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

AITCS

Vol. 6 No. 2 (2026) 733-752
https://publisher.uthm.edu.my/periodicals/index.php/aitcs

Employee Management System for SMK Ilhami Aikmel with Role-Based Access Control (RBAC)

Atiqah Baharuddin[1], Zubaile Abdullah[1]*

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

*Corresponding Author: zubaile@uthm.edu.my
DOI: https://doi.org/10.30880/aitcs.2025.06.02.040

Article Info

Received: 16 July 2025
Accepted: 19 November 2025
Available online: 30 November 2025

Keywords

Employee Management System, Role-Based Access Control (RBAC), SMK Ilhami Aikmel, Human Resource, Management Information System

Abstract

Efficient employee management is essential for the smooth operation of an organization. At SMK Ilhami Aikmel, employee-related processes such as attendance, payroll and leave management are still handled manually, resulting in inefficiencies, data inconsistencies and potential security vulnerabilities. To address these challenges, this study developed a web-based Employee Management System (EMS) integrated with Role-Based Access Control (RBAC). The system was built using the Agile methodology, allowing for iterative development and continuous stakeholder feedback. User roles were structured into Admin, HR, and Employee with further sub-roles to ensure accurate and secure access control. Key modules include employee registration, attendance tracking, payroll automation, leave management, and audit logging. Comprehensive testing including functional, security, and user acceptance testing (UAT) demonstrated improved efficiency, reduced manual workload, and strengthened data security. In conclusion, the EMS modernizes employee management at SMK Ilhami Aikmel. Future enhancements may include multi-factor authentication, analytics integration, and broader institutional deployment.

1. Introduction

Efficient management of employees is essential for the smooth operation of organizations. Such a system streamlines administrative tasks, enhances workforce productivity, and ensures secure management of staff information, ultimately supporting the institution's academic and organizational goals [1]. However, SMK Ilhami Aikmel, a private vocational high school located in East Lombok, Indonesia, still manages its staff inefficiently by relying on manual, paper-based processes for managing staff records, attendance, payroll, and leave. This results in inefficiencies, data inconsistencies, and security risks, highlighting the need for digital solutions.

To address these challenges, this paper presents the development of an Employee Management System (EMS) with Role-Based Access Control (RBAC) tailored for SMK Ilhami Aikmel. The solution transforms manual workflows into digital processes while implementing structured access control through RBAC, ensuring users only access relevant modules based on their roles and responsibilities. Users are categorized into defined roles and sub roles, including Admin (Admin Manager, Admin Officer), HR (HR Manager, HR Officer), and Employee (Vice Principal, Teachers). This hierarchical access model enhances control over sensitive data and minimizes security risks. For example, the Admin Manager has full access to critical functions such as audit logs and edit user account details, while the Admin Officer is limited to basic administrative tasks. This hierarchical access model enhances control over sensitive data and minimizes security risks.

The primary objectives of this project include designing and develop an Employee Management System (EMS) specifically for SMK Ilhami Aikmel that streamlines employee related processes to improve efficiency, accuracy, and data management. Additionally, the project will implement a robust Role-Based Access Control (RBAC) framework, structuring system access through defined hierarchical roles (Admin, HR, and Employee) with further refined sub roles (Admin Manager/ Admin Officer, HR Manager/HR Officer, Vice Principal/Teachers) to ensure strict alignment between user permissions and organizational responsibilities. Furthermore, the project will test the effectiveness and security of the implemented RBAC system to ensure it meets the specific requirements of SMK Ilhami Aikmel.

The scope of the project focuses exclusively on employee management functions, excluding student-related or academic planning modules. Key modules include user authentication, employee registration, attendance tracking, payroll automation, leave management, and audit logging, with strict access permissions based on RBAC implementation.

By implementing this EMS with RBAC, *SMK Ilhami Aikmel* is expected to reduce administrative workload, improve data security, and increase overall efficiency. The system will streamline HR processes, ensuring better visibility into workforce management while minimizing errors and unauthorized access. Additionally, this EMS serves as a model for other institutions, demonstrating how technology can modernize workforce management in resource-limited environments while enforcing structured access control.

2. Related Work

This section provides related work on topics related to the development of the EMS. The review aims to gain a comprehensive understanding, highlighting relevant studies for the development of the EMS for SMK Ilhami Aikmel.

2.1 Management Information System (MIS)

Management Information Systems, or MIS, are used to collect, process, store, and share important data to help with decision-making and management in organizations. Firstly, MIS mainly focused on handling transactions and producing reports. Over time, it developed to also support things like strategic planning and daily operations, helping organizations respond better to their needs [2]. Using MIS can improve efficiency, support better decisions, and make communication within an organization smoother. It's made up of several components like hardware, software, databases, procedures, and people which all this work together to keep the system running properly [3]. A good example is an Employee Management System (EMS), which is a more specific type of MIS. EMS helps manage tasks like employee attendance, salary, and performance tracking [4]. When EMS is combined with MIS, it allows for better control of employee data. Features like access control are added to protect sensitive information by making sure only the right people have access to certain data [5].

2.2 Access Control

Access control is a core security mechanism that manages permissions over software and system resources. It consists of subjects (users, processes, devices), objects (resources), operations (actions), permissions (access rights), and policies (rules) to regulate interactions [6]. Traditional models include Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-Based Access Control (RBAC) [6]. DAC grants users control over access permissions but poses risks such as unauthorized privilege transfers. MAC enforces strict classification rules, providing greater security but less flexibility. RBAC assigns permissions based on predefined roles, simplifying access management and securing critical data, while Attribute-Based Access Control (ABAC) enhances flexibility by considering user attributes in decision-making. Access control improves security by preventing unauthorized data exposure, ensures compliance through detailed access logs, and enhances operational efficiency by automating permission adjustments [7]. Strong authentication methods, such as multi-factor authentication (MFA), secure user identity verification, while regular security audits help identify vulnerabilities and ensure regulatory compliance [7].

2.3 Role Based Access Control (RBAC)

RBAC assigns user permissions based on job roles, improving security and access management efficiency within organizations [8]. Unlike traditional models, RBAC group permissions into roles rather than assigning them individually to streamlining administrative tasks while enforcing the principle of least privilege [8]. The RBAC architecture consists of four main components: roles, which define job functions; permissions, which specify access rights; users, who are assigned to roles; and sessions, which manage active login instances. This structure ensures that access is granted systematically based on responsibility. Higher-level roles inherit permissions through role hierarchies to simplifying permission management. Integrating RBAC in Employee Management Systems (EMS) enhances security, compliance, and administrative efficiency. It minimizes

unauthorized data exposure and ensures seamless role-based permission updates during staff transitions [9]. By enforcing least privilege and audit capabilities, RBAC provides a scalable, structured approach to securing employee data within organizational systems.

2.4 Study of Existing Related Systems

This section explores existing systems related to employee management. By comparing these systems with the proposed Employee Management System (EMS) for SMK Ilhami Aikmel, the improvements and advantages offered by the proposed system can be identified.

2.4.1 Vendor and Employee Management System (VEMS)

The Vendor and Employee Management System (VEMS), developed by Alabama A&M University [10], functions as a robust database solution for managing both employee and vendor information. While it successfully implements basic employee and vendor data management functionalities, the system operates on a conventional database architecture with a basic user interface. Despite its utility in managing personnel and payment information, VEMS demonstrates significant limitations in terms of security features and access control mechanisms, making it less suitable for modern institutional requirements.

2.4.2 University Employee Management System

The University Employee Management System, designed for Nigerian universities [11], the University Employee Management System includes fundamental HR functions such as leave management and payroll processing. However, it faces significant limitations in scalability and system integration. The absence of advanced security features and restricted integration capabilities reduces its effectiveness in addressing contemporary institutional needs [11].

2.4.3 Web-Based Employee Management System

The Web-Based Employee Management System, developed at the Sri Lanka Institute of Information Technology, represents a more modern approach to employee management [12]. This system is built using the MERN (MongoDB, Express.js, React.js, Node.js) stack, offering improved performance and user experience compared to traditional systems. Although it improves responsiveness and data handling, the system's access control remains basic with limited security features. These constraints affect its suitability for schools requiring detailed control over system access and data protection.

