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

AITCS

Vol. 6 No. 2 (2025) 568-585
https://publisher.uthm.edu.my/periodicals/index.php/aitcs

Unsafe Condition and Unsafe Act (UCUA) Reporting System for Johor Port with OTP Authentication

Nursyahmina Mosdy[1], Cik Feresa Mohd Foozy[1]

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

*Corresponding Author: feresa@uthm.edu.my
DOI: https://doi.org/10.30880/aitcs.2025.06.02.031

Article Info

Received: 18 November 2025
Accepted: 19 November 2025
Available online: 30 November 2025

Keywords

Safety Reporting System, Unsafe Condition and Unsafe Act, Web-based Application

Abstract

The Johor Port Unsafe Condition and Unsafe Act (UCUA) Reporting System handles the issues of managing safety reports, which are currently handled via paper forms and limited online submissions, resulting in delays and increased safety concerns. The goal of this project is to create a web-based UCUA Reporting System applying the Laravel framework, which will streamline the reporting and tracking processes for port personnel and the Health, Safety, Security, and Environment (HSSE) department. The key components like incident reporting, compliance tracking, and notifications are all part of the system, which was created using structured web application approach. The system incorporates important security features like input validation, role-based access control, user authentication, and encrypted data processing to guarantee safe and dependable operations. By improving efficiency, accountability, security, and data management, this system's operation enables quicker reactions to safety concerns and better regulatory compliance. It is expected that future advancements like advanced analytics integration and mobile accessibility would enhance Johor Port's reporting system even more.

1. Introduction

In the context of port operations, managing Unsafe Condition and Unsafe Act (UCUA) is crucial to assure user safety and regulatory compliance. As highlighted in previous studies, an effective online reporting system is essential for addressing the challenges associated with safety reporting in the port industry [1]. The current reporting procedure is open to miscommunication, manual errors, and a lack of accountability, which prevents the identification and resolution of recurrent safety issues. The World Bank's Environmental and Social Commitment Plan (ESCP) emphasizes the importance of effective communication and reporting to ensure compliance with safety laws [2]. The existing reporting system suffers several issues which hinder the Health, Safety, Security and Environment (HSSE) department's ability to manage penalties, track unsafe acts, and enhance safety standards. These gaps raise the possibility of unresolved safety concerns, accidents, and compliance issues. As noted in, near-miss incidents can serve as critical indicators of potential hazards, emphasising the need for an automated system that facilitates timely reporting and evaluation [3]. The system will contain modules for incident reporting, alerts, compliance tracking, and data analytics, resulting in shorter response times and improved management of safety risks. The objective of the project is to create a user friendly and reliable UCUA Reporting System for Johor Port by developing the system using a Laravel

framework. Core modules such user registration and login, incident reporting, report approval, notification alerts, and compliance tracking are all included in the system's scope.Additionally to make sure the system satisfies operational safety standards, the project also proposes to evaluate the system's use and functionality among port workers and HSSE personnel.The study also intends to show how safety online reporting systems may enhance safety compliance and regulatory outcomes which will benefit the port environment as well as the stakeholders [4].

2. Related Work

This section discusses the literature review related to the Unsafe Condition and Unsafe Act (UCUA) Reporting System. It covers three major topics which are the concepts of reporting systems, authentication procedures, and current related systems.

2.1 Reporting System

A reporting system is a structured process for managing, documenting, and analysing data related to incidents or events in a certain domain. High-risk areas, such as ports, require enhanced safety management due to heavy machinery, hazardous materials, and prohibited zone[5]. Online reporting solutions are more efficient than traditional paper-based alternatives, allowing for real-time reporting, greater tracking, and enhanced regulatory compliance. The UCUA Reporting System for Johor Port aims to use these advantages to build a safer workplace through a reliable and efficient safety reporting system.

2.2 Authentication

Authentication is crucial for system security since it ensures that only authorized users have access to sensitive data. Single-Factor Authentication (SFA), which uses a single credential like a password, provides a basic level of protection. To address the limitations of SFA, Two-Factor Authentication (2FA) combines knowledge-based credentials like passwords with possession-based methods like One-Time Passwords (OTPs). Studies suggest that this strategy considerably strengthens security, reducing the likelihood of unauthorized access to critical information [6]. Multi-Factor Authentication (MFA) adds levels of protection, such as biometric verification, for environments that require even more [11]. MFA's integration of multiple authentication techniques makes it suited for high-security applications and these advances in authentication technology not only ensure user confidential data but also improve the overall security of systems such as the UCUA Reporting System, which protects crucial safety data.

2.2.1 Existing Reporting System

This section focusses on existing systems related to the Unsafe Condition and Unsafe Act (UCUA) Reporting System in Johor Port. The goal is to gain an understanding of the functioning of other systems to provide more useful information for the development of the UCUA Reporting System. The following sections give a detailed overview of three related systems: DEFTECH UCUA System, the Civil Aviation Authority of Malaysia (CAAM) Safety Reporting System, and Procore Quality and Safety

2.2.2 DEFTECH UCUA System

Defence Technologies Sdn Bhd (DEFTECH) created the UCUA (Unsafe Condition and Unsafe Act) Reporting System to improve safety management across a variety of industries as in Fig. 1. The system fosters a proactive safety culture by enabling stakeholders, contractors, and employees to report harmful acts and conditions. Its primary aim is to speed incident reporting and resolution using a web-based platform.

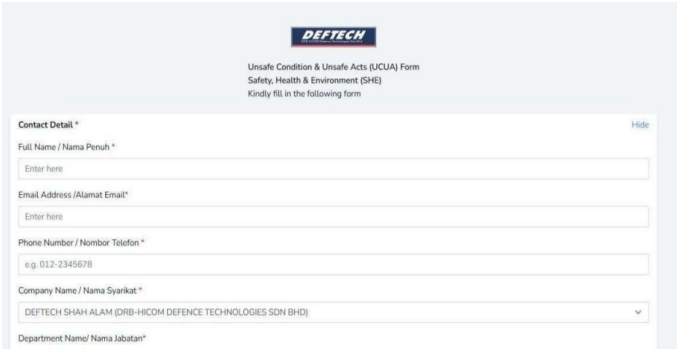

Fig.1 *The DEFTECH UCUA System*

2.2.3 Civil Aviation Authority of Malaysia (CAAM) Safety Reporting System

The CAReS platform as in Fig. 2 is created by the Civil Aviation Authority of Malaysia (CAAM), allows aviation workers, including pilots, air traffic controllers, and ground crew, to report issues with safety. The system facilitates both mandatory and voluntary reporting of safety incidents to enhance safety standards and ensure compliance to regulations. CAReS encompass various features: a confidential reporting system, classification of safety incidents, and data analysis to discern potential dangers and trends.

The CAReS platform's category and confidential reporting capabilities can enhance the UCUA Reporting System. The system promotes proactive reporting and ensures proper documentation and resolution of essential safety information by facilitating secure, anonymous reporting and classifying occurrences by risk category.

Fig.2 *The CAAM Reporting System*

2.2.4 Procore Quality and Safety

The Procore Quality and Safety in Fig. 3 is a digital platform that is commonly used in the construction sector to monitor and document safety incidents and quality assurance. It contains tools for reporting events, conducting safety inspections, and addressing identified concerns.

This solution provides mobile accessibility, allowing on-site staff to submit reports in real time, attach photographs, and update statuses while on the go. In addition, it connects with other Procore project management products, allowing for smooth communication and coordination between teams. Procore's mobile reporting and inspection modules serve as a model for the UCUA Reporting System by allowing for instant on-site incident logging. The use of multimedia attachments and a mobile-friendly design can improve system performance in Johor Port by ensuring that safety data is captured accurately and in real time.

