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

AITCS

Vol. 6 No. 2 (2025) 509-527
https://publisher.uthm.edu.my/periodicals/index.php/aitcs

Kumon Tuition Student Information Management and Academic Monitoring System with Secure Access Control and Data Privacy

Fatin Aqilah Mohd Puad[1], Zubaile Abdullah[1]*

[1] *Faculty of Computer Science and Information Technology*
Universiti Tun Hussein Onn Malaysia, Parit Raja, Batu Pahat, 86400, MALAYSIA

*Corresponding Author: zubaile@uthm.edu.my
DOI: https://doi.org/10.30880/aitcs.2025.06.02.028

Article Info

Received: 20 July 2025
Accepted: 19 November 2025
Available online: 30 November 2025

Keywords

Management Information System, Role-Based Access Control, Two-Factor Authentication, Web-Based System

Abstract

The Kumon Tuition Student Information Management and Academic Monitoring System with Secure Access Control and Data privacy aims to develop an information management system for students that includes academic tracking with security features. The current non-existing system results in disorganization and inefficiency in managing student data. Additionally, sensitive student data remains unprotected due to the absence of an existing system. The system implements security mechanisms such as two-factor authentication (2FA) using one-time password (OTP), Bcrypt for password hashing, role-based access control (RBAC) and reCAPTCHA. Agile methodology was used to ensure flexible and efficient development. The method of securing sensitive information and managing data interactions is applied in web-based academic platforms. The system is expected to address challenges in managing student data and protecting sensitive information, while providing key benefits such as reliability, efficiency, user-friendliness and security. A User Acceptance Testing (UAT) survey involving admins, parents, and teachers showed 100% agreement on all functional, usability, and security aspects, except one disagreement on unauthorized access, confirming effective role-based access control. The system demonstrates significant improvements in reliability, efficiency, and data security for managing student tuition information.

1. Introduction

In today's digital era, Management Information Systems (MIS) enhanced efficiency, decision-making and competitiveness across industries, including education. MIS streamlines administrative tasks, supports educators and improves learning experiences through better data management [1]. Kumon is a popular math and reading program that helps students learn independently through worksheets. Teachers give lessons and check progress, but managing all the student data can be time-consuming. This is where Management Information Systems (MIS) could help.

Kumon centers currently rely on paper-based systems, making student data management slow and disorganized without a centralized Management Information System (MIS). This leads to inefficiencies in tracking progress, security risks and limited parent access to student records. The developed MIS automates registration, attendance, classwork and performance tracking while enhancing security through two-factor authentication, role-based access and data encryption [2]. By digitizing operations, the system reduces

administrative workload, improves accuracy and safeguards student information, addressing key challenges in Kumon current setup.

Kumon centers currently rely entirely on paper folders to store student records, attendance and classwork, leading to disorganization and security risks. Physical folders often get misplaced, making it hard for teachers and students to track progress, while unprotected sensitive data raises privacy concerns. Parents also struggle to monitor their child performance since records remain at the center. Manual processes increase errors like incorrect classwork assignments or lost folders, forcing teachers to recreate lost data [3]. A digital system would prevent these issues by securely organizing records and allowing real-time progress tracking.

The new Kumon Student Management System replaces paper records with a secure digital platform, solving current organizational and security issues. It implements registration, student management and progress monitoring while implementing strong security measures like two-factor authentication, password hashing, role-based access control, and reCAPTCHA [4]. Teachers save time on recording student academic performance, parents gain real-time access to student progress and sensitive data remains protected [5], making education management as secure as online banking systems.

2. Literature Review

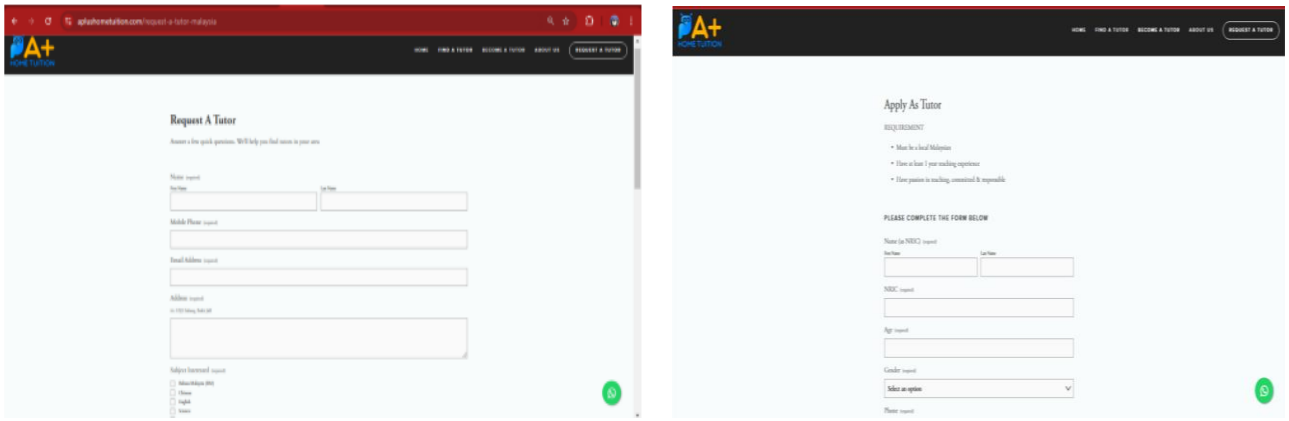
This section discusses the literature review that has been done related to the management information system including authentication, one-time password (OTP), password hashing, access control, reCAPTCHA and comparison between existing systems and the developed system.

2.1 Study of Related System

A study of related systems is conducted by examining existing student information management and academic monitoring systems with security features. The aim is to gain insights into their functionality and security implementations, allowing for relevant comparisons and the identification of best practices that could be applied to the Kumon Tuition Student Information Management and Academic Monitoring System with Secure Access Control and Data Privacy.

2.1.1 A+ Home Tuition

A+ Home Tuition [6] is a web-based tutoring system in Malaysia offering home and online tuition services for students from primary school to university, covering all subjects. The system has a user-friendly, minimalist interface designed for students but lacks key functionalities like account registration and academic monitoring. It also lacks security features such as authentication, user login, sign-up or password hashing. Users are not required to create accounts. Instead, they can use forms for tutor applications and student tutor requests, which function like registration without the need for password creation. Fig. 1 shows the student tutor request page and application page.

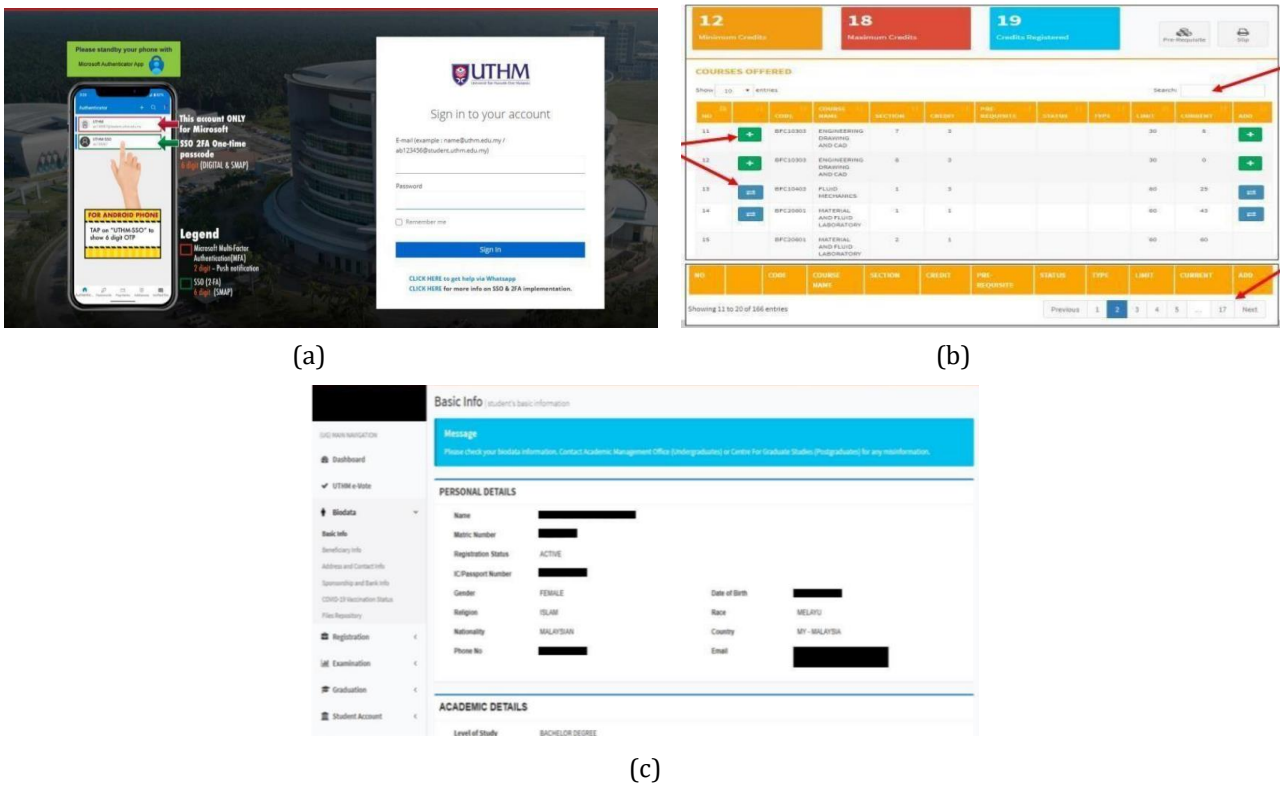


(a) (b)

Fig. 1 *A+ Home Tuition (a) Tutor request page*; *(b) Tutor application page*

2.1.2 UTHM Student Academic Information Management (SMAPOnline)

UTHM SMAP Online (Sistem Maklumat Akademik Pelajar) [7] is the academic information management system used by Universiti Tun Hussein Onn (UTHM), providing students, faculty and staff access to services like course registration, exam results, academic records and financial status. It features security measures such as password hashing, role-based access control (RBAC) and two-factor authentication (2FA) using Microsoft Authenticator, which generates a 30-second OTP for verification. Fig. 2 shows the system login page, course registration page and basic info page.



