UMYU Scientifica, Vol. 4 NO. 3, September 2025, Pp 189 – 204
https://doi.org/10.56919/usci.2543.019
ISSN: 2955 – 1145 (print); 2955 – 1153 (online)
A periodical of the Faculty of Natural and Applied Sciences, UMYU, Katsina

ORIGINAL RESEARCH ARTICLE

Development of a Secure Web-Based Crime Information Management System for Nigerian Campuses

Lasotte Yakubu Boyi-Musa[1], Elijah Micah Gidado[1], Lawal Olamilekan Lawal[1], Abubakar Suleiman Tukur[1], Saidu Ahmed Abubakar[1], and Idris Mohammed Kolo[1]
[1]Department of Computer Science, School of Information and Communication Technology, Federal University of Technology Minna, Nigeria

ABSTRACT
Effective security systems are a crucial concern for all stakeholders of global tertiary institutions, as they guarantee human safety and infrastructure protection. The continued use of manual crime reporting systems in many Nigerian institutions results in significant inefficiencies, such as delayed replies, weak record-keeping, and poor data analytics. While digital solutions exist, they often lack the integrated, campus-specific focus that is necessary. This study designs, develops, and evaluates a secure, web-based Crime Information Management System (CIMS) that integrates real-time reporting with multi-factor authentication, role-based access, and data analytics to address these challenges. The system was developed using Next.js, Node.js, and MongoDB. Multi-factor authentication and other advanced features ensure data security, and data analytics tools enable security personnel to identify patterns and efficiently allocate resources. A comprehensive evaluation was conducted over a four-week pilot with 10 users confirming the system's robustness. Performance benchmarking with Google Lighthouse yielded perfect scores of 100% in Performance and Best Practices, and a 96% score in Accessibility. Importantly, a security assessment using OWASP ZAP revealed no high-risk vulnerabilities, confirming the effectiveness of the basic security architecture. Medium and low-risk vulnerabilities identified were remediated. Usability testing with students and security personnel yielded a mean System Usability Scale (SUS) score of 77.5, signifying "good" usability. The findings confirm that the CIMS significantly enhances the efficiency, security, and usability of campus crime management compared to manual processes. While the results are promising, the study's limitations, such as its design as a single-campus pilot test with a limited duration, suggest that further multi-institutional and long-term studies are recommended before any broader national rollout.

ARTICLE HISTORY
Received June 29, 2025
Accepted September 18, 2025
Published September 30, 2025

KEYWORDS
Crime Information Management System (CIMS), Campus Security, Automation, Real-Time Reporting, Data Analytics.

INTRODUCTION
Effective security systems are a crucial concern for all stakeholders in global tertiary institutions, as they guarantee human safety and infrastructure protection. Security and education are integral components of the Universal Declaration of Human Rights, and it is anticipated that educational institutions serve as secure environments (Azevedo et al., 2022). A safe campus environment supports efficient study, research, and extracurricular activities. According to Abdullahi & Orukpe (2016) and Puckett (2022), a primary goal of colleges and universities is to provide a safe and secure environment for employees, students, and visitors, which is essential for personal development and academic success. Therefore, ensuring a secure campus is not merely an administrative task but a core responsibility of educational institutions to fulfill their primary mission.

Despite the importance of safety, Nigerian universities continue to face challenges related to crime and insecurity. Cases of theft, assault, sexual harassment, vandalism, and other forms of misconduct are still common in campuses (Asiyai & Oghuvbu, 2020). While universities have rules and security units in place, the effectiveness of these measures is often undermined by outdated manual systems of crime reporting and record keeping. Paper-based approaches delay responses, make data retrieval difficult, are vulnerable to unauthorized access, and are difficult to use for analysis or information sharing. Furthermore, incidents frequently go unreported due to

Correspondence: Lasotte Yakubu Boyi-Musa. Department of Computer Science, School of Information and Communication Technology, Federal University of Technology Minna, Nigeria. ✉ y.lasotte@futminna.edu.ng.
How to cite: Lasotte, Y. B., Elijah, M. G., Lawal, O. L., Abubakar, S. T., Saidu, A. A. & Mohammed, I. K. (2025). Development of a Secure Web-Based Crime Information Management System for Nigerian Campusea. *UMYU Scientifica*, 4(3), 189 – 204. https://doi.org/10.56919/usci.2543.019

fear of victimization or lack of trust in existing systems (Jimoh et al., 2023). These inefficiencies in managing crime data undermine the goal of maintaining safe and secure learning environments.

The rise of digital technologies offers a promising way to improve crime reporting and management processes. Web–based systems are interesting for numerous reasons, but largely because people are typically getting more acquainted with using computers to conduct all sorts of tasks, such as shopping, electronic transactions. It allows people to report crime easily, helping to reduce the rate of delay, which affects prompt detection and control of crime, which ranks as the top malady affecting the policing process all over the world (Akpan et al., 2022). Unfortunately, many Nigerian universities still rely on outdated manual systems, which suffer from inefficiencies, including delays in reporting, vulnerability to data breaches, and difficulties in retrieving and analyzing records. Paper records can be lost, tampered with, or accessed by unauthorized individuals, while the absence of centralized databases impedes effective crime tracking and strategic decision-making. Furthermore, although digital solutions such as national police databases or simple SMS reporting apps exist, they are frequently inadequate for the university context. Systems created for broad law enforcement are often too complex when compared to the specialized hierarchical structure of a campus, and basic reporting tools lack the security and analytical skills required in a campus setting (Jimoh et al., 2023). The issue is not simply the lack of a digital system, but of a comprehensive, secure, and intelligent system. To address these challenges, this study suggests an effective automated system that is both sophisticated enough for secure administrative use and accessible enough for the entire university community.

This study, therefore, addresses the gap for a secure, integrated web-based system specifically designed for the Nigerian campus environment, which combines real-time reporting with robust data management, analytics, and role-based access control. This research aims to develop a web-based Crime Information Management System (CIMS) to streamline crime reporting and administration for a Nigerian university. This study is guided by the following research questions:

i. To what extent does the CIMS reduce incident-reporting latency compared to the manual system?
ii. How does the system perform against standard benchmarks for web accessibility (WCAG) and security best practices (OWASP ZAP)?
iii. How do key stakeholders, including students and security staff, perceive the CIMS's usability?

The proposed CIMS is a web-based platform that enables online crime reporting, secures user data through multi-factor authentication, and supports hierarchical access levels for different categories of users. It also includes an analytics dashboard that allows security personnel to identify patterns, generate reports, and make informed decisions. The system was developed using an Agile methodology and evaluated through performance testing, security audits, and usability assessments.

REVIEW OF RELATED LITERATURE

The shift from manual to digital crime management systems is a global trend, motivated by the desire for greater efficiency, accuracy, and response time. This review organizes existing studies into key thematic areas to provide a clear context for the current research, examining web-based platforms for law enforcement, mobile and SMS-based reporting solutions, and the application of emerging technologies.

Several studies show the efficiency of web-based platforms in crime reporting and data management. Akinyede et al. (2023) developed a comprehensive website for managing crime reports. Data was collected through a mobile application and rendered into different categories on the admin dashboard. The dashboard offers multilevel accessibility, report creation, viewing, and security features. The platform offers transparency, accountability, and inclusivity. A beta test showed a 2.2s responsiveness time, indicating potential for improvement in emergency reporting. Tomas et al. (2019) developed an online reporting system that reduces manual work, though internet dependency and user literacy remain challenges. Although this research affirms the fundamental efficiency of digital platforms, it often focuses on broad applications or specific technical aspects. Importantly, it fails to offer a system built for the distinct requirements of a campus environment, which demands controlled access levels and integrated reporting and management tools. This study aims to bridge this gap.

A substantial amount of research has concentrated on creating web-based tools to help official law enforcement agencies handle crime data more efficiently. For instance, Jimoh et al. (2022) developed a web-based Graphical User Interface (GUI) application for the Nigerian police to aid in capturing criminal records, using Object Oriented Analysis and Design and UML tools, resulting in successful implementation. Oludele et al. (2015) developed a computerized real-time Crime record management system (CRMS) for the Nigerian Police Force. The CRMS promotes efficiency in record-keeping and decision-making using structured databases. Uchenna et al. (2022) designed an Integrated Unified Crime Information Management System (IUCIMS) to streamline crime data management across law enforcement agencies. The system uses web-based technologies and follows the Waterfall model of development. Similarly, Sharma and Shahnawaz (2014) implemented a CRMS for police stations across India. However, these systems are mainly designed for professional law enforcement settings; they often overlook the specific needs, user-friendliness, and access-control hierarchies required in a university campus setting, where users include students, staff, and campus security personnel with different levels of privilege.

Table 1: Comparative Analysis of Related Crime Management Systems

Feature/ Study	Akinyede et al. (2023)	Kommey et al. (2023)	Jimoh et al., 2023	Jimoh et al. (2022)	Proposed System (CIMS)
Platform	Mobile App	Mobile App (Android, iOS) + Web Dashboard	SMS-based system	Web Application	Web Application
MFA	Not Specified	Not Specified	Not Specified	Not Specified	Yes (Two-Factor Authentication)
Campus-Focused	No (Regional: Southwestern Nigeria)	No (General public use in Ghana)	Yes	No (National Police Focus)	Yes (Specifically for Nigerian university campuses)
Data Analytics	Yes (Dashboard with crime statistics)	Yes (Crime trends, hotspots, generated reports)	No	Yes (Data export for analysis)	Yes (Dashboard with crime statistics, trends, and actionable insights)
Role-Based Access	Yes (Admin, SuperAdmin)l	Yes (Public users, Police staff, System administrators)	Yes (via SMS)	Yes (Admin, IGP, CP, Police Officer, Criminologist)	Yes (Regular User, Admin, Super-Admin)
Evaluation Focus	Lighthouse & Beta Testing (Performance, UX)	System architecture, usability, deployment scenarios	Functional Testing (Does it work?)	Functional Testing & Data Export	Comprehensive: Performance, Accessibility, Usability, Security
Formal Usability Study	No (Beta Testing only)	No	No	No	Yes (System Usability Scale - SUS)
Security Testing	No	No	No	No	Yes (OWASP ZAP vulnerability assessment)
Primary Innovation	Separates reporting (mobile) from management (web)	"Critical" panic button for high-risk situations	Use of basic SMS for campus reporting	Focus on criminal biometrics & data export for analysis.	MFA, High-Performance Web App, and Integrated Analytics.