2.5 Comparison between Proposed System and Existing Related Systems

The proposed Employee Management System (EMS) for SMK Ilhami Aikmel incorporates RBAC frameworks, offering significant improvements over existing systems. Unlike traditional systems, the proposed EMS is designed to reduce administrative workload, enhance data security, and provide a user-friendly interface tailored to the specific needs of the school. This system streamlines core processes such as employee data management, attendance tracking, leave requests, and payroll processing, while ensuring that access to sensitive information is strictly controlled according to staff roles and sub roles. Table 1 compares the main features of the proposed system with several existing EMS platforms, including VEMS, University EMS, and a generic Web-Based EMS:

Table 1 *Comparison between EMS and existing related systems*

Application Features	VEMS (Vendor and Employee Management System) [10]	University EMS [11]	Web-Based EMS [12]	Proposed System
Platform	Windows Forms Application	Web-Based	Web-Based	Web-Based
Salary Management	Yes	No	Yes	Yes
Leave Management	Yes	Yes	Yes	Yes
Attendance Management	No	Yes	Yes	Yes
Email/Username Password Login	Yes	Yes	Yes	Yes
Strong password policy	Yes	Yes	Yes	Yes
Password Hashing	No	Yes	Yes	Yes
Session management	No	No	Yes	Yes

Table 1 (*Cont.*)

Application Features	VEMS (Vendor and Employee Management System) [10]	University EMS [11]	Web-Based EMS [12]	Proposed System
Password Stregth Check	No	No	No	Yes
Data Sanitization	No	No	Yes	Yes
Prepared statement	No	No	Yes	Yes
One-Time (OTP) verification	No	No	No	Yes
Secure password reset handling	No	No	No	Yes
Audit Logging	No	No	No	Yes
Role-Based Access Control	Yes	Yes	Yes	Yes

As shown in Table 1, the proposed EMS not only matches the core functionalities of other systems but also incorporates advanced security features such as password hashing, session management, strong password policy enforcement, secure password reset handling, prepared statements, data sanitization, OTP verification, and audit logging. These features, combined with a structured RBAC mechanism, ensure that access permissions are tightly managed, and user accountability is maintained. Overall, the proposed EMS offers a more secure, efficient, and tailored solution for SMK Ilhami Aikmel, addressing the specific challenges faced by the school and setting a benchmark for similar institutions seeking to modernize their employee management processes.

3. Methodology

This study employs the Agile methodology to develop the Employee Management System (EMS) for SMK Ilhami Aikmel, chosen for its flexibility and iterative approach that supports continuous feedback and adaptation throughout the development process. The Agile framework enabled the system to evolve in alignment with the school's requirements and ensured active stakeholder involvement at every stage.

3.1.1 Planning and Analysis Phase

The project began with the planning and analysis phase, where goals and system requirements were defined through stakeholder interviews conducted via Google Meet. Key features included employee registration, user authentication, attendance tracking, leave management, payroll generation, and role-based access control (RBAC). User roles were structured into main roles (Admin, HR Staff, Employee) and sub-roles (Admin Manager, Admin Officer, HR Manager, HR Officer, Vice Principal, Teacher) to ensure proper access permissions. System functionality was clarified using UML diagrams such as use case, sequence, activity, and class diagrams, mapping out processes and data relationships.

3.1.2 Design Phase

In the design phase, a system flowchart that provided an overview of data flow and interface designs were created for key screens to ensure user-friendliness. Then, the database schema was finalized with well-organized tables for employee data, roles, attendance, leave, payroll, and audit logs, following RBAC principles for secure and scalable data management.

3.1.3 Implementation Phase

Implementation was performed using PHP for backend development, HTML, CSS, and JavaScript for the frontend, and MariaDB for database management. Core modules including employee registration, attendance tracking, payroll processing and leave management were developed alongside a Role-Based Access Control (RBAC) system to safeguard sensitive data. Security measures such as password hashing, session management, strong password policies, two-factor authentication (2FA), and input sanitization were integrated to ensure data confidentiality and integrity.

3.1.4 Testing Phase

In testing phase, comprehensive testing was conducted, including functional, security and user acceptance testing, to validate system functionality, usability, and resilience against vulnerabilities like SQL injection and session hijacking. User Acceptance Testing (UAT) involved stakeholder feedback collection using google form to confirm system alignment with institutional needs.

3.1.5 Deployment Phase

Upon successful testing, the EMS was deployed on a local server environment configured with PHP, MariaDB, and Apache, and reviewed by administrative and HR staff before launch.

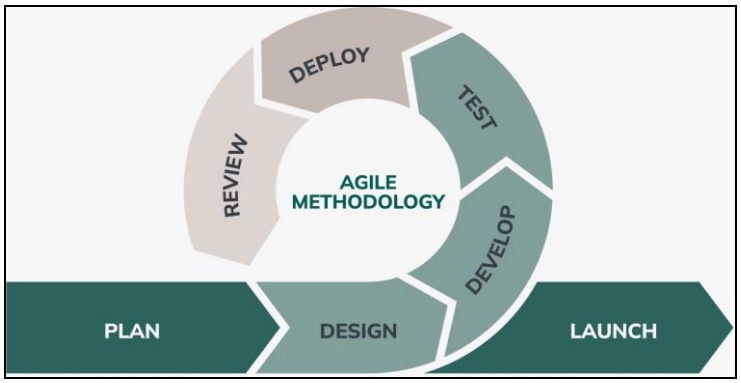


Fig. 1 *Agile model phases*

4. System Analysis and Design

This section provides an in-depth analysis and design of the proposed Employee Management System (EMS) for SMK Ilhami Aikmel. It covers the system requirements, system analysis and system design.

4.1 System Requirements

The system requirements outline the essential criteria needed for the development and effective operation of the employee management system. These requirements ensure that the system will function effectively in its intended context and satisfy the needs of its users.

4.2 Functional Requirements

Functional requirements specify the actions and operations that the system must be able to perform. These requirements describe what the system must do to ensure the utility and effectiveness of the system in managing employee-related tasks. In Table 2, the functional requirements for each module are detailed.

Table 2 *Functional Requirements*

No	Module	Functionality
1	User Authentication	• The system sNohould allow users to log in using a valid username and password. • The system should restrict access based on the user's assigned roles. • The system should provide a "Forgot Password" functionality to reset the password securely.
2	User Registration and Management	• The system should allow only Admin to register new user with appropriate roles and subrole. • The system should validate user input during registration • The system should notify the Admin of successful user registration.
4	Employee directory	• The system should allow HR and Admin to view all registered employees. • The system should allow authorized roles to edit or delete employee records.
5	Attendance Management	• The system should enable all users to record daily attendance, including clock-in and clock-out times. • The system should store attendance records based on months and date.

Table 2 *Cont.*

No	Module	Functionality
6	Leave Management	• The system should allow all users to submit leave requests with details such as leave type, dates, and reason. • HR Manager and HR Officer shall be able to approve or reject leave requests. • The system should notify users of the leave approval status. • The system should allow authorized sub roles to view all users leave summary.
7	Payroll management module	• The system should allow HR to auto-generate payroll using attendance and salary data. • The system should allow HR and Admin Manager to view payroll summaries. • The system should allow users (employees, teachers, HR) to view their own payslip.
8	Profile management	• The system should enable all types of users to update their information.
9	Audit log module	• The system shall log critical actions performed by users • Only Admin Manager shall be able to view the audit logs.

4.3 Non-Functional Requirements

Non-functional requirements describe the characteristics and performance constraints of a system. Non-functional requirements ensure that the system functions well, under a variety of conditions and remains secure and user-friendly. In Table 3, the non-functional requirements for the Employee Management System for SMK Ilhami Aikmel are detailed.

Table 3 *Non-Functional Requirements*

No	Non-Functional Requirement	Description
1	Availability	The EMS should be available for access all the time, especially during working hours.
2	Scalability	The system should be able to scale to accommodate a growing number of users and data such as the addition of new users, departments, or modules.
3	Security	• Access to system features and data must be controlled through Role-Based Access Control (RBAC). • The system should also include password hashing, session management, strong password policy enforcement, two-factor authentication (2FA) via OTP email, secure password reset handling, prepared statements and input sanitization.
4	Usability	The system should be user-friendly and easy to navigate.
5	Maintainability	The system should be easy to maintain and update.

4.4 System Analysis

System analysis is a crucial step in developing an employee management system for SMK Ilhami Aikmel. It involves carefully examining the project requirements and breaking down how the system will work in practice. This section includes various diagrams that provide a visual representation of the system's processes, interactions, and architecture.

4.4.1 Use Case

The use case diagrams illustrate the interactions between different user roles (actors) and the system, highlighting the primary functions and scenarios for each user type. Specifically, Fig. 2 presents the use case diagram for the Admin role, including its sub roles: Admin Manager and Admin Officer. Fig. 3 depicts the use case diagram for the HR role, covering HR Manager and HR Officer sub roles. Meanwhile, Fig. 4 illustrates the use case diagram for the Employee role, consisting of Vice Principal and Teachers. These diagrams collectively

provide a comprehensive overview of user-system interactions tailored to the organizational structure of SMK Ilhami Aikmel.