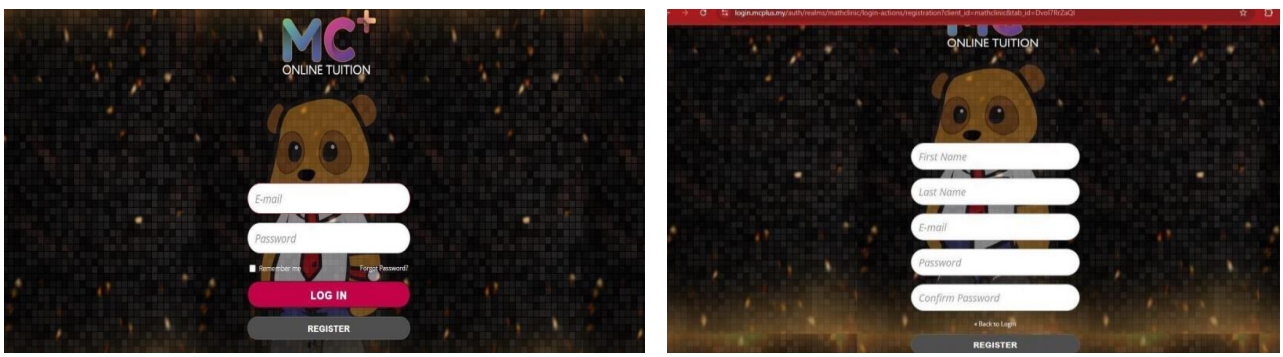
(a) (b)

(c)

Fig. 2 *UTHM SMAP (a) Login page*; *(b) Course registration page; (c) Student basic info page*

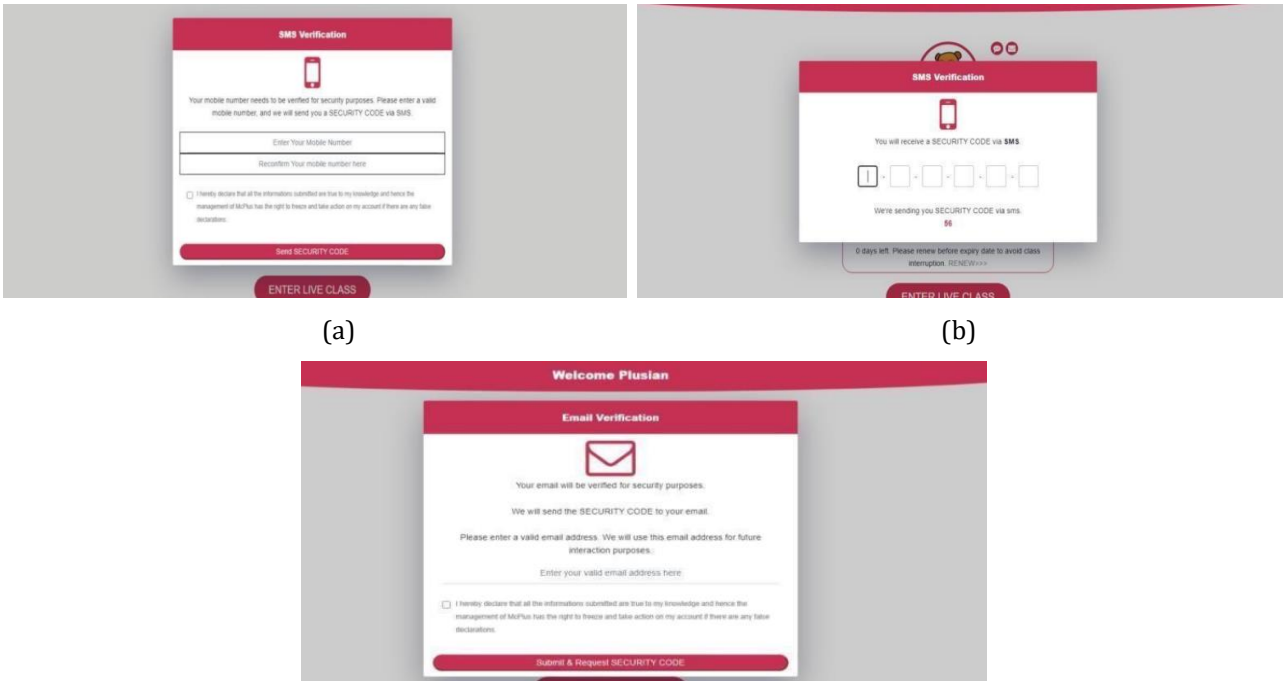
2.1.3 MCPlus Online Tuition (MC+)

MCPlus [8], a Malaysian online education organization founded during the pandemic in April 2020, has become one of the country largest online tuition centers. The system features security measures like login and signup functionalities for new students. It also implements multi-factor authentication (MFA), requiring three factors such as user password, a verification code sent via SMS to the registered phone number and a code sent to the student registered email. The verification codes are time-sensitive, expiring after 60 seconds to ensure secure access to the system. Fig. 3 shows the login and signup pages, and Fig. 4 shows the verification process.



(a) (b)

Fig. 3 *MC+ (a) Login page*; *(b) Signup page*



(a) (b)

(c)

Fig. 4 *MC+ (a) Users provide mobile number page*; *(b) SMS verification code page; (c) Users provide email*

2.1.4 Comparison Between Related System and Developed System

Table 1 shows the comparison between three related systems, A+ Home Tuition [6], UTHM SMAP Online [7] and MCPlus Online Tuition [8] to identify and gain insights into their functionalities and security features, providing a basis for comparison with the developed system.

Table 1 *Comparison Between Related System and Developed System*

System/Feature	A+ Home Tuition [6]	UTHM Student Academic Information Management (SMAPOnline) [7]	MCPlus Online Tuition [8]	Kumon Tuition Information Management and Academic Monitoring System with Secure Access Control and Data Privacy
Platform	Web-based	Web-based	Web-based	Web-based
Email and Password Login	No	Yes	Yes	Yes
Two-Factor Authentication (2FA)	No	Yes	Yes	Yes
Account or Course Registration	Yes	Yes	Yes	Yes
Password Hashing	No	Yes	No	Yes
Academic Monitoring	No	Yes	No	Yes
Role-Based Access Control	No	Yes	No	Yes
reCAPTCHA	No	No	No	Yes
Organized Student Information	No	Yes	No	Yes

The developed Kumon system stands out by combining advanced security features such as 2FA, password hashing, RBAC, and reCAPTCHA with academic monitoring and organized student data management. Unlike A+ Home Tuition and MCPlus, which lack both strong security and academic tracking, and UTHM SMAP which is university-focused, this system offers a comprehensive, secure, and user-friendly platform tailored specifically for tuition centers.

2.2 Management Information System

Management Information System (MIS) is a structured framework designed to efficiently collect, manage, and store information from various sources, enhancing business operations and decision-making [9]. It uses tools like MySQL, Oracle and Microsoft SQL Server to organize data and ensure security through encryption, access controls and backups. MIS architecture includes a data management layer for storage, an application layer for processing, and a user interface layer for accessibility, all contributing to improved productivity and professional data handling [10].

2.3 Access Control

Access control is a security mechanism that regulates who can access systems and data, ensuring confidentiality, integrity and availability. It grants permissions based on verified identities and can include types like Discretionary Access Control (DAC), Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) [11]. Access control is vital for protecting sensitive information but can be challenging to manage, especially in large organizations with frequent personnel changes, as seen in systems like UTHM network access control.

Role-Based Access Control (RBAC) is a widely implemented access control function that grants access to authorized users based on their roles and privileges within an organization. A role in RBAC defines a set of permissions based on job positions held by employees, making it easy to manage and update access. RBAC follows the principle of least privilege by granting permissions based on roles, which helps safeguard sensitive data and reduce the risk of data breaches. Additionally, RBAC supports auditing by tracking activities such as who did what in the application, providing a way to monitor actions within the organization [12].

2.4 Authentication

Authentication verifies the identity of individuals, devices or systems before granting access, ensuring users are who they claim to be [13]. It secures sensitive systems and prevents unauthorized access through methods like passwords, biometric traits and OTPs. Authentication types, including single-factor, two-factor and multi-factor authentication, offer varying security levels, with multi-factor preferred for sensitive data. However, vulnerabilities like weak passwords and brute-force attacks highlight the need for strong, complex passwords. The Kumon Tuition Student Information Management System implements authentication to safeguard organizational data.

Two-factor authentication (2FA) strengthens security by requiring two authentication factors from categories such as something you know, have, or are. This additional layer of protection reduces risks even if one factor is compromised, making it more secure than single-factor methods. Organizations handling sensitive data commonly use 2FA with tokens like hardware devices, app-generated codes or SMS or email-delivered codes [14].

2.5 One-Time Password (OTP)

One-Time Password (OTP) is a widely used authentication mechanism employed by companies, institutions and governments to enhance security strategies [15]. OTP generates a unique, temporary code valid for a single login session or transaction, typically expiring within 30 seconds, minimizing the risk of attacks like phishing. Common OTP types include time-based OTP (TOTP), push notification OTP, SMS OTP and email OTP, providing high security and convenience for sectors like e-commerce, online banking and healthcare. Its short validity and single-use nature make OTP significantly more secure than traditional password-based methods.

