APPLIED INFORMATION TECHNOLOGY AND COMPUTER SCIENCE
e-ISSN: 2773-5141

AITCS

Vol. 6 No. 1 (2025) 415-433
https://publisher.uthm.edu.my/periodicals/index.php/aitcs

Go2Work: A Staff Attendance System using QR Code with CAOQTP Algorithm for Pejabat Pendidikan Hulu Langat

Muhammad Nafies Riza[1], Nor bakiah Abd Warif[1]*

[1] *Fakulti Sains Komputer dan Teknologi Maklumat,*
Universiti Tun Hussein Onn Malaysia, Parit Raja, Batu Pahat, 86400, MALAYSIA

*Corresponding Author: norbakiah@uthm.edu.my
DOI: https://doi.org/10.30880/aitcs.2025.06.01.023

Article Info

Received: 27 July 2024
Accepted: 18 June 2025
Available online: 30 June 2025

Keywords

Attendance, QR code, CAOQTP algorithm.

Abstract

Nowadays, attendance systems play a pivotal role in diverse sectors, ranging from educational institutions to corporate settings. The evolution of these systems has witnessed a shift from traditional manual methods to more advanced and technology-driven solutions. The creation of GO2WORK, a sophisticated staff attendance system that makes use of QR codes and the CAOQTP algorithm, is the project's primary goal. To solve the problem that OTP randomly generated characters that can be predicted by bots, CAOQTP adds an extra layer of security by adding CAPTCHA images that user must rearrange according to the received OTP. Additionally, to solve the problem of attendance fraud, the QR code can only be generated at designated kiosk. Moreover, user must scan the QR code within the range of the kiosk. Hence, preventing user from taking attendance outside the range of the workplace area. Furthermore, the project moves through steps including requirement gathering, quick design, building a prototype, user evaluation, refining the prototype, implementation, and maintenance using the prototyping model. GO2WORK is designed specifically to be used in educational institutions and organizational contexts, with the goal of transforming attendance tracking. A user-friendly, safe, and effective system with real-time monitoring capabilities is what's anticipated, offering improved security, accuracy, and administrative effectiveness. A revolutionary step towards modernizing attendance management procedures is GO2WORK. The system includes modules for login, registration, attendance, QR code generation, reporting, profile management, and logs. Each module has been thoroughly tested: login processes, including first-time and new device logins, passed successfully; registration functions were validated for all user roles; QR code generation and scanning were effective within the designated range; attendance logging was accurate; and reporting features met user needs.

1. Introduction

The rapid advancement of technology makes Pejabat Pendidikan Daerah Hulu Langat an ideal target for this project. The reason is the use of an old-school method for the attendance system, which is punched cards.

Punched cards are outdated technology that requires a manual process for data entry and are prone to physical damage, leading to loss or misplacement. Furthermore, this problem leads to unauthorized access and potential breaches. The process is also time-consuming, as accessing specific data on punched cards is slow. To retrieve a particular record or piece of information, manual sorting through stacks of cards is necessary.

The primary objectives are to design Go2Work, a Staff Attendance System using QR codes and the CAOQTP Algorithm for Pejabat Pendidikan Daerah Hulu Langat. The system will feature a user-friendly interface, developed in Visual Studio Code, and thoroughly tested for functionality. The project scope encompasses admin, superior, and staff roles involved in the attendance process at PPD Hulu Langat. The system aims to address key issues such as manual data entry, inefficient data retrieval, attendance fraud, and lack of security protocols leading to unauthorized access, utilizing CAOQTP and QR codes.

The expected outcomes for the GO2WORK system include transforming staff attendance management with the innovative CAOQTP Algorithm. This algorithm will enhance data integrity and security, protecting attendance data from unauthorized access and breaches. The system will improve reporting capabilities, providing detailed insights into better decision-making. It will streamline attendance processes, increasing operational efficiency and user satisfaction. The user-friendly interface and smooth integration of CAOQTP will lead to cost savings for Pejabat Pendidikan Daerah Hulu Langat. Additionally, the system will reduce legal risks by complying with strict data security regulations. The GO2WORK system aspires to set a new industry standard for secure and efficient attendance management, benefiting stakeholders and paving the way for future innovations in the field.

2. Literature Review

This section explains the two-factor authentication, password, OTP, CAPTCHA, and review on attendance authentication systems and comparison between existing systems and proposed system.

2.1 Two Factor Authentication

Two-Factor Authentication (2FA) represents an advanced security measure in the realm of authentication systems. The goal of two-factor authentication (2FA) is to improve resilience of authentication based on passwords by mandating users to give a second authentication factor, such as a code produced by a token of security [1]. Moreover, by adding a second layer of verification, 2FA improves security in contrast to single- factor authentication (SFA), which depends on a single set of credentials, such as password. In the implementation of 2FA, the user must provide something to complete the second factor, such as a code that is sent to their mobile device or is created by an authentication app. Furthermore, the procedure entails entering the conventional password first, then the second factor. Therefore, this adds another degree of complexity and strengthens the authentication process considerably.

2.2 Password

A password, which is usually known only to the authorized user, functions as a digital lock, guaranteeing that access is only granted to those who have the right combination of characters [2]. Moreover, an essential component of authentication systems, a password acts as a private key that unlocks accounts, systems, and other protected data. Furthermore, creating a strong and secure password is crucial when it comes to cybersecurity. In addition, it should include a mix of letters, numbers, and symbols to increase its resistance to brute-force attacks and other forms of unauthorized access. Other than that, changing passwords frequently and steering clear of combinations that are simple to figure out are standard procedures to improve security. Hence, passwords play a vital role in maintaining the integrity and privacy of various online accounts by serving as a cornerstone for protecting digital identities and sensitive data.

2.3 CAPTCHA

One essential tool for internet security is CAPTCHA. Its main purpose is to differentiate between automated bots and human users by posing problems that are simple for people to solve but challenging for machines to imitate. CAPTCHA is an application that can create and score tests that most people can complete, and most computer programs are unable to complete [4].

2.3.1 Image CAPTCHA

The purpose of Image CAPTCHA, also known as the Fully Automated Public Turing Test to Tell Computers and Humans Apart, is to differentiate between automated bots and real users. When completing an image CAPTCHA users are usually shown distorted characters, numbers, or symbols. Users must accurately interpret and input the data to prove that users are human. Additionally, online systems are further secured by this visual challenge, which stops automated scripts from misusing the system by fabricating accounts or carrying out destructive operations like distributed denial-of-service assaults.[5] Furthermore, by presenting tasks that are simple for people to perform but difficult for automated programs to comprehend, image CAPTCHAs work as an

essential gatekeeper, maintaining the integrity of online interactions and guarding against unauthorized intrusions.

2.4 OTP

OTPs are a time-sensitive and dynamic way to improve online security, especially during authentication procedures. Moreover, OTPs are temporary codes created for one use only within a predetermined window of time, as opposed to static passwords, which stay the same throughout [3]. Furthermore, these codes are usually sent to users via email, text messages, or mobile applications. As a result, OTPs' transience and uniqueness greatly improve security by reducing the possibility of password reuse or compromise. In addition, this authentication technique provides an extra degree of security since the time-limited nature of OTPs makes unauthorized access much more difficult, even in the unlikely event that a static password is compromised. OTPs remain a vital part of multi-factor authentication systems as technology develops, providing a flexible and efficient way to thwart potential security risks in online settings.

2.4.1 Email OTP

One-time passwords sent by email (OTPs) are a dependable way to improve the security of online authentication procedures. This is because during sensitive transactions or login attempts, users using this method must enter one-of-a-kind, time-sensitive code that they receive to their registered email address in addition to their regular login credentials.

2.5 Existing System related to attendance system

There are three existing systems which are Manual Attendance System (Punched cards), Barcoded Attendance System (TMS Client-Server Attendance System), Web-based Attendance System (Office Timer). Every system and application have unique advantages and variations that might be used to enhance the proposed system.

2.5.1 Manual Attendance System (Punched Cards)

In the manual attendance system utilizing punched cards at PPD Hulu Langat, each staff member is assigned a unique card, crucial for meticulously tracking their daily attendance. The system is dependent on a dedicated timekeeping device located in Block B of PPD Hulu Langat's Administration Block as in Fig 1. Furthermore, this device meticulously logs each employee's arrival and departure times, guaranteeing accurate and trustworthy attendance records. Organizations such as PPD Hulu Langat still utilize the manual attendance system, which uses punched cards. Employees in this system has a distinct punched card, which is essential for closely monitoring their daily attendance. The technique depends on a specific timekeeping gadget, which is often housed in the administrative block of the company. The entrance time is recorded in red ink by the system when employees come at work and tap their individually punched cards on the terminal. In a similar vein, employees are discouraged from working over the specified hours if they depart before the appointed time and their return time is indicated in red type. Furthermore, this technique aids in locating instances of early returns or late attendance

Fig. 1 *Punch Card Machine at PPD Hulu Langat*

2.5.2 TMS Client-Server Attendance System

Utilizing a network environment, a client-server-based attendance system permits resource sharing by exchanging data between server and client computers [6]. The TMS Client-Server Attendance System, which allows businesses to track employees' attendance in real-time across multiple branches, is an example of this architecture. Fig 2 shows the client, and the server module are the two components that make up the system. Features like client login, barcode scanning for punching in and out, and an attendance report function for simple report printing are all included in the client module. Conversely, the server module includes administration settings for scheduling, employee information, and leave management, giving administrators a methodical approach to manage data.