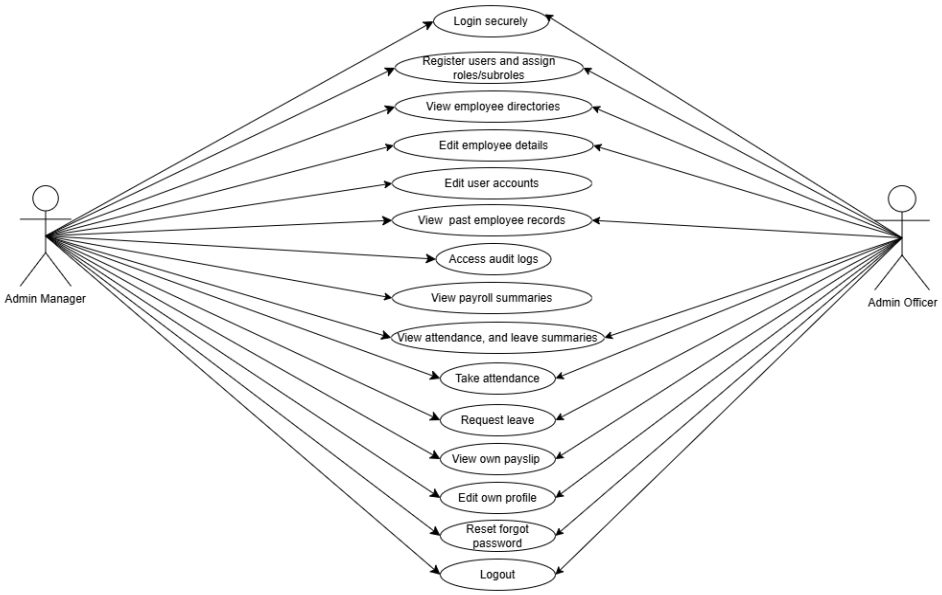


Fig. 2 *Use Case Diagram for Admin Role (Admin Manager and Admin Officer)*

Fig. 3 *Use Case Diagram for HR Role (HR Manager and HR Officer)*

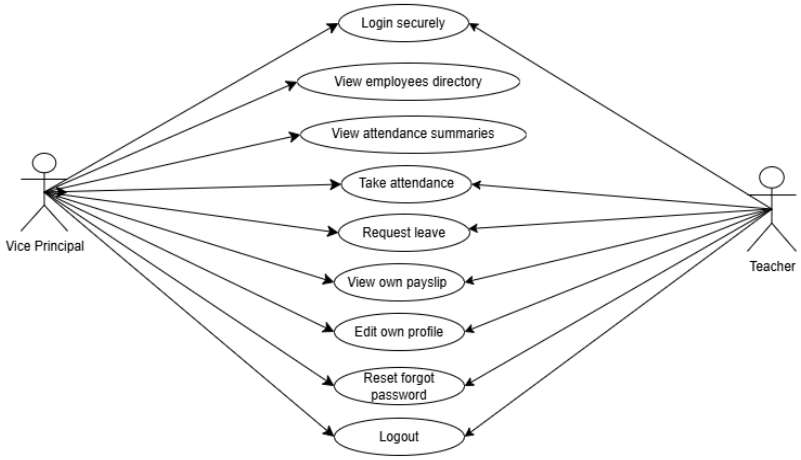


Fig. 4 *Use Case Diagram for Employee Role (Vice Principal and Teacher)*

4.4.2 Class Diagram

Fig. 5 shows the class diagram for the Employee Management System (EMS) for SMK Ilhami Aikmel, illustrating the relationships between key system components. The diagram includes classes such as Employees, Admins, HRStaff, EmployeeAccount, Role, SubRole, Attendance, Payroll, LeaveRequest, and ActivityLog, defining their attributes and functionalities. The `employee_ref_id` in multiple classes serves as a reference to the `id` in Employees, ensuring data consistency and proper linking of records. RBAC is implemented through Role and SubRole, enforcing structured access control for users. This model strengthens data integrity, security, and accountability within the system. The class structure ensures that all employee-related actions are efficiently managed and securely stored.

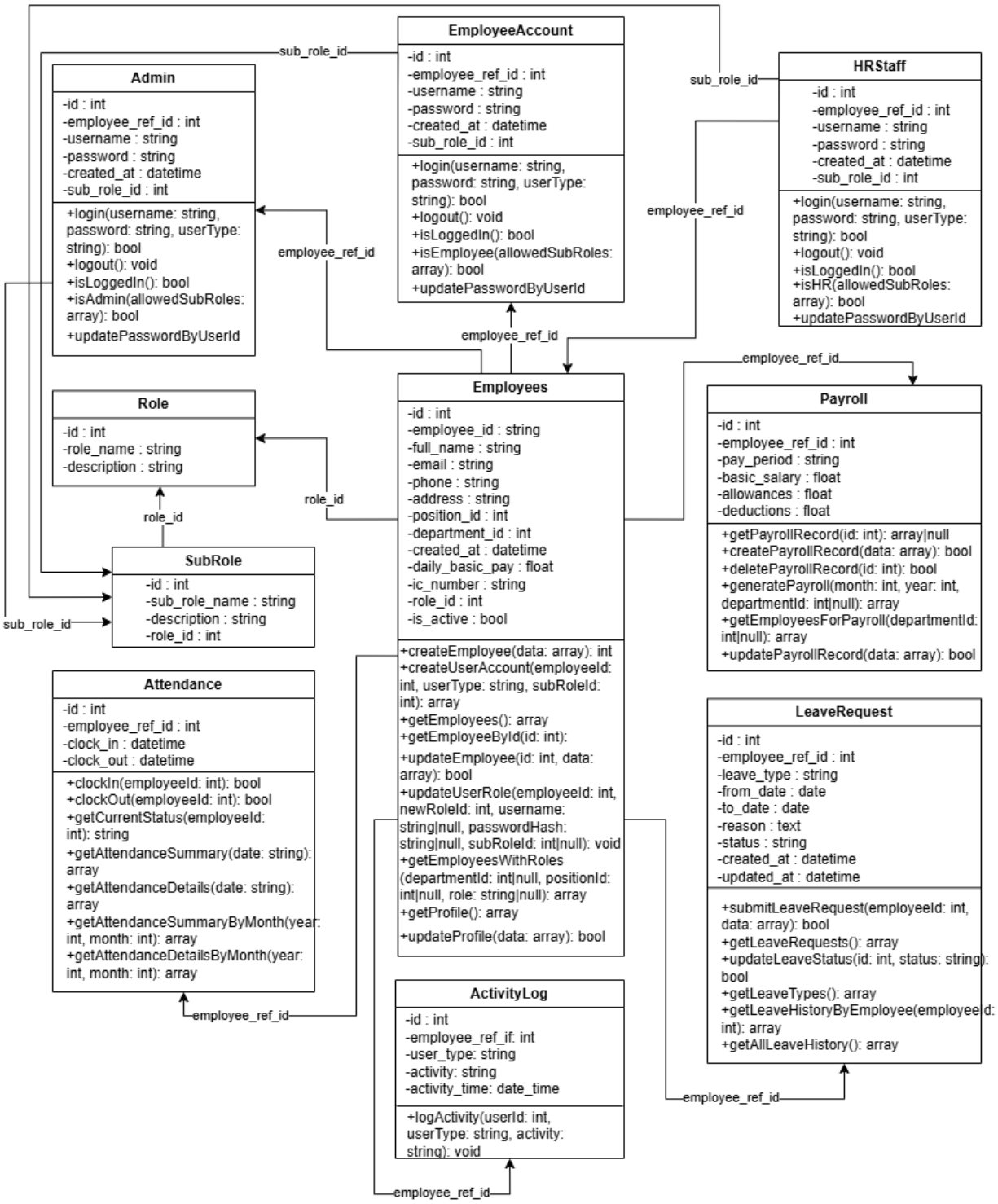


Fig. 5 *Class Diagram of proposed system*

4.5 System Design

Fig. 6 illustrates the overall system flow for the Employee Management System at SMK Ilhami Aikmel. The process begins when a user attempts to log in by entering their username and password. If the credentials are valid, the system proceeds to identify the user's main role either Admin, HR Staff, or Employee. Once the main role is determined, the system further checks the sub-role associated with that user. Each sub-role has its own designated dashboard. BY identifying the correct sub-role, the user is redirected to their respective dashboard where they can access specific modules based on their responsibilities. If either the role or sub-role is not recognized, an appropriate error message is displayed. If login credentials are invalid, the system prompts a login error. This flow ensures secure and role-based access control, aligning with the system's core goal of managing employees efficiently through customized dashboards.