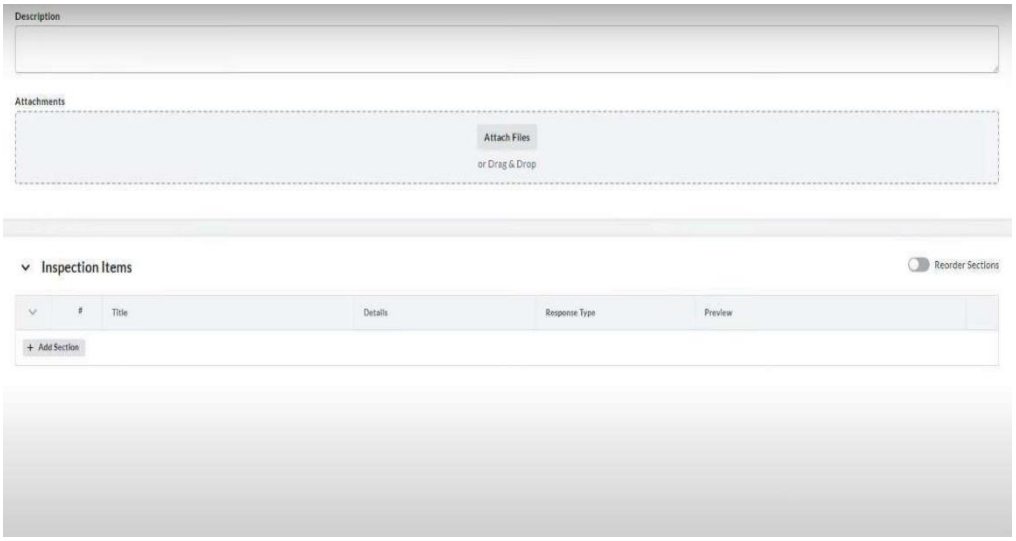

Fig.3 *The Procore Quality and Safety System*

Table 1 compares existing reporting systems DEFTECH UCUA Safety System, Civil Aviation Authority of Malaysia (CAAM) Safety Reporting System, and Procore Quality and Safety) to the proposed Unsafe Condition and Unsafe Act (UCUA) Reporting System in Johor Port.

Table 1: Comparison table between reviewed applications and Proposed System

Features / Systems	DEFTECH UCUA Safety System [7]	Civil Aviation Authority of Malaysia (CAAM) Safety Reporting System [8]	Procore Quality and Safety [9]	Unsafe Condition and Unsafe Act (UCUA) Reporting System in Johor Port
Platform	Web-base	Web-based	Web-based and mobile based	Web-based
Complaint Submission	Yes	Yes	Yes	Yes
Incident Tracking	Yes	No	Yes	Yes
Confidential Reporting	No	Yes	No	Yes
Use Risk Categorization	No	Yes	No	Yes
Trend Complain Analysis	Yes	No	Yes	Yes
Status Update	Yes	No	Yes	Yes
Authentication	Yes	Yes	Unknown	Yes
Role Based Access Control (RBAC)	Yes	Yes	Yes	Yes
Email OTP	No	No	No	Yes
Target Users	DEFTECH staff and stakeholders	Aviation personnel	Personal site construction	Johor Port staff and HSSE personnel

Table 1 shows the similarities and differences between the UCUA Reporting System at Johor Port and the three current systems: the CAAM Safety Reporting System, the DEFTECH UCUA Safety System, and the Procore Quality and Safety System. To begin with, in terms of platform accessibility, all four systems provide a web-based platform for incident or complaint submissions, with Procore also offering a mobile app for on-site reporting. When it comes to tracking incidents, DEFTECH, Procore, and the UCUA system let users see the progress of their reports right away. On the other hand, CAAM is more focused on collecting reports than on giving users regular updates on their status. CAAM, UCUA, and DEFTECH promote anonymous reporting to enable whistleblowers without fear of being attack, hence increasing user trust. However, UCUA and DEFTECH go beyond anonymity by implementing role-based access control (RBAC), which ensures that only authorised workers have access to certain system features. The UCUA system also uses email-based One-Time Password (OTP) verification upon login to prevent unauthorised access. Furthermore, DEFTECH and UCUA use risk categorisation systems that assist prioritisation while in contrast, Procore's security features are limited in publicly available documentation. This makes UCUA the most comprehensive system in terms of access control and data confidentiality when compared to other systems.

3. Methodology

The Agile Model is the software development technique used for Johor Port's Unsafe Condition and Unsafe Act (UCUA) Reporting System. Agile is a flexible process that focusses on iterative development, collaboration, and flexibility to changing requirements. Fig. 4 shows the Agile Model's phases: requirement gathering, design, development, testing, deployment, and review. These phases are conducted iteratively to ensure that the system meets stakeholder requirements and expectations.

Fig.4 *The Agile Model*

3.1 Requirements Phase

During the requirements phase, early information and resources required for system development were collected. This involved doing a thorough review of relevant articles, journals, and case studies on Agile techniques and their implementation in similar systems. Interviews with Johor Port workers were undertaken to determine specific safety reporting difficulties and requirements. The information obtained formed the groundwork for the creation of a web-based safety reporting system adapted to the needs of Johor Port and its stakeholder.

3.2 Design Phase

The design phase focused on developing efficient, user-friendly, and secure system architecture with Laravel, a PHP framework chosen for its scalability and ease of implementation. Unified Modelling Language (UML) diagrams, such as use case diagrams and sequence diagrams, were created to explain the system's workflow and interactions with users and system components. The iterative design process used stakeholder feedback during sprint reviews to improve the user interface and overall system structure. Using Laravel's built-in features, the solution assured compliance with confidentiality while also providing interactive user experience.

3.3 Development Phase

During the development phase, the focus was on coding and putting the system's functionalities into action in sync with the concept. Using Laravel, features were built in iterative phases according to the Agile project management methodology. In order ensure that the functionality was correct, unit testing was performed on each iteration. After identifying any problems, quick action was taken to resolve them before moving on to the following cycle. Throughout this phase, continuous feedback from stakeholders was incorporated to guarantee that the system was in sync with the requirements of the users. By using an iterative development method, a web application that was both dependable and secure was created and made ready for deployment.

3.4 Testing Phase

The testing phase ensured that the system was reliable, functional, and met user needs. The method started with Unit Testing, in which individual functions, classes, and modules were tested separately. Laravel's built-in testing tools were used to ensure that these components worked as intended. Following that, Integration Testing was carried out to check that all system components, including the database, user interface, and backend logic, worked together seamlessly. This stage confirmed the accuracy and consistency of the data flow and communications. System Testing was then carried out to evaluate the overall performance of the system. This thorough evaluation guaranteed that all features worked as intended and met usability and security standards. Finally, during User Acceptance Testing (UAT), real stakeholders and end users tested the system in real-world scenarios. Their feedback was gathered to identify potential usability issues and to ensure that the system met their expectations and requirements. These iterative testing operations ensured that the final product was functional and user friendly, making it suitable for deployment.

3.5 Deployment Phase

The UCUA Reporting System moves from the development environment to a live, functional platform during the deployment phase. The database is complete to guarantee the data handling, and the system is set up on a secure server. To help administrators and end users, thorough documentation is provided, including installation instructions and user guide. Training sessions are held for Johor Port's port workers and HSSE personnel to promote adoption. The functions of the system, such as tracking submissions and reporting incidents are covered in these sessions. To assist users, onboarding resources including FAQs and user manual are offered.

3.6 Review Phase

The review phase included evaluating the system's overall performance and gathering feedback from stakeholders to guide future enhancements. Personnel at Johor Port were surveyed to analyse their experiences, issues, and suggestions for system improvements. Feedback was documented to assist future development and keep the UCUA Reporting System up-to-date effective, and user-friendly.