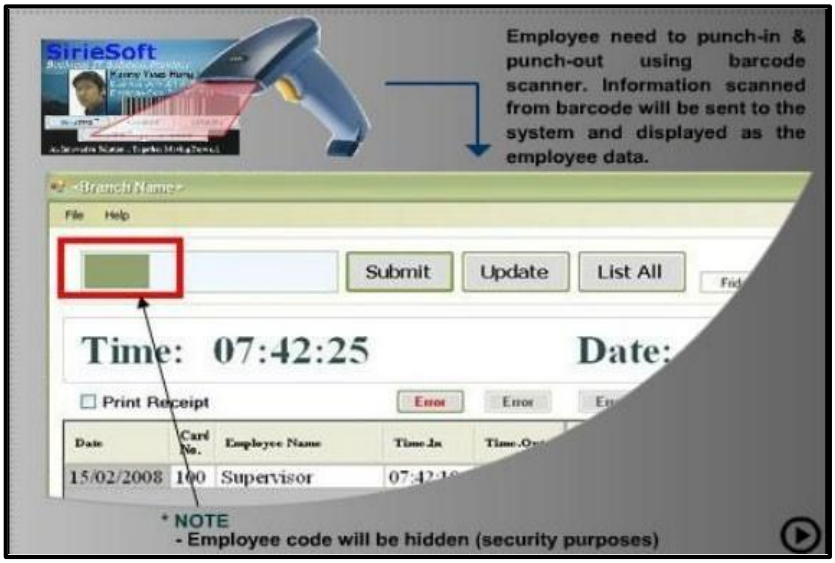

Fig. 2 *Punch in & out page* [6]

2.5.3 Office Timer

Office Timer (Fig. 3) offers a user-friendly web-based attendance management system, simplifying the process of tracking employee attendance and ensuring compliance with company policies. Furthermore, Office Timer has a feature- rich leave management module that expedites the processing of leave requests in addition to attendance tracking. It facilitates the establishment of leave policies, supports a variety of leave kinds, and encourages openness in the workplace. Office Timer's geo-tagging feature helps businesses with distributed workforces by reliably recording employee check-ins and check-outs globally, improving attendance tracking and encouraging accountability among remote workers. The reporting features of the system offer thorough insights into trends in productivity and attendance. Managers are able to make well-informed decisions to maximize scheduling and quickly resolve issues related to attendance.

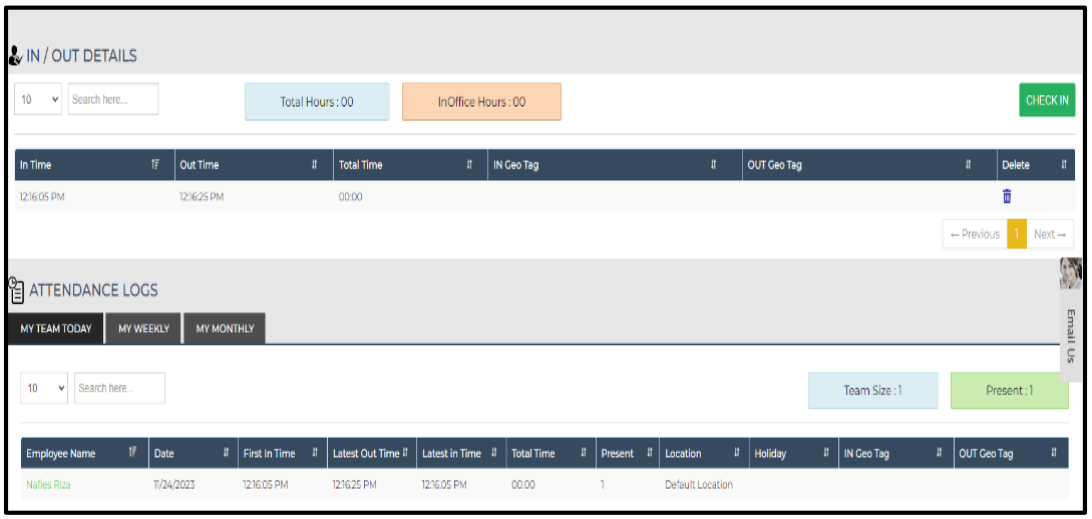

Fig. 3 *Clock in and out page*

2.6 Comparison of the Existing System with the proposed System

The characteristics and security measures of three current attendance systems that use conventional techniques are compared with GO2WORK which is the proposed system that uses a QR code-based mechanism. Important details are covered in the analysis to help readers grasp each company's unique capacity for managing attendance as shown in Table 1.

Table 1 *Comparison Existing System with the proposed System*

Features	PPD HuluLangat Manual System	TMS Client- Server Attendance System	Office Timer	Propose System
Type of System	Manual System	Online System	Online System	Online System
Authentication	Physical Punched Cards	Password & Employee code	Geo-Tagging	OTP using CAOQTP Algorithm
Two Factor Authentication	No	No	Not Mentioned	Yes
Real-Time Monitoring	No	Yes	Yes	Yes
User Accessibility	Physical card tapping at dedicated machine	Barcode scanning for punching in and out	Web-based attendance system, clock in and clock out online	Web and mobile application using QR code

3. Methodology/Framework

The Prototyping Model in Fig. 4 is a dynamic approach to software development that centers around the creation of a preliminary version of the system, known as a prototype, to elicit user feedback and refine requirements.

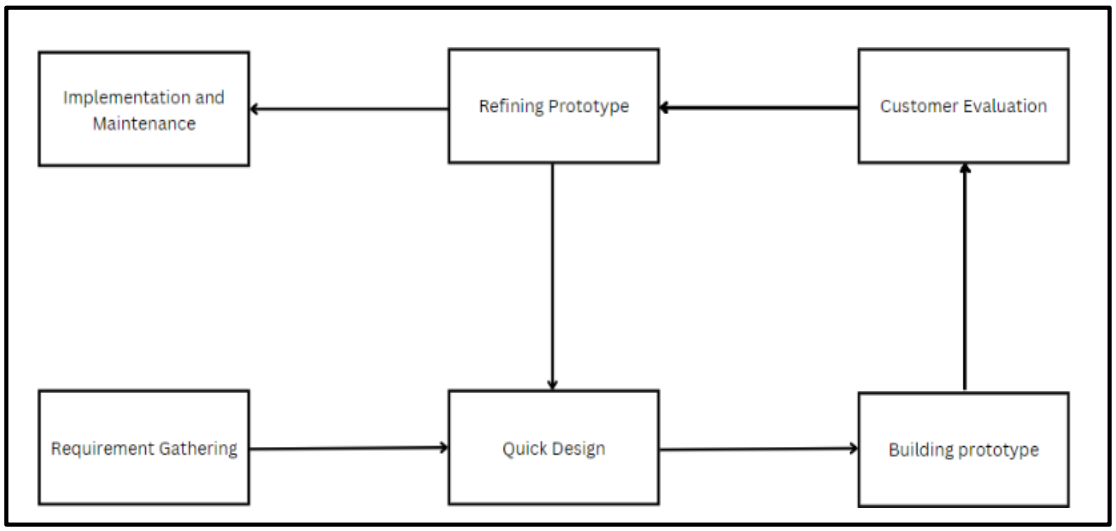

Fig. 4 *Prototype Model [7]*

3.1 Requirements Gathering and Analysis Phase

Several tasks are included in the requirement collection and analysis phase with the goal of fully comprehending the context of the project. First, the scope, objectives, and problem description are determined. Interviews with personnel and administrators are then conducted in order to obtain a variety of viewpoints from stakeholders. The functional and non-functional user requirements are described in detail, together with the intended project outcomes and importance. Additionally, software and hardware requirements for GO2WORK are also studied in this phase as display in Table 2.

Table 2 *Software & Hardware Requirements*

Software	Specification
Visual Studio Code	PHP
Xampp	Cross platform for PHP, MYSQL
PhpMyAdmin	MySQL database
Hardware	Specification
Processor	AMD Ryzen 5 3500 6-Core Processor 3.60 GHZ
Random Access Memory (RAM)	16.0 GB
Graphics Card	Radeon RX 580 8GB Virtual RAM(VRAM)
System Type	64-bit operating system, x64-based processor
Storage solid-state drives (SSD)	1.0 TB

3.2 Quick Design Phase

Essential parts are quickly developed during the Quick Design phase, which is a fast iteration step based on requirements received. This includes building the system's navigation flow, developing the database structure to make collecting attendance data easier, and designing the user interface, which includes key features like QR code scanning. This phase also covers security components like the CAOQTP algorithm-based integration of OTP and Captcha.

3.3 Build a Prototype Phase

The Build a Prototype phase involves transforming rapid design requirements into a physical, workable prototype. At this point in the development process, the main goal is to create a working prototype of Go2Work. Implementing QR code generation and scanning functionality, two essential components of the suggested attendance management system, receive particular attention.