Email OTP is another effective authentication method, frequently used for login verification or password resets, as it enables users to receive codes on registered email addresses accessible from any internet-enabled device [16]. While widely used, it is vulnerable to phishing attacks where attackers mimic legitimate email addresses to trick users. PHPMailer, an open-source PHP library, is often used to send email OTPs efficiently and securely.

2.6 Hashing Algorithms

Hashing algorithms are cryptographic functions that convert a password into a fixed-length string, known as hash, which is stored in a database for enhanced security. The hash cannot easily be reversed, ensuring password integrity. A salt function adds random data before hashing, further strengthening security by making it harder for attackers to use brute-force attacks or rainbow tables. Common hashing algorithms include SHA-1, MD5, SHA-256 and Bcrypt, with tools like Secrets used to generate cryptographically strong random strings for salting, ensuring password confidentiality is maintained [17].

2.7 reCAPTCHA

reCAPTCHA, developed by Google, is a security feature used to distinguish between human users and automated bots, protecting websites and systems from unauthorized access, spam submissions and brute-force attacks. It presents challenges like identifying images or verifying distorted text that are easy for humans but difficult for bots. Integrated into online forms and login pages, reCAPTCHA provides an extra layer of protection to safeguard sensitive information and reduce the risk of automated breaches.

3. Methodology

This section discusses the methodology used in the development of the system, which is agile model including planning phase, design phase, development phase, testing phase, deployment phase, review phase, launch phase and project planning.

3.1 Agile Software Development Model

This project used the Agile methodology, which involved seven phases including planning, design, development, testing, deployment, review, and launch. Its iterative nature allowed flexibility and ongoing improvements based on feedback. The process began with planning and identifying user needs through stakeholder interviews. Design phases included flowcharts and system design diagrams. Development was done step by step, allowing changes when needed. Testing ensured the system worked properly and it was then deployed locally using XAMPP. Feedback from users and the supervisor was used to make improvements and meet expectations. Finally, the system was launched after all essential modules were completed and tested. Fig. 5 shows the agile methodology.

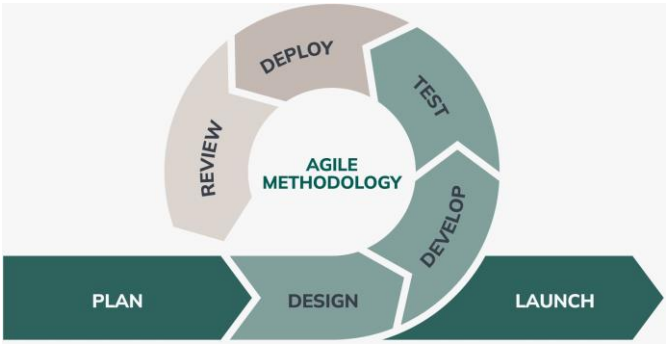


Fig. 5 *Agile Methodology*

The first phase of the project using Agile methodology is the planning phase, where all the important system needs were identified. The system aims to offer a secure and user-friendly platform for the owner, teachers and parents. Requirements were gathered through interviews. The owner requested secure access, proper data handling and report generation. Teachers needed features to key in performance, manage attendance and track progress. Parents wanted to register their children and view their academic performance. These needs helped guide the design of a secure web-based system with features like two-factor authentication, RBAC and password hashing. This phase also involved identifying the right software tools, programming languages and hardware needed to ensure the system runs efficiently.

The design phase focused on turning user needs into system plans through mock-ups and diagrams. For the Kumon Tuition Student Information Management and Academic Monitoring System, mock-ups like parent and student registration, dashboards and classwork pages helped visualize the system early. Design tools such as the DFD, ERD, context diagram and system flowchart were used to show data flow, system structure and user interaction. This phase ensured everything was well-organized before development began.

The development phase is where the Kumon system was built into a working application based on the earlier designs. This phase involved coding the main features and adding security elements like password hashing and role-based access. Tools like Visual Studio Code were used for both frontend and backend development using HTML, CSS, PHP and JavaScript to create user-friendly interfaces. XAMPP provided a local server environment that made it easier to install and run components like the Apache web server and MySQL (MariaDB) database. It is a software package that includes Apache, MySQL, PHP and phpMyAdmin, which helped in managing databases and testing PHP functions during development. For example, the registration form was tested using PHP and MySQL within XAMPP to ensure it functioned correctly before local deployment.

The testing phase is important to make sure the Kumon system works smoothly, is secure and meets user needs. This phase helps find bugs, improve system functions and ensure a user-friendly interface. Unit testing was done by developers to check each part, like login and OTP verification, and to test student data and

performance tracking. User acceptance testing (UAT) involved teachers, parents and the admin to confirm that the system works as expected. For example, teachers tested classwork and attendance features, while parents tested registration, login, and OTP. Testing also checked password strength and proper error handling.

The deployment phase is when the Kumon system is launched for real-world use. After testing, the system is improved with new features, bug fixes and monitored regularly to ensure smooth performance. Feedback from users like teachers, parents and admins is collected to spot issues and improve the system in future updates. This helps make the system more secure, user-friendly, and suited to user needs.

The review phase is the final step in the Agile methodology, where the system is evaluated and improved based on feedback from teachers, parents, and admin. The system is demonstrated to show its features, like student registration, academic tracking, and login security. Stakeholders test the system and suggest improvements, such as adding a password strength checker or improving the dashboard layout. This phase helps ensure the system meets user needs and regular updates are made to keep it secure, stable and easy to use.

The launch phase is where the Kumon system is fully released and made ready for actual use by parents, teachers and admins. After completing all the previous phases and applying necessary improvements based on feedback, the system is now stable, secure and user-friendly. It can be accessed through a web browser, allowing users to perform real tasks like registration, monitoring and updating student data. This phase marks the completion of the development process and the beginning of real-world usage.

3.2 Project Planning

Project planning is vital for managing this project as it establishes a clear, organized plan from inception to completion. It helps developers anticipate challenges and minimize errors during development. Involving stakeholders in the planning process ensures feedback is gathered, user requirements are understood and project goals are achieved. Table 2 shows the tasks and outcomes of each phase in project planning using Agile methodology.

Table 2 *Software requirements for the developed system*

Phase	Task	Outcome
Planning	Conduct stakeholder interviews, justify software and hardware requirements and identify issues in the non-existing system.	Collect stakeholder data on user requirements, identify the suitable programming language and web server, define hardware specifications and propose solutions to address the issues.
Design	Create a prototype with a basic UI design for user modules, showcasing functionalities and security features.	Develop a visual model of the system structure with a clear, user-friendly design for modules and define functionalities and security features.
Development	Transform the basic design into a fully functional system using Visual Studio Code for webpage creation and MySQL in XAMPP for managing student information.	A fully functional and user-friendly interface for the developed system.
Testing	Perform unit testing on security features and conduct user acceptance testing with the end-user.	Ensure security features function as intended and verify system functionalities from the user perspective to ensure alignment with user needs.
Deployment	Release the completed system for user access and make improvements and updates to enhance its user-friendliness.	The system is deployed and ready for use, with ongoing enhancements to functionalities and bug fixes.
Review	Showcase the finished system to stakeholders, gather their feedback and monitor system operations and performance.	Stakeholders evaluate the system progress to ensure it aligns with their needs, and their feedback helps assess the system. Regular monitoring identifies any unusual activities.
Launch	Officially release the system for real-world use, provide access to users and monitor system behavior after launch.	The system is fully operational and accessible to intended users such as admins, teachers and parents, ensuring a smooth transition from development to active use.

4. System Analysis and Design

This section outlines system analysis and design, covering the requirements needed to meet its goals, including functional and non-functional requirements. It justifies the system analysis using tools like the Data Flow Diagram, context diagram and Entity Relationship Diagram and then discusses system and interface design.

4.1 Functional and Non-Functional Requirements Analysis

System requirements explain what the system needs to work properly and meet user needs. These include functional and non-functional requirements. Functional requirements are defined as the processes and tasks that the system must perform to support user activities and ensure it meets their needs. These requirements explain the functionalities of the system and the actions carried out by the system to assist users in completing the tasks. Functional requirements play a vital role in making the system functionalities effective and deliver tasks that align with user expectation. Table 3 shows the functional requirements, outlining the key capabilities needed to manage the Kumon Tuition Student Information Management and Academic Monitoring System with Secure Access Control and Data Privacy effectively.

Table 3 *Functional Requirements*

Module	Functionalities
Register	Parents can create account and register student in the system while admin can create teacher account.
Login	Users can login to their account using email and password with two verification steps such as reCAPTCHA and OTP.
Forgot password	Users able to reset passwords by verifying themselves with OTP verification.
Data management	Admin able to read, update and delete students and teachers' information.
Generate reports	System generates reports of students and teachers' records.
Academic monitoring	Teachers able to key in student academic performance and test result while parents can monitor them.
Classwork assessment	Teachers able to assign classwork for students, track and record student submission and attendance while parents can monitor them.
Change password	Users are allowed to change password.

Non-functional requirements define the performance and feature necessary for the system to operate efficiently and meet user needs, including speed, security, usability and a user-friendly interface. These requirements are crucial for ensuring the system is reliable, efficient, secure and user-friendly. Table 4 outlines the key non-functional requirements for managing the Kumon Tuition Student Information Management and Academic Monitoring System with Secure Access Control and Data Privacy effectively.

Table 4 *Non-Functional Requirements*

Category	Non-Functionalities
Performance	The system must perform quickly without issues and handle a large volume of user data.
Security	The system secure user data by implementing two-factor authentication, role-based access control, password hashing, reCAPTCHA verification and session expiration timeout.
Operation	The system should be easy to use with a user-friendly interface, available most of the time for user access and compatible with any web browser.