Table 2. Pilot deployment summary

Metric	Details
Site	A Nigerian University
Deployment Dates	4-week period
Registered Users (by Role)	Total: 10 • Students (Regular Users): 5 • Security Personnel (Admins): 4 • Head of Security (Super-Admin): 1
Reports Received	15 mock incident reports during the testing period
Average Response Time	Not quantitatively measured in the pilot. Qualitative feedback indicated a perceived significant reduction in reporting latency compared to the manual system.
Uptime %	70% (Achieved acceptable reliability with moderate service availability during pilot deployment on Vercel)
Major Incidents	None. The system operated stably throughout the pilot with no security breaches or significant functional failures.

Given how common mobile phones are, a number of researchers have leveraged mobile technology to facilitate instantaneous crime reporting. Kommey et al. (2023) developed a smartphone application that allows victims or witnesses to report incidents in real-time, including GPS coordinates. In a similar vein but using simpler technology, Jimoh et al. (2023) proposed a framework for campus crime reporting using Short Message Service (SMS), which allows students to send basic incident details directly to security agents. These described techniques are effective for reporting incidents quickly and are easy to access. However, they have some limitations: they are primarily concerned with the initial report and lack robust capabilities for managing cases, analyzing data, and keeping information secure, as well as a complete system for tracking case progress, identifying patterns, and protecting sensitive information.

Emerging technologies like blockchain and predictive analytics are transforming the way crimes are addressed. Hingorani et al. (2020) built a Police Complaint Management System using blockchain to ensure the integrity and immutability of First Information Reports (FIRs). Similarly, Kumar et al. (2024) created a criminal investigation tracker system that tracks case status and predicts suspects. The case summary, parties involved, disagreements, prior criminal history, and recovered objects are all recorded by the system. Authorized officers can manage cases and update information using its admin dashboard. The Python programming language, MySQL database, HTML, and CSS were all used for the development of the system. In order to analyze web-based crimes and identify trends, Dereje and Nixon (2020) developed a system that uses data mining, machine learning, and web scraping tools. These solutions are innovative and effective for large crime-fighting agencies. However, they may not be suitable or cost-effective for a university campus in Nigeria, which has different and more localized security needs.

In summary, the existing literature reveals a clear gap that this study aims to fill**.** Existing methods are frequently inadequate for the university context, as they are often designed for broad city-wide law enforcement rather than the specific hierarchical structure of a campus. Others are functionally segmented; they focus either on backend record management or on front-end reporting. They lack a unified system that integrates reporting, security management, and data analysis, which is essential for effective security operations. Finally, many existing systems are too limited in features**.** They fail to incorporate critical technologies such as strong security (for example, Multi-Factor Authentication), levels of access for various authorities (hierarchical access control), and data analysis capable of identifying and explaining campus-specific crime patterns. Consequently**,** this study aims to bridge this gap by developing a web-based Crime Information Management System (CIMS) that is specifically designed for the Nigerian tertiary institution context. Table 1 shows the comparative analysis of related crime management systems.

METHODOLOGY

The system was developed using the agile methodology. The Agile development methodology is shown in Figure 1. Agile is an iterative software development methodology that makes sure that software is delivered as quickly as possible. It gives room for easy incorporation of new software changes throughout the development process. This approach ensures software is delivered on time and can adapt to new requirements. The design approach utilized Unified Modeling Language (UML) tools to model the system's architecture and processes. Node.js was used for the backend, and Next.js was used for designing the user interface at the frontend. Node.js was chosen for its efficient and scalable backend runtime, and Next.js for its server-side rendering capabilities to guarantee fast frontend performance. MongoDB was selected for its flexibility in storing diverse and unstructured crime report data.

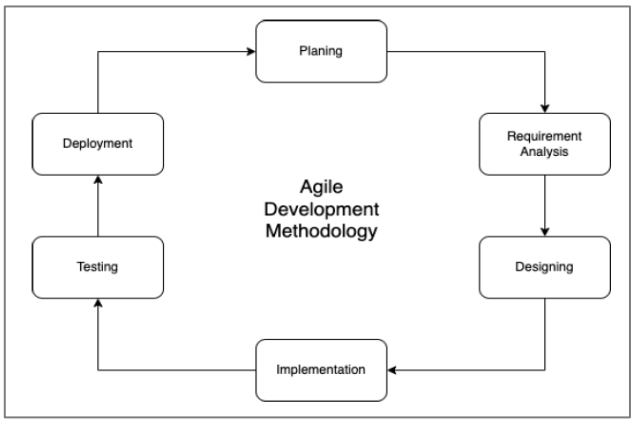

Fig 1. Agile development methodology

3.1 System Architecture

The system has a three-tiered architecture. The front-end client was created using Next.js (v14.2.5) and hosted on Vercel. The back-end API was built with Node.js (v22.20.0 LTS) and the Express.js framework (v4.18.2). MongoDB (v8.0) was chosen as the non-relational database because of its flexibility with unstructured data. JSON Web Tokens (v9.0.1) were utilized for session management, and the speakeasy library (v2.0.0) was used to implement Time-based One-Time Password (TOTP) multi-factor authentication.

The system was deployed on a single server for the pilot, with the backend and database co-located. For data integrity, automated daily backups of the MongoDB database were enabled on Atlas (MongoDB's cloud database service) to ensure data can be recovered in the event of a catastrophic system failure. A comprehensive audit trail was implemented using the Winston logger, recording all user logins, report submissions, and data modifications. Figure 2 shows the system architecture.

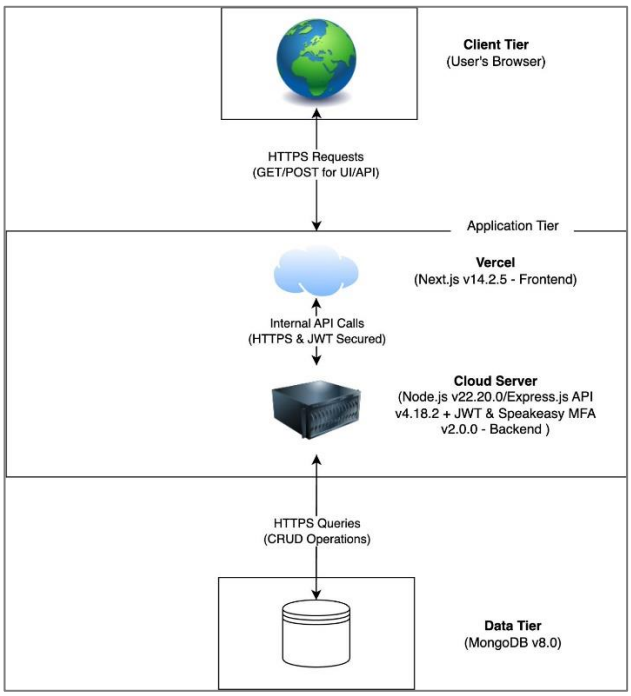

Fig 2. System architecture

3.2 Description and Analysis of the Existing System

Many Nigerian institutions still use a manual approach for reporting crimes. Crime records are written down on paper and kept in physical files, which are stored in cabinets or on shelves. In order to record their reports under this system, reporters must be physically present at the security office. There are certain limitations on the current system:

i. Unauthorized Access: Because anyone with access to the record room can alter or destroy files, physical records are vulnerable to unauthorized access.
ii. Inefficiency: Reporters (staff or students) and security personnel must communicate directly during the manual data recording and processing process. This will lead to delays and inefficiencies.
iii. Tedious Record Retrieval: It can be difficult and time-consuming to find particular records, particularly those that are older or located in a large archive.
iv. Risk of Data Loss: In the case of natural disasters, fires, or other unforeseen circumstances, physical records can be permanently destroyed, which will result in irreversible data loss.

3.3 Description and Analysis of the Proposed System

The proposed web-based Crime Reporting and Management System will solve the problems with the current system by giving people a safe, user-friendly, and efficient way to report and manage crimes. Important features of the current system include the following:

i. Reporting Crimes in Real Time: Victims or witnesses can report crimes using the web application. Therefore, there will be no need to go to the security office in person.
ii. Secure Access: The system uses cutting-edge security features like multi-factor authentication (MFA) to stop unauthorized access to sensitive data.
iii. Efficient Data Retrieval: Both victims and security personnel can locate and access reported cases with ease. This will reduce the time and effort required to retrieve records.
iv. Remote Accessibility: Stakeholders can access the system from anywhere as long as they have the right login credentials. This will ensure convenience and flexibility.
v. Data Visualization and Analytics: The system has strong data visualization and analytics features. This will help security staff spot trends and patterns and make informed decisions.
vi. Instant Reporting: Reporting will be easy and quick. Reports from any location will be instantly available to security personnel.

3.4. System Design

The new system's design contains Unified Modeling Language (UML) diagrams as well as Entity Relationship Diagrams. These design tools generate a visual depiction of the system's architecture and workflows.

3.4.1 Unified Modeling Language (UML) Diagram

UML diagrams are used to visualize the system's design. The web-based crime reporting and management system includes the following UML diagrams:

i. **Class Diagram**

The class diagram, as depicted in Figure 3, illustrates the structure of the system by describing the classes, their characteristics, and the relationships between them. Attributes such as the case number, date, time, location, and related victims and files are included in every criminal record. A status attribute is also included in the diagram to indicate if the case is closed or open. A thorough crime management system with well-defined roles, duties, and data structures is supported by this configuration.

ii. **Data Model (ER Diagram)**

Figure 4 depicts the Entity-Relationship Diagrams, which explain how each entity relates to its attributes throughout the system. The ER diagram models a system in which users can create and manage criminal records. Each user has a set of attributes, such as email, password, and access level, and they can create many crime records, each of which contains detailed information about the crime.