3.4 User Evaluation Phase

Throughout the User Evaluation stage of the Prototyping Model for GO2WORK, engaging potential users is essential. During this stage, the prototype is shown to the target end users, which include personnel, administrators, and other stakeholders involved in attendance management. The principal responsibilities are gathering input from prospective clients, particularly the PPD Hulu Langat personnel, and executing assessments of user contentment. Users must interact with the prototype at this phase in order to assess its functioning, offer suggestions, and communicate their preferences through interactive sessions.

3.5 Refining Prototype Phase

The refining Prototype stage is centered on iteratively improving and fine-tuning in response to user input. In this stage, the development team works to improve the system's functionality, user interface, and security protocols by refining the current prototype and incorporating user feedback. By using an iterative approach, the objective is to maximize functionality, user experience, and overall system performance.

3.6 Implementation and Maintenance Phase

The final version of the system is deployed at PPD Hulu Langat as part of the Implementation and Maintenance Phase. This stage includes setting up hardware, installing necessary software, integrating the attendance management system with the organization's infrastructure, and ensuring that it is compatible with current systems. To guarantee a smooth transfer to the new attendance system, user training and assistance are also offered.

4. System Analysis and Design

Functional requirements define the function or services that will be implemented in the system to achieve user's needs meanwhile non-functional requirements define system behavior rather than what the system should do. Table 3 and Table 4 are a list of functional requirements and list of non-functional requirements of for Go2Work an Attendance System using QR code with CAOQTP Algorithm for Pejabat Pendidikan Daerah Hulu Langat.

Table 3 *List of Functional Requirement for Go2Work an Attendance System using QR code with CAOQTP*

Algorithm for Pejabat Pendidikan Daerah Hulu Langat

Modules	Functionality
Login	The system should permit the administrator, superior and staff to login using username and password for first layer authentication.
	The system should redirect user to first time login page if user first time logging in to the system.
	The system should redirect user to the new device login page if the system detects user logging in with new device.
	The system should allow error when there is an empty field.
Registration	The system should allow error when there is an empty field.
	The system should allow registration for new users.
	The system should allow administrators to register new users.
Attendance	The system should allow administrator to take manual attendance for users.
	The system should allow users to take attendance using QR code scanner provided in the system.
Reporting	Superior able to generate monthly attendance report
QR code	The system should allow users to generate the QR codes.
	QR code must have longitude and latitude of PPD Hulu Langat.
	QR code can only be scanned in the radius of 50 meters from the kiosk.
	The system asks location of user during scanning QR code
Profile	The system should allow users to update profile picture.
Logs	The system should allow administrators to view all staff's attendance logs.
	The system should allow staff to view their own attendance logs.

Table 4 *List of Non-Functional Requirement for Go2Work an Attendance System using QR code with CAOQTP Algorithm for Pejabat Pendidikan Daerah Hulu Langat*

Modules	Functionality
Operational	The system can be accessed when there is an internet connection.
Performance	All users should be able to access the correct assigned pages. The system can allocate the user to the correct session.
Usability	The system interface is user-friendly and easy to navigate.
Security	• The user may access the system with username, password and should be able to go through CAOQTP process during first-time login and new device login. • Password should be hashed in the database. • Users be able to change their password via the forgot password module.

4.1 System Architecture

The architectural design of the system defines the structure and behavior of its various components. Fig. 5 illustrates the system architecture for the GO2WORK staff attendance system, incorporating QR codes.

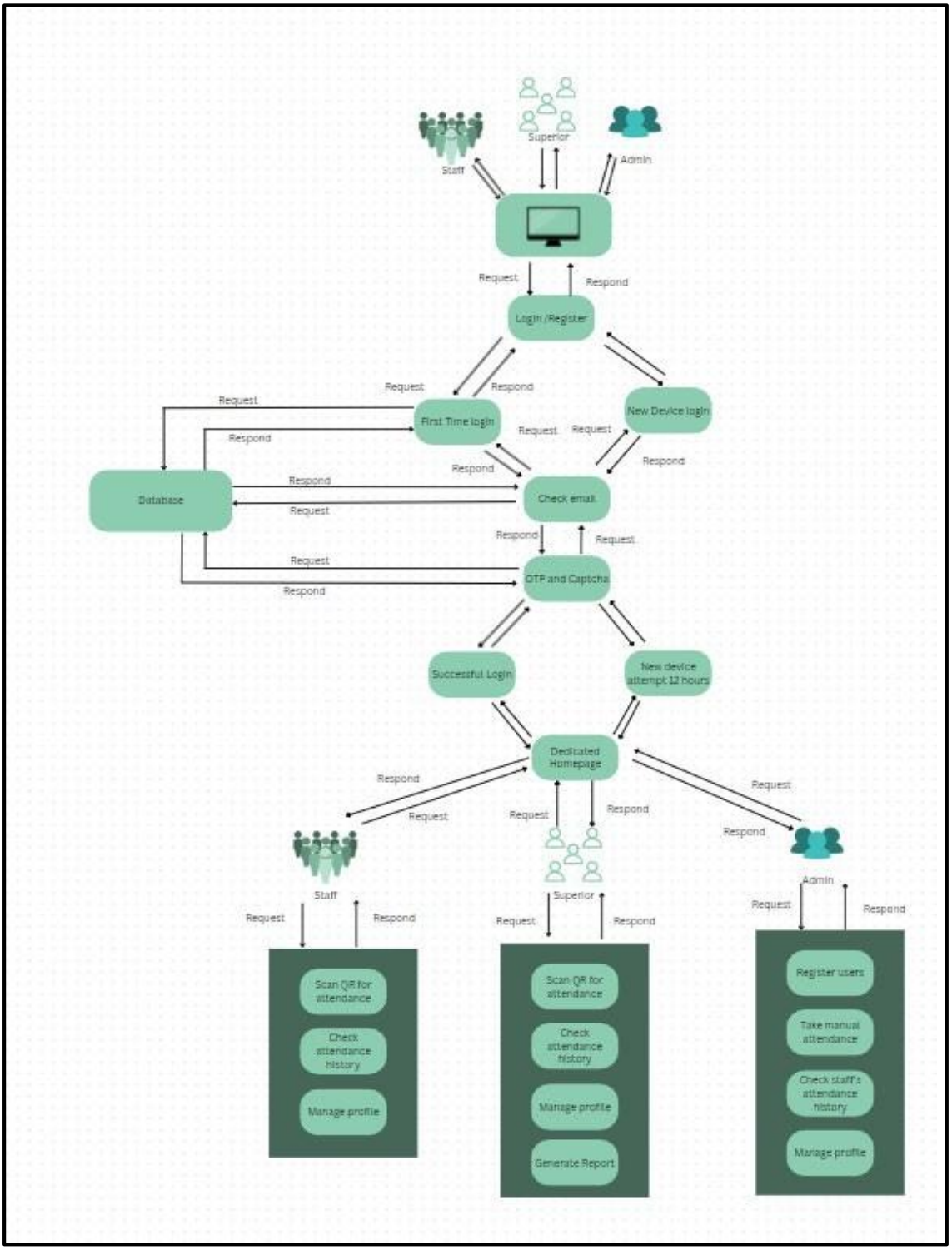

Fig. 5 *System Architecture of Go2Work: A Staff Attendance System*

4.2 Use Case Diagram

A use case diagram is a picture that shows how users (actors) and a system interact, displaying what the system can do from user's point of view. It points out main functions or tasks (use cases) that the system does and explains how different people or things interact with these tasks. The diagram usually has actors (users or other systems), use cases (what the system does), and how it relates to each other. It is helpful for understanding what the system needs to do and planning its structure, making sure all ways users interact with it are included. Fig. 6 presents the use case diagram for the Go2Work staff attendance system with QR code and CAOQTP security algorithm.

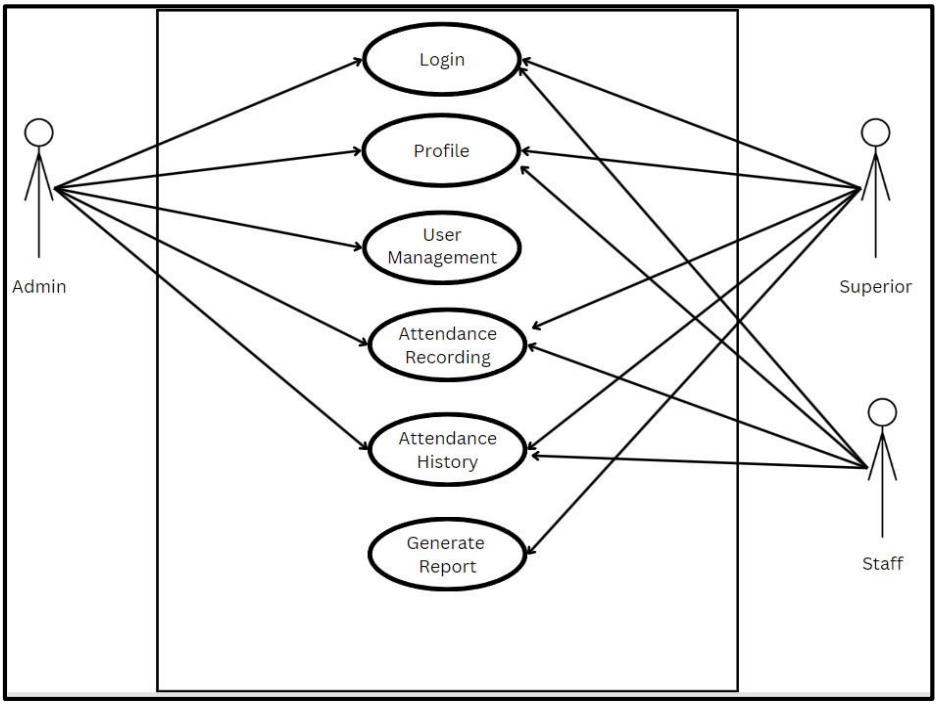

Fig. 6 *Use case Diagram of Go2Work: A Staff Attendance System*

4.3 Sequence Diagram

The sequence diagrams illustrate the interactions within the Go2Work staff attendance system for three user types: Admin, Superior, and Staff. Each diagram outlines the login process, access to the dashboard, and interaction with the attendance logs. Admins log in, verify credentials, view the dashboard, and manage attendance records shown in Fig. 7. Superiors follow a similar login process, accessing their dashboard to review and approve attendance logs as shown in Fig 8. Staff members log in, record their attendance, and view their attendance history as shown in Fig. 9.