4. System Analysis and Design

This section shows how the UCUA Reporting System for Johor Port was developed based on the system analysis and design processes used. It includes identifying system requirements, modelling with UML diagrams, architectural design, and implementing security measures to ensure safe and reliable operations as implemented, tested, and evaluated. The system was built utilising the Laravel framework for backend functionality and HTML, CSS, and JavaScript for frontend development, with MySQL serving as the database. User Acceptance Testing (UAT) was carried out to ensure that the system's functionality and usability met user criteria.

4.1 System Requirements

System requirements analysis is critical for structuring the system based on its modules and characteristics, assuring maximum performance and efficiency. Both functional and non-functional requirements are listed below.

4.1.1 Functional Requirements

Functional requirement is a function or module parts that developers need to implement to make sure the system is running and accomplished its task. Functional requirements can be defined as how the system should be used and how it performs. It is important to implement the function accordingly to make sure the system works well as it intended. The functional requirement in this project is summarized in Table 2.

Table 2 *Functional Requirements UCUA Reporting System for Johor Port*

No	Function	Functionalities
1.	Login Module	Allow users such as HSSE personnels and port workers to log in using the account that they had created.
2.	Register Module	Allow the user to sign up as a new user with validated information. Allow users to create new accounts before using the system.
3.	Report Submission Module	Allow the port workers to submit UCUA reports describing unsafe conditions or acts.
4.	Approval Module	Allow HSSE personnel to review and approve the reports according to the report that they had sent by the port workers.
5.	Notification Module	Send notification about the penalty, the status of their reports and there are also reminders about penalties for their banned actions at the restricted area.

4.1.2 Non- Functional Requirements

In contrast to functional requirements, non-functional requirements specify how the system must operate to satisfy user expectations. To improve user expectations when using the system, it describes its capabilities. The non- functional requirements are presented in Table 3.

Table 3 *Non- Functional Requirement for UCUA Reporting System*

No	Requirement	Description
1.	Performance	Increase the user efficiency to make reports that happen in port when using the website.
2.	Operational	The system should be user friendly.
		The system is only available when there is an internet connection.
3.	Security	Only admin can generate the report that has been submitted.
		Users can only access their own account with user id and password
4.	Availability	The system should be able to use for website browsers.

4.1.3 System Analysis

Several UML diagrams, including use case, sequence, activity, and class diagrams, were created as part of the system analysis to guarantee a complete understanding of the Unsafe Condition and Unsafe Act (UCUA) Reporting System's operation and design.

4.1.4 Class Diagram

A class diagram is a form of diagram in the Unified Modelling Language (UML) that depicts the system's structure through classes, attributes, and their interactions. The class diagram in Fig. 5 for Johor Port's UCUA Reporting System shows the essential elements of the reporting process. For example, while Admin oversees and issues warnings, PortWorker can submit reports. Both UnsafeCondition and UnsafeAct are connected to the Report class, demonstrating the categorisation of reports. The sequence of processes, including department assignment, warnings, and generating notification is shown as well in the diagram. Fig. 5 shows the class diagram of UCUA Reporting System in Johor Port.

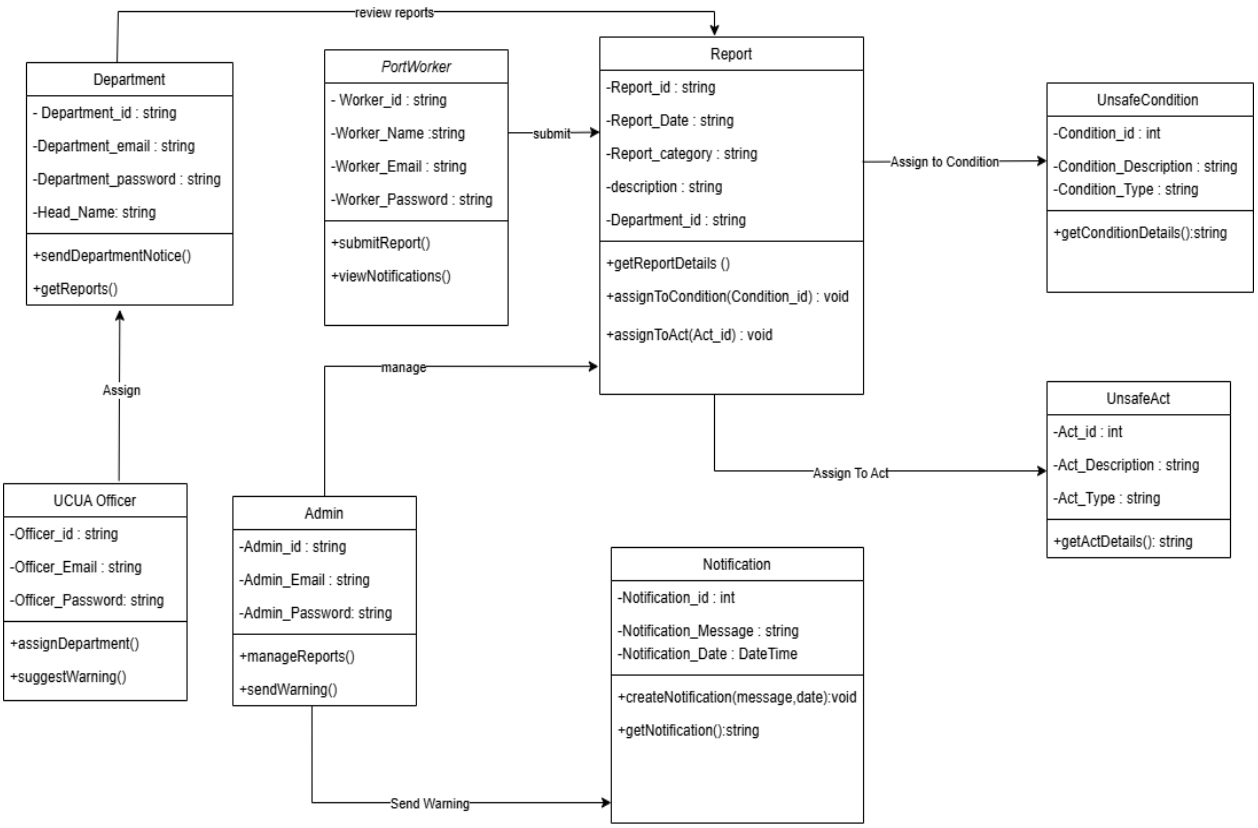

Fig.5 *Class Diagram of UCUA Reporting System for Johor Port*

4.1.5 Use Case Diagram

The use case diagram was created as part of a study of the system's overall functionality. It reflects the system's technique for identifying and organising the system needs of the UCUA Reporting System. The actors are user, admin, UCUA Officer and Head of Department who conduct different tasks within the modules illustrated in theuse case diagram. Fig. 6 shows use case Diagram of UCUA Reporting System in Johor Port.