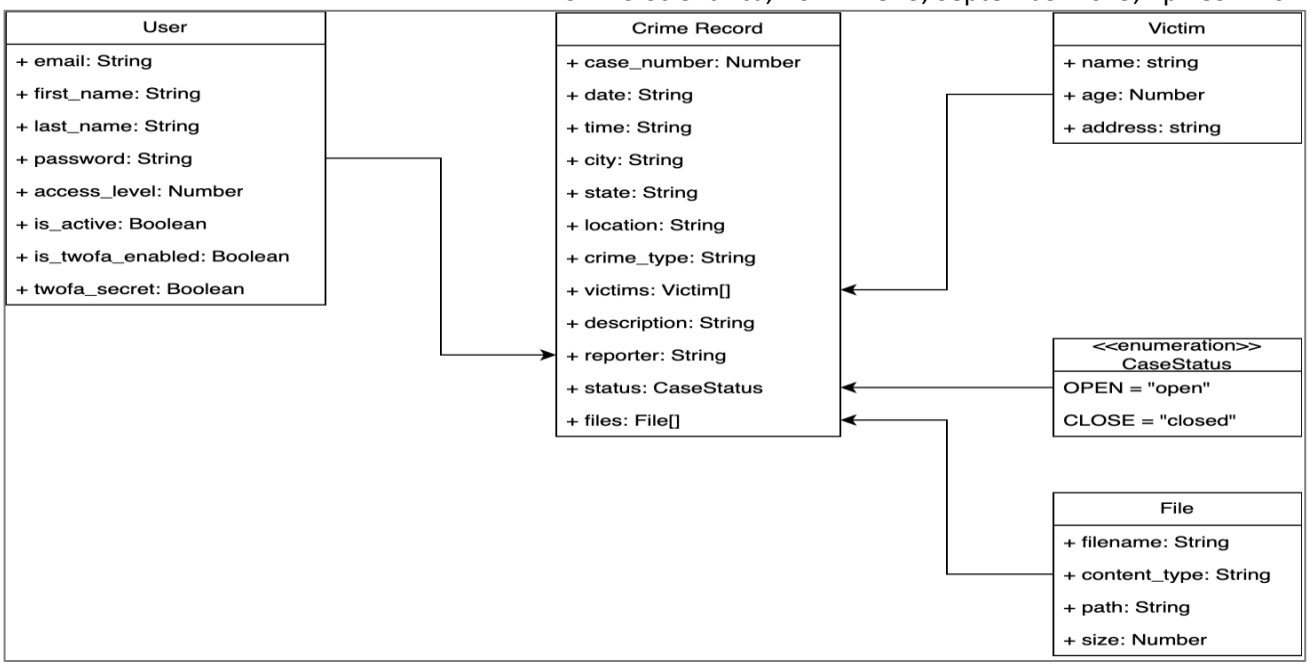

Fig 3. Class diagram

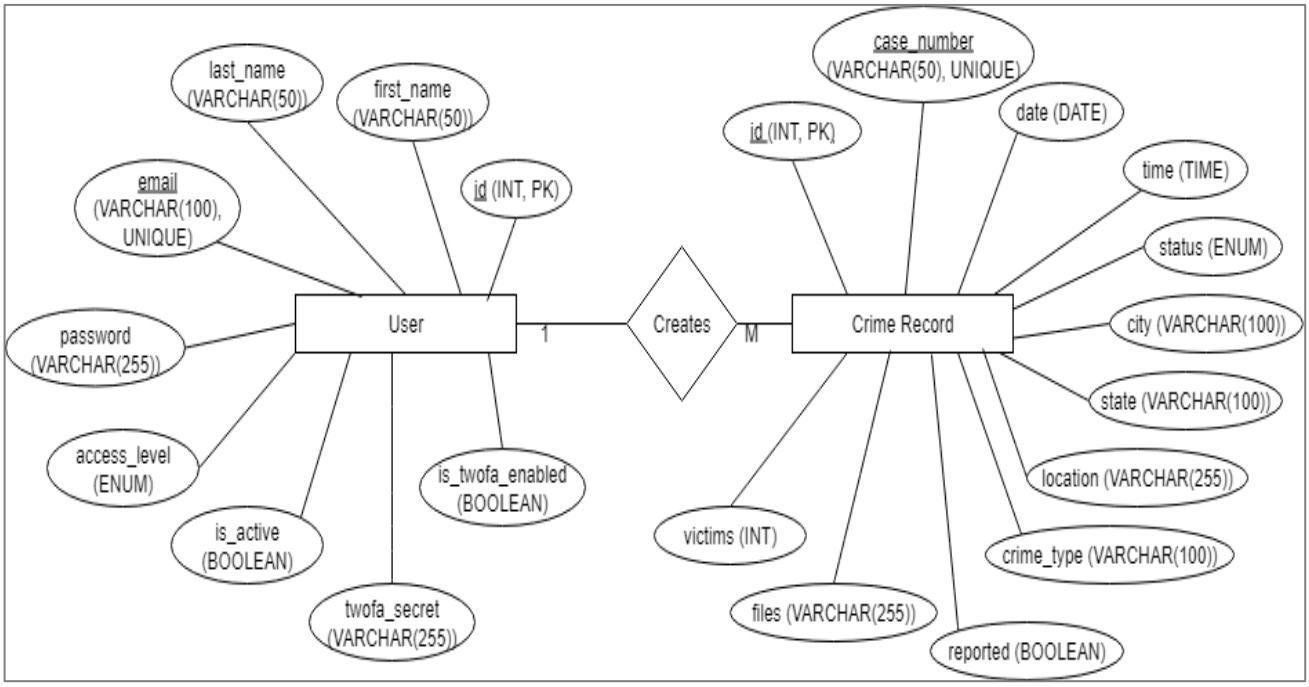

Fig 4. Entity-relationship diagram

iii. Use Case Diagram

A use case diagram, as shown in Figure 5, shows how users and the system interact. The primary features, including report case, view case, view own case analytics, manage case, and manage admin, are highlighted. Three main user types (access levels) are supported by the system:

a. **Regular user (Access level 1)**

This is the most fundamental of all users. Users at this level can only report new cases and view the cases they have reported. After submitting a report, they cannot modify any information in the system. Students and non-security personnel are usually included at this level.

b. **Admin (Access level 2)**

Admin privileges are granted to users at this level. They can report, view, and manage cases reported by themselves and others. They can also update case statuses and manage regular users. Security personnel are usually assigned to this level.

c. **Super-admin (Access level 3)**

This is the most privileged user level. Super-admins can manage other administrators, including adding or removing them from the system, and can carry out any action permitted for administrators. The head of the security department, who is in charge of managing the

administrative staff, is the most qualified candidate for this level.

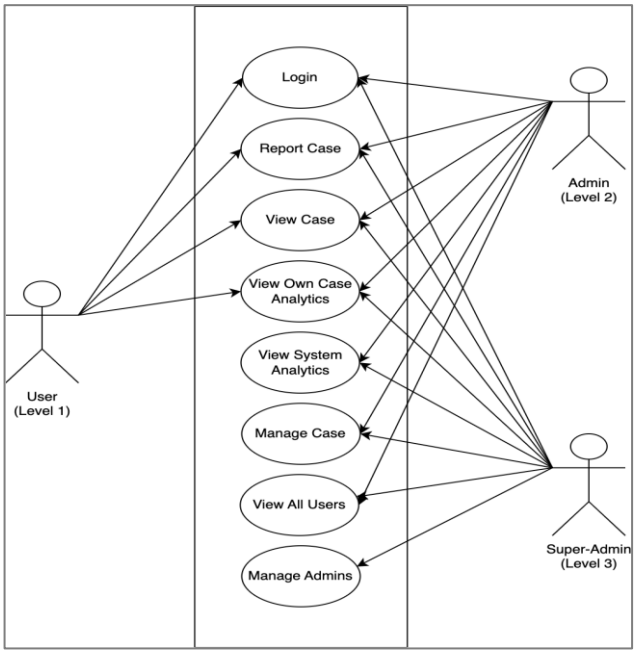

Fig 5. Use case diagram

iv.Sequence Diagram

Figure 6 depicts the sequence of interactions in the crime reporting system. A Reporter (user) signs in with their credentials, and the back-end authenticates them, returning a Java Web Token (JWT) that grants system access. The authenticated reporter submits a crime report, which the system validates before adding a new case entry to the database with the status 'open'. This sends a real-time notification to a Security Administrator, who can log in, collect case data, and change the status (for example, to 'Under Investigation') if needed. The system records this change and may notify the original reporter of the update.

3.5. System Evaluation

The Crime Information Management System (CIMS) was evaluated using a multi-method approach to assess its technical performance, security, functionality, and usability.

1. **Frontend Technical Benchmarking:** The application's frontend quality was audited using **Google Lighthouse (v12.6.0)** against three core metrics: **Performance, Accessibility, and Best Practices.**

2. Performance and Latency Testing: Frontend performance and user experience were quantitatively measured using Google's PageSpeed Insights API. Key web vitals were monitored, including:

   a. Time to First Byte (TTFB) to evaluate server response speed;

   b. Largest Contentful Paint (LCP) to assess loading performance of main content;

   c. First Input Delay (FID)/Interaction to Next Paint (INP) to measure responsiveness to user interactions; and

   d. Cumulative Layout Shift (CLS) to evaluate visual stability.

Real Experience Score (RES) was used to summarize the overall user experience.

3. Usability Testing: A usability study was conducted with ten participants, comprising five 5 students and five security officers, who were randomly selected from a volunteer pool within the pilot university. During the testing session, Participants completed essential tasks, including registering, reporting a mock crime, updating case status, and using the analytics dashboard, and subsequently provided feedback via the System Usability Scale (SUS) questionnaire. **A score above 68 on the SUS was established as the benchmark for acceptable usability.**

4. Accessibility Evaluation: A comprehensive accessibility assessment was conducted to evaluate compliance with WCAG 2.2 standards. The evaluation focused on five key areas: Keyboard accessibility, color contrast, screen reader compatibility, zoom functionality and interactive elements accessibility.