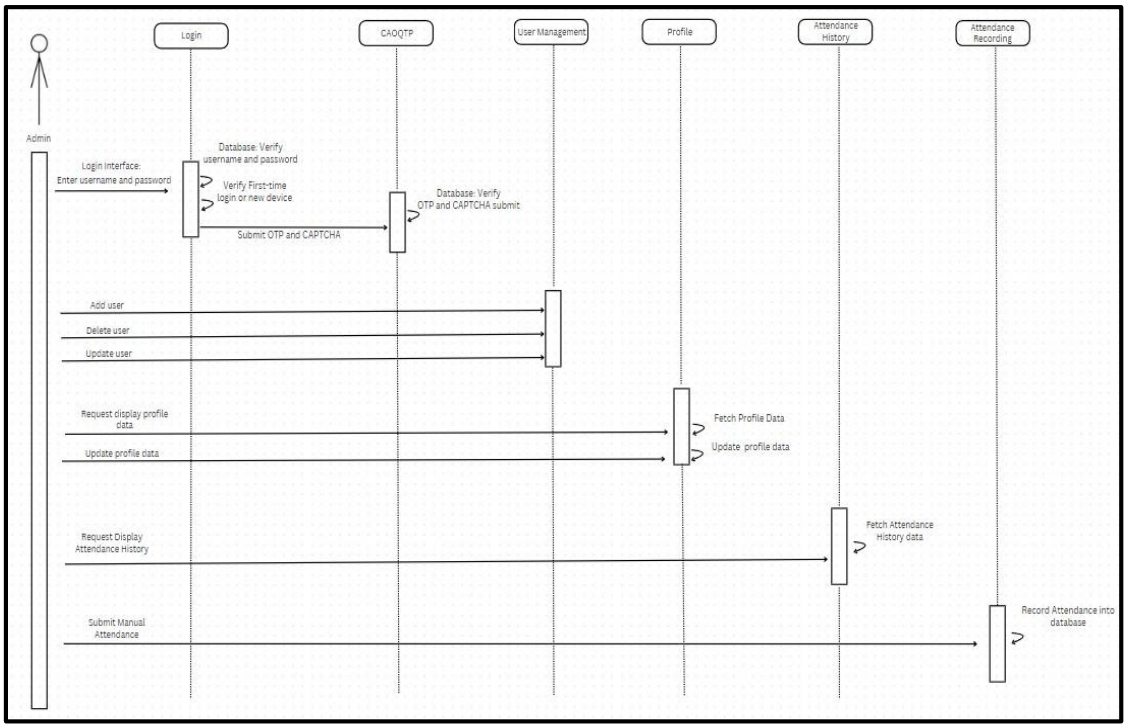

Fig. 7 *Sequence Diagram for Admin*

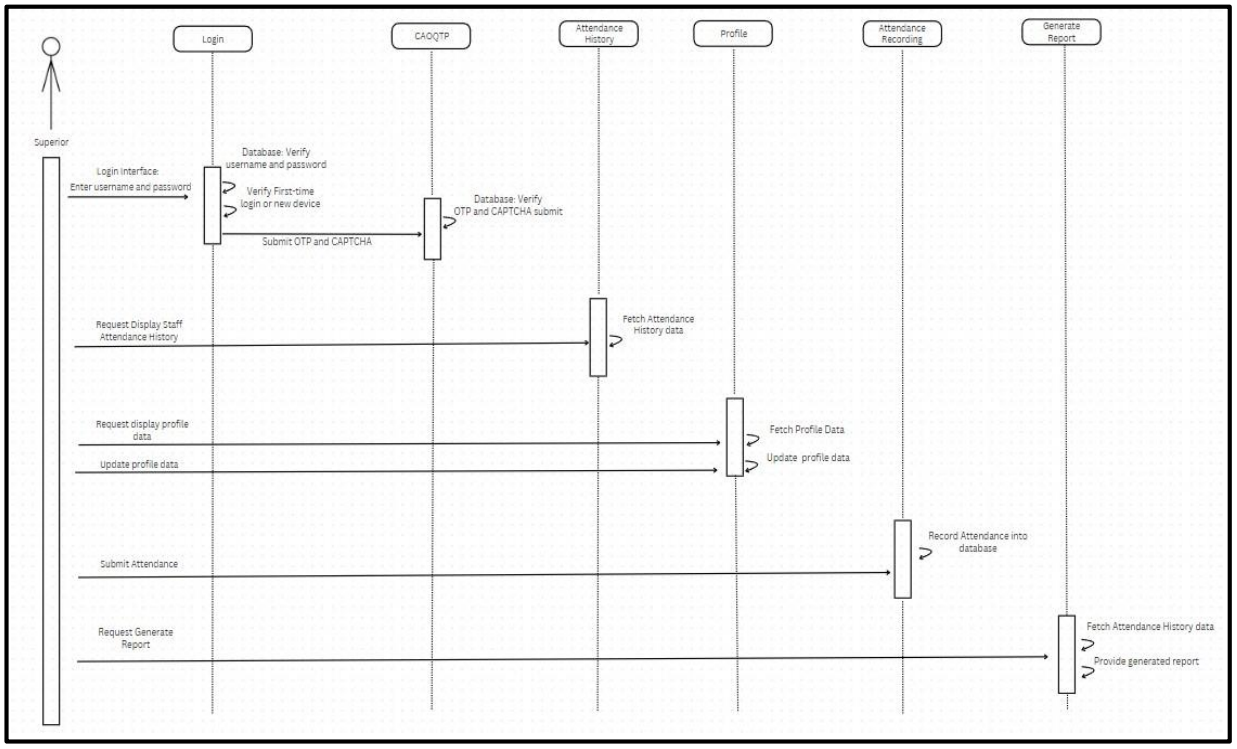

Fig. 8 *Sequence Diagram for Superior*

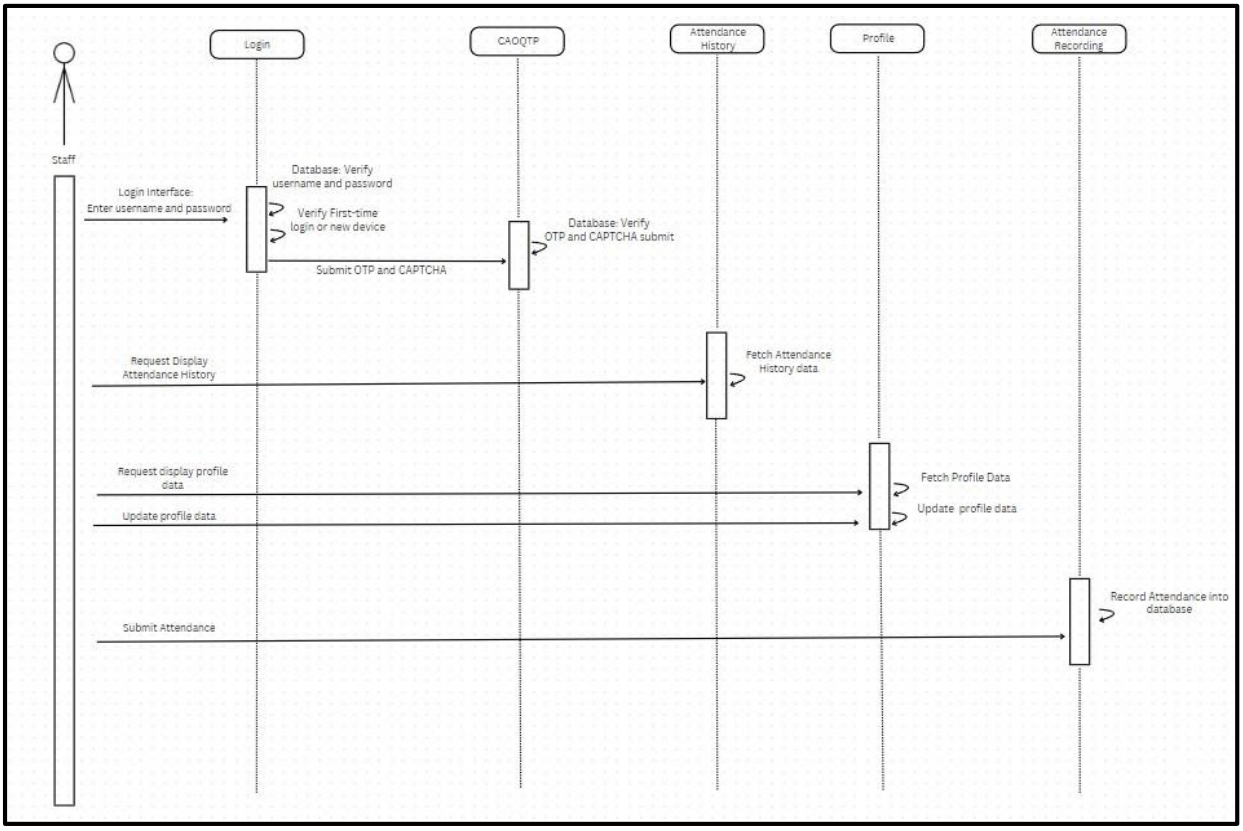

Fig. 9 *Sequence Diagram for Staff*

4.4 Entity Relation Diagram (ERD)

The Entity Relationship Diagram (ERD) in Fig. 10 illustrates the relationships between entities in the system. It provides a visual representation of how different entities, such as staff, superior, QRCode, kiosk, clock in and out are connected and interact within the database.

Applied Information Technology and Computer Science Vol. 6 No. 1 (2025) p. 415-433

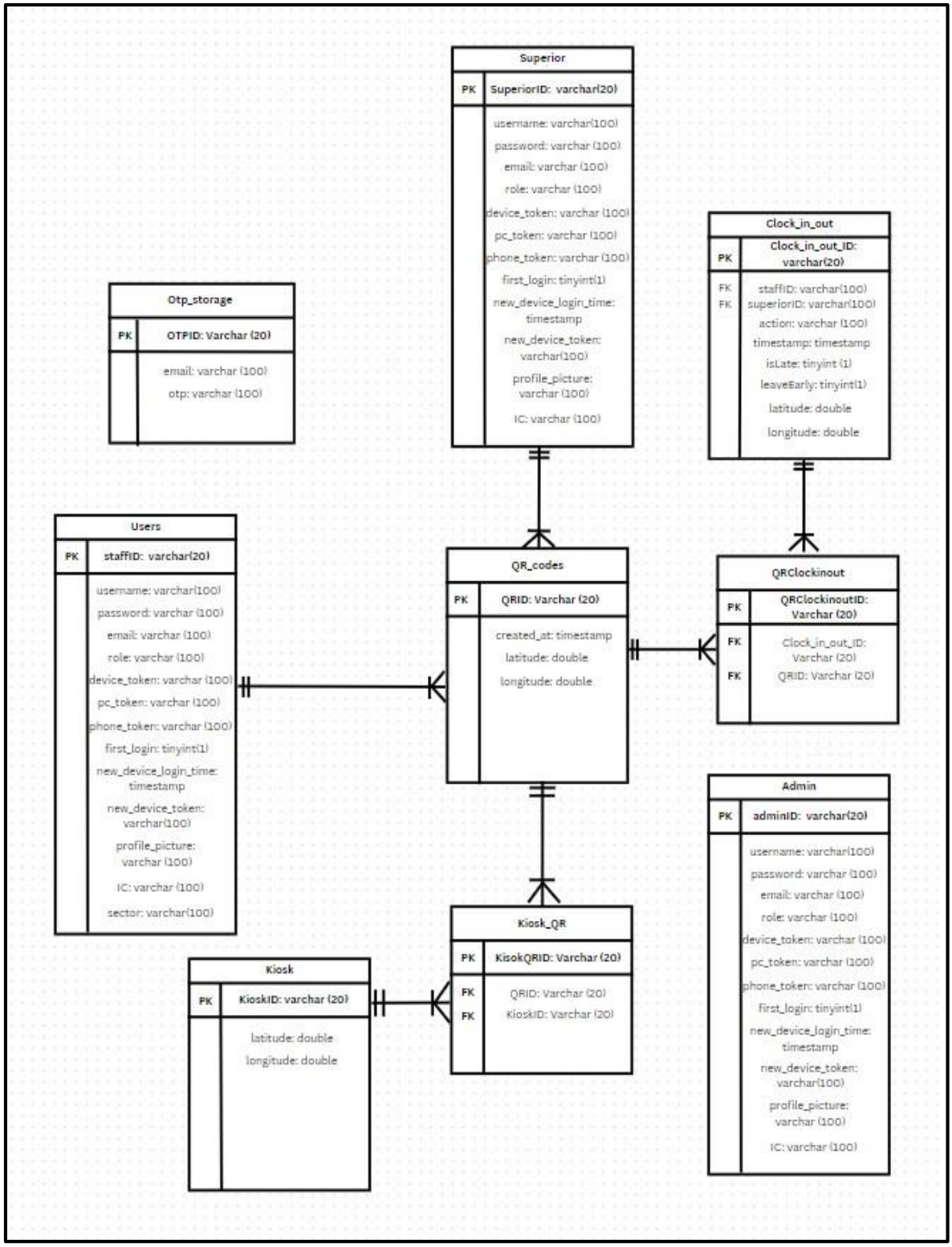

Fig. 10 *Entity Relation Diagram*

5. Implementation and Testing

Implementation is the process of developing and building the software system from the design whereas testing is the process of determining whether the system is reliable and accurate.

5.1 Implementation

The following section will cover the modules that were utilized in this system. The modules for registration, login, attendance, and QR code generation will be covered. The several sections will each contain a description of the program's partial code for a particular module.

5.1.1 Login

Fig. 11 displays the login page, Fig 12 shows the first-time login and Fig. 13 shows the new device login. Users will have to login first, after login process the system will check whether the user is first time login or login from new device, if the system