4.2 System Analysis

System analysis helps developers understand the system by identifying its purpose, data flow and user interactions. It is divided into three parts, the Context Diagram illustrates interactions with external entities, the Data Flow Diagram Level 1 (DFD) shows how data moves through the system and the Entity Relationship Diagram (ERD) highlights relationships between data entities.

4.2.1 Context Diagram

The Context Diagram provides a high-level view of the system's interaction with external entities like students, teachers and administrators. It helps stakeholders understand system processes, including data flows such as student registration, academic performance and classwork assessment. Fig. 6 illustrates the context diagram for the Kumon Tuition Student Information Management and Academic Monitoring System.

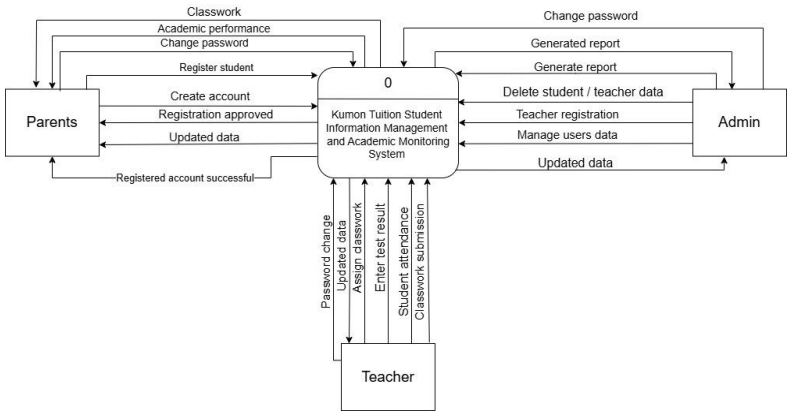


Fig. 6 *Context Diagram for the Kumon Tuition Student Information Management and Academic Monitoring System*

4.2.2 Data Flow Diagram Level 1 (DFD)

Data Flow Diagram (DFD) Level 1 gives a clearer picture of how data flows in a system by showing the connections between external entities, processes and where data is stored. This diagram includes important stakeholders like users and other systems, highlighting how they interact and exchange information. Unlike DFD Level 0, which shows just one overall process, Level 1 breaks this down into several subprocesses. For example, in the DFD Level 1 for the Kumon Tuition Student Information Management and Academic Monitoring System, you can see all the different interactions and data movements, helping everyone involved to understand how the system works without going into too much detail. For the Kumon system, DFD Level 1 helps show the flow of data between users and the system, as shown in Fig. 7.

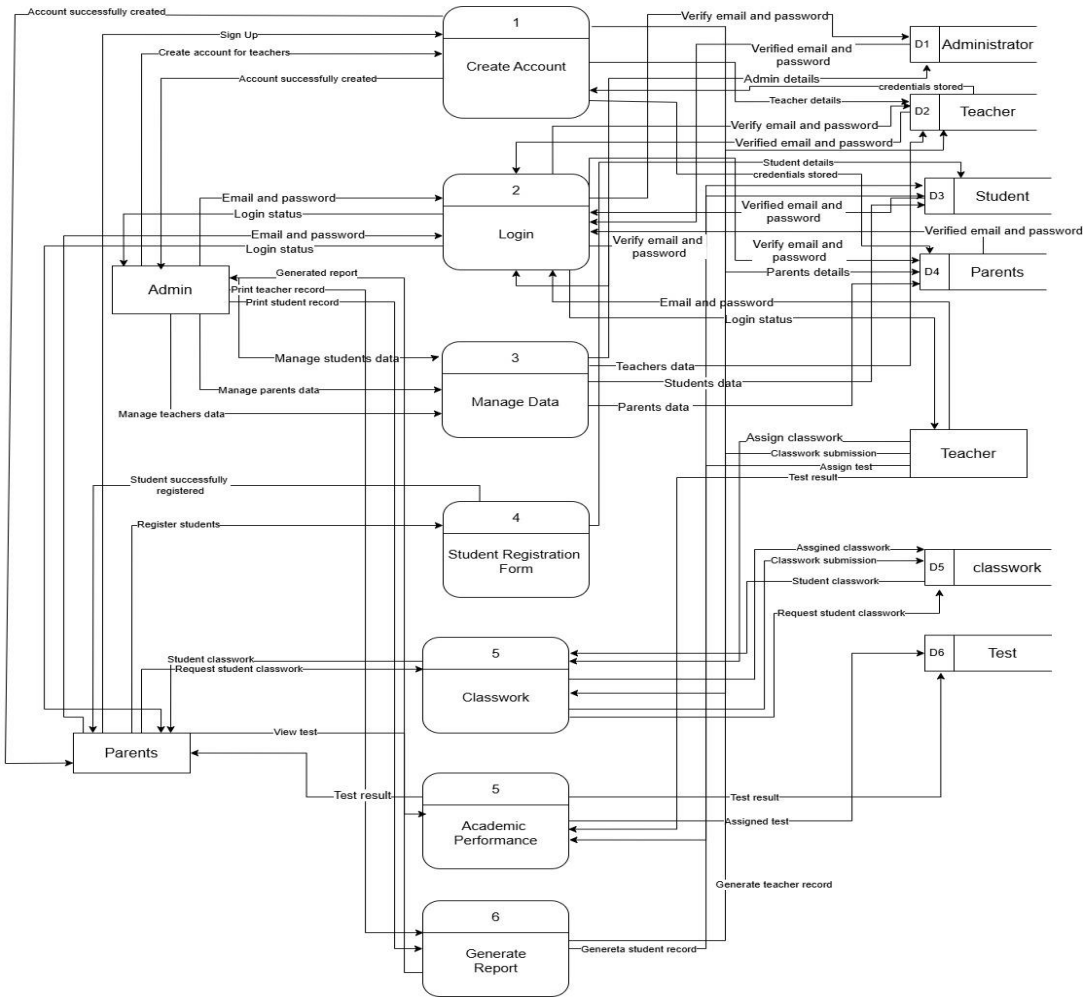


Fig. 7 *Data Flow Diagram (DFD) Level 1 for the Kumon Tuition Student Information Management and Academic Monitoring System*

4.2.3 Entity Relationship Diagram (ERD)

Entity Relationship Diagram illustrates how entities such as admin, teacher and student relate to each other within a system. It shows the information that is created, stored and used by a system. ERD symbol can show when one instance of an entity can be related to only one or to many instances of another entity such as relationships among entities in database. Fig. 8 shows Entity Relationship Diagram (ERD) for the Kumon Tuition Student Information Management and Academic Monitoring System

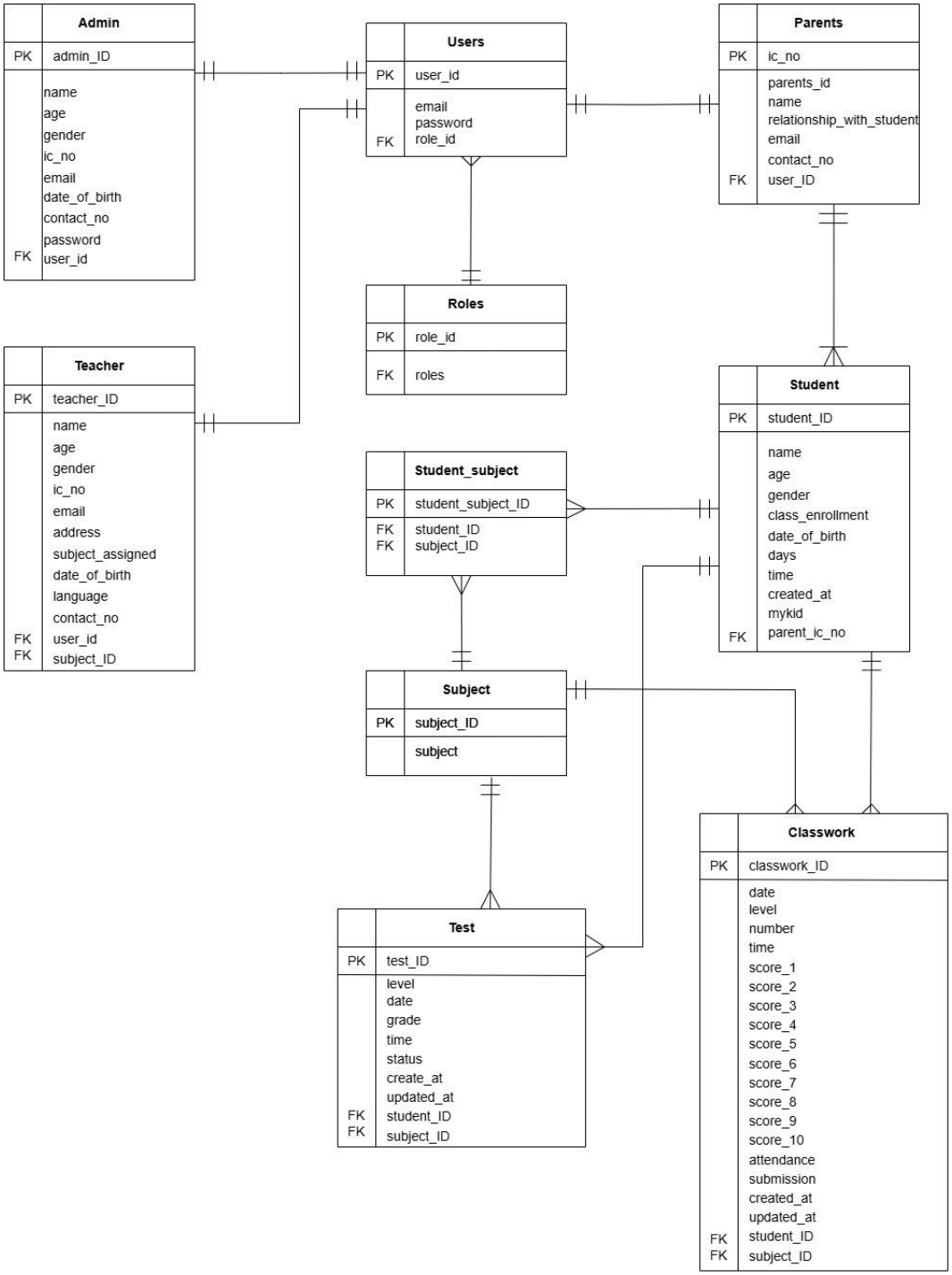


Fig. 8 *Entity Relationship Diagram (ERD) for the Kumon Tuition Student Information Management and Academic Monitoring System*

4.2.4 System Flowchart

A flowchart visually represents the steps or workflow within a process, illustrating the system operations, including processes, decisions, inputs and outputs, helping stakeholders understand actions and decisions. Fig.s 9 show various interfaces of the Kumon Tuition Student Information Management and Academic Monitoring System. The home interface, the parent interface, the teacher interface and the admin interface.