5. Data Analytics Dashboard Evaluation: The analytics dashboard was evaluated for its capability to transform raw incident data into actionable insights.

6. Security Testing: A baseline vulnerability assessment was performed using OWASP ZAP tool (Version 2.16.1) to identify potential security weaknesses in authentication

3.6. System Requirements

The components needed by the system before it can run successfully are known as the system requirements. The following is the list of system requirements. The computer to install and run the application should have a minimum of an Intel Pentium IV or above processor, a 1.3 GHz processor speed, 4 GB RAM, a 50 GB hard drive, and a 15" SVGA color monitor as the hardware requirement. At the same time, the software required for the implementation of the new system is Windows 7 or higher, XAMPP, Microsoft Edge, Google Chrome, etc., and a good antivirus program to ensure system security.

SYSTEM IMPLEMENTATION

The screenshot images that illustrate the functionalities of the Crime Information Management System provide a visual representation of some of the experimental outcomes. The system was implemented and tested in one of the Nigerian universities. The following features were implemented during the system's development:

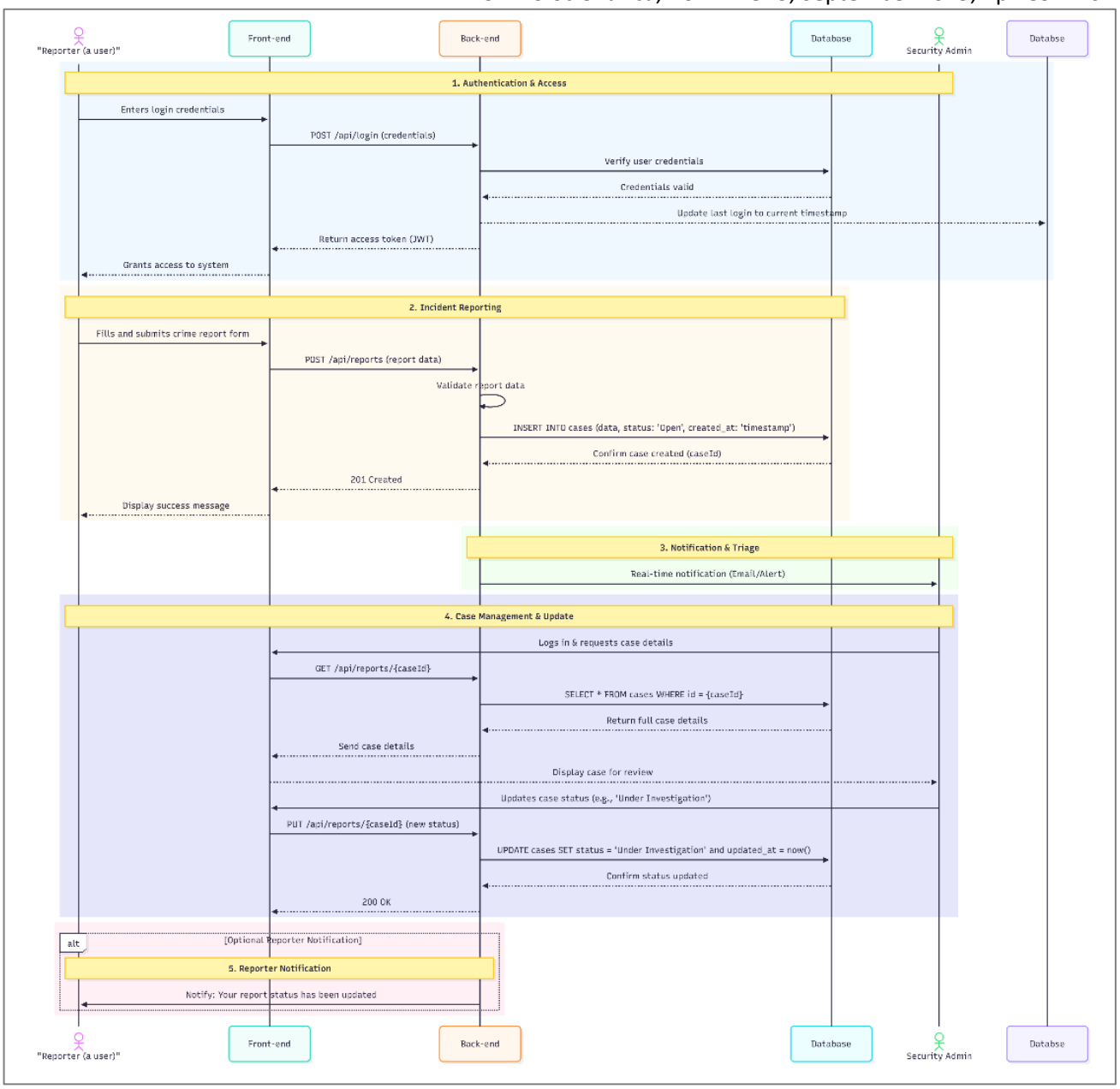

Fig 6. Crime report workflow sequence

4.1. Login Page

The application's entry point is the login page, as presented in Figure 7, where users submit their credentials for validation before being granted access to the system.

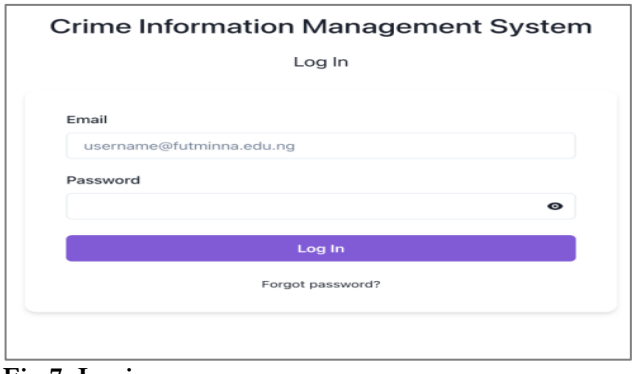

Fig 7. Login page

4.2. Two-Factor Authentication Page

Accounts with two-factor authentication enabled will be forwarded to the page, as shown in Figure 8, to enter a code from the authenticator app. This is an additional layer of security to defend against credential theft and brute force assaults, as email and password alone are not sufficient to provide access to the system.

Fig 8. Two-factor authentication page

4.3. Dashboard Home Page

The home page features a comprehensive analytics dashboard, as presented in Figure 9, designed to provide

an overview of the entire system and convey essential information concisely. This page includes information such as: Total Cases, Total Victims, Total Users, Average Victim Age, Average Victims per Case, Victims by Day, Cases Reported by Day, Victims by Age Group, and Cases by Type