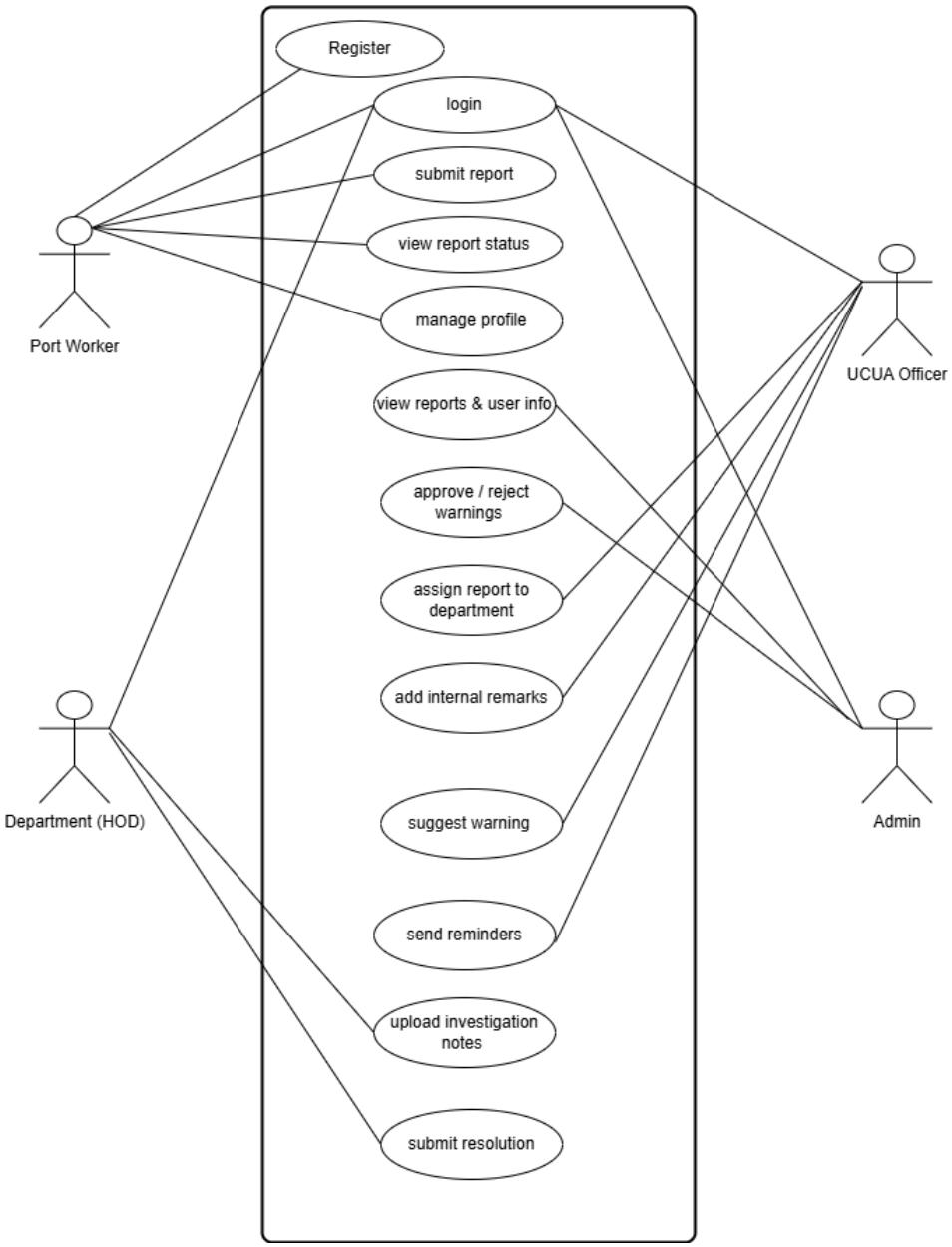

Fig.6 *Use Case Diagram of UCUA Reporting System for Johor Port*

4.1.6 Flowchart

A user's step-by-step procedure in the Unsafe Condition and Unsafe Act (UCUA) Reporting System is shown in the flowchart. The system's objectives of enhancing safety and accountability are in line with this organised flow, which guarantees that users can report problems effectively while being held responsible for unsafe behaviour. Fig. 7 shows flowchart user, admin, UCUA Officer and Head of Department of UCUA Reporting System in Johor Port.

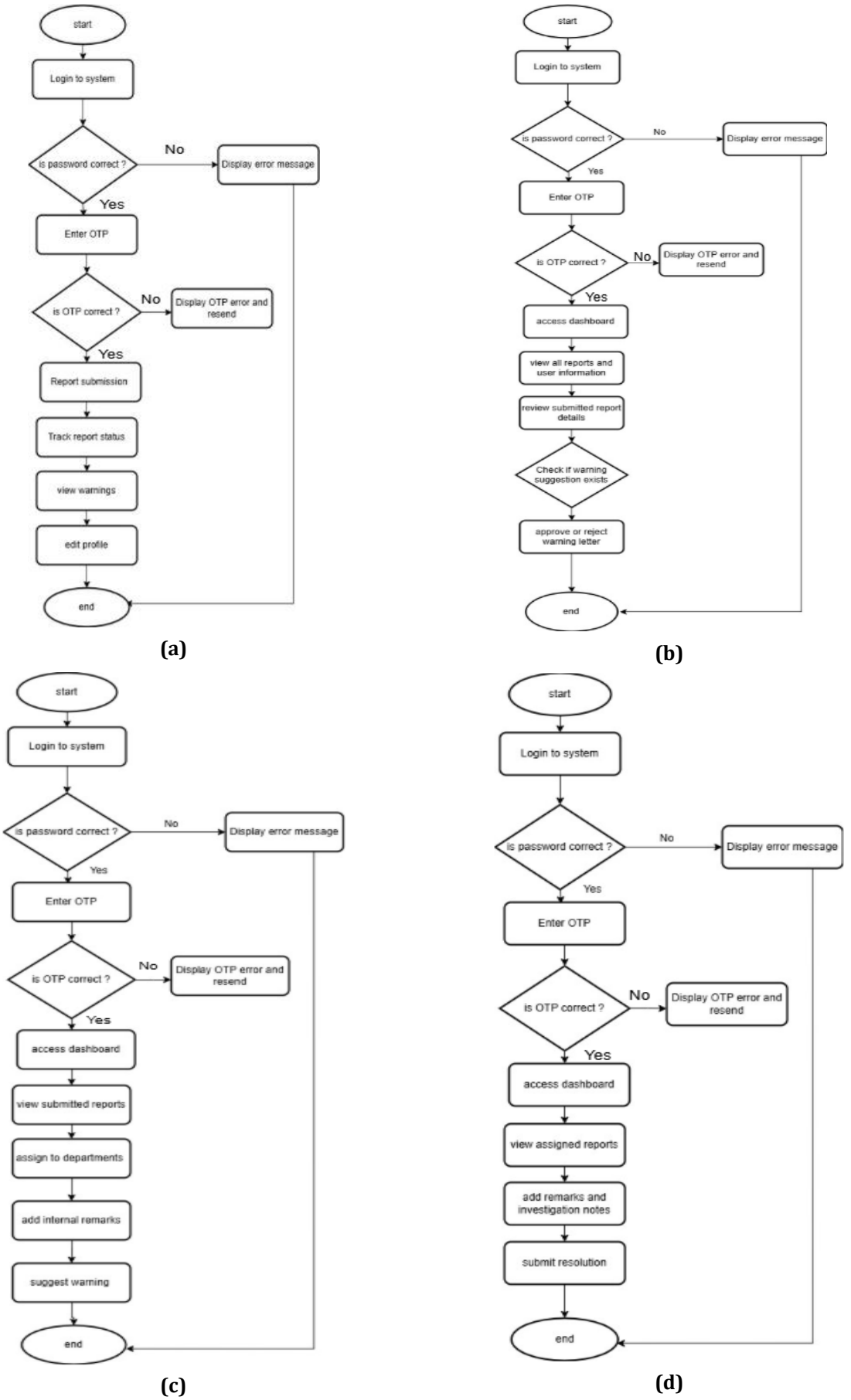

Fig. 7 *The flowchart for the system (a)flowchart for user; (b) shows flowchart for admin* (c)flowchart for UCUA Officer; (d) shows flowchart for HOD

4.2 System Design

A conceptual representation of the components and subcomponents that define a system's behaviour is known as system architecture design. This blueprint serves as a reference for defining the project's goals and designing the system. The system is designed to be used via a web browser, giving users greater flexibility and convenience by the UCUA Reporting System in Johor Port.

4.2.1 System Architecture

The front end serves as the system's user interface, bridging the gap between users and internal system activities which are displayed in Fig. 8. The User Interface (front end) allows users to register, log in, submit, and view report status. It is built using HTML, CSS, and JavaScript, as well as Laravel Blade for templating, to create a responsive and intuitive user experience.