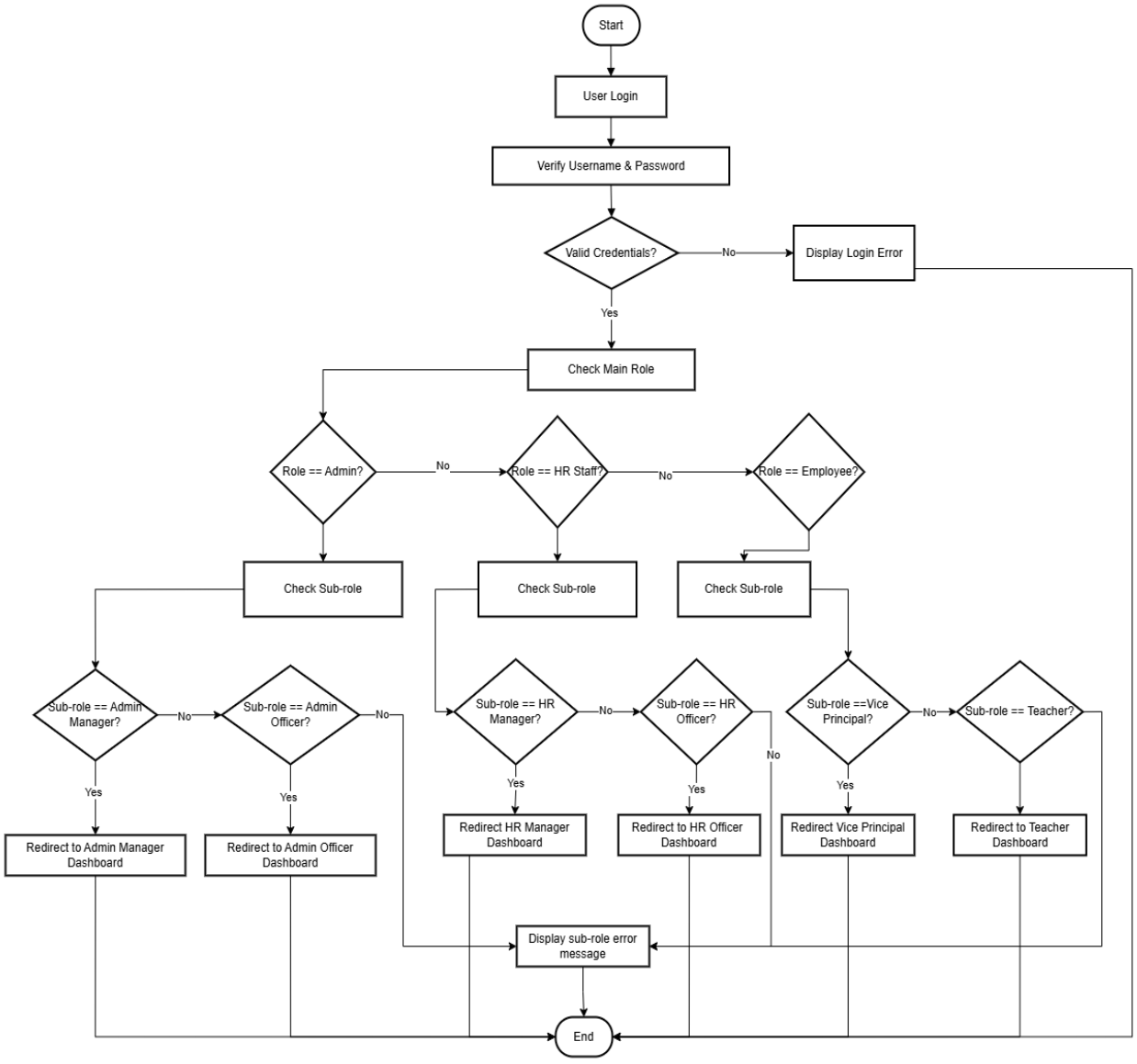


Fig. 6 System design of proposed system

5. Implementation and Testing

This section focuses on the functional, security, and user acceptance testing (UAT) conducted for the Employee Management System (EMS) for SMK Ilhami Aikmel. Functional testing validates whether system modules operate correctly, ensuring that authentication, role-based access control (RBAC), attendance tracking, leave management, payroll processing, and audit logging function as expected. Security testing assesses vulnerabilities, verifying resilience against unauthorized access, SQL injection, and session management flaws. Additionally, UAT was performed with stakeholders, ensuring usability and alignment with operational needs. These comprehensive tests confirm the system's reliability, security, and compliance with best practices.

5.1 Implementation of Role-Based Access Control

Role-Based Access Control (RBAC) was implemented in the Employee Management System for SMK Ilhami Aikmel to ensure structured access and security. This system assigns users specific roles with predefined permissions, restricting their access to only relevant functionalities. The RBAC structure in this system consists of three primary roles with it corresponding sub roles including Admin (Admin Manager, Admin Officer), HR (HR Manager, HR Officer), Employee (Vice Principal, Teacher).

RBAC was implemented using a structured database design where roles, sub-roles, and user accounts are stored across multiple tables. As shown in Fig. 7 (a) and (b), the `roles` table defines the main roles, while the `sub_roles` table links specific sub-roles to their respective parent roles. The roles table ensures each user is mapped to a designated role, enforcing structured access control. Then, user accounts are stored in separate tables based on their roles, such as admins, hr_staff, and employee_accounts, and include their corresponding sub-role IDs.

id	role_name	description
1	admin	NULL
2	hr	NULL
3	employee	NULL

(a)

id	sub_role_name	description	role_id
1	Admin Manager	NULL	1
2	Admin Officer	NULL	1
3	HR Manager	NULL	2
4	HR Officer	NULL	2
5	Vice Principal	NULL	3
6	Teacher	NULL	3

(b)

Fig. 7 (a) *roles table in database; (b) sub_roles tables in database*

Additionally, role-based navigation directs users to their appropriate dashboards immediately after login as shown in Fig. 8. to prevent access to unauthorized sections of the system. Upon successful authentication, the system retrieves the user's ID, main role, and sub-role from session data. Based on the user's role and sub-role, it then checks the correct dashboard to display.

```
} elseif ($auth->verifyCode(code: $code)) {
        $userId = $_SESSION['user_id'] ?? null;
        $userType = $_SESSION['user_type'] ?? null;
        $subRole = $_SESSION['sub_role_id'] ?? null;

        if ($userId && $userType) {
            logActivity(db: $db, userId: $userId, userType: $userType, activity: 'User logged in');

            // Redirect based on user_type and sub_role
            if ($userType === 'admin') {
                if ($subRole == 1) {  // Admin Manager
                    header(header: "Location: ../dashboard/admin_manager.php");
                } else {
                    header(header: "Location: ../dashboard/admin_officer.php");
                }
            } elseif ($userType === 'hr') {
                if ($subRole == 3) { // HR Manager
                    header(header: "Location: ../dashboard/hr_manager.php");
                } else {
                    header(header: "Location: ../dashboard/hr_officer.php");
                }
            } elseif ($userType === 'employee') {
                if ($subRole == 5) { // vice principal(sub_role id 6)
                    header(header: "Location: ../dashboard/vp_dashboard.php");
                } else {
                    header(header: "Location: ../dashboard/teacher.php");
                }
            } else {
                // fallback dashboard
                header(header: "Location: ../login/login.php");
            }
```

Fig. 8 *Code sinppet for Role-Based Access Control navigation upon login*

For example, if the sub role is Admin Manager, it will be redirected to the admin manager dashboard, while Admin Officers are sent to their respective dashboard. Similarly, sub roles like HR Managers and HR Officers, as well as Vice Principals and Teachers, are directed at their designated dashboards. If the user's role is unrecognized, the system defaults to redirecting back to the login page. This approach ensures that each user accesses only the features and information relevant to their responsibilities, reinforcing security and improving overall user experience.

In addition, the system employs redirect functions to prevent unauthorized users from accessing restricted pages by verifying the user's role and sub-role upon page access. The functions used was *redirectIfNotAdmin(array $allowedSubRoles=[]), redirectIfNotHR(array $allowedSubRoles=[]),* and

redirectIfNotEmployee(array $allowedSubRoles = []) as illustrated in Fig. 9 and 10. If the user is not logged in, or their role or sub-role is unauthorized, these functions immediately redirect them to the login page which means blocking access.

```php
public function redirectIfNotAdmin(array $allowedSubRoles = []): void {
    $this->redirectIfNotLoggedIn();

    $userType = $_SESSION['user_type'] ?? null;
    $subRole  = $_SESSION['sub_role_id'] ?? null;

    // Redirect if not admin
    if ($userType !== 'admin') {
        header(header: "Location: ../../modules/login/login.php");
        exit();
    }

    // Redirect if subRole is not allowed
    if (!empty($allowedSubRoles) && !in_array(needle: $subRole, haystack: $allowedSubRoles)) {
        header(header: "Location: ../../modules/login/login.php");
        exit();
    }
}


5 references | 0 overrides
public function redirectIfNotHR(array $allowedSubRoles = []): void {
    $this->redirectIfNotLoggedIn();

    $userType = $_SESSION['user_type'] ?? null;
    $subRole  = $_SESSION['sub_role_id'] ?? null;

    if ($userType !== 'hr') {
        header(header: "Location: ../../modules/login/login.php");
        exit();
    }

    if (!empty($allowedSubRoles) && !in_array(needle: $subRole, haystack: $allowedSubRoles)) {
        header(header: "Location: ../../modules/login/login.php");
        exit();
    }
}
```

Fig. 9 *code snippet for redirectIfNotAdmin(), redirectIfNotHR() function*

```php
public function redirectIfNotEmployee(array $allowedSubRoles = []): void {
    $this->redirectIfNotLoggedIn();

    $userType = $_SESSION['user_type'] ?? null;
    $subRole  = $_SESSION['sub_role_id'] ?? null;

    if ($userType !== 'employee') {
        header(header: "Location: ../../modules/login/login.php");
        exit();
    }

    if (!empty($allowedSubRoles) && !in_array(needle: $subRole, haystack: $allowedSubRoles)) {
        header(header: "Location: ../../modules/login/login.php");
        exit();
    }
}
```