detects the user first time logging in then user will redirect to first-time login page as shown in Fig. 10. Meanwhile, if the system detects user logging in with new device, user will be redirected to new device login as shown in Fig. 11. If the user neither of the conditions met, then user can login as usual.

Fig. 11 *Login page*

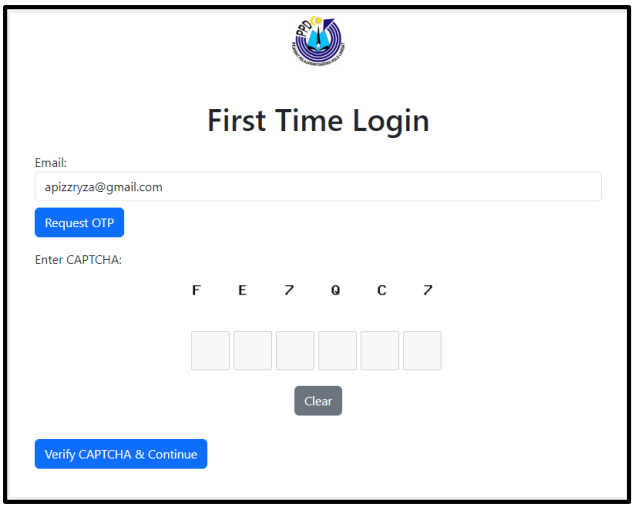

Fig. 12 *First Time Login Page*

Fig. 13 *New Device Login*

Fig. 14 shows during the login process username and hashed password input by the user will be compared to the username and hashed password in the database. If both username and hashed password are matched, user will be redirected to dedicated homepage.

```php
if ($_SERVER['REQUEST_METHOD'] == 'POST') {
    $username = $_POST['username'];
    $password = $_POST['password'];
    $hashed_password = hash('sha256', $password);

    // Query the users table using a prepared statement to prevent SQL injection
    $user_query = $conn->prepare("SELECT * FROM users WHERE username = ? AND password = ?");
    $user_query->bind_param('ss', $username, $hashed_password);
    $user_query->execute();
    $user_result = $user_query->get_result();

    // Query the admin table using a prepared statement to prevent SQL injection
    $admin_query = $conn->prepare("SELECT * FROM admin WHERE username = ? AND password = ?");
    $admin_query->bind_param('ss', $username, $hashed_password);
    $admin_query->execute();
    $admin_result = $admin_query->get_result();
```

