cham: Springer International Publishing. [Doi:10.1007/978-3-031-24863-4_19](https://doi.org/10.1007/978-3-031-24863-4_19)

Lin, H., Jain, A.K., Pankanti, S., and Bolle, R., 1997. An identity-authentication system using fingerprints. *Proceedings of the IEEE*, 85(9), pp. 1365 – 1388. [Doi:10.1109/5.628674](https://doi.org/10.1109/5.628674).

Mahmood, B.M.R., Younis, M.I., and Ali, H.M., 2013. Construction of a general-purpose infrastructure for Rfid – Based applications. *Journal of Engineering*, 11(19), pp. 1425-1442. [Doi:10.31026/j.eng.2013.11.06](https://doi.org/10.31026/j.eng.2013.11.06)

Miguel, G., 2018. How Fingerprint Scanners Work: Optical vs Capacitive Scanners. <https://www.arrow.com/en/research-and-events/articles/how-fingerprint-sensors-work>.

Mishra, A., Kamble, R., Pare, V., and Sahu, R., 2020. Multimodal Biometric Attendance System. In *Proceedings of the International Conference on Innovative Computing & Communications (ICICC)*, April 2020. [Doi:10.2139/ssrn.3568531](https://doi.org/10.2139/ssrn.3568531)

Mohamed, B.K., and Raghu, C.V., 2012. Fingerprint attendance system for classroom needs. In *2012 Annual IEEE India Conference (INDICON)*, December, (pp. 433-438). IEEE. [Doi:10.1109/INDCON.2012.6420657](https://doi.org/10.1109/INDCON.2012.6420657)

Mohammed, A., Mohammed, A., Mohammed, O., and Amin, E., 2015. Fingerprint attendance system for educational institutes. *Journal of Science and Technology*, 20(1), pp. 34-44. [Doi:10.20428/JST.20.1.4](https://doi.org/10.20428/JST.20.1.4)

OKTA, 2023. Fingerprint Biometrics: Definition & how secure It Is. <https://www.okta.com/identity101/fingerprint-biometrics-definition-how-secure-it-is/>.

Peralta, D., Galar, M., Triguero, I., Miguel-Hurtado, O., Benitez, J.M. and Herrera, F., 2014. Minutiae filtering to improve both efficacy and efficiency of fingerprint matching algorithms. *Engineering Applications of Artificial Intelligence*, 32, pp. 37-53. [Doi:10.1016/j.engappai.2014.02.016](https://doi.org/10.1016/j.engappai.2014.02.016).

Rahman, S.M., Rumman K.M., Ahmmed R., and Rahman A., 2023. Fingerprint Based Biometric Attendance System. *European Chemical Bulletin*, 12(S3), pp. 184-190. [Doi:10.31838/ecb/2023.12.s3.026](https://doi.org/10.31838/ecb/2023.12.s3.026)



- Rivera, R.B., 2021. Enhanced attendance monitoring system using biometric fingerprint recognition. *International Journal of Recent Technology and Engineering*, 9(5), pp. 1-4. [Doi:10.35940/ijrte.E5070.019521](https://doi.org/10.35940/ijrte.E5070.019521)
- Seelam, V., kumar Penugonda, A., Kalyan, B.P., Priya, M.B., and Prakash, M.D., 2021. Smart attendance using deep learning and computer vision. *Materials Today: Proceedings*, 46, pp. 4091-4094. [Doi:10.1016/j.matpr.2021.02.625](https://doi.org/10.1016/j.matpr.2021.02.625)
- Socheat, S., and Wang, T., 2020. Fingerprint Enhancement, Minutiae Extraction and Matching Techniques. *Journal of Computer and Communications*, 8(5), pp. 55-74. [Doi:10.4236/jcc.2020.85003](https://doi.org/10.4236/jcc.2020.85003).
- Thales, G., 2021. Biometrics in 2020 (A helpful illustrated overview). <https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics>.
- Yongqiang, Z., and Ji, L., 2006. The design of wireless fingerprint attendance system. *International Conference on Communication Technology*. [Doi:10.1109/ICCT.2006.341990](https://doi.org/10.1109/ICCT.2006.341990)
- Younis, M.I., Abdulkareem, H.F., and Ali, H.M., 2015. Construction of graduation certificate issuing system based on digital signature technique. *Journal of Engineering*, 6(21), pp. 15–36. [Doi:10.31026/j.eng.2015.06.02](https://doi.org/10.31026/j.eng.2015.06.02)
- Younis, M.I., and Abdulkareem, M., 2020. Pilgrim tracking and monitoring based on IoT. *Journal of Physics: Conference Series*, 1530(1), P. 012015. [Doi:10.1088/1742-6596/1530/1/012015](https://doi.org/10.1088/1742-6596/1530/1/012015)
- Younis, M.I., and Hussein, T.F., 2018. Design and implementation of a contactless smart house network system. *International Journal of Electrical and Computer Engineering (IJECE)*, 8(6), pp. 4663-4672. [Doi:10.11591/ijece.v8i6.pp4663-4672](https://doi.org/10.11591/ijece.v8i6.pp4663-4672)
- Younis M.I., and Muhammad R.S., 2018. IFRS: An indexed face recognition system based on face recognition and RFID technologies. *Wireless Personal Communications*, 101, pp. 1939–1966. [Doi:10.1007/s11277-018-5800-8](https://doi.org/10.1007/s11277-018-5800-8)
- Younis, M.I., and Alwan, A.H., 2021. Design and implementation of an IoT-based transactional system for quality management. *Iraqi Journal of Science*, pp. 658-675. [Doi:10.24996/ijcs.2021.62.2.30](https://doi.org/10.24996/ijcs.2021.62.2.30)
- Younis, M.I., 2014. Design and implementation of ICT-based recycle-rewarding system for green environment. *Journal of Engineering*, 20(7), pp. 36-47. [Doi:10.31026/j.eng.2014.07.03](https://doi.org/10.31026/j.eng.2014.07.03)
- Younis, M.I., Al-Tameemi, Z.F.A., Ismail, W., and Zamli, K.Z., 2013. Design and implementation of a scalable RFID-based attendance system with an intelligent scheduling technique. *Wireless personal communications*, 71, pp. 2161-2179. [Doi:10.1007/s11277-012-0929-3](https://doi.org/10.1007/s11277-012-0929-3)
- Yuan, C., Zhang, Q., Wu, S., and Wu, J. Q., 2023. Chapter Four-A real-time fingerprint liveness detection method for fingerprint authentication systems. *Advances of Computers*, 131, pp. 149-180. [Doi:10.1016/bs.adcom.2023.04.004](https://doi.org/10.1016/bs.adcom.2023.04.004)