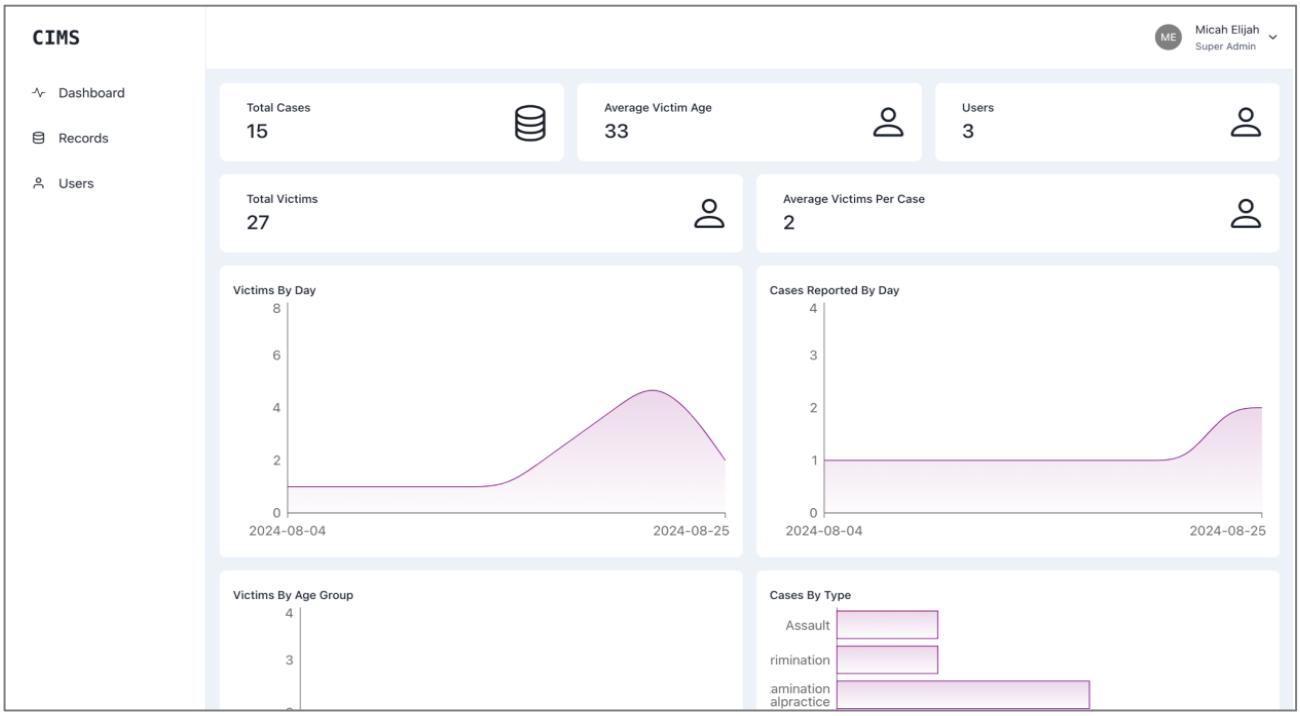

Fig 9. Dashboard home page

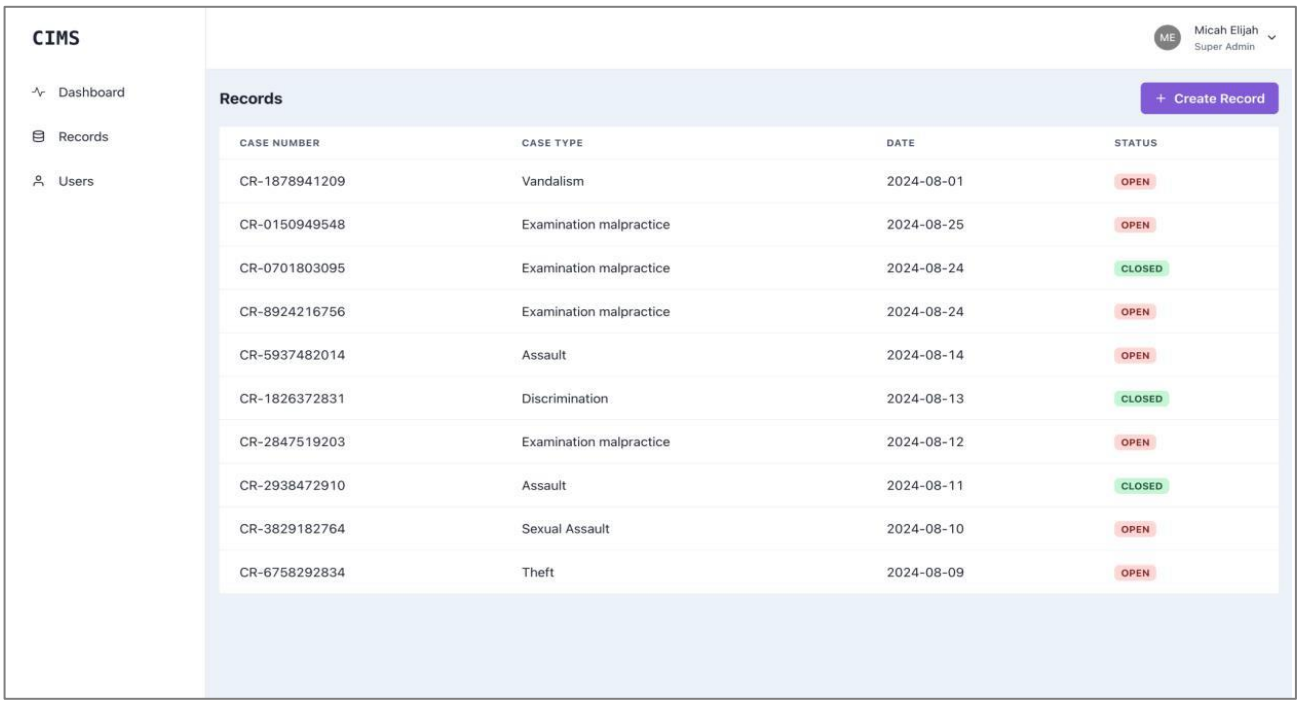

Fig 10: Records page

4.4. Records Page

The record page. as depicted in Figure 10, presents a tabular overview of all cases recorded in the system. The page displays information, including the case number, type, date, and status at a glance. The top-right corner of the page has a button to create a new record/case, which leads the user to the page where they will enter the record.

4.5. Create Record Page

The create record page, as illustrated in Figure 11, enables users to report a crime by providing details about the incident. The page is split into sections, each containing distinct facts about the case. The first section collects basic information about the offense, such as the crime type, date, time, location, description, and offender description. The second segment gathers information about the casualties. The final page allows you to upload media files, such as films, photographs, documents, and any other media related to the incident.