Fig.14 *Snippet code of comparing hashed password*

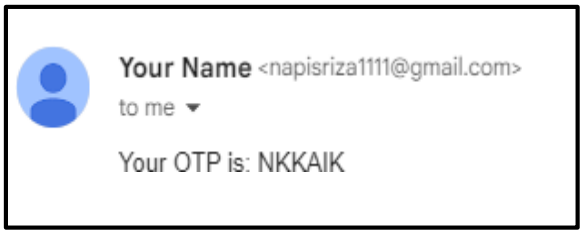

Fig. 15 *OTP sent to an email*

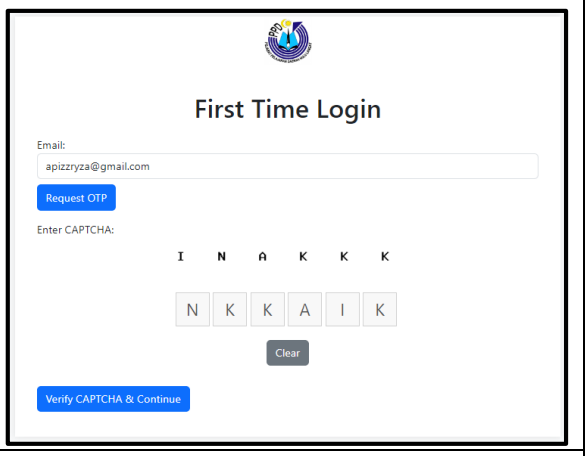

Fig. 16 *First time login*

Fig. 16 displays a CAOQTP process during first-time login. The process is when user request for OTP, server will generate a six characters OTP and an OTP will be sent to user's email address as shown in Fig. 15. After user getting an OTP, server will generate CAPTCHA images that are shuffled based on OTP given. User will have to rearrange the CAPTCHA images based on OTP that have been sent to user's email.

```php
if ($_SERVER['REQUEST_METHOD'] === 'POST' && !isset($_POST['request_otp'])) {
    // Retrieve and clean the input from the form
    $enteredOtp = strtoupper(str_replace(' ', '', $_POST['otp_input']));
    $enteredCaptcha = strtoupper($_POST['otp_input'] ?? '');

    // Debugging: Print entered and stored values
    error_log("Entered OTP: $enteredOtp");
    error_log("Stored OTP: " . $_SESSION['otp']);

    // Retrieve the stored OTP from the session
    $storedOtp = $_SESSION['otp'];

    // Validate entered CAPTCHA and stored OTP
    if ($enteredCaptcha === $storedOtp) {
        // OTP and CAPTCHA validated successfully
        $username = $_SESSION['username'] ?? '';
        $role = $_SESSION['role'] ?? '';
        $deviceToken = $_SESSION['new_device_token'] ?? generateDeviceToken(); // Generate a new device token if not set
        $deviceType = getDeviceType();
        $pcDeviceToken = ($deviceType == 'pc') ? $deviceToken : NULL;
        $phoneDeviceToken = ($deviceType == 'phone') ? $deviceToken : NULL;

        // Debugging: Print the values before the update
        error_log("Username: $username");
        error_log("Role: $role");
        error_log("Device Token: $deviceToken");

        // Set cookie with device token first
        setcookie('device_token', $deviceToken, time() + (86400 * 30), "/"); // 30 days expiry
```

Fig. 17 *Snippet code of comparing logic between OTP and CAPTCHA*

Fig. 17 shows the code that handles the comparing logic between OTP and CAPTCHA. If the entered CAPTCHA is matched with the stored OTP and new password have been filled, the system will create a cookie for the device the user logged in with. This cookie ensures that the user does not have to go through the first-time login process during subsequent logins on the same device. This mechanism streamlines the login process for returning users by recognizing their devices and skipping repetitive verification steps.

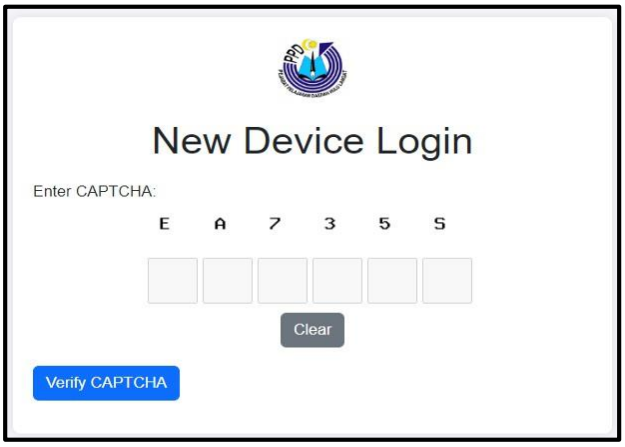

Fig. 18 *New Device Login*

Fig. 19 *New Device Login Attempt*

Fig. 18 shows the new device login, the CAOQTP process is the same as the first-time login. However, new device login users do not have to request an OTP, OTP will be sent right away after the user redirected to new device login. After completing CAOQTP process, user will have to wait for twelve hours before able to access the system as shown in Fig. 19.

5.1.2 Registration

Fig. 20 and 21 shows registration form for users. Only administrators able to register new users. For administrator and superior registration, it requires to fill the field of name, ID, IC number, password, email address, and choose role as shown in Fig 20. Meanwhile for staff registration, it requires to fill name, ID, IC number, password, email address, choose role and sector as shown in Fig. 21.

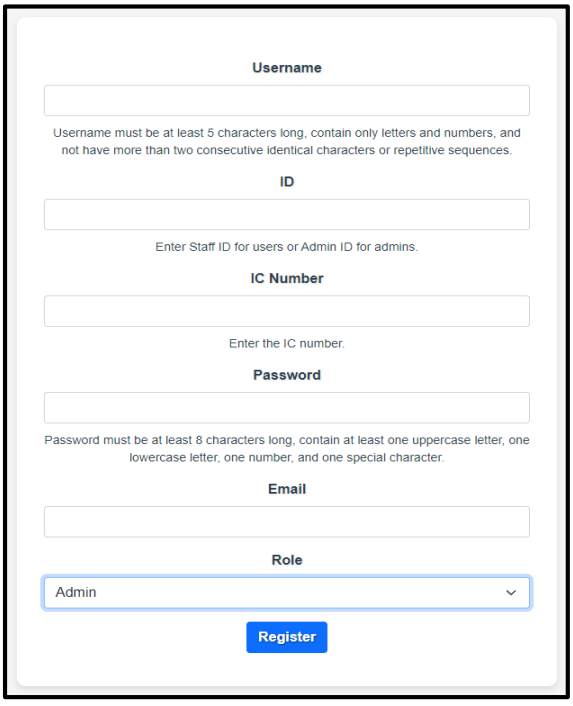

Fig. 20 *Registration Form for admin and superior*

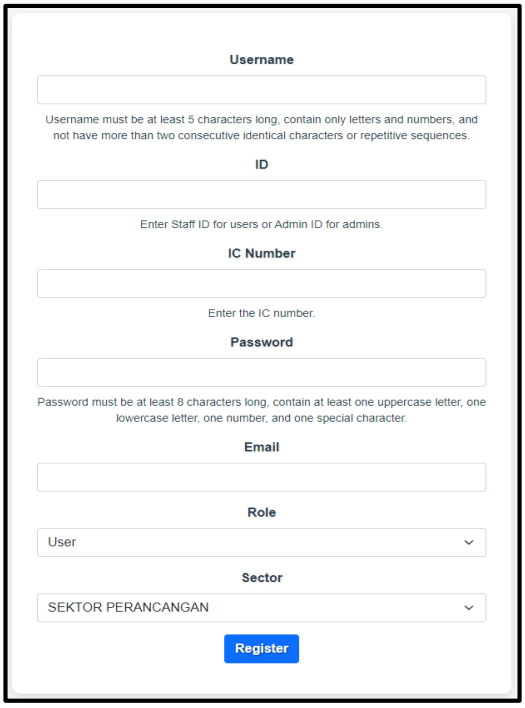

Fig. 21 *Registration Form for staff*

```
    document.getElementById('username').addEventListener('input', function (e) {
var usernameInput = e.target.value;
var message = '';
if (usernameInput.length < 5) {
    message = 'Username must be at least 5 characters long.';
} else if (!/^[A-Za-z]+$/.test(usernameInput)) {
    message = 'Username should contain only letters.';
} else if (/(.)\1{2,}/.test(usernameInput) || /(.{2,})\1{1,}/.test(usernameInput)) {
    message = 'Username cannot have more than two consecutive identical characters or repetitive sequences.';
}
document.getElementById('usernameHelp').textContent = message;
});

    document.getElementById('password').addEventListener('input', function (e) {
        var passwordInput = e.target.value;
        var message = '';
        var passwordErrorDiv = document.getElementById('passwordError');
        if (!/^(?=.*[A-Z])(?=.*[a-z])(?=.*\d)(?=.*[@$!%*?&])[A-Za-z\d@$!%*?&]{8,}$/.test(passwordInput)) {
            message = 'Password must be at least 8 characters long, contain at least one uppercase letter, one lowercase letter, one number, and one special character.';
            passwordErrorDiv.style.display = 'block';
        } else {
            passwordErrorDiv.style.display = 'none';
        }
        document.getElementById('passwordHelp').textContent = message;
    });
```

Fig. 22 *Snippet code of validate username and password.*

Fig. 22 shows snippet code for validating password input which minimum length of 8 characters, one upper case, one lower case, and a special character. Meanwhile for username, username length must be at least 5 characters long, letters only and username cannot have more than two consecutive identical characters or repetitive sequences.

5.1.3 QR code

QR code module, there will be a kiosk that will handle QR code generation. The main interface for the kiosk is shown as Fig. 23. The QR code can only be generated at kiosk only. After generating QR code, it will redirect to QR code interface as in Fig. 24 where the QR code is being generated dynamically. it has interval of 5 seconds, after 5 seconds it will change to a different QR codes. Other than that, each QR codes has set of longitude and latitude coordinates. the QR codes scan only be scanned within a certain distance from these coordinates. Therefore, the QR codes can only be used in its specific location. Furthermore, the coordinates of the QR code can be setup in QR code table as shown in Fig. 25. Moreover, the QR code page after sixty seconds of being idle, the page will close itself.