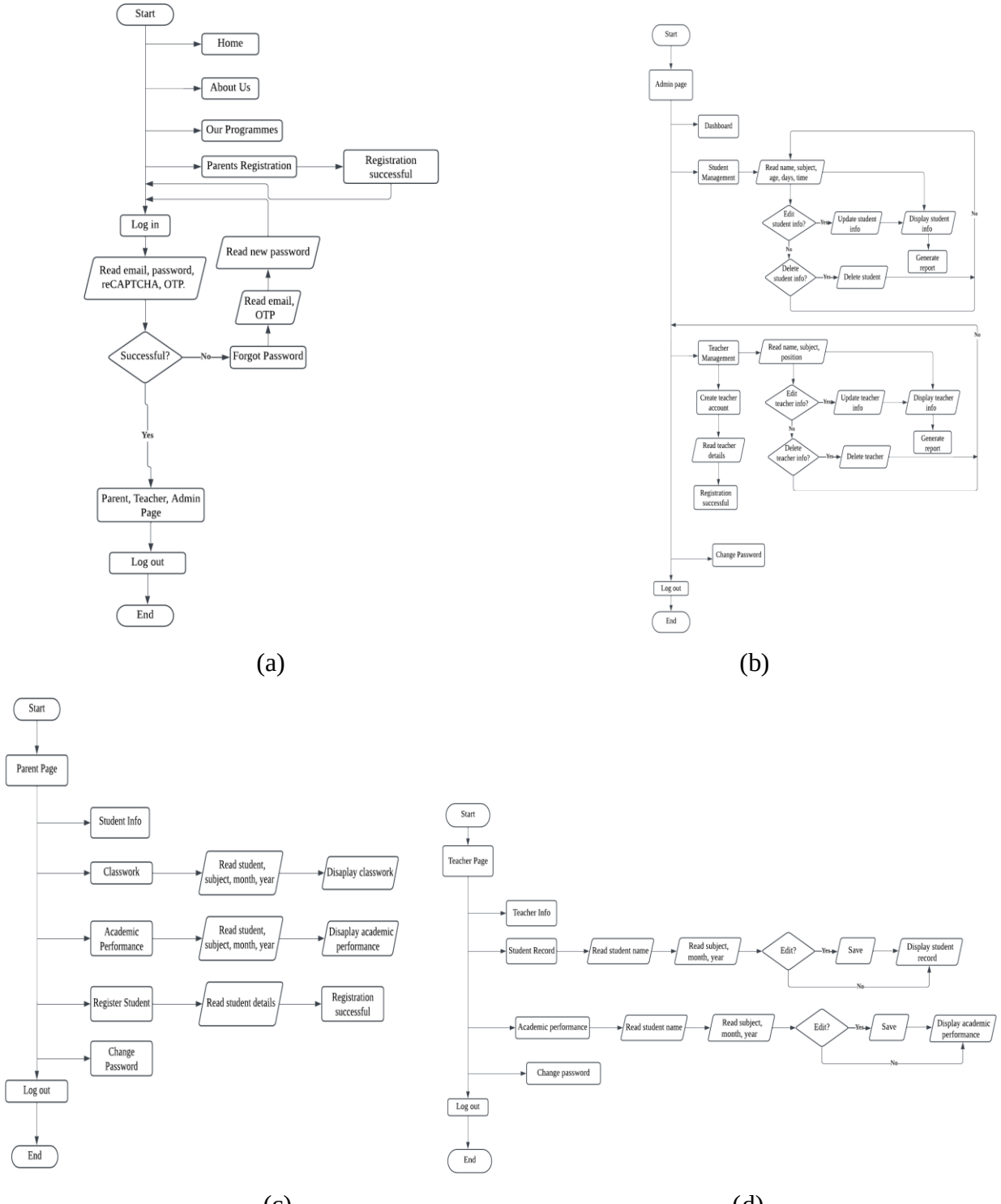
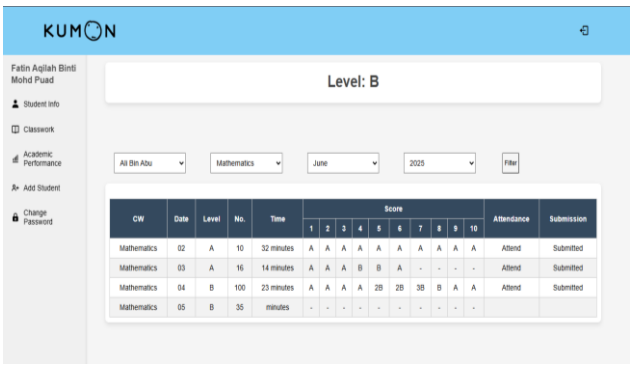


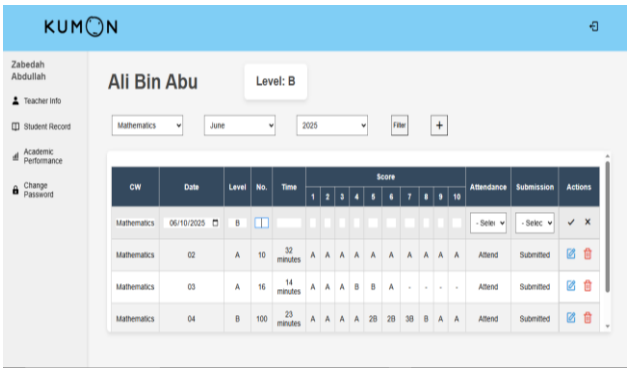
Fig. 9 *Flowchart of Kumon Tuition Student Information Management and Academic Monitoring System (a) Home interface; (b) Admin interface; (c) Parent interface; (d) Teacher interface*

4.3 Interface Design

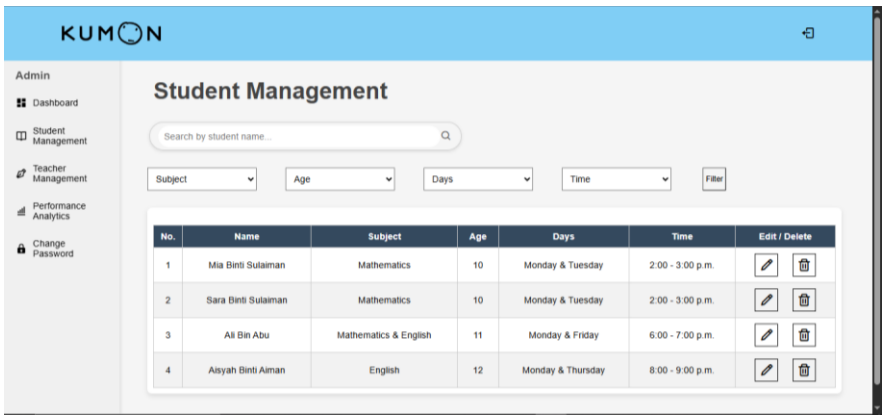
This section illustrates the user interface design wireframe for Kumon Tuition Student Information Management and Academic Monitoring System. Creating a visually appealing and user-friendly experience for students, administrators and teachers is essential. Fig. 10 present the user interface of the system including admin interface, student interface and teacher interface.



(a)



(b)



(c)

Fig. 10 *User Interface (a) Parent Interface*; *(b) Teacher Interface; (c) Admin Interface*

5. Implementation and Testing

This section discusses about system implementation and testing, where the system is fully built and checked to make sure everything works properly. During implementation, the main functions based on stakeholder requirements were developed including the security features to ensure the system is secured. Testing was done to identify issues and vulnerabilities that need to be addressed.

5.1 Implementation of Security Module

This section outlines the implementation of various security mechanisms in the Kumon system to protect user data and ensure secure access. The key features include two-factor authentication (2FA), password hashing, reCAPTCHA, session timeout, strong password and role-based access control.