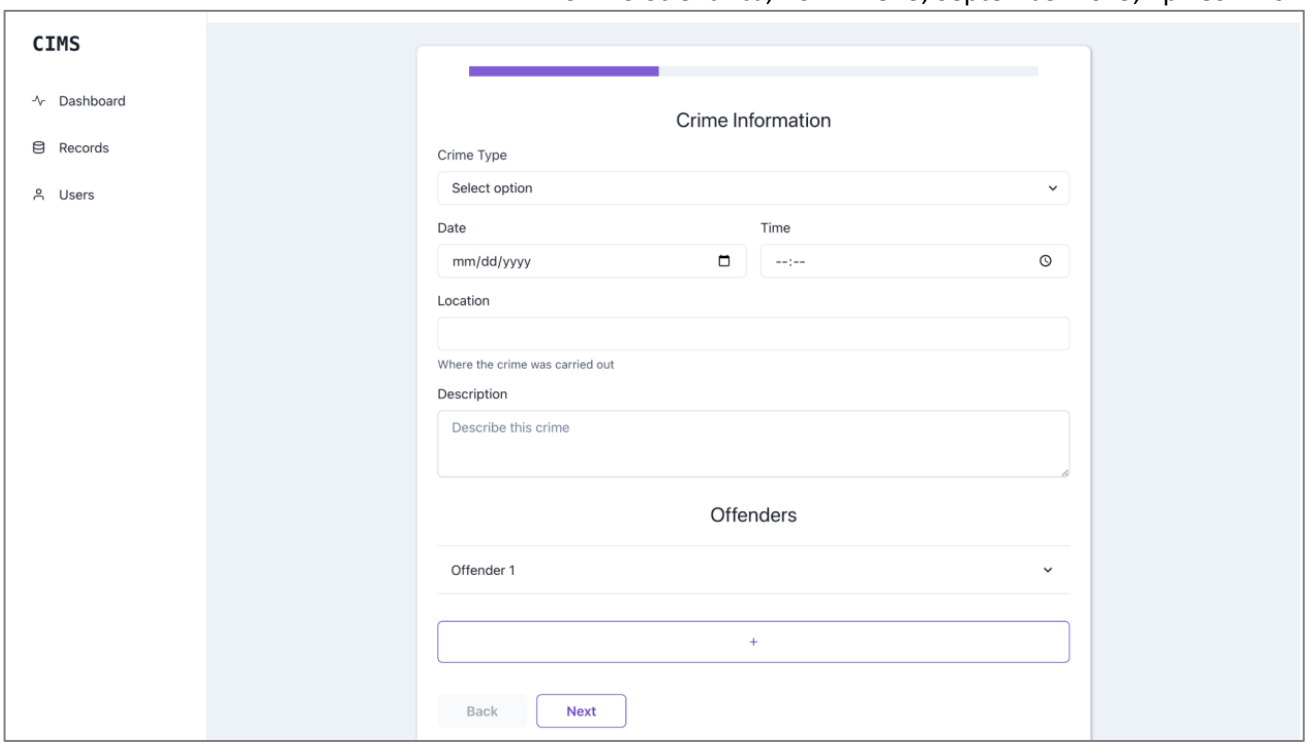

Fig 11. Create record page

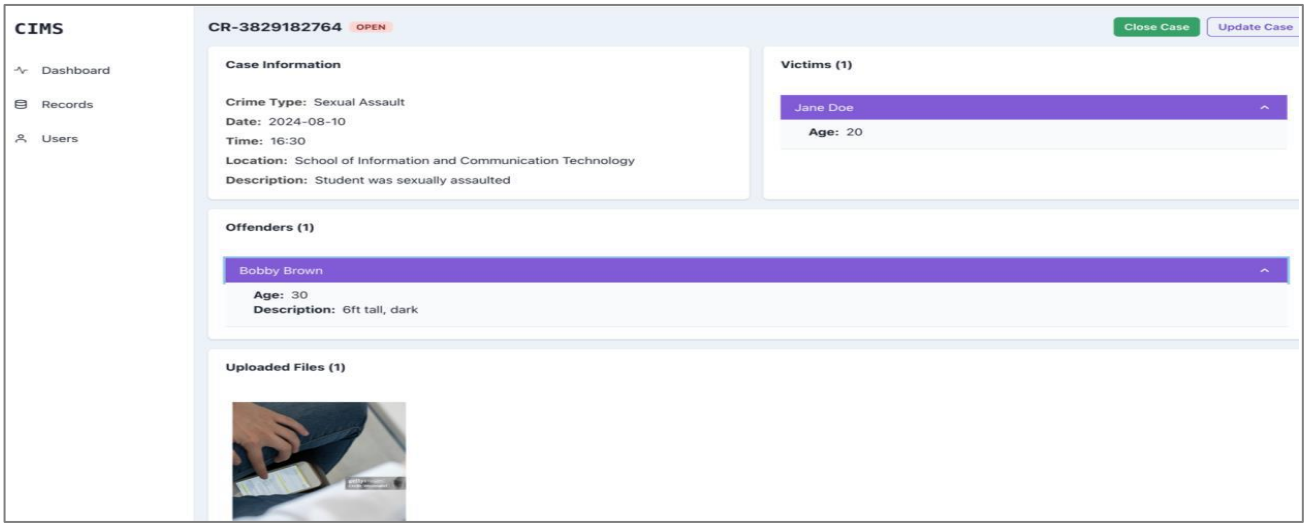

Fig 12. Record detail page

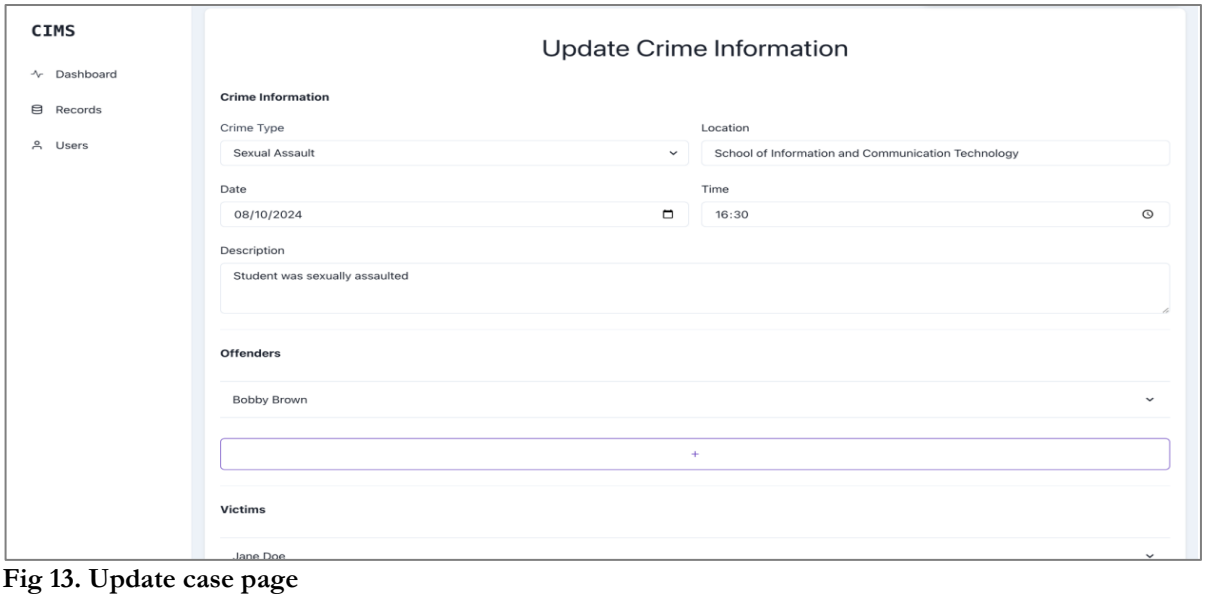

Fig 13. Update case page

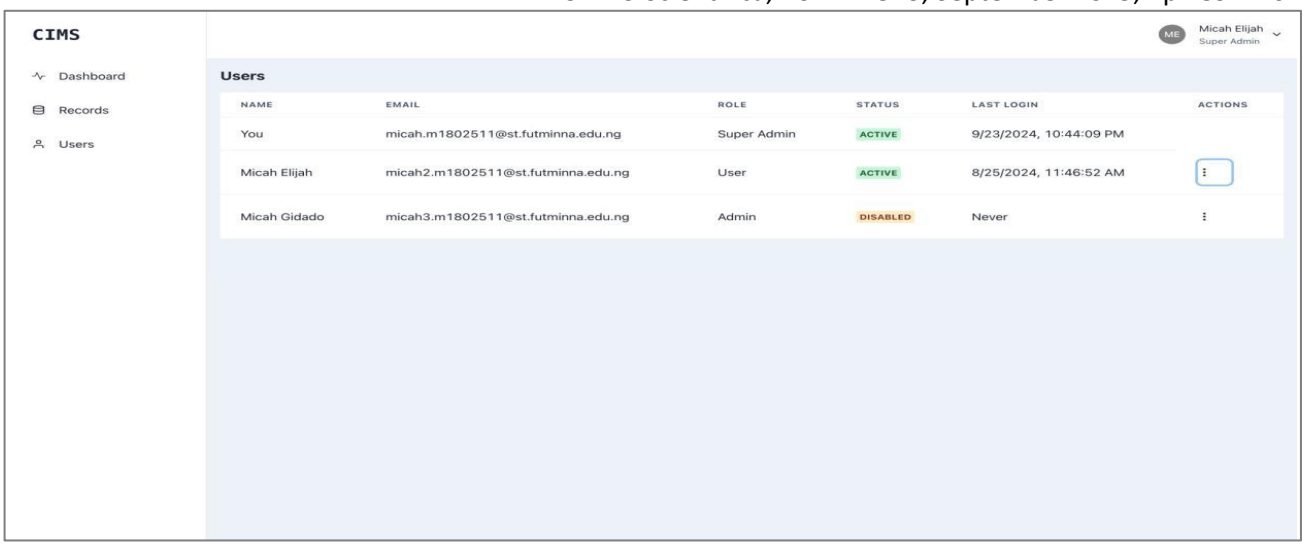

Fig 14. Users page

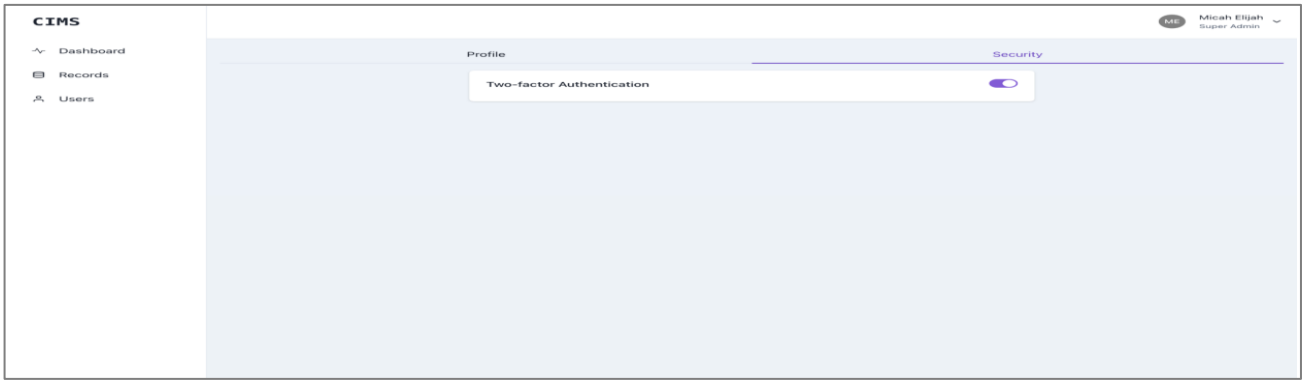

Fig 15. Security page

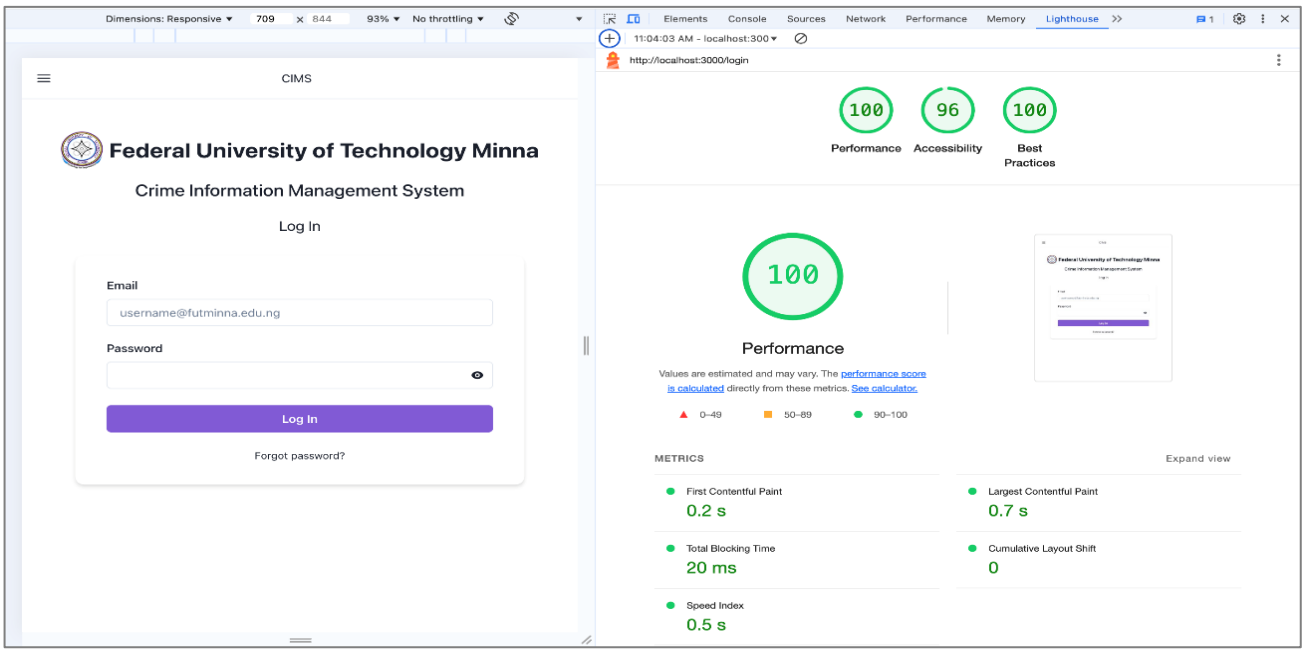

Fig 16. System assessment report

4.6. Record Detail Page

The Record Detail Page, as shown in Figure 12, offers a more comprehensive view of the record. Information on this page includes:

i. Case Number, Case Status, Crime Type, Date, Time, Location, Description, Victims, Offender's details, and Uploaded Files. In the top-right corner of the page, there are two buttons: the case status update button and the update case button, which toggles the case status between closed and open, and updates the case information, respectively.