Fig. 10 *code snippet for redirectIfNotAdmin(), redirectIfNotHR() and* redirectIfNotEmployee () function

Additionally, to enforce role-based access in the system, functions such as *isAdmin(array $allowedSubRoles = []), isHR(array $allowedSubRoles = []),* and *isEmployee(array $allowedSubRoles = [])* showed in Fig. 11 was used to validate user permissions before allowing access to modules. These functions verify the main role and if a list of allowed sub-roles is provided, it further checks whether the user's sub-role is included in that list to grant access to the user as illustrated in Fig. 12. This ensures refined access control within each primary role, enhancing security by restricting actions to authorized sub-roles only.

```php
public function isAdmin($allowedSubRoles = []): bool {
    if (!$this->isLoggedIn() || ($_SESSION['user_type'] ?? '') !== 'admin') {
        return false;
    }

    if (!empty($allowedSubRoles)) {
        $subRole = $_SESSION['sub_role_id'] ?? null;
        if (!in_array(needle: $subRole, haystack: $allowedSubRoles)) {
            return false;
        }
    }
    return true;
}

6 references | 0 overrides
public function isHR($allowedSubRoles = []): bool {
    if (!$this->isLoggedIn() || ($_SESSION['user_type'] ?? '') !== 'hr') {
        return false;
    }

    if (!empty($allowedSubRoles)) {
        $subRole = $_SESSION['sub_role_id'] ?? null;
        if (!in_array(needle: $subRole, haystack: $allowedSubRoles)) {
            return false;
        }
    }
    return true;
}
```

```php
0 references | 0 overrides
public function isEmployee($allowedSubRoles = []): bool {
    if (!$this->isLoggedIn() || ($_SESSION['user_type'] ?? '') !== 'empl
        return false;
    }

    if (!empty($allowedSubRoles)) {
        $subRole = $_SESSION['sub_role_id'] ?? null;
        if (!in_array(needle: $subRole, haystack: $allowedSubRoles)) {
            return false;
        }
    }
    return true;
}
```

Fig. 11 *isAdmin($allowedSubRoles) isHR($allowedSubRoles) and isEmplooyee($allowedSubRoles) function*

```php
<?php if ($auth->isAdmin()): ?>
<a href="../../modules/users/register.php" class="add-btn">+ Add Employee</a>
<?php endif; ?>
```

Fig. 12 *Permission check using isAdmin()*

Overall, implementing RBAC in the Employee Management System for SMK Ilhami Aikmel improves security, workflow efficiency, and operational control. By structuring access based on user roles and sub-roles, the system ensures that employees interact with only the necessary features while maintaining data integrity and accountability. The combination of database-level role management, session-based authentication, and permission validation creates a robust and scalable security framework.

5.2 Implementation of Module

The Employee Management System (EMS) has been successfully developed with key modules fully implemented. These modules include authentication, attendance tracking, leave management, payroll processing, and audit logging. Each module ensures efficient system operation, enhancing security, usability, and overall functionality. The following pages showcase the actual system output, illustrating the working interfaces and functionalities of the EMS.

5.2.1 User Authentication module

As shown in Fig. 13, the login interface includes an account type selector, username and password fields, a login button, and a password recovery link, ensuring a structured authentication flow. To access the system, users must enter their username, password, and select their account type according to their roles, such as Admin, HR, or Employee. Upon submission, the system performs backend validation to verify the credentials before proceeding with authentication.

Once the login details are validated, the system generates and sends a one-time password (OTP) via email, adding an extra layer of security through two-factor authentication (2FA). Users must enter the received OTP to complete authentication. Upon successful verification, the system redirects users to their respective dashboards based on their assigned sub-roles.

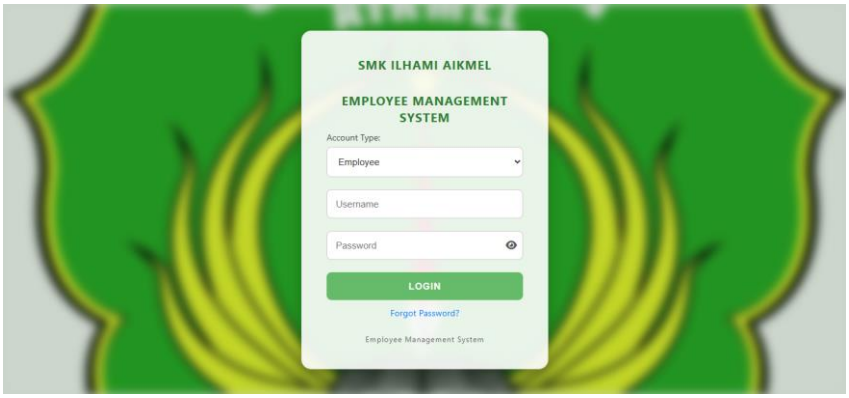


Fig. 13 *Login Page*

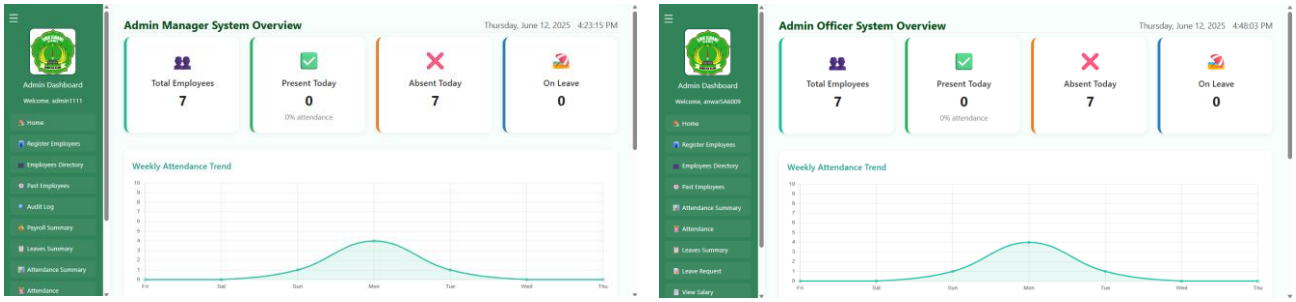
5.2.2 Dashboard Module

The Dashboard Module acts as the central navigation hub for all users upon a successful login. It dynamically displays content and access features based on each user's assigned role and sub-role using a Role-Based Access Control (RBAC) mechanism. The dashboard interface is customized to reflect only the functionalities permitted for that particular sub role. Each sub-role is granted access to specific modules and actions through the dashboard.

For the Admin Manager, the dashboard provides comprehensive administrative functionality as shown in Fig. 14 (a). They can register new users, assign appropriate roles and sub-roles, view and edit the employee details, manage user accounts and manage past employee records. They also have access to the audit logs for tracking system activities and can view summarized reports on payroll, attendance, and leave. Additional features include the ability to take attendance, submit personal leave requests, view their own payslip, update their own profile and securely log out.

As for the Admin Officer dashboard shown in Fig. 14 (b), it has access to a slightly more limited version of administration. They can view and edit employee details, access past employee information, and view summaries of attendance and leave. They are also allowed to take attendance, request leave for themselves, view

their own payslip, manage their profile and log out of the system. However, unlike the Admin Manager, they do not have access to audit logs or payroll summary modules.

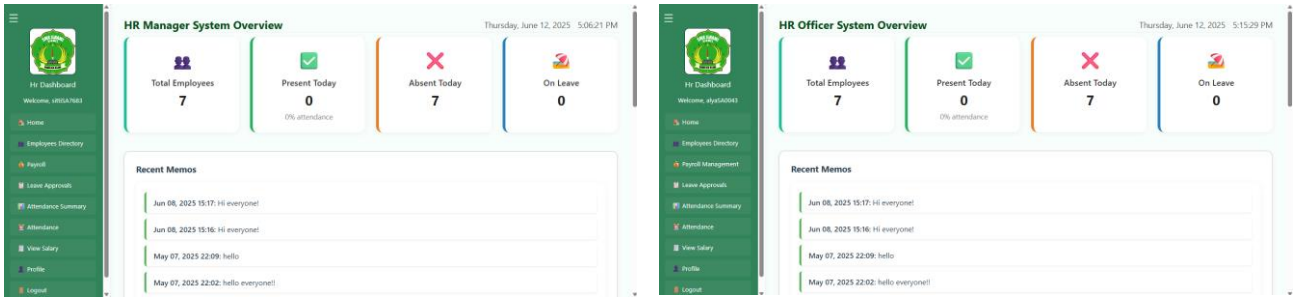


(a) **(b)**

Fig. 14 (a) *Admin manager dashboard; (b) Admin Officer dashboard*

For the HR Manager shown in Fig. 15 (a), the dashboard serves as a command center for human resource management tasks. They are granted access to edit employee details, generate and view payroll summaries, and monitor attendance and approve leave requests. Like other roles, the HR Manager can take attendanceview their payslip, manage their personal profile, reset their password, and log out securely.