5.1.1 Two-Factor Authentication (2FA)

The system implemented two-factor authentication in both the login and forgot password pages, where users must enter their email, password and a one-time password (OTP) to access the system. The OTP is sent to the user registered email and is valid for only 30 seconds. If not used within this time frame, the OTP expires and becomes invalid, adding an extra layer of security against unauthorized access. Fig. 11 shows the implementation of password, one-time password (OTP), login page and OTP that is sent to the email.

```php
// Verify password
if (password_verify($password, $user['password'])) {
    $role_stmt = null;
    $session_key = '';
    $redirect_page = 'logout.php';
```

(a)

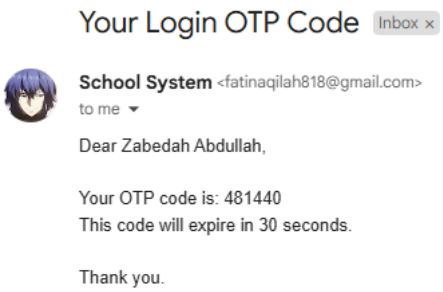
```php
// Handle OTP verification
if (isset($_POST['verify_otp'])) {
    if (
        !isset($_SESSION['otp']) || !isset($_SESSION['otp_created_at']) ||
        time() - $_SESSION['otp_created_at'] > 30
    ) {
        $otp_error = "OTP expired. Please
        unset($_SESSION['otp'], $_SESSION['otp_created_at'], $_SESSION['otp_user_data']);
        $show_login_form = true;
    } elseif ($_POST['otp'] == $_SESSION['otp']) {
        // OTP is valid, log the user in
        $_SESSION = array_merge($_SESSION, $_SESSION['otp_user_data']);
        unset($_SESSION['otp'], $_SESSION['otp_created_at'], $_SESSION['otp_user_data']);
        header("Location: {$_SESSION['otp_redirect_page']}");
        exit();
    } else {
        $otp_error = "Invalid OTP code.";
        $show_otp_form = true;
    }
}
```

@var mixed

(b)

(c)

(d)



(e)

Fig. 11 *Two-Factor Authentication (a) Verify Password*; *(b) Verify OTP; (c) Login Page*; *(d) OTP Verification Page (c) Email OTP*

5.1.2 Password Hashing

The system used Bcrypt with salting to securely store user passwords, providing strong protection against common attacks like brute-force and rainbow table attacks. When a user sets or changes a password, the system automatically generates a unique salt and uses Bcrypt to hash the password. This ensures that even if two users use the same password, their stored hashes will be different due to the random salt. The fixed hash length of Bcrypt is 60 characters, it ensures consistency in storage, regardless of the original password length. Fig. 12 shows the implementation of password hashing using Bcrypt in registration page and the hashed password in database.

```php
$role_id = 3;

// Hash the password before storing it
$hashed_password = password_hash($password, PASSWORD_DEFAULT);

// Insert into users table first
$userSql = "INSERT INTO users (email, password, role_id) VALUES (?, ?, ?)";
$userStmt = $conn->prepare($userSql);
$userStmt->bind_param("ssi", $email, $password, $role_id);
```

(a)

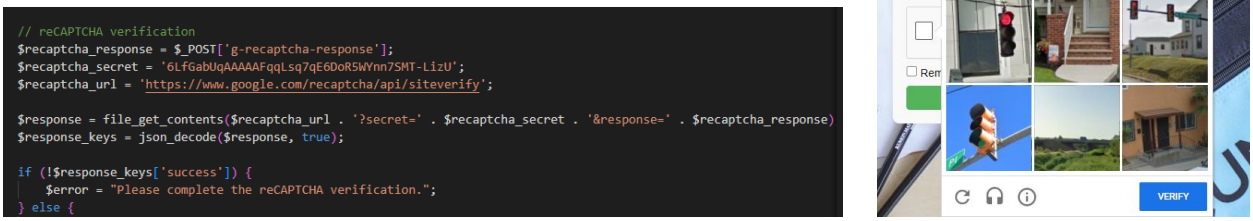
user_id	email	password	role_id
1	ravenmoonworld@gmail.com	$2y$10$/VcOHy/hvzkiLkZZm/GPC.ZtmkI6XYmGTAaJUBV.cp0...	1
2	fatinaqilah@gmail.com	$2y$10$dY7JEQ/m5FlQr4Cj6i40Bu8j40Nr5N9yV5luAyKYP10...	3
3	fatinaqilah818@gmail.com	$2y$10$PpzkC7T..PS5y76.T5KvLOVEsy3.hy9PSGVP3.RVEux...	2
6	atika@gmail.com	$2y$10$etd5H8IIAOtvieMkaG4DEuG062Swng.1J1O9XdJoGBX...	3
12	nizam@gmail.com	$2y$10$mOdlAMPGFSWbygj1xXDd2ev65nV754zE3gkTSwA.BYE...	2
13	farhan@gmail.com	$2y$10$hX.8Sj7HNI8d7BD1/NDH4OdMAwZ9K5pmV0xLNdkvG4V...	2
14	syakila@gmail.com	$2y$10$ERpPCMVY2DVrAPugjxCsjuXTuuGm6qXYbwFWOV/O5LM...	2

(b)

Fig. 12 *Password Hashing (a) Hash Password in Registration Coding*; *(b) Hashed Password in Database*

5.1.3 reCAPTCHA

The system implemented reCAPTCHA in the login page to prevent spam bots from accessing or abusing the system. It protects the system from spam submissions, brute-force attack and denial-of-service (DOS). reCAPTCHA able to distinguish between humans and bots by requiring users to complete a task, such as selecting images that reCAPTCHA asks for, like buses, cars, or stairs. User able to login successfully after completing the task. Fig. 13 presents the coding of reCAPTCHA and images task.



(a) (b)

Fig. 13 *reCAPTCHA (a) reCAPTCHA in Login Page; (b) reCAPTCHA Images Task*

5.1.4 Session Timeout

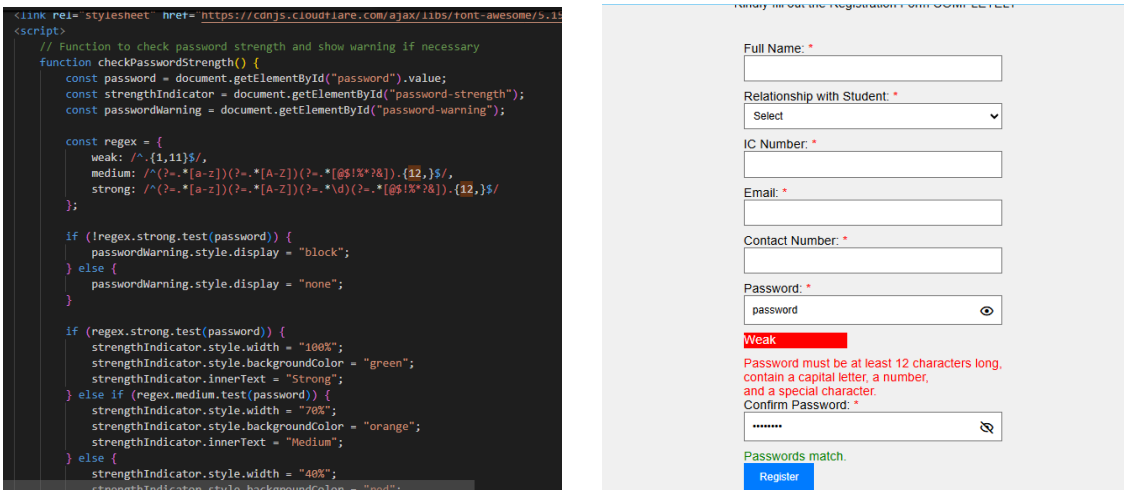
The system includes a session timeout feature set to 10 minutes. If a user remains inactive for this duration, they will be automatically logged out. This helps prevent unauthorized access, especially if someone forgets to log out on a shared or public device. It improves the security of the system by making sure inactive sessions are closed, reducing the chances of data being misused. A 10-minute timeout is considered suitable for educational systems, balancing convenience and security. If the user stays idle beyond this time and refreshes the page, they will be logged out and redirected to the login page. Fig. 14 shows the implementation of session timeout in all user pages.

```php
<?php
session_start();

// Set timeout duration in seconds (10 minutes)
$timeout_duration = 600;

// Check for timeout
if (isset($_SESSION['LAST_ACTIVITY']) && (time() - $_SESSION['LAST_ACTIVITY']) > $timeout_duration) {
    // Session expired
    session_unset();
    session_destroy();
    header("Location: login.php?timeout=1");
    exit();
}

// Update last activity time
$_SESSION['LAST_ACTIVITY'] = time();
```

Fig. 14 *Session Timeout*

5.1.5 Strong Password

The system applies strong password policies on the parent registration page, teacher registration page and change password page to enhance account security. Users are required to create strong passwords when registering or updating their account to protect against unauthorized access. If a weak password is entered, an error message will appear, indicating that the password is not secure and prompting the user to enter a stronger one. The system enforces passwords with at least 12 characters, including one uppercase letter, one number, and one special character, based on the NIST password guidelines. This helps ensure that users choose passwords that are difficult to guess or crack. Once a strong password is entered, a confirmation message will appear, stating that the password is strong. Fig. 15 the implementation of strong password and the password strength in parent registration page.