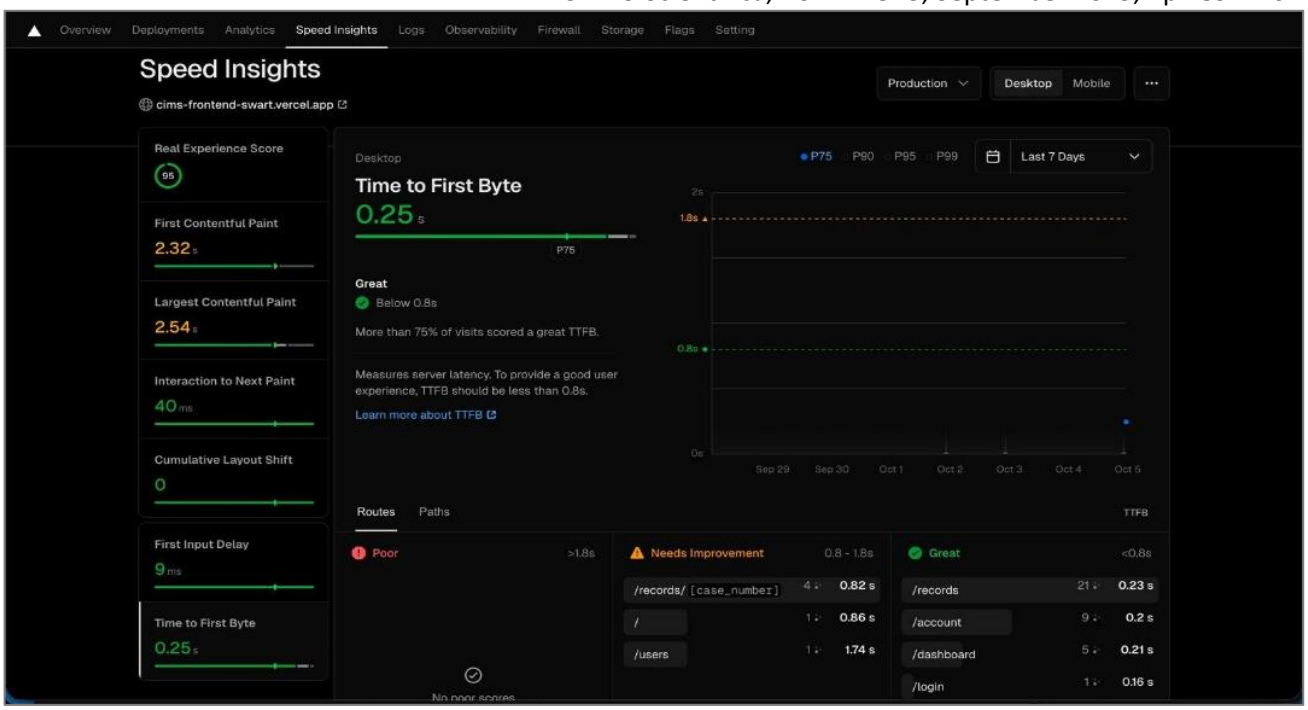

Fig 17. Frontend performance latency metrics

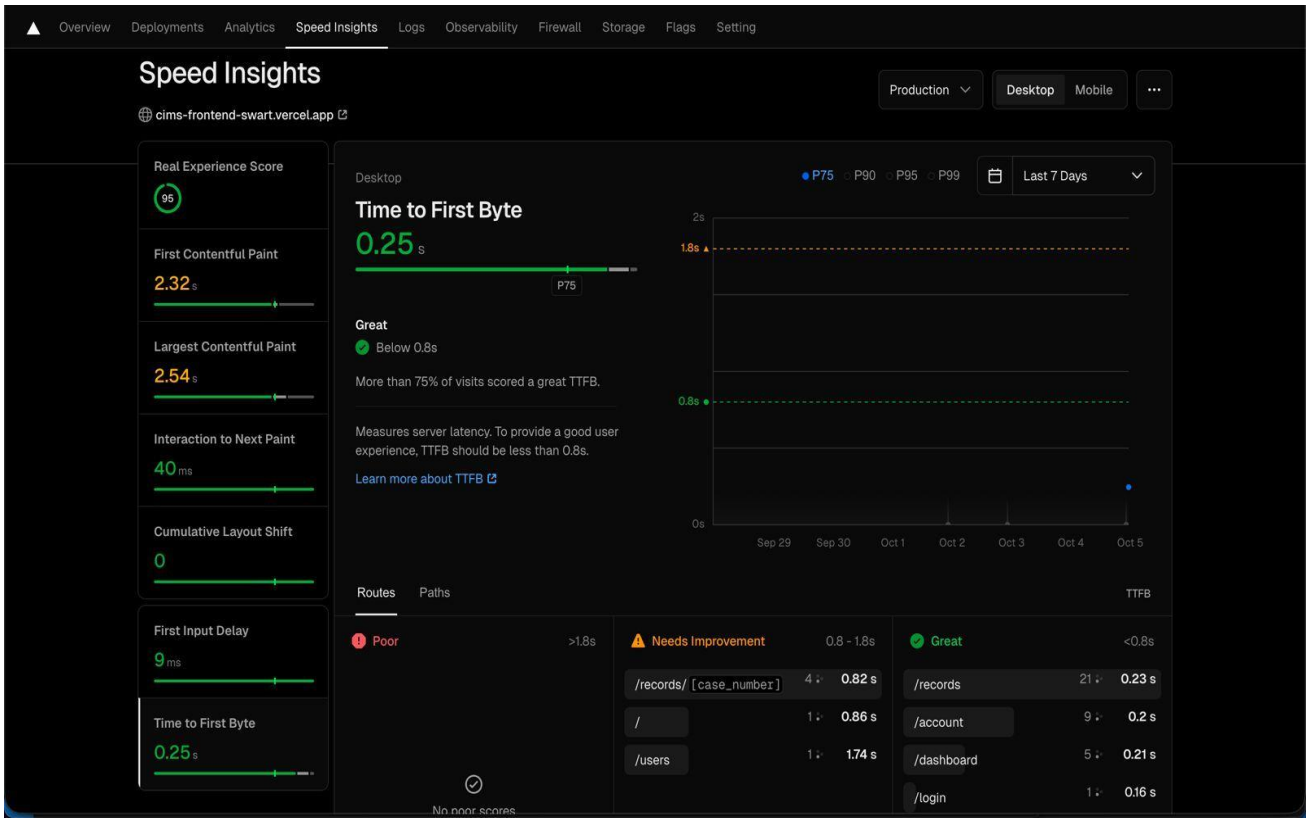

Fig 18. Overall user experience score

4.7. **Update Case Page**

The record may require updating if a discovery is made regarding an offense. This page allows users to update the records after discovering new evidence or other information pertinent to the case. This functionality is illustrated in Figure 13.

4.8. **Users Page**

The users page, as depicted in Figure 14, displays a list of all the system's users, including their names, roles, email addresses, and last login date, which indicates when they last signed in. An action pop-up is also provided, which contains the following capabilities.

i. Disable/Enable User: This action enables system administrators to enable or disable a user's account, thereby denying them access to the system.

ii. Manage User Privileges: This enables the super administrator (super admin) to manage the roles of other users. The super admin can make a regular user an administrator or downgrade the privileges of an administrator to a regular user.

Table 3: System assessment report

Metric	Performance (%)	Accessibility (%)	Best Practices (%)
Result	100	96	100

Table 4: Usability testing results

Metric	**Value**
Mean SUS Score	77.5
SUS Rating	Good
Standard Deviation	14.95
Score Range	40 – 95
Mean Task Completion Time	3:48
Task Success Rate	90% (9 out of 10 participants scored ≥70)

Table 5: Accessibility evaluation summary

Assessment	**Result**	**Severity**	**WCAG Compliance**
Keyboard Accessibility	Pass (Minor Gaps)	Moderate	Largely Compliant
Color Contrast	Pass		AAA Compliant (16.31:1)
Screen Reader	Pass	Moderate	Partially Compliant
Zoom Functionality	Pass		AA Compliant

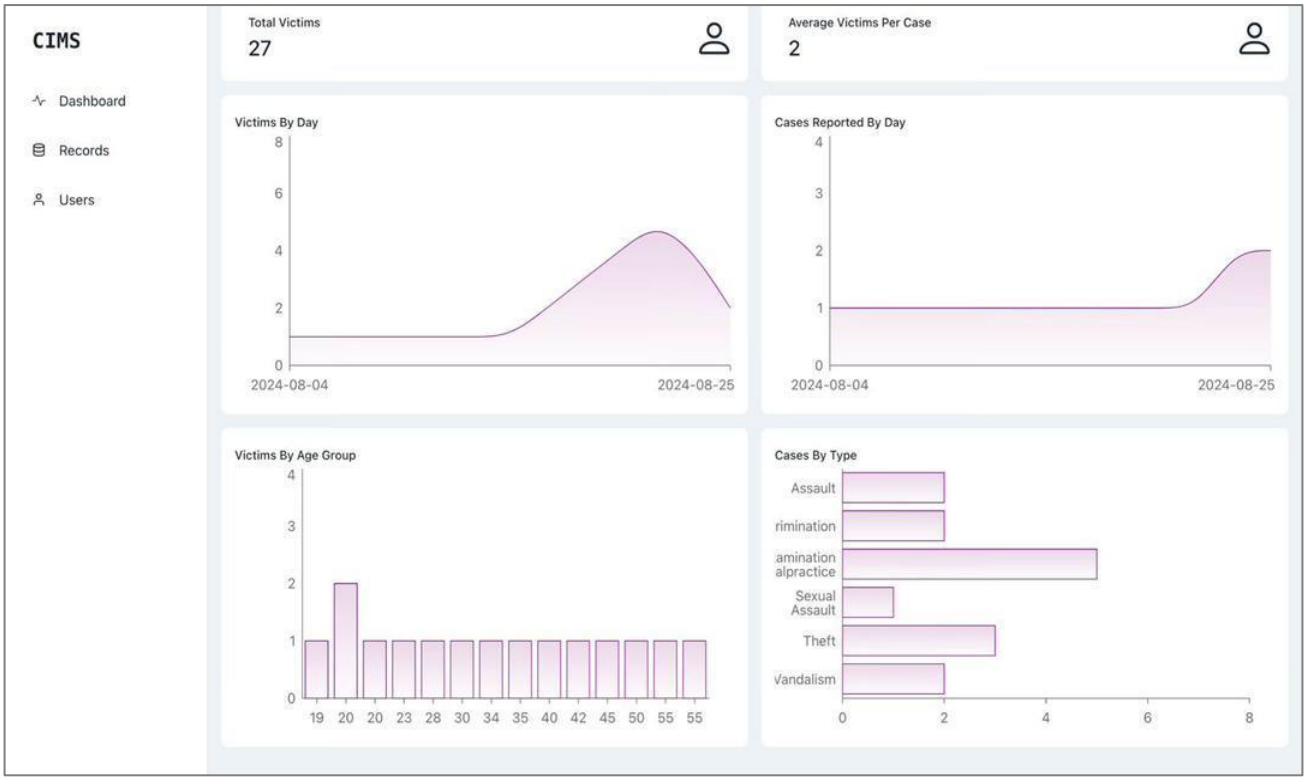

Fig 19. Analytical dashboard

Table 6. Evaluation metrics and results

Metric Name (Definition)	Tool/Method	Sample Size / Scope	Numeric Result	Pass/Fail vs Threshold
Frontend Performance (Loading speed & responsiveness)	Google Lighthouse	Full Application	100%	Pass (Target: >90%)
Accessibility (WCAG 2.2 Compliance)	Google Lighthouse & Manual Audit	Full Application	96%	Pass (Target: >90%)
Best Practices (Web development standards)	Google Lighthouse	Full Application	100%	Pass (Target: >90%)
Time to First Byte (TTFB) (Server response speed)	PageSpeed Insights API	Key Workflows	0.25 seconds	Pass (Target: < 0.6s)
Input Delay (INP) (Interface responsiveness)	PageSpeed Insights API	Key Workflows	9 milliseconds	Pass (Target: < 200ms)
Largest Contentful Paint (LCP) (Main content load time)	PageSpeed Insights API	Key Workflows	2.54 seconds	Pass (Target: < 2.5s)
System Usability Scale (SUS) (Perceived usability score)	SUS Questionnaire	10 users	77.5 (Mean Score)	Pass (Target: > 68)
Security Vulnerabilities (Presence of high-risk flaws)	OWASP ZAP (v2.16.1)	Full Application	0 High-Risk Alerts	Pass (Target: 0 High-Risk)

4.9. Security Page

The security page, as shown in Figure 15, enables users to manage their account security, such as implementing two-factor authentication. Two-factor authentication (2FA) is a security protocol necessitating users to present two distinct forms of verification to gain system access. This provides an additional layer of security beyond merely a username and password.