Administrators can log in to view reports and update report statuses to ensure reports are processed efficiently. Using Laravel, the back end is responsible for processing user requests, validating all data, and doing any computations or actions necessary by the system. The system's database is MySQL, which was chosen for its stability and efficiency.

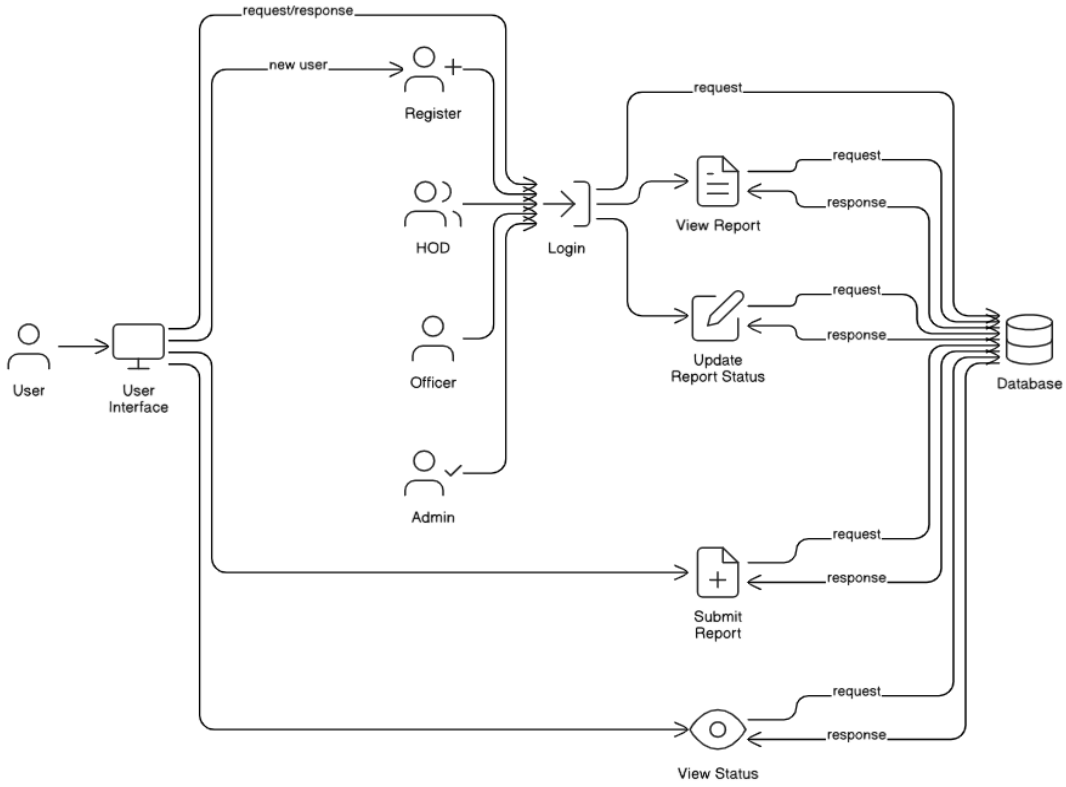

Fig. 8 *The system's architecture for UCUA Reporting System for Johor Port*

5. Implementation and Testing

The section outlines the implementation of various module in UCUA Reporting System in which consists of all security implementation. Before the system was fully launched, it went through several rounds of testing to make sure everything worked well.

5.1 Security Implementation

The security measures implemented into the Johor Port Unsafe Condition and Unsafe Act (UCUA) Reporting System are thoroughly described in this section. It describes the approaches and controls put in place to protect the system from different kinds of online threats and illegal access. Every security feature is covered in detail, including its function, way of implementation, and contribution to the platform's overall resilience.

5.1.1 Enhance One-Time Password (OTP)

Fig 9 and Fig. 10 illustrate how to implement an enhanced One-Time Password generating process that serves as the system's second-factor authentication mechanism. Following successful completion of the first

authentication stage (password and username matching), it is activated each time a user signs in. The approach is intended to generate a 6-character OTP that is both secure and randomised. The first step is to make sure that each of the following character types is represented: capital, lowercase, special, and number characters.

This ensures that the OTP is complex and covers a wide variety of character types. Following the inclusion of one character from each category, the function uses random selections from the combined pool of all permitted characters to fill the remaining OTP characters. The generated OTP string undergoes to a shuffling operation to randomly arrange the characters to further improve security and unpredictability. Because of this, it is more difficult to forecast or reverse-engineer the final OTP. The user will be requested to request a new OTP after the five minutes that it is supposed to be valid expire.

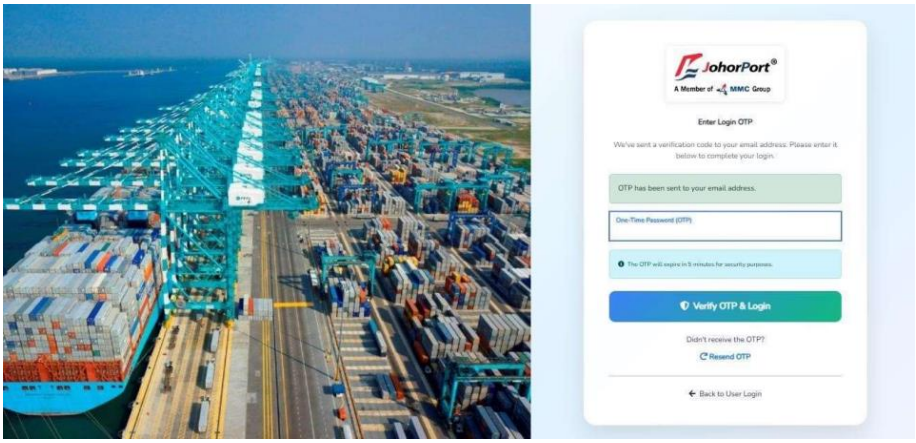

Fig. 9 *OTP's algorithm a forming pattern interface*

```php
public function generateSecureOtp(): string
{
    $uppercase = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ';
    $lowercase = 'abcdefghijklmnopqrstuvwxyz';
    $numbers = '0123456789';
    $specialChars = '!@#$%^&*';

    $otp = '';

    // Ensure at least one character from each category
    $otp .= $uppercase[random_int(min: 0, max: strlen(string: $uppercase) - 1)];
    $otp .= $lowercase[random_int(min: 0, max: strlen(string: $lowercase) - 1)];
    $otp .= $numbers[random_int(min: 0, max: strlen(string: $numbers) - 1)];
    $otp .= $specialChars[random_int(min: 0, max: strlen(string: $specialChars) - 1)];

    // Fill remaining positions with random characters from all categories
    $allChars = $uppercase . $lowercase . $numbers . $specialChars;
    for ($i = 4; $i < 6; $i++) {
        $otp .= $allChars[random_int(min: 0, max: strlen(string: $allChars) - 1)];
    }

    // Shuffle the OTP to randomize the order
    return str_shuffle(string: $otp);
```

Fig. 10 *Code snippet of enhanced OTP's algorithm a forming pattern*

5.1.2 Strong Password Policy

The system enforces a strong password policy during user registration to improve security and reduce unauthorised access as in Fig. 11. This policy lowers the danger of brute-force attacks by requiring users to create passwords that are at least 12 characters long and no more than 32 characters. At least one lowercase letter (a–z), one uppercase letter (A–Z), one numeric digit (0–9), and one special character from the set [@$! %*? &] must be included in the password, as indicated by the code shown in Fig. 12. By ensuring that the password is sufficiently complicated, these requirements greatly improve resistance to typical attack patterns like dictionary attacks and simple guesses. To ensure accuracy and minimise user entry errors, users must also validate the password field by entering it again. All users, administrators, and department heads are subject to strong password hygiene across the system.