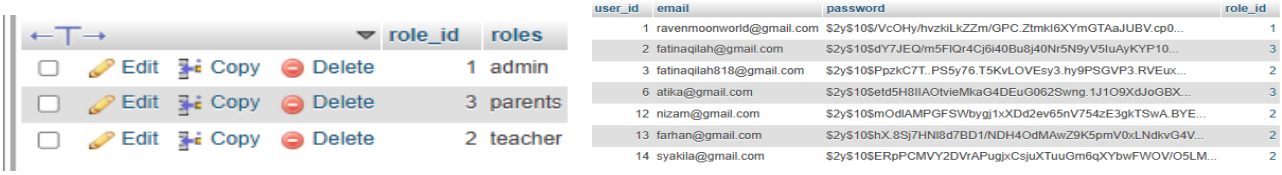


(a) (b)

Fig. 15 *Strong Password Policies (a) Check Password Strength*; *(b) Password Strength in Registration*

5.1.6 Role-Based Access Control

The most suitable access control to implement in the system is role-based access control (RBAC). It assigns a specific role to every user in the system to prevent users from accessing unauthorized features or data. Each role such as admin, teacher, or parent has defined permissions that limit what the user can view or do within the system. For example, teachers can manage classwork and student performance, while parents can only view the student progress. Admin can manage student and teacher data. This approach enhances security and ensures that sensitive information and functions are only accessible to authorized users based on their role. User roles have been predefined in the database. Fig. 16 shows the predefined roles in the database.



	role_id	roles
Edit Copy Delete	1	admin
Edit Copy Delete	3	parents
Edit Copy Delete	2	teacher

user_id	email	password	role_id
1	ravenmoonworld@gmail.com	$2y$10$/VcOHy/hvzkiLkZZm/GPC.ZtmkI6XYmGTAaJUBV.cp0...	1
2	fatinaqilah@gmail.com	$2y$10$dY7JEQ/m5FlQr4Cj6i40Bu8j40Nr5N9yV5IuAyKYP10...	3
3	fatinaqilah818@gmail.com	$2y$10$PpzkC7T..PS5y76.T5KvLOVEsy3.hy9PSGVP3.RVEux...	2
6	atika@gmail.com	$2y$10$etd5H8IIAOtvieMkaG4DEuG062Swng.1J1O9XdJoGBX...	3
12	nizam@gmail.com	$2y$10$mOdlAMPGFSWbygj1xXDd2ev65nV754zE3gkTSwA.BYE...	2
13	farhan@gmail.com	$2y$10$hX.8Sj7HNl8d7BD1/NDH4OdMAwZ9K5pmV0xLNdkvG4V...	2
14	syakila@gmail.com	$2y$10$ERpPCMVY2DVrAPugjxCsjuXTuuGm6qXYbwFWOV/O5LM...	2

(a) (b)

Fig. 16 *Role-Based Access Control (a) Roles table*; *(b) Users table*

5.2 Implementation of Module

Implementation of module streamline the implementation of various user modules for admin, teacher and parent in the Kumon Tuition Student Information Management and Academic Monitoring System with Secure Access Control and Data Privacy. This includes login module, registration module, classwork module, academic performance module and data management module.

5.2.1 Login Module

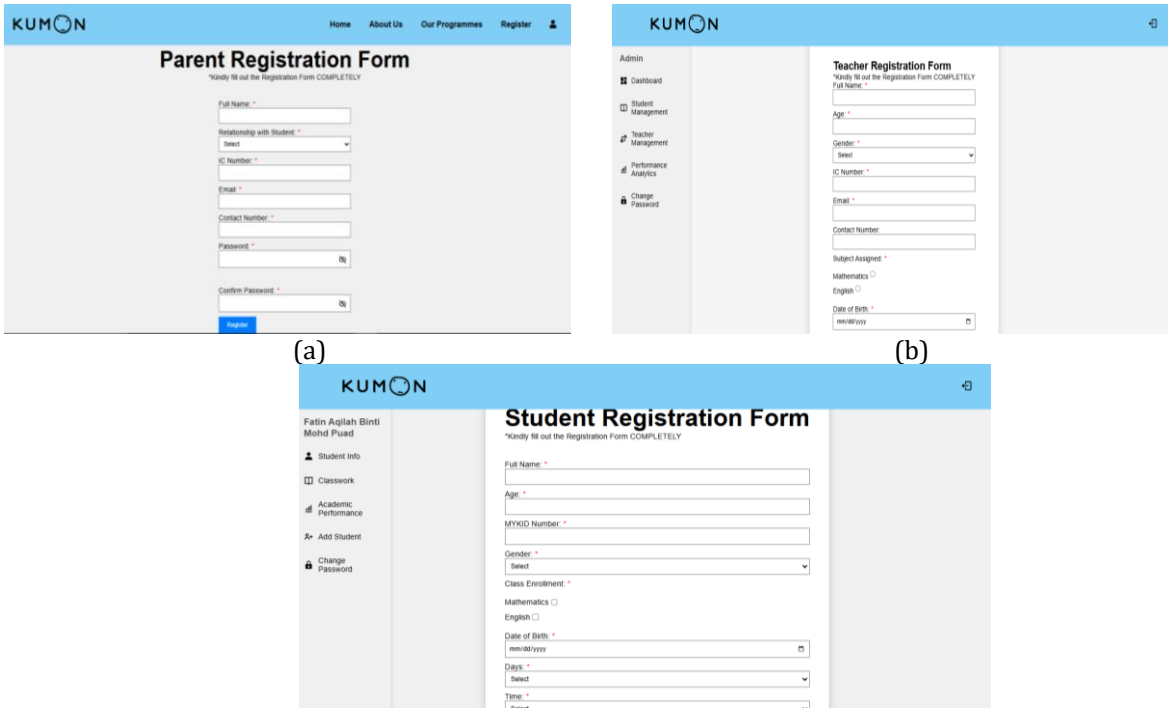
Fig. 17 shows the login page of all users including admin, parent and teacher with an interactive interface where the users need to enter their credentials such as correct email and password. If the credentials are invalid, it will display an error message. Although, users are allowed to reset passwords in forgot password page. The page includes reCAPTCHA verification as a second layer of security to verify whether the user is a human or not. After successfully verified, it will direct users to another page to verify users' OTP number sent via email. This is an extra layer of security. The OTP number will expire in 30 seconds.

(a) (b)

Fig. 17 *Login Module (a) Login Page*; *(b) OTP Page*

5.2.2 Registration Module

Fig. 18 shows the registration pages for parents, students and teachers. In the system, parents are allowed to create their own accounts, while teacher accounts are created by the admin through the teacher registration page. Once the teacher account is created, a default password will be set by the admin, and teachers will be required to change it upon their first login. Both the parent and teacher registration pages require users to provide an email and a strong password that follows the system password policy. Parents can also register their children into the Kumon program by choosing their preferred subject, class days and time slots based on their availability and interest.



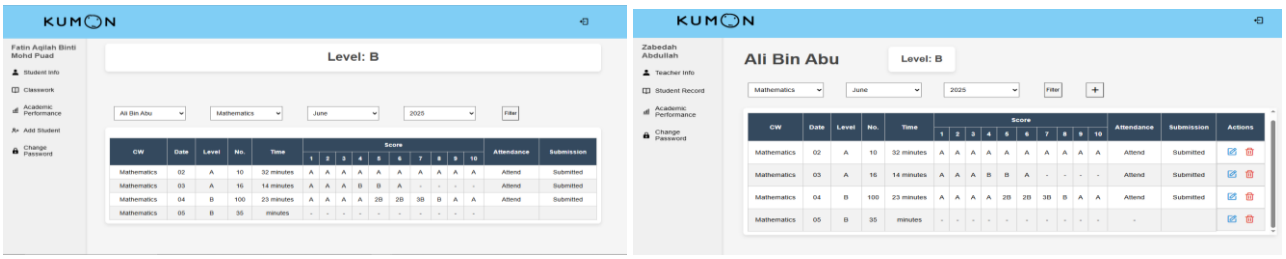
(a) (b)

(c)

Fig. 18 *Registration Module (a) Parent Registration Form*; *(b) Teacher Registration Form*; *(c) Student Registration Form*

5.2.3 Classwork Module

Fig. 19 shows the classwork page from both parent and teacher interfaces. Parents can monitor the student level, classwork progress, time spent completing each classwork, attendance and submission status. They can do this by selecting the student's name, subject and date of the assigned classwork. Parents can also view classwork materials for upcoming classes. Teachers are responsible for creating, updating and deleting student classwork records and attendance in the system. Teachers also can assign new classwork to students in the upcoming classes.

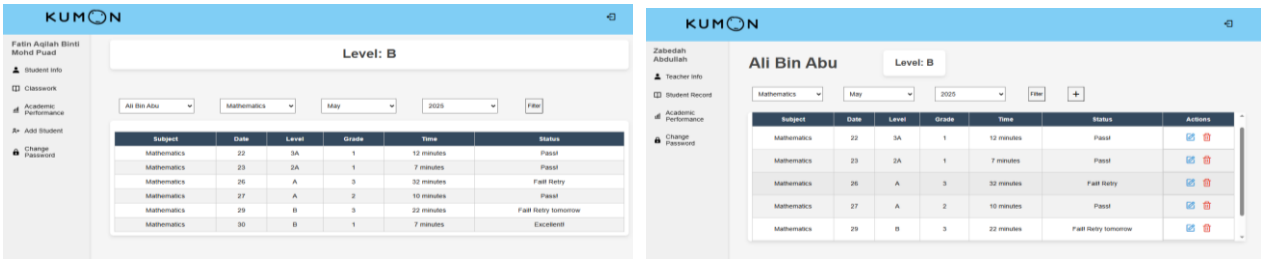


(a) (b)

Fig. 19 *Classwork Module (a) Parent Interface*; *(b) Teacher Interface*

5.2.4 Academic Performance Module

Fig. 20 shows the academic performance page from both parent and teacher interfaces. Parents can monitor the student level, test result, time spent completing each test and status. They can do this by selecting the student's name, subject and date of the assigned test. Teachers are responsible for key in test result including creating, updating and deleting student academic performance records in the system. Teachers also can assign new tests to students.