RESULTS AND DISCUSSION

This section presents the findings from testing the Crime Information Management System (CIMS) during its pilot run at a Nigerian university. The system was evaluated to determine whether it was usable, accessible, fast, secure, and truly helpful for improving campus security.

5.1. Pilot Deployment Summary

Table 2 summarizes the key operational metrics from the four-week pilot deployment at the participating Nigerian university.

5.2. Frontend Performance Results

Google Lighthouse was utilized to evaluate the Crime Information Management System (CIMS), which looked at three main areas: performance, accessibility, and best practices. A perfect performance score of 100% suggests that the system is highly optimized, loads rapidly, and handles real-time data efficiently. This will ensure timely incident reporting and response. The system also received an accessibility score of 96%, indicating that it is highly usable for a wide range of users, including those with disabilities, and that it complies with WCAG 2.2 standards like proper semantic HTML, keyboard navigation, and screen reader compatibility. The system also complies with contemporary web development standards, guaranteeing security, dependability, and maintainability, as evidenced by its flawless 100% Best Practices score. These findings confirm that the CIMS is a superior, user-friendly, and technically sound system that can solve the limitations of manual crime reporting systems. The findings of the system evaluation were depicted in Figure 16 and Table 3.

5.3. Performance and Latency Testing Result

Frontend performance testing, as shown in Figure 17, demonstrates that the system provides a fast and responsive user experience. Key metrics, such as a Time to First Byte (TTFB) at 0.25 seconds, a 9-millisecond input delay, and a full content render in 2.54 seconds, show exceptional efficiency. The interface stays stable, with no disruptive layout changes, achieving modern performance criteria required for effective crime reporting. The Real Experience Score (RES) results in Figure 18 show that the system has high frontend usability, with the system achieving a score of 95. This reflects primarily "Great" user visits and is due to its strong core web vitals: a 0.25s server response, a 9ms input delay, and flawless visual stability.

5.4. Usability Testing Results

A usability study was conducted with ten participants (5 students and 5 security personnel) who completed basic activities such as registering, reporting a mock crime, updating case status, and accessing the analytics dashboard. They then completed the System Usability Scale (SUS) questionnaire. Table 4 reveals that the average

SUS score of 77.5 places the system in the "good" usability category, which is higher than the industry average of 68. This suggests that the CIMS interface is intuitive and user-friendly for the vast majority of users. The average task completion time of 3 minutes and 48 seconds shows that users can efficiently complete crucial duties like criminal reporting. However, the standard deviation of 14.95 indicates considerable variety in the user.

5.5. Accessibility Evaluation Results

A comprehensive accessibility assessment was carried out to test WCAG 2.2 compliance across several dimensions. The findings highlighted both strengths and important areas for improvement. Table 5 illustrates that, while the system adheres strongly to key accessibility principles, some assistive technologies highlight areas for improvement. The successful keyboard operability and high color contrast suggest that visually oriented users and those who rely on basic navigation can easily interact with the system. The color contrast ratio of 16.31:1, which exceeds WCAG AAA standards, confirms excellent visual clarity.

5.6. Data Analytics Testing

The analytics dashboard depicted in Figure 19 provides university management and security personnel with actionable insights. It shows that intimidation and examination malpractice are the most frequently reported crimes on campus, with approximately seven incidents recorded. Compared to other cases like theft or assault, this is significantly higher. According to the data, social and academic misconduct is more common and calls for quick action, even though physical crimes like assault and theft do happen. For the security team, this means that preventive measures should not only focus on physical safety through patrols but also involve collaboration with academic and administrative units to combat intimidation and malpractice. Possible measures include awareness campaigns, stricter monitoring during academic activities, and improved victim reporting channels. Additionally, security operations can concentrate on sensitization programs for new and young students who may be more vulnerable, as the majority of victims are between the ages of 20 and 23.

5.7 Security Evaluation

A security assessment of the CIMS frontend application using the OWASP ZAP tool (Version 2.16.1) revealed a total of 10 alerts, which comprised 3 medium-risk and 2 low-risk vulnerabilities, alongside 5 informational findings, as depicted in Figure 20. Critically, the scan revealed no high-risk vulnerabilities. This indicates that the system's fundamental integrity, authentication mechanisms, and data protection controls are sound. The authentication mechanisms were successful in preventing unauthorized access during pilot testing. The results show that the core security architecture is strong, even though client-side security configurations need only minor remediation.

Summary of Alerts

Risk Level	Number of Alerts
High	0
Medium	3
Low	2
Informational	5

Fig 20. Summary table alert.

5.8, Evaluation Metrics and Results

Table 6 consolidates the quantitative and qualitative results from the multi-method system evaluation.

CONCLUSION

This study successfully designed and evaluated a web-based Crime Information Management System (CIMS) to modernize security operations on Nigerian campuses. The findings show that the CIMS significantly streamlines incident reporting, enhances data management, and provides actionable insights through analytics, thereby addressing critical gaps in traditional manual methods. Evaluation confirmed that the system meets essential benchmarks for security, performance, and usability. While the study acknowledges its scope as a single-campus pilot and identifies areas for future improvement in security configurations and accessibility features, the results provide compelling evidence of the system's efficacy and potential. It is therefore recommended as a viable solution for improving campus security and warrants further longitudinal and multi-institutional studies to explore its full potential for wider national adoption.

CONFLICT OF INTEREST

The authors declare that they do not have any conflict of interest.

REFERENCES

Abdullahi, A., & Orukpe, P. (2016). Development of an integrated campus security alerting system. *Nigerian Journal of Technology, 35*(4), 895. [Crossref]

Akinyede, J., Ponnle, A., Olebu, C., Akinluyi, F., Thompson, A., Dahunsi, O., & Oyinloye, M. (2023). Development of a software system for real-time management of crime reports in Southwestern Nigeria: The administrative approach. *American Journal of Science, Engineering and Technology, 8*(1). [Crossref]

Akpan, A., Ugah, J., & Ezeano, V. (2022). An intelligent crime reporting system: A proactive method for crime prevention. *Journal of Scientific and Engineering Research, 9*(8), 78–93.

Asiyai, R. I., & Oghuvbu, E. P. (2020). Prevalent crime in Nigerian tertiary institutions and administrative strategies for its effective

management. *International Journal of Higher Education, 9*(2), 270–282. [Crossref]

Azevedo, V., Nunes, L. M., & Sani, A. (2022). Is campus a place of (in)security and crime? Perceptions and predictors among higher education students. *European Journal of Investigation in Health, Psychology and Education, 12*(2), 142–155. [Crossref]

Dereje, A., & Nixon, J. S. (2020). Execution of web-based crime and criminals tracking system to enable security and quick access. *International Journal of Advanced Engineering Research and Science, 7*(8), 140–179. [Crossref]

Hingorani, I., Khara, R., Pomendkar, D., & Raul, N. (2020). Police complaint management system using blockchain technology. In *Proceedings of the 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)* (pp. 1214–1219). [Crossref]

Jimoh, A. A., Ibrahim, M. A., Ibrahim, R. T., Olawale, T. G., Yusuf, A. K., & Folorunso, M. I. (2023). Campus crime reporting software framework using short message services (SMS). *International Journal of Innovative Research in Education, Technology & Social Strategies, 10*(2). [Crossref]

Jimoh, A. A., Wajiga, G. M., & Garba, E. J. (2022). Software development for crime management in Nigeria University of Ibadan. *Journal of Science and Logics in ICT Research, 8*(1), 1–13.

Kommey, B., Opoku, D., Asare-Appiah, A., Wiredu, G. O., & Baah, P. K. (2023). An ad-hoc crime reporting information management system. *International Journal of Informatics, Information System and Computer Engineering, 4*(2), 122–146. [Crossref]

Kumar, K. K., Pravina, M., Nireesha, B., Tharun, M., & Krishna, B. Y. (2024). Crime investigation management system. *Journal of Engineering Sciences, 15*(2), 410–416.

Oludele, A., Onuiri, E. E., Olaore, O. A., Sowunmi, O. O., & Ugo-Ezeaba, A. A. (2015). A real-time crime records management system for national security agencies. *European Journal of Computer Science and Information Technology, 3*(2), 1–12.

Puckett, K. (2022). *Safety and security on campus: Student perceptions and influence on enrollment* [Master's thesis, East Tennessee State University]. Digital Commons @ East Tennessee State University. [Link]

Sharma, A., & Shahnawaz, M. (2014). Crime records management system. In *Proceedings of the 3rd International Conference on System Modeling & Advancement in Research Trends* (pp. 6–9). Teerthanker Mahaveer University.

Tomas, U. G., John, S. C., Ronalyn, D. C., & Jeromme, G. P. (2019). *Development of an online crime management & reporting system*. Asian Development Bank. [Link]

Uchenna, O. F., Kelechi, U. I., Kelechi, D. A., & Okorie, K. M. (2022). Integrated unified crime information management system. *International Journal of Innovative Technology and Exploring Engineering, 11*(8), 87–92. [Crossref]