Fig. 23 *Generate QR code interface*

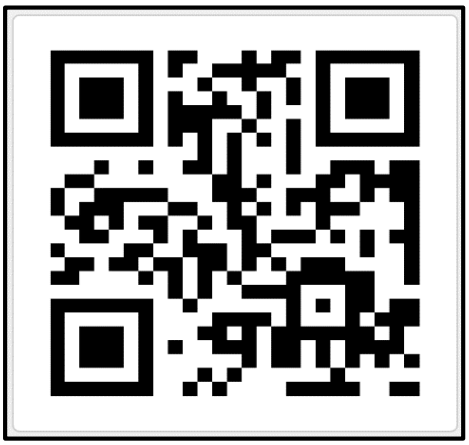

Fig. 24 *QR code interface*

id	qr_code	created_at	latitude	longitude
1	y8SO5jlsm1	2024-06-03 02:17:22	1.8651403	103.1051246

Fig. 25 *QR code table in database*

5.1.4 Attendance

Attendance modules have two separate functions for administrators, staff and superiors. For administrators, administrators manually take attendance for staff as shown in Fig. 26. For example, when staff log in from a new device staff must wait for twelve hours. During that waiting period, administrators need to manually take their attendance.

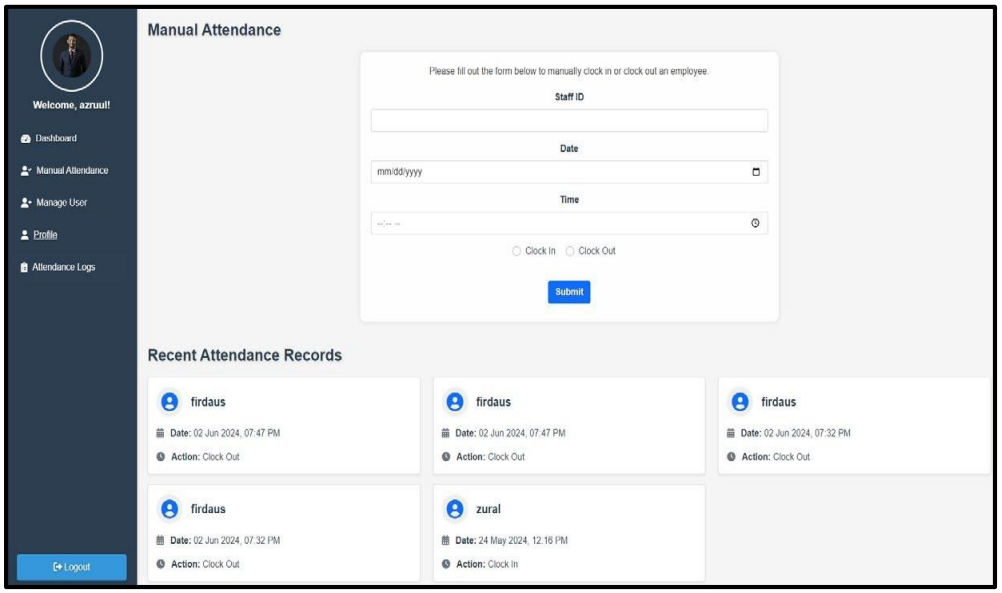

Fig. 26 *Manual Attendance Interface*

Attendance module for staff and superior is completely different. Where user must scan QR code for clock in and clock out at dedicated kiosk. User cannot scan the QR code outside the range or radius the kiosk. Furthermore, during scanning QR code process, the system will ask to allow give location to system, and it will compare the location with the stored location. If user scan within the range of the kiosk it will prompt a message as shown in Fig. 28. However, if user scan outside the range of the kiosk, as a result, it will prompt an error message as shown in Fig. 29.

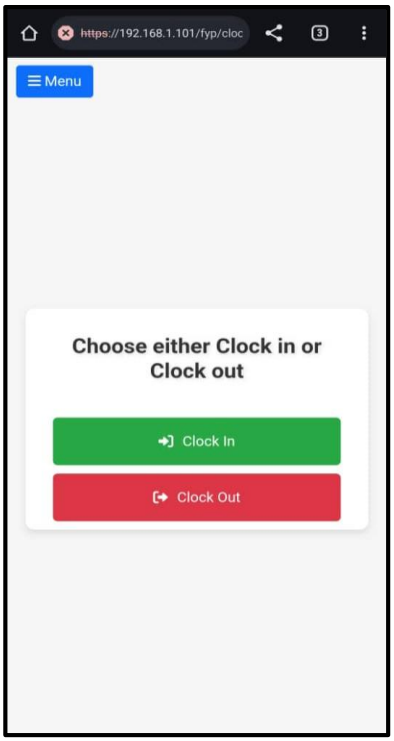

Fig. 27 *Clock in or Out Interface*

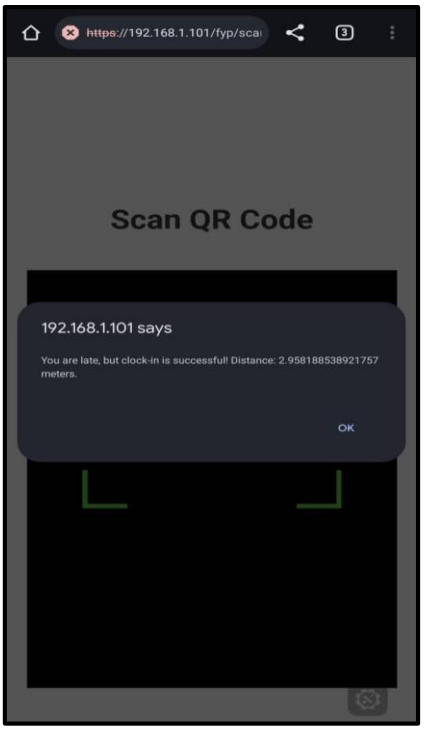

Fig. 28 *Successfully scan QR code*

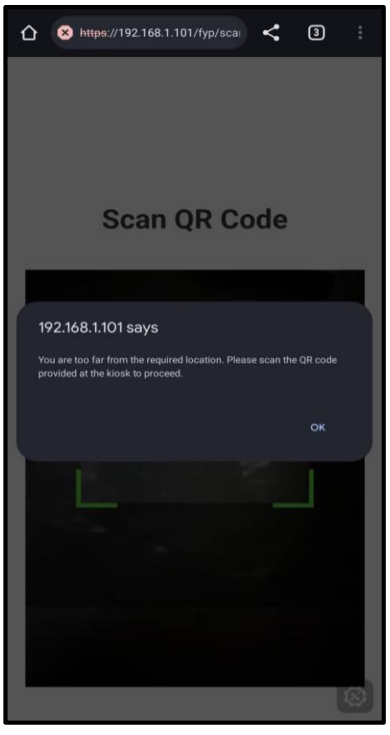

Fig. 29 *User Alert Message When Scanning Outside the Permitted 10-Meter Range*

5.1.5 Attendance Logs

Attendance logs module for staff, staff can only view individual attendance as shown in Fig. 30 Staff able to filter by daily, monthly, and yearly. Also, staff able to filter by date. Meanwhile, Attendance logs module for administrators and superior, administrators and superior able to view all the staff's attendance. Furthermore, administrators and superior able to filter by daily, monthly, and yearly. Other than that, administrators and superior also able to filter by date, sector and staff id as shown in Fig. 30 and Fig. 31.

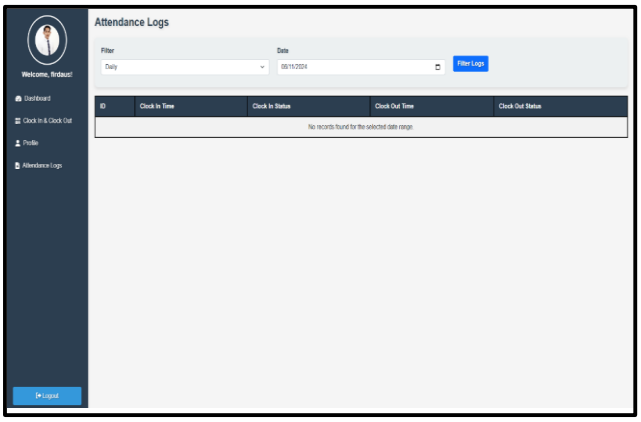

Fig. 30 *Attendance logs for staff*

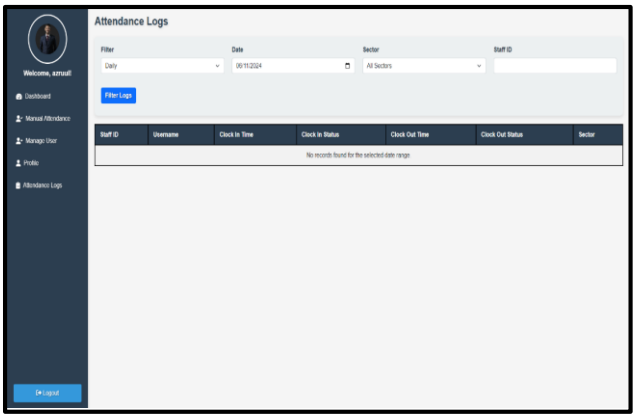

Fig. 31 *Attendance logs for administrators*

5.2 Testing

The testing phase for the Go2Work system involved thorough functionality and security testing to ensure the system operates as expected and meets security standards. Table 5 and Table 6 show the results of functionality and security testing.