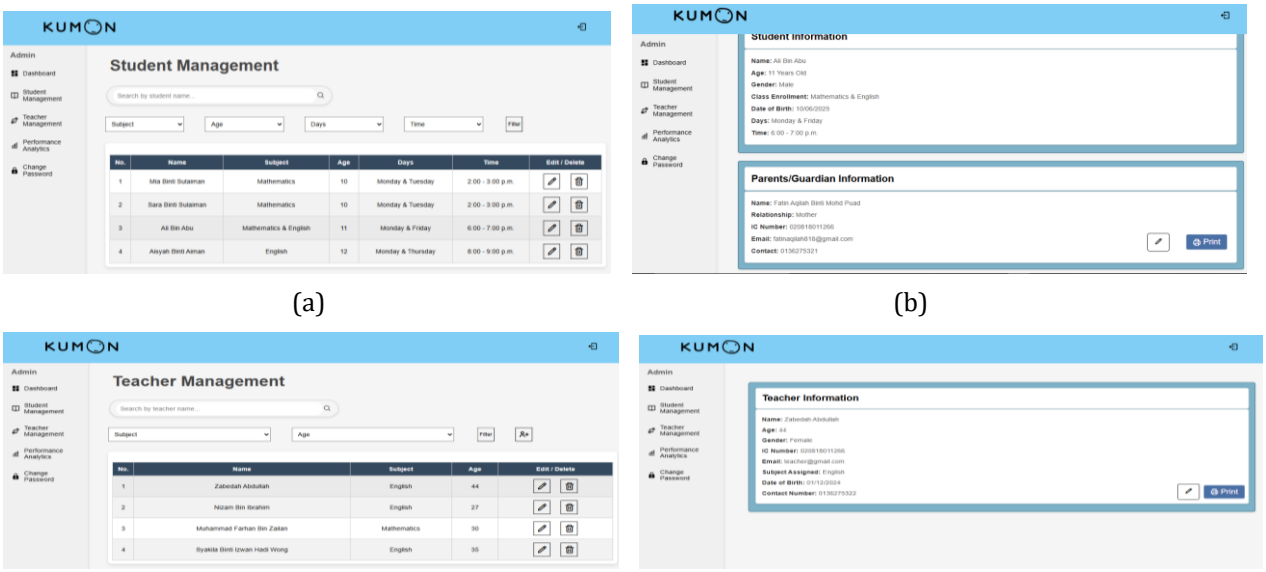


(a) (b)

Fig. 20 *Academic Performance Module (a) Parent Interface*; *(b) Teacher Interface*

5.2.5 Data Management Module

Fig. 21 shows the student and teacher management page from the admin interface. Admin can use the search bar to quickly find specific students or teachers, or filter students by subject, age, class days and time. Similarly, teachers can be filtered by subject and age. Admin can update student and teacher information in the system, generate reports or documents and delete records when necessary. In addition, admins can create teacher accounts and assign a default password, which teachers are required to change after logging in.



(a) (b)

(c) (d)

Fig. 21 *Data Management Module (a) Student Management Page*; *(b) Student Information Page; (c) Teacher Management Page*; *(d) Teacher Information Page*

5.3 User Acceptance Testing

User Acceptance Testing is conducted after the completion of the system development to ensure that the system functions well and it meets user requirements. UAT was conducted with 7 participants that include admin, parents and teachers. They will be given an evaluation form via Google form to answer the survey about the developed system. The purpose of gathering feedback is to identify whether the system meets user satisfaction, functionality, secure and easy to use. The evaluation form contains five sections including user information, functionality testing, security testing, usability and interface and overall satisfaction. The results showed 100% agreement in all areas, with one exception in security related to unauthorized access. The UAT results confirm that the system is functional, secure, user-friendly, and meets stakeholder expectations. Table 5 shows the questions provided in the form and percentage of respondents

Table 5 *User Acceptance Testing (UAT) For Kumon Tuition Student Information Management and Academic Monitoring System with Secure Access Control and Data Privacy*

Sections	Questions	Agree	Disagree
User Information	Name		
	Role (admin, parents, teachers)		
Functional Testing	Are you able to register an account?	100%	
	Are you able to reset password?	100%	
	Are you able to log in and log out?	100%	
	Are you able to view your information?	100%	
	Are you able to view student classwork and academic performance?	100%	
	Are you able to add, edit, and delete student classwork and academic performance?	100%	
	Are you able to edit and delete student and teacher information?	100%	
	Are you able to create teacher account?	100%	
	Are you able to generate reports?	100%	
	Are you able to change password?	100%	
Security Testing	Does the system require strong password policies?	100%	
	Do you receive a One-Time Password (OTP) via your email?	100%	
	Do you verify reCAPTCHA before login?	100%	
	Do you automatically get logged out after 10 minutes of inactivity?	100%	
	Are you able to access features that are meant for other user roles?		100%
Usability and Interface	Was the system easy to navigate?	100%	
	Were error messages clear and helpful?	100%	
	Were instructions and icons easy to understand?	100%	
	Were you able to complete task without confusion?	100%	
Overall satisfaction	Overall, how satisfied are you with Kumon system	100%	

6. Conclusion

In conclusion, the Kumon Tuition Student Information Management and Academic Monitoring System with Secure Access Control and Data Privacy offers a clear, user-friendly and secure solution for managing student data, tracking academic progress and simplifying administrative tasks. With features like role-based access control, data encryption and responsive interfaces for students, parents, teachers and administrators, the system ensures ease of use, reliability and security. Its thoughtful design, practical functionality and regular monitoring make it an effective tool for meeting user needs, improving workflows and supporting stakeholders in achieving their goals. It is important to keep improving the system to match changing user needs and new technology. The future work in Kumon Tuition Student Information Management and Academic Monitoring System with Secure Access Control and Data Privacy could include development of mobile application for easier access by parents, teachers and admin. Furthermore, notification for student classwork in the upcoming class via email as an update and integrating a tuition fee payment module, allowing parents to view invoices, make secure online payments and receive automated payment reminders.

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 interest regarding the publication of the paper.

Author Contribution

The authors confirm contribution to the paper as follows: ***study conception and design:*** *F. A. Mohd Puad, Z. Abdullah;* ***data collection:*** *F. A. Mohd. Puad, Z. Abdullah;* ***analysis and interpretation of results:*** *F. A. Mohd. Puad, Z. Abdullah;* ***draft manuscript preparation:*** *F. A. Mohd. Puad, Z. Abdullah. All authors reviewed the results and approved the final version of the manuscript.*

References

[1] H. A. Alawamleh, B. J. A Ali, A. Fadel Ali Tommalieh and M. Qasem Hasan Al-Qaryouti, "The Challenges, Barriers qnd Advantages of Management Information System Development: Comprehensive Review," 2021. [Online]. Available: https://www.researchgate.net/publication/358357374

[2] M. Shah, "Impact of Management Information Systems (MIS) on School Administration: What the Literature Says," *Procedia Soc Behav Sci*, vol. 116, pp. 2799–2804, Feb. 2014, doi: 10.1016/j.sbspro.2014.01.659.

[3] M. A. Baballe, "Impact and Challenges of Implementing Management Information System," 2021. [Online]. Available: https://gjrpublication.com/journals/

[4] M. Al-Ibrahim and Y. Shams Al-Deen, "The Reality of Applying Security in Web Applications in Academia," 2014. [Online]. Available: www.ijacsa.thesai.org

[5] S. E. A. Ali, F. W. Lai, A. Aman, M. F. Saleem, and S. Hamad, "Do Information Security Breach and Its Factors Have a Long-Run Competitive Effect on Breached Firms' Equity Risk?," *Journal of Competitiveness*, vol. 14, no. 1, pp. 23–42, Mar. 2022, doi: 10.7441/joc.2022.01.02.

[6] "A+ Home Tuition Malaysia," A+ Home Tuition. [Online]. Available: https://www.aplushometuition.com/. [Accessed: 14-Nov-2024].

[7] "Sign in to UTHM-SSO," Edu.my. [Online]. Available: https://sso.uthm.edu.my/realms/UTHM-SSO/protocol/openidconnect/auth?client_id=smap&redirect_uri=https%3A%2F%2 Fsmap.uthm.edu.my%2F&state=f2fee823-e17f-48ed-99da-b05b98cdef74&response_mode=fragment&response_type=code&scope=open id&nonce=8b4f422f-2702-4ec7-8c79-b1c19facbcaf. [Accessed: 14-Nov-2024].

[8] "MCPLUS - The Biggest Online Tuition in Malaysia," MCPlus, Sep. 19, 2021. https://mcplus.my/

[9] D. A. Ahmed, M. A. Ibrahim, and Y. J. Saeed, "THE ROLE OF INFORMATION MANAGEMENT SYSTEMS IN THE IMPLEMENTATION OF THE DIGITAL ECONOMY DEVELOPMENT STRATEGY," *International Journal of Professional Business Review*, vol. 8, no. 5, 2023, doi: 10.26668/businessreview/2023.v8i5.1419.

[10] U. M. Melendres and K. M. Aranda, "Development and Evaluation of a Web-Based Resident Information Management System," *Journal of Computer, Software, and Program*, vol. 1, no. 1, pp. 14–22, Jun. 2024, doi: 10.69739/jcsp.v1i1.50.

[11] S. G. Mohammed and H. Siraj Ibrahim, "Access Control Security Review: Concepts and Models." [Online]. Available: www.solidstatetechnology.us

[12] D. Salunke *et al.*, "A survey paper on Role Based Access Control," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 2, 2013, [Online]. Available: https://www.researchgate.net/publication/368755664

[13] D. Singla and N. Verma, "Performance Analysis of Authentication system: A Systematic Literature Review," Jan. 31, 2023. doi: 10.21203/rs.3.rs-2520547/v1

[14] P. Sahu, "Enhancing Cybersecurity with 2FA and Future Chat-bot Integration." [Online]. Available: https://www.researchgate.net/publication/375526474

[15] J. Berrios, E. Mosher, S. Benzo, C. Grajeda, and I. Baggili, "Factorizing 2FA: Forensic analysis of two-factor authentication applications," *Forensic Science International: Digital Investigation*, vol. 45, Jul. 2023, doi: 10.1016/j.fsidi.2023.301569.

[16] N. Labhade-Kumar, N. Kumar, R. Kamje, P. Landge, S. Shitole, and B. Takale, "OTP-Based Authentication System." [Online]. Available: https://www.researchgate.net/publication/387079266

[17] T. P. Batubara, S. Efendi, and E. B. Nababan, "Analysis Performance BCRYPT Algorithm to Improve Password Security from Brute Force," in *Journal of Physics: Conference Series*, IOP Publishing Ltd, 2021. doi: 10.1088/1742-6596/1811/1/012129.