The HR Officer dashboard, as shown in Fig. 15 (b), provides access to essential functions aligned with their role. Although HR Officers are not authorized to edit employee information, they can view employee details, assist in payroll generation, and approve or reject leave requests directly from their dashboard. They can also access attendance summaries, take attendance, submit their own leave requests, and view their own payslip. Similar to other roles, profile editing, password recovery, and logout functionalities are also available.

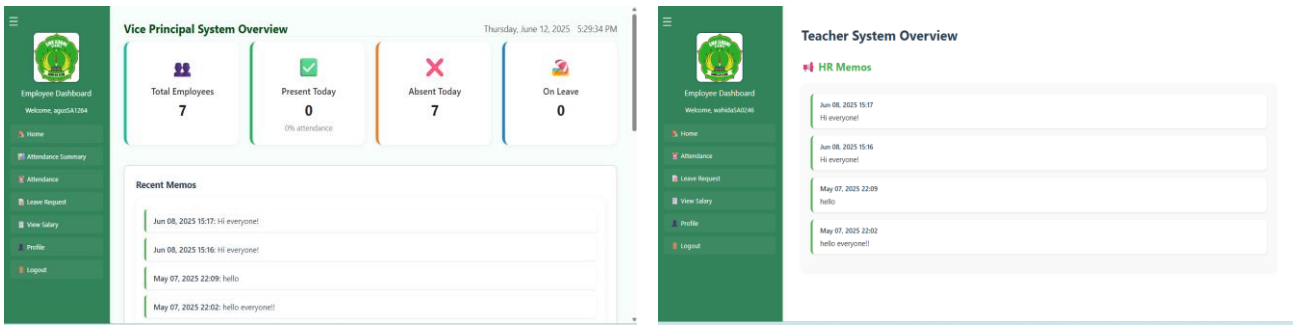


(a) **(b)**

Fig. 15 (a) *HR manager dashboard; (b) HR Officer dashboard*

For Vice Principal, their dashboard is shown in Fig. 16 (a). It allows them to view employee profiles, access attendance summaries, and take attendance for relevant staff. They can also request leave, view their payslip, update their profile, reset a forgotten password, and securely log out. However, they do not have access to payroll or user account management modules.

Lastly, the Teacher role is provided with a minimalistic dashboard interface (see Fig. 16 (a)), allowing access to personal functions such as taking attendance, submitting leave requests, viewing payslips, editing personal information, resetting passwords, and logging out of the system.



(a) **(b)**

Fig. 16 (a) *Vice Principal dashboard; (b) Teacher dashboard*

5.2.3 Employee Registration

The Employee Registration Module as shown in Fig. 17 serves as the entry point for adding new staff members to the system and assigning their respective roles and sub roles. During registration, admin must input essential employee details, select the appropriate role and sub roles, and the system automatically generates unique login credentials. The username is created by combining the employee's first name with their employee ID, while the password is generated using the first name, the last four digits of the employee's identification card (IC), and the symbol "@" Upon successful registration, the system automatically sends an email containing the account credentials to the employee, ensuring a secure and efficient onboarding process.

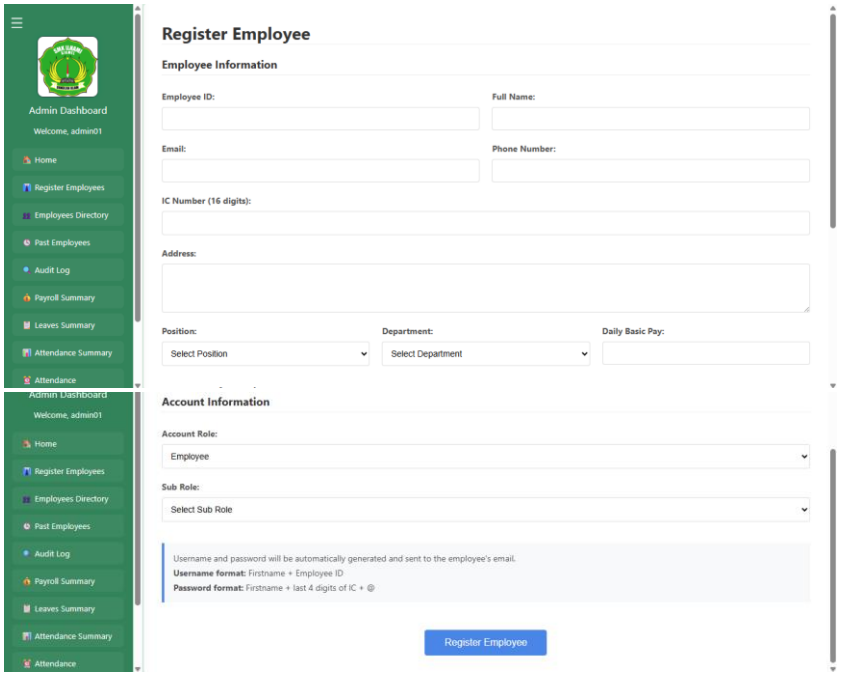


Fig 17 *Employee registration page*

5.2.4 Employee directory

The Employee Directory module provides authorized users to access and manage all registered employees in the system. It ensures efficient personnel management by allowing users to view essential staff details such as Employee ID, Name, Position, Department, Role, Email, and Phone Number. The directory is accessible to users based on their assigned roles and sub roles, ensuring proper access control. Admin Manager has full privileges to view and edit both employee details and account information, while Admin Officer and HR Manager can edit employee details but do not have permission to modify account-related information. HR Officer has viewing rights only, preventing unauthorized modifications. This structured access control approach, enforced through Role-Based Access Control (RBAC), minimizes security risks and enhances data accuracy. Fig. 18 illustrates the Employee Directory interface of registered employees.

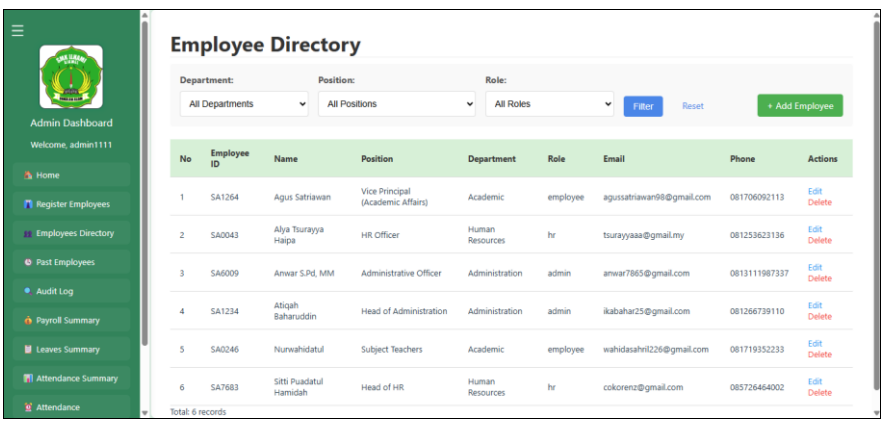
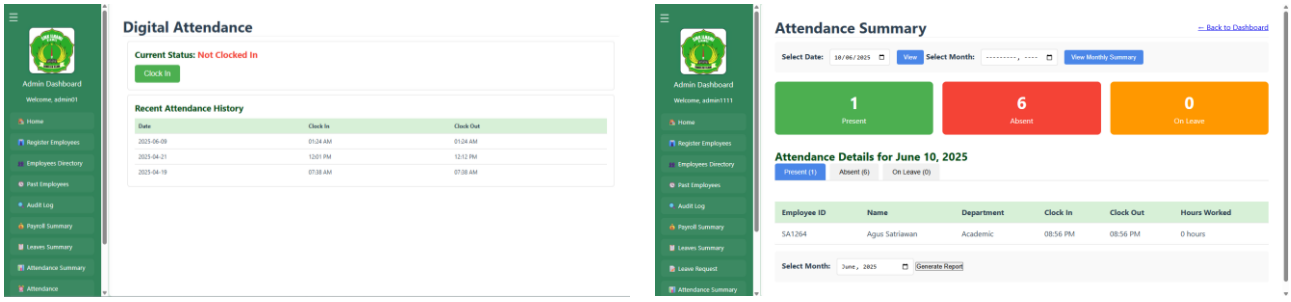


Fig 18 *Employee directory page*

5.2.5 Attendance Management

The Attendance Management module consists of two key components: Digital Attendance and Attendance Summary (Fig. 19 (a) and (b)), ensuring accurate tracking and monitoring of employee work hours. The Digital Attendance page allows employees to clock in and clock out, recording timestamps that reflect their daily attendance status. These records help track working hours and support payroll calculations.

The Attendance Summary page is accessible to authorized users, including Admin and HR personnel, allowing them to review attendance records, detect trends, and generate reports. This dashboard provides a real-time overview of employee attendance, including present, absent, and on-leave staff, aiding workforce management and decision-making.