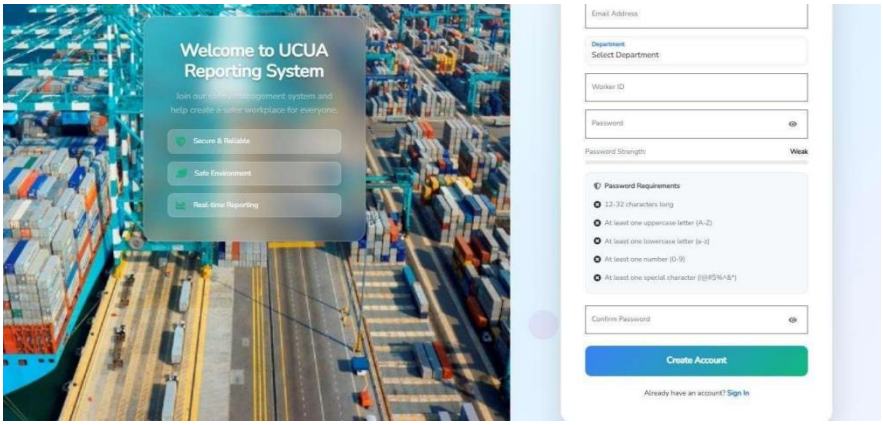

Fig. 11 *Password policy implementation*

```php
protected function validator(array $data): Validator
{
    return Validator::make(data: $data, rules: [
        'name' => ['required', 'string', 'max:255'],
        'email' => ['required', 'string', 'email', 'max:255', 'unique:users'],
        'worker_id' => ['required', 'string', 'unique:users'],
        'department_id' => ['required', 'exists:departments,id'],
        'password' => [
            'required',
            'string',
            'min:12',
            'max:32',
            'regex:/^(?=.*[a-z])(?=.*[A-Z])(?=.*\d)(?=.*[@$!%*?&])[A-Za-z\d@$!%*?&]{12,32}$/',
            'confirmed'
        ],
    ]);
}
```

Fig. 12 *Code snippet of password policy implementation*

5.1.3 Identity Management Based on the Role

The system carefully handles and assigns user access and privileges according to their assigned roles (Fig. 13). As seen in Fig. 14, the roles that have been defined are Web, Admin, UCUA, and Department. To guarantee that access is limited to the relevant information and features, each position is set up with its own user provider and authentication guard. The application maintains a clear division of responsibilities, reduces internal risks, and enhances overall security and organisation by utilising a role-based access control (RBAC) framework.

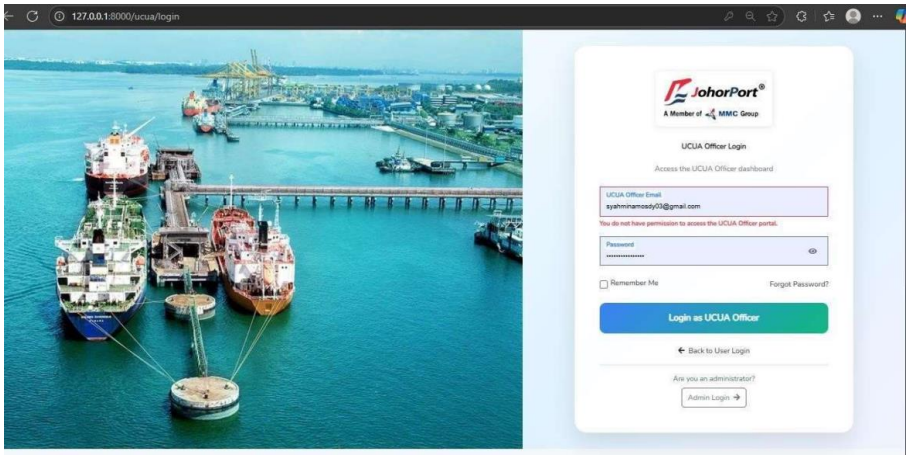

Fig. 13 *Role definition before login*

```
'guards' => [
    'web' => [
        'driver' => 'session',
        'provider' => 'users',
    ],
    'admin' => [
        'driver' => 'session',
        'provider' => 'users',
    ],
    'ucua' => [
        'driver' => 'session',
        'provider' => 'users',
    ],
    'department' => [
        'driver' => 'session',
        'provider' => 'departments',
    ],
],
```

Fig. 14 *Code snippet of role definition before login*

5.2 Module Implementation

5.2.1 Reporting and Tracking Module

Fig. 15 shows the report submission form, where users can submit unsafe condition or unsafe act reports. The form includes fields such as report category, location of event, date and time, detailed description and upload attachments.

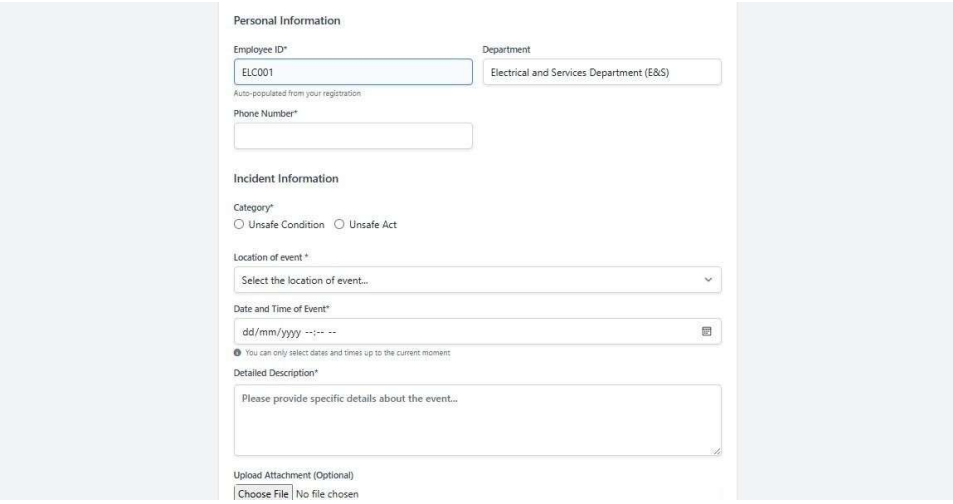

Fig. 15 *Record submission form*

Fig. 16 displays the report tracking interface accessible to users. This page presents a compilation of submitted reports alongside their current statuses, including "submitted," "under review," "investigation," and "resolved." Users can access comprehensive comments and updates from the Heads of Departments managing their report.

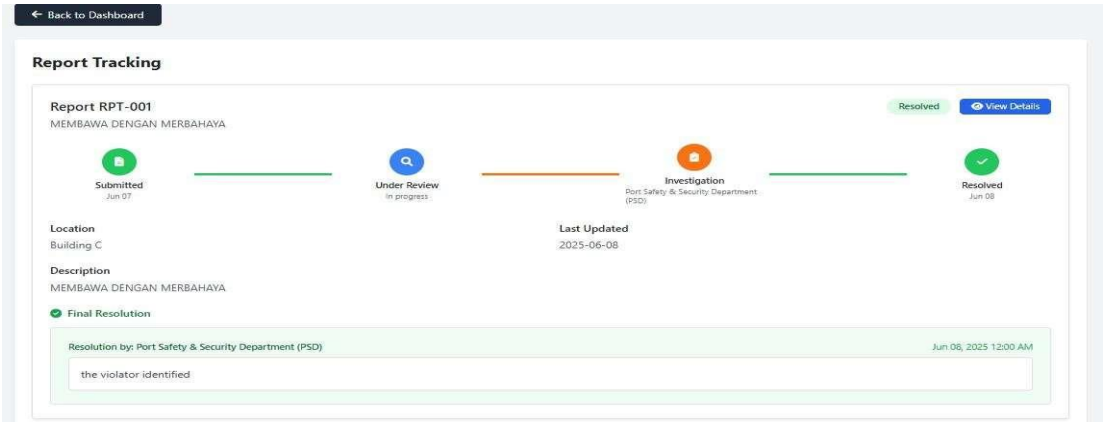

Fig. 16 *Report tracking interface*

5.2.2 Admin and UCUA Officer Dashboard

Fig. 17 illustrates the administrative dashboard that offers an outline of submitted reports, user engagement, and expedited access to management tools. It assists administrators in overseeing the system's comprehensive performance.