Table 5 *Functionality Testing*

No.	Modules	Functionality	Pass	Fail
1.	Register	• The system should allow registration for new users. • The system should allow errors when there is an empty field. • The system should allow errors when password is not more than 8 characters and do not have special symbols	Yes	
2	Login	• The system should permit the administrator, superior and staff to login using username and password for first layer authentication. • The system should redirect user to first time login page if user first time logging in to the system. • The system should redirect user to the new device login page if the system detects user logging in with new device. • The system should allow errors when there is an empty field	Yes	
3.	QR code	• QR code must have longitude and latitude of PPD Hulu Langat. • QR code can only be scanned in the radius of 50 meters from the kiosk. • The system asks location of user during scanning QR code	Yes	
4.	Attendance Recording	• Staff and superior should be able to use the dedicated QR scanner to scan QR code for marking attendance. • The system needs to maintain an attendance history that user can access through the Go2Work website. • Admin able to take manual attendance.	Yes	

Table 6 *Security Testing*

No.	Test Case	Pass	Fail
1.	Password must contain alphabet, number, special character and must be longer than 8 characters	Yes	
2.	System will show message of "wrong credential"	Yes	
3.	Password must not be shown in the text box in the login page	Yes	
4.	New users must go through first time login and change password	Yes	
5.	Users with new device must go through new device login and wait for 12 hours to enter the system	Yes	
6.	System will request and detects the location of user during scanning QR code process	Yes	
7.	System will show message of "You are too far from the kiosk, please scan at the kiosk provided."	Yes	
8.	The SESSION variable can be used after the entering the correct credentials.	Yes	
9.	Email OTP able to send to user for first time login, new device and forgot password	Yes	
10.	User able to get shuffled CAPTCHA after requesting OTP	Yes	
11.	The QR code able to detect the location of the user during scanning the QR code for attendance module	Yes	
12.	An error message will prompt if user scan outside the radius	Yes	
13.	OTP expired in 1 minute	Yes	
14.	The password will be hash before stored into database	Yes	
15.	Error message will be shown if use expired OTP	Yes	
16.	Error message will be shown if user put the incorrect arrangement CAPTCHA images	Yes	
17.	After requesting an OTP, CAPTCHA images will appear	Yes	
18.	Refresh webpage will not give new OTP	Yes	

5.2.1 User Acceptance Test

User testing is performed using Google Forms, evaluated by two system administrators, eleven staff and two superiors from Pejabat Pendidikan Daerah Hulu Langat. The Google Form consists of two sections: Section A for the system interface and Section B for system functionality. In Section A, users rate the interface on a scale from one (very dissatisfied) to five (very satisfied). In Section B, users indicate whether the system functionality meets expectations by selecting pass or fail. This testing process ensures the Go2Work system meets client requirements.

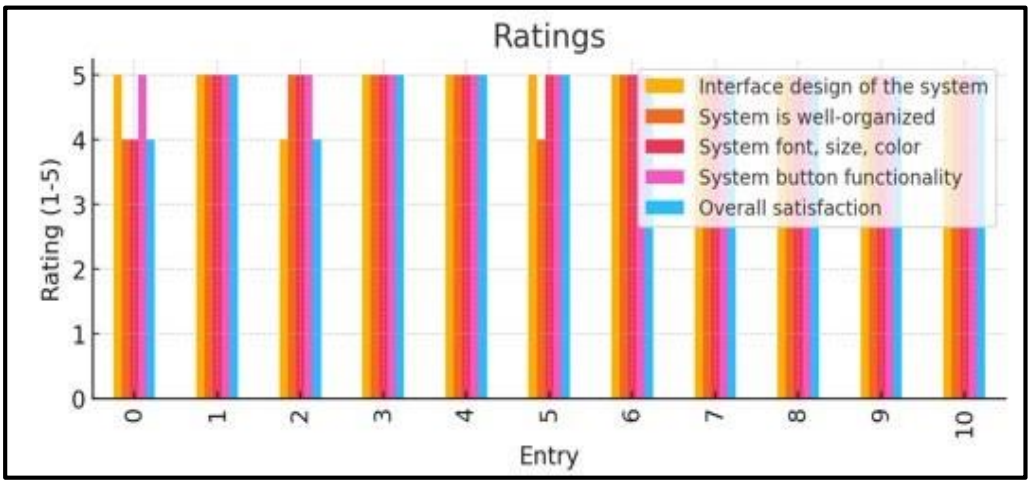

Fig. 32 *System design testing result*

Fig. 32 illustrates user feedback on various aspects of a system, ranging from the interface design to overall satisfaction. Each of the 13 entries, numbered from 0 to 10, represents individual user ratings across five categories: interface design, organization, font and color scheme, button functionality, and overall satisfaction. These ratings are depicted on a scale from 1 to 5, with 5 being the highest. The chart reveals a general trend of

high satisfaction, as indicated by the consistently elevated bars across most categories. The system's interface design and organization received particularly strong positive feedback, reflecting a well-structured and visually appealing user experience. Additionally, aspects like font, color, and button functionality were also rated favorably, indicating that users found these elements effective and user-friendly. Overall, the chart suggests that users are largely satisfied with the system, with most ratings clustering at the higher end of the scale, demonstrating a successful implementation in meeting user expectations and needs.

6. Conclusion

The Go2Work attendance system, enhanced by the CAOQTP algorithm, has proven to be a robust and effective solution for managing staff attendance at Pejabat Pendidikan Daerah Hulu Langat. The system successfully integrates QR code scanning with the dual verification process of CAPTCHA and OTP, providing a high level of security and ensuring accurate attendance tracking.

Despite its strengths, the system does face some limitations, such as the need for a dedicated QR code scanner application, dependency on internet connectivity, and potential challenges for less tech-savvy users. Addressing these limitations through future improvements, such as developing a dedicated application, enhancing offline functionality, and making the CAOQTP process more user-friendly, will further enhance the system's effectiveness and user satisfaction.

The implementation of additional features, such as scalability enhancements, advanced security measures, a resend OTP feature, and integration with other management systems, will ensure that the Go2Work attendance system continues to meet the evolving needs of its users. Overall, the system has demonstrated its capability to provide a secure, efficient, and user-friendly solution for attendance management, and with ongoing improvements, it will become an even more valuable tool for Pejabat Pendidikan Daerah Hulu Langat.

Acknowledgement

The authors would like to thank the Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia for its support.

Conflict of Interest

Authors declare that there is no conflict of interests regarding the publication of the paper.

Author Contribution

The authors confirm contribution to the paper as follows: ***study conception and design****: M. N. R. Mohd Khairi, N. B. Abd Warif;* ***data collection****: M. N. R. Mohd Khairi, N. B. Abd Warif;* ***analysis and interpretation of results****: M. N. R. Mohd Khairi, N. B. Abd Warif;* ***draft manuscript preparation****: M. N. R. Mohd Khairi, N. B. Abd Warif. All authors reviewed the results and approved the final version of the manuscript.*

References

[1] B. MacIej, E. F. Imed, and M. Kurkowski, "Multifactor Authentication Protocol in a Mobile Environment," IEEE Access, vol. 7, pp. 157185–157199, 2019,
[2] doi: 10.1109/ACCESS.2019.2948922.
[3] W. Ma, J. Campbell, D. Tran, and D. Kleeman, "Password entropy and password quality," in Proceedings - 2010 4th International Conference on Network and System Security, NSS 2010, 2010, pp. 583–587. doi: 10.1109/NSS.2010.18.
[4] M. H. Eldefrawy, K. Alghathbar, and M. K. Khan, "OTP-based two-factor authentication using mobile phones," in Proceedings - 2011 8th International Conference on Information Technology: New Generations, ITNG 2011, IEEE Computer Society, 2011, pp. 327–331. doi: 10.1109/ITNG.2011.64.
[5] L. Von Ahn, M. Blum, N. J. Hopper, and J. Langford, "CAPTCHA: Using Hard AI Problems for Security." [Online]. Available: http://www.spamarrest.com
[6] R. U. Rahman, D. S. Tomar, and S. Das, "Dynamic image-based CAPTCHA," in Proceedings - International Conference on Communication Systems and Network Technologies, CSNT 2012, 2012, pp. 90–94. doi: 10.1109/CSNT.2012.29.
[7] "PEK LING, W. (2012) INTEGRATED STAFF ATTENDANCE SYSTEM (ISAS). rep. Kuantan, PAHANG: WEE PEK LING, pp. 7–9.
[8] http://umpir.ump.edu.my/id/eprint/4420/1/CD6576_WEE_PEK_LING.pdf
[9] M. Martin, "Prototype model in software engineering."
[10] [Online]. Available: https://www.guru99.com/software-engineering-prototyping-model.html
[11] P. H. J. Chong, P. L. So, P. Shum, X. J. Li, and D. Goyal, "Design and Implementation of User Interface for Mobile Devices," 2004.