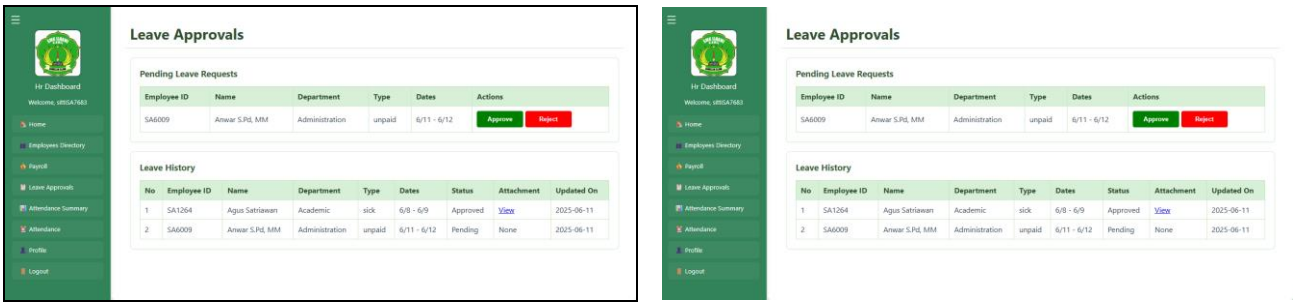


(a) **(b)**

Fig. 19 (a) *Digital Attendance Page; (b) Attendance Summary Page*

5.2.6 Leave Management

The Leave Management module facilitates a streamlined process for employees to submit, review, and approve leave requests within the system as illustrated in Fig. 20 (a) and (b). It consists of two key components, which is Leave Request and Leave Approval, ensuring efficient workforce coordination and record keeping. The Leave Request page allows all employees to submit leave applications by selecting the leave type, specifying start and end dates, and providing a reason. Employees can track the status of their requests in the Leave History section, ensuring transparency in leave processing. As for Leave Approval page, it is accessible only to HR roles (HR Manager and HR Officer), who can review applications and either approve or reject requests based on availability and leave policies. Once processed, the system updates the records and notifies employees of their request status. Additionally, the Admin Manager can view payroll summaries, ensuring leave data is properly reflected in payroll calculations.



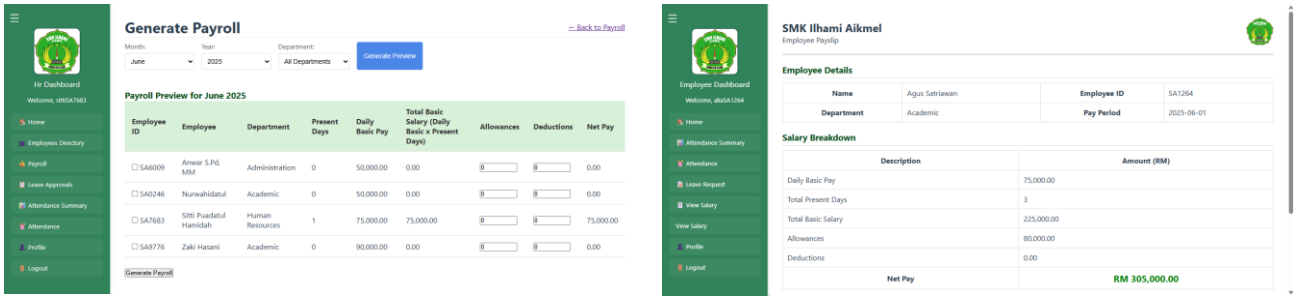
(a) **(b)**

Fig. 20 (a) *Leave Approvals Page; (b) Leave Request Page*

5.2.7 Payroll Management

The Payroll Management module ensures accurate salary processing by integrating attendance data and structured access control. It consists of two main components: Generate Payroll and View Salary, each tailored to specific roles as in Fig. 21. The Generate Payroll page is exclusively accessible to HR roles (HR Manager and HR Officer), allowing them to process employee salaries based on recorded attendance and predefined salary structures. HR users can select the month, year, and department to generate payroll, with calculations including daily basic pay, allowances, and deductions, ensuring transparent salary computation. As for View Salary page, it allows all employees to access their individual payslips, detailing essential salary components such as daily basic salary and and net pay. Employees can review their earnings, ensuring clarity in payroll transactions while

maintaining read-only access to prevent unauthorized modifications. Additionally, the Admin Manager has access to payroll summaries, providing an overview of employee salary distributions across departments.



(a) **(b)**

Fig. 21 (a) *Leave Approvals Page; (b) Leave Request Page*

5.2.8 Audit Logging

Audit logging, as depicted in Fig. 22, is a critical feature in the Employee Management System (EMS) that ensures transparency and security by tracking all user activities within the system. This module records key interactions, including login attempts, logout events, and administrative actions, providing a detailed timestamped record for monitoring system usage. Only the Admin Manager has access to the audit log, enabling them to review system events, detect anomalies, and ensure compliance with security policies. This restricted access ensures that sensitive operational data is protected, preventing unauthorized users from altering or reviewing historical records. The audit log serves as an essential tool for accountability, troubleshooting, and security enforcement, helping administrators maintain system integrity.

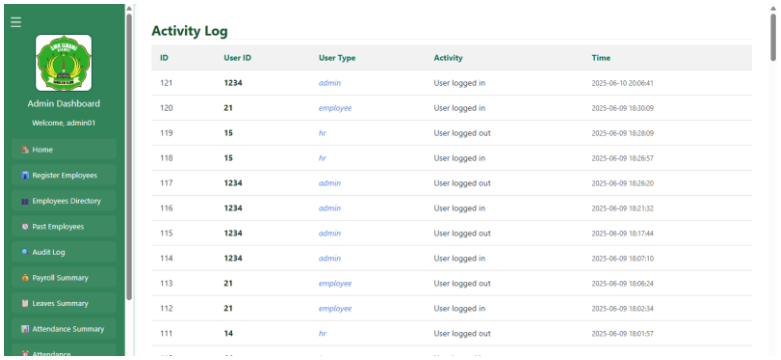


Fig. 22 *Activity Log page*

5.3 Testing

This section focuses on the functional, security, and user acceptance testing (UAT) conducted for the Employee Management System (EMS) for SMK Ilhami Aikmel. Functional testing validates whether system modules operate correctly, ensuring that authentication, role-based access control (RBAC), attendance tracking, leave management, payroll processing, and audit logging function as expected. Security testing assesses vulnerabilities, verifying resilience against unauthorized access, SQL injection, and session management flaws. Additionally, UAT was performed with stakeholders, ensuring usability and alignment with operational needs. These comprehensive tests confirm the system's reliability, security, and compliance with best practices.

5.3.1 Functional Testing

Functional testing of the Employee Management System (EMS) for SMK Ilhami Aikmel was conducted to verify that all modules including user authentication, registration, employee directory, attendance, leave, payroll, profile management, and audit logging to make sure it operates according to requirements and that the role-based access control (RBAC) mechanisms function effectively. Test cases shown in Table 4 covered both typical and exceptional scenarios, confirming that only authorized users could access or modify data, with the system appropriately handling invalid actions and unauthorized access attempts. The results demonstrated that the EMS meets its functional and security requirements, with RBAC successfully restricting access based on user roles, ensuring the system is robust, secure, and ready to support the operational needs of the school.

Table 4 *Functional testing*

No.	Module	Test Case Description	Expected Output	Pass/ Fail
1	User Authentication	Login with valid username and password	Users are logged in and redirected to their dashboard based on role and sub roles	Pass
2	User Authentication	Login with invalid username or password	Error message displayed; access denied	Pass
3	User Authentication	User logs out from the system	User session ends; redirected to login page; access to protected pages is denied until login again	Pass
4	User Authentication	Use "Forgot Password" with registered email	Password reset link sent to email; user can reset password	Pass
5	User Registration	Admin registers a new user with valid data and assigns role/subrole	User is created, credentials generated, admin receives success notification and automate email contain credentials sent to users.	Pass
6	User Registration	Non-admin attempts to register a new user	Access denied; registration option not available	Pass
7	User Registration	Admin registers users with invalid/incomplete data	Error message displayed; user does not create	Pass
8	Employee Directory	Admin/HR Manager views employee directory	List of all registered employees displayed	Pass
9	Employee Directory	HR Officer/Vice Principal views employee directory	List of employees displayed (view-only mode)	Pass
10	Employee Directory	Authorized roles (Admin/HR Manager) edit employee details.	Changes saved and reflected in directory	Pass
11	Employee Directory	Admin Manager edits user accounts details.	Changes saved and reflected in directory	Pass
12	Employee Directory	Unauthorized role attempts to edit/delete employee record	Access denied; no edit/delete option available	Pass
13	Attendance Management	User records daily attendance (clock-in/clock-out)	Attendance recorded for the day; confirmation shown	Pass
14	AttendanceManagement	System stores attendance records by month and date	Attendance data saved and retrievable by date/month	Pass
15	Attendance Management	Authorized user views/downloads attendance summary	Attendance summary displayed and downloadable	Pass
16	Leave Management	User submits leave request with details	Leave request submitted; status set to pending	Pass
17	Leave Management	HR Manager/Officer approves/rejects leave request	Leave status updated; user notified	Pass
18	Leave Management	Authorized user views all users' leave summary	Leave summary displayed as per permissions	Pass
19	Payroll Management	HR auto-generates payroll using attendance and salary data	Payroll generated; summarydisplayed	Pass
20	Payroll Management	HR/Admin Manager views payroll summaries	Payroll summary displayed	Pass
21	Payroll Management	User views own payslip	Payslip displayed for logged-in user only	Pass
22	Profile Management	Users update their profile information	Profile updated; changes saved	Pass
23	Audit Log Module	System logs critical actions performed by users	Actions recorded in audit log	Pass
24	Audit Log Module	Admin Manager views audit logs	Audit log entries displayed	Pass
25	Audit Log Module	Non-admin manager attempts to view audit logs	Access denied; no audit log access	Pass

5.3.2 Security Testing

Security testing was conducted to evaluate the Employee Management System (EMS) against potential vulnerabilities and unauthorized access attempts. The test cases focused on verifying authentication security, session management, access control, password protection, data sanitization, prepared statements, and audit logging to ensure compliance with best security practices.