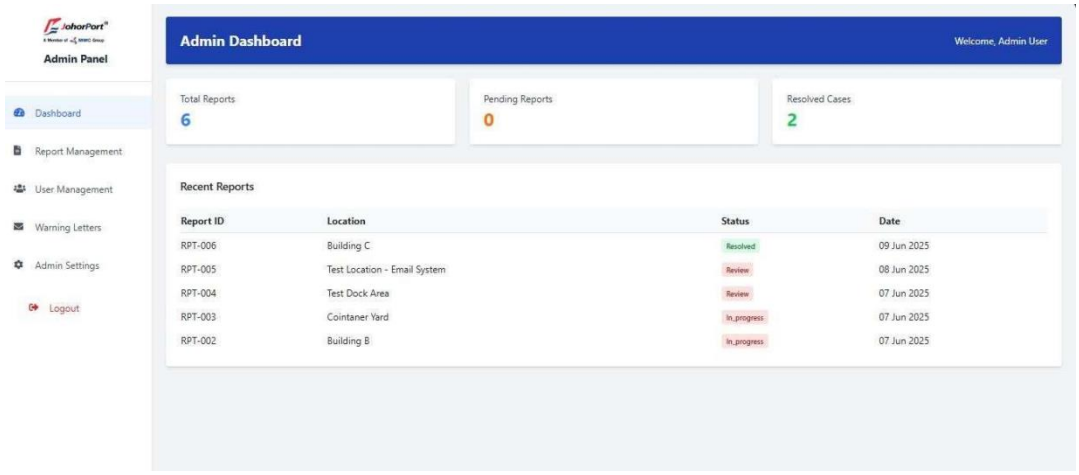

Fig. 17 *Administrative dashboard*

Fig. 18 shows the UCUA Officer Dashboard Management Table in which the officers can the list of reports and the violator status that had been assigned by the department based on the case of reports.

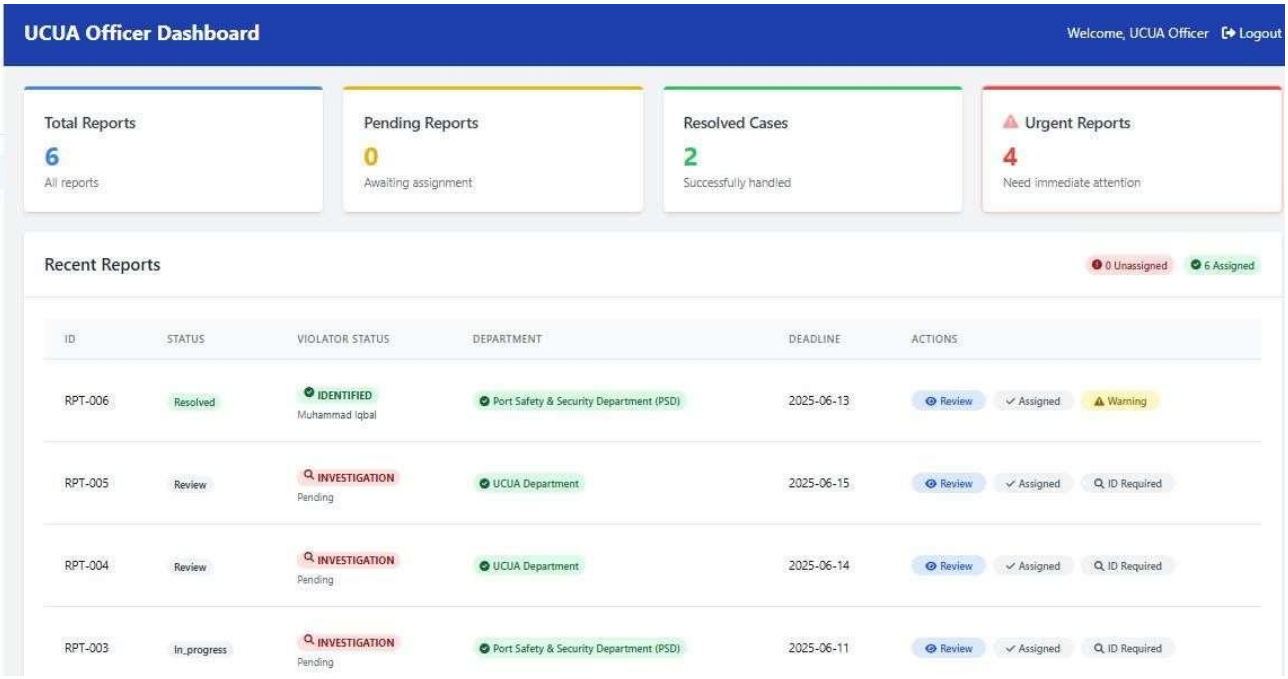

Fig. 18 *UCUA Officer Dashboard Management Table*

5.1.1 Head of Department (HOD) Dashboard

The security measures implemented into the Johor Port Unsafe Condition and Unsafe Act (UCUA) Reporting System are thoroughly. Fig. 19 illustrates the review page for the Head of Department report. HODs could evaluate the reports that are related to their respective departments. The investigation details, actions performed, and a section for final remarks are all include in each report.

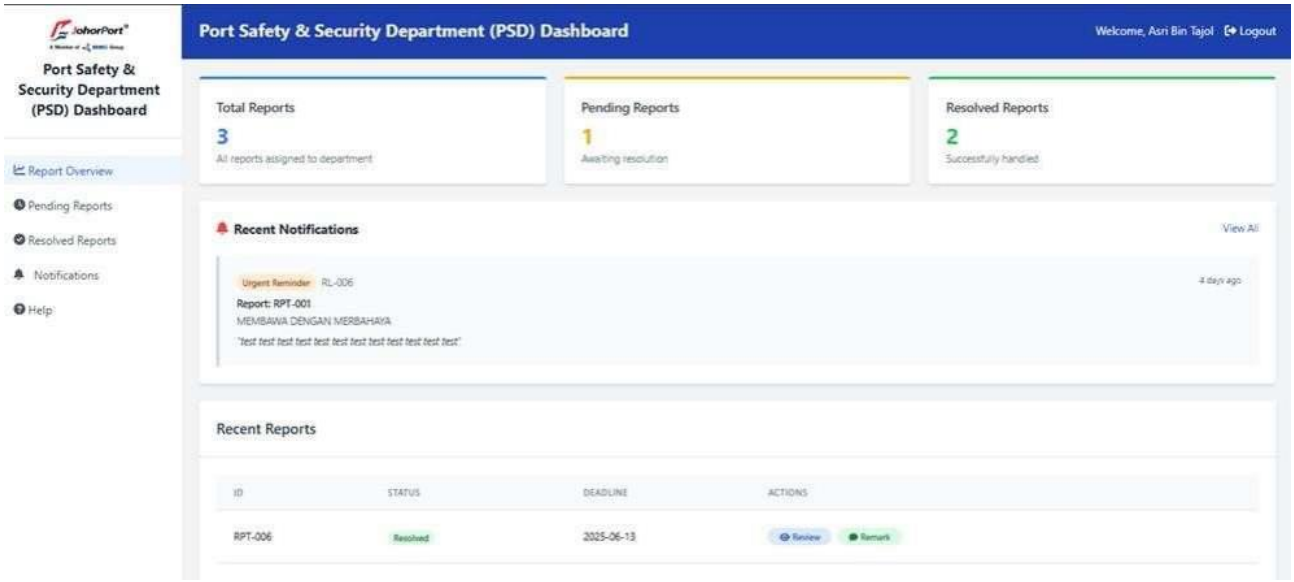

Fig. 19 *UCUA Officer Dashboard Management Table*

5.2 Security Checklist Result

The security measures implemented into the Johor Port Unsafe Condition and Unsafe Act (UCUA) Reporting System are thoroughly described in this section. It describes the approaches and controls put in place to protect the system from different kinds of online threats and illegal access. Every security feature is covered in detail, including its function, way of implementation, and contribution to the platform's overall resilience.