Authentication tests confirmed that weak passwords are rejected, enforcing strong password policies, while valid credentials triggered OTP verification before allowing access. Session management testing verified automatic logouts after inactivity, preventing unauthorized use of active sessions. Access control tests ensured restricted actions were correctly denied based on RBAC permissions. Password security validation confirmed that the database stores only hashed credentials, preventing plaintext exposure. SQL injection prevention was tested through data sanitization and prepared statements, successfully blocking malicious queries. Lastly, audit logging was validated, ensuring all critical actions are securely recorded for tracking user activity. These tests confirm that the EMS is resilient against security threats, reinforcing authentication security and data protection.

Table 5 *Security testing*

No.	Module	Test Case Description	Expected Output	Pass/ Fail
1	User Authentication	Login with valid username and password	Users are logged in and redirected to their dashboard based on role and sub roles	Pass
1	Authentication	Login with weak password	Password rejected, error displayed	Pass
2	Authentication	Login with valid credentials	OTP sent via email, user redirected upon verification	Pass
3	Session Management	Auto logout after inactivity	Session terminated, user redirected to login	Pass
4	Access Control	Unauthorized user attempts restricted action	Access denied, error message displayed	Pass
5	Password Security	Attempt to retrieve unhashed passwords	Database stores only hashed credentials	Pass
6	Data Sanitization	Submit login with SQL injection attempt	Query execution blocked, input sanitized	Pass
7	Prepared Statements	Attempt SQL injection with parameterized query	Malicious query rejected	Pass
8	Audit Logging	Check recorded user actions	Log entries correctly stored	Pass

5.3.3 User Acceptance Testing

Users from various roles at SMK Ilhami Aikmel evaluated the Employee Management System (EMS) across core functionalities including, login, dashboard, employee management, attendance, payroll, leave, and audit logging. Ratings were given on a scale from 1 (strongly disagree) to 5 (strongly agree). As shown in Table 6, users expressed high satisfaction with system usability, role-based access, and core features. The login and dashboard functions were seamless, and modules like payroll and leave management were efficient and accurate. Furthermore, the attendance module received positive remarks for its real-time updates and comprehensive reporting capabilities. While the audit logging feature was generally well regarded, a user suggested minor improvements to enhance readability and clarity. Overall, the system met user expectations and is ready for deployment with only minor refinements recommended.

Table 6 *UAT testing*

No	UAT Question	Average Score	Result
1	I was able to login successfully with my role credentials.	5	Pass
2	The dashboard displayed matches my role and responsibilities.	5	Pass
3	The Forgot Password function works correctly and sends a reset link.	5	Pass
4	The system is easy to use and navigate.	5	Pass
5	I was able to register a new user.	5	Pass
6	The registration form is complete and functional.		Pass
7	The newly registered user can log in successfully.	5	Pass

Table 6 *(Cont.)*

No	UAT Question	Average Score	Result
8	I can view the list of all employees with correct details.	5	Pass
9	The Edit and Delete functions work (if accessible to my role).	5	Pass
10	The employee directory layout is clear and user-friendly.	5	Pass
11	I can take attendance without issues.	5	Pass
12	The attendance taking interface is easy to use.	5	Pass
13	I can view attendance summaries clearly and accurately.	5	Pass
14	The attendance system updates in real-time.	5	Pass
15	Attendance summary reports are updated in real time.	5	Pass
16	I can generate and download an attendance report.	5	Pass
17	I can view payroll summaries (if applicable).	5	Pass
18	I can generate payroll accurately (if applicable).	5	Pass
19	I can view my own payslip/salary details.	5	Pass
20	The salary information shown is correct and updated.	5	Pass
21	I can request leave without issues.	5	Pass
22	I receive proper feedback or updates on my leave application.	5	Pass
23	I can approve/reject leave applications if I have the role permission.	5	Pass
24	I can view the system audit log.	5	Pass
25	The log entries are detailed and useful.	4	Pass
26	The system meets my work needs effectively.	5	Pass
27	I am satisfied with the performance and design.	5	Pass

6. Conclusion and Future Work

The Employee Management System (EMS) developed for SMK Ilhami Aikmel successfully automates key employee-related processes, integrating modules such as user authentication, attendance tracking, leave management, payroll processing, and audit logging. The implementation of Role-Based Access Control (RBAC) ensures secure, role-specific access, protecting sensitive data and preventing unauthorized actions. Functional and security testing confirmed the system's reliability and resilience against common cyber threats, while features like password hashing, session management, and two-factor authentication enhance overall security.

The EMS meets its objectives by streamlining administrative tasks, reducing manual errors, and improving HR efficiency. Audit logging provides accountability and security monitoring, supporting compliance with industry standards. Although minor challenges exist such as dependency on email-based OTP and session timeout usability, these do not detract from the system's effectiveness.

Future improvements will focus on expanding multi-factor authentication options, refining RBAC flexibility, enhancing payroll automation, and incorporating advanced analytics and security measures. Overall, the EMS provides a robust, scalable foundation for efficient and secure workforce management at SMK Ilhami Aikmel.

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:*** *A. Baharuddin, Z. Abdullah;* ***data collection:*** *A. Baharuddin, Z. Abdullah;* ***analysis and interpretation of results:*** *A. Baharuddin, Z. Abdullah;* ***draft manuscript preparation:*** *A. Baharuddin, Z. Abdullah. All authors reviewed the results and approved the final version of the manuscript.*

References

[1] K. C. Laudon and J. P. Laudon, Management Information Systems: Managing the Digital Firm, 15th ed. Pearson, 2018.
[2] A. Kumar, "What is MIS? Characteristics, objectives, role, component," Geektonight, May 04, 2023. https://www.geektonight.com/what-is-mis/#google_vignette
[3] "Management Information Systems (MIS) – Types and roles," Communication Theory, Nov. 18, 2024. https://www.communicationtheory.org/management-information-systems-mis-types-and-roles/
[4] N. Fitria, I. Wijayanti, A. Santoso, S. Romadon, and K. Kraugusteeliana, "The role of management information systems in human resource competency development," Jurnal Minfo Polgan, vol. 12, pp. 1387-1396, Jul. 2023. doi: 10.33395/jmp.v12i1.12764.
[5] P. Gajendrakar, "Management Information System," WallStreetMojo, Dec. 18, 2024. https://www.wallstreetmojo.com/management-information-system/
[6] Z. Liu, W. Gu, and J. Xia, "Review of access control model," Computers, Materials & Continua/Computers, Materials & Continua (Print), vol. 61, no. 3, pp. 43–50, Jan. 2019, doi: 10.32604/jcs.2019.06070.
[7] S. Lanchec, "Implementing Access Control: Best Practices for Developers," Forest Admin Blog, Apr. 30, 2024. Available: https://www.forestadmin.com/blog/access-control-implementation/
[8] R. S. Sandhu, E. J. Coyne, H. L. Feinstein and C. E. Youman, "Role-based access control models," in Computer, vol. 29, no. 2, pp. 38-47, Feb. 1996, doi: 10.1109/2.485845.
[9] M. Krystian, "Role-Based Access Control: Definition and Benefits | Rippling," Rippling, Oct. 23, 2024. https://www.rippling.com/blog/role-based-access-control
[10] [10] M. Porter, R. Bording, and Y. Fu, "UML-based Design of Vendor and Employee Management System," ASEE Annual Conference and Exposition, Conference Proceedings, 2021. Available: https://doi.org/10.18260/1-2--37945
[11] R. E. Ozighor, V. O. Adebola, and F. Uloko, "Employee Management System for Nigerian Universities," International Journal of Scientific Research and Management, vol. 11, no. 02, 2023. Available: https://doi.org/10.18535/ijsrm/v11i02.em13
[12] S. Nanayakkara, U. Ekanayake, G. Subasinghe, C. Jayasena, D. I. De Silva, and D. Cooray, "A Web Based Employee Management System," International Journal of Engineering and Management Research, vol. 12, no. 5, 2022. Available: https://doi.org/10.31033/ijemr.12.5.10