5.2.1 Test Case

The test plan outlines the main test cases that will assure the system's functionality, reliability, and security. Each test case focuses on validating the system's main modules, which include the Reporting Module, Notifications Module and Compliance Tracking Module as well as critical features such as multi-factor authentication (MFA). The test cases were created to evaluate appropriate procedure, discover potential errors, and guarantee that the system fulfils the requirements and standards for a consistent user experience. The test case results are presented in Table 4.

Table 4 *Test Case Result*

Description	Expected Result	Actual Result
User registers with valid information	User registers and logs in successfully	Pass
User logs in with valid credentials	User accesses dashboard without errors	Pass
User submits report with attachment	Report submitted successfully with file uploaded	Pass
User views submitted reports	Submitted reports are displayed correctly	Pass
User tracks report status updates	Report status changes are reflected in real-time	Pass
Warning notification through emails	User receives notification in their email	Pass
Admin logs in with valid credentials	Admin accesses dashboard without errors	Pass
Verification of new reports	Admin verifies report data and marks status	Pass
Changes report status (e.g., to Reviewed)	Report status updates correctly	Pass
Sends suggested warning letter	User receives warning letter notification	Pass
Assign report to department	Case assigned to the correct department	Pass
Suggests warning letter content	Letter content suggested and visible to admin	Pass
Sends reminder for unresolved case	Reminder is sent to HOD	Pass
Adds resolution note to report	Resolution note is saved with the report	Pass

Table 4 *(Cont.)*

Description	Expected Result	Actual Result
Have remarks and resolves assigned report	Status is updated to Resolved with remarks	Pass
OTP is sent to user email during registration	OTP email is delivered successfully	Pass
All users can only login with correct OTP	Login succeeds only with valid OTP within time limit	Pass
Password complexity validation works	Weak passwords are rejected during registration	Pass
Login and logout process	login and logout process run smoothly	Pass

5.2.2 User Acceptance Testing

The objective of this User Acceptance Testing (UAT) form is to evaluate the Unsafe Condition and Unsafe Act (UCUA) Reporting System's functionality, security, and performance. It guarantees that the system is user-friendly and satisfies the requirements that are required. System Testing, which concentrates on system functionality and usability. During this testing, port workers and the administrative staff which is the ICT manager had provided some feedback about this system.

Table 5 *UAT Result for Section A -interface & Usability*

No.	Description	Expected Result	Actual Result
A1	User-friendly and well-organized	Interface is intuitive and clean	Pass
A2	Simple and smooth login/navigation	Login and navigation are seamless	Pass
A3	Responsive system without delays	System loads quickly and performs actions smoothly	Pass
A4	Important features are easy to access	Key tools and options are clearly accessible	Pass
A5	Visually appealing design/layout	Layout is professional and aesthetically pleasing	Pass
A6	Enhances safety reporting and management	System supports better reporting and tracking	Pass
A7	Overall user satisfaction	Users express satisfaction with the system	Pass

Table 6 *UAT Result for Section B-Report Submission*

No.	Description	Expected Result	Actual Result
B1	Clean and easy-to-use report form.	Form layout is clear and easy to complete. Clean and easy-to-use report form.	Pass
B2	Clear understanding of required information.	Fields and instructions are understandable.	Pass
B3	Responsive system without delays.	System loads quickly and performs actions smoothly.	Pass
B4	Feedback or confirmation after submission.	User receives confirmation message or alert.	Pass

6. Conclusion

By the completion of this project, the Unsafe Condition and Unsafe Act (UCUA) Reporting System for Johor Port had been successfully designed and deployed. The technology solves the shortcomings of the old manual safety reporting process, increasing report submission efficiency and promoting greater openness and responsibility. The system's capabilities, which include real-time tracking, automated notifications, and analytic dashboards, allow HSSE professionals to monitor and control harmful conditions while acting effectively.

Secure authentication procedures improve system security by preventing unwanted access to user data and submitted reports. The dynamic and user-friendly interface enables seamless interaction between port workers and administrators. Despite meeting its primary objectives, the UCUA Reporting System for Johor Port has several notable limitations. It is only accessible via web browsers, with no mobile app or offline support—hindering reporting in real-time operational areas. The system also lacks advanced data analytics and visualisation tools, which limits actionable insights. OTP delivery depends solely on email, risking login delays, while anonymous reporting lacks full backend privacy. Additionally, the system supports only one language, reducing accessibility for a multilingual workforce. These weaknesses should be addressed in future enhancements to improve usability, security, and user trust.

In conclusion, the dynamic and user-friendly interface enables seamless interaction between port workers and administrators. In the future, the technology could be extended into mobile applications for the Android and iOS platforms to improve user accessibility and convenience.

Acknowledgement

This work was supported by the Universiti Tun Hussein Onn Malaysia (UTHM) through Contract Grant (Vot Q840).

Conflict of Interest

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

Author Contribution

This journal requires that all authors take public responsibility for the content of the work submitted for review. The contributions of all authors must be described in the following manner:

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

.

References

[1] S. Nur, A. Zolkefli, Z. A. Kadir, and A. Hannan Ensan, "Improvement of Unsafe Act and Unsafe Condition Online Reporting System at Port," vol. 5, no. 1, pp. 776–785, 2024, doi: 10.30880/peat.2024.05.01.084.
[2] Environmental and Social Commitment Plan Afghanistan's Community Resilience and Livelihoods Project," Mar. 2021.Accessed: Oct. 31, 2024. [Online]. Available: https://documents1.worldbank.org/curated/en/099030624225017246/pdf/P17876013749f50b1b25c1009be 8e68d6e.pdf
[3] The Editorial Team, "Near-miss reporting and Stop Work Authority: The pillars of safety."
[4] C. Chlomoudis, P. Kostagiolas, P. Pallis, and C. Platias, "Quality, Safety, and Security Systems in the Greek Port Industry: Over Twenty Years of Research, Empirical Evidence, and Future Perspectives," *Logistics*, vol. 8, no. 4, p. 98, Oct. 2024, doi: 10.3390/logistics8040098.
[5] K. L. A. Yau, S. Peng, J. Qadir, Y. C. Low, and M. H. Ling, "Towards Smart Port Infrastructures: Enhancing Port Activities Using Information and Communications Technology," *IEEE Access*, vol. 8, pp. 83387–83404, 2020, doi: 10.1109/ACCESS.2020.2990961.
[6] M. Karovaliya, S. Karedia, S. Oza, and D. R. Kalbande, "Enhanced security for ATM machine with OTP and facial recognition features," in *Procedia Computer Science*, Elsevier B.V., 2015, pp. 390–396. doi: 10.1016/j.procs.2015.03.166.
[7] Defence Technologies Sdn Bhd (DefTech), "DEFTECH UCUA System."
[8] "Civil Aviation Authority of Malaysia (CAAM) Safety Reporting System," Civil Aviation Regulations (CAR) 2016 and CAD 1900.
[9] "Construction Site Safety & Quality Management Software Solutions," Autodesk's Construction Cloud.
[10] D.Isler, A. Küpçü, and A. Coskun, "User Perceptions of Security and Usability of Mobile-Based Single Password Authentication and Two-Factor Authentication," 2019, pp. 99–117. doi: 10.1007/978-3-030- 31500-9_7.
[11] B. O. ALSaleem and A. I. Alshoshan, "Multi-Factor Authentication to Systems Login," in *2021 National Computing Colleges Conference (NCCC)*, I