Science Journal of University of Zakho
DOI: https://doi.org/10.25271/sjuoz.2026.14.3.1906

**Original Article**

# DEVELOPMENT OF A CHATBOT CYBERCRIME REPORTING SYSTEM

**Azeez Olawale Akinlolu[1,*], Ebunayo Rachael Jimoh[2], Adesoji Henry Adeshina[2], Abubakar Oladimeji Abubakar[3], and Mawada M. Elkhalifa[4]**

[1]Department of Mathematical and Computer Sciences, Fountain University Osogbo, Nigeria.
[2]Department of Computer Science, Ajayi Crowther University, Oyo, Oyo State, Nigeria.
[3]Department of Physical Sciences, Ojaja University, Eiyekorin, Kwara State, Nigeria.
[4]Department of Informatics and Computing, University Sultan Zainal Abidin, Malaysia.

[*]*Corresponding author, E-mail:*akinlolu.azeez@fuo.edu.ng (Tel: +234-8050313501)

Received
March 25, 2026

Accepted
July 1, 2026

Published
July 15, 2026

## ABSTRACT

Groundnut (The issue of cybercrime in Nigeria is of great concern, as the nation is ranked number five in the world and encountered more than 12.9 million attacks in the 2023 general elections. The old system of cybercrime reporting is still inefficient with a completion rate of 45-60% and 15-30 minutes per report. Although chatbot reporting systems, which are AI-based (in India and Singapore) have enhanced accessibility and interaction with citizens, similar solutions based on the specifics of the socio-cultural, linguistic, and technological environment of Nigeria have not had many opportunities to emerge. The current platforms are mostly based on the use of static web forms with little user instructions provided, and do not have real-time feedback, built-in evidence management, and proper case tracking. This paper introduces the creation of a Chatbot Cybercrime Reporting System (CCRS), which uses conversational AI to simplify the reporting for victims of online fraud and other cyber threats. Implementation was done on a Python Flask backend, PostgreSQL database, and a responsive frontend interface and tested with unit testing, integration testing and user acceptance testing (15 participants), six-week performance monitoring and security audits. Findings show significant increases compared to conventional solutions, such as a report completion rate of 94.2% and an average reporting time of 2.1 minutes, 99.5% operational uptime, and satisfaction with the chatbot user interface (4.6/5), with 93% of respondents choosing to use the chatbot user interface. There were also 150 simultaneous users that the system was handling with no security weaknesses reported. Incorporating more languages, covering a wider range of crime types, incorporating sophisticated natural language processing, and linking with law enforcement databases to provide a more comprehensive approach to cybersecurity nationally could become the focus of future research.

**Keywords:** Artificial Intelligence, Digital Forensics, Incident Response, Online Fraud.

## 1. INTRODUCTION

The recent high rates of digitalization and the increased availability of the internet have made cybercrime a significant international menace. The expanding attack surface has enabled large-scale phishing, ransomware, identity theft, and financial fraud, with global cybercrime losses projected to reach USD 10.5 trillion annually by 2025 (Lewis, 2018). Emerging economies are especially susceptible because of the inadequate cybersecurity infrastructure and awareness among the population. This is the case with Nigeria. Due to the growth of its digital economy, cybercriminal activities have increased in size and complexity. It is said that the Nigerian financial institutions had lost more than N.1.1 trillion to cybercrime over the last seven years, and the country had almost 13 million cyber-attacks during the 2023 general elections alone (Asoquo *et al*., 2020; NITDA, 2023). The fact that Nigeria is ranked number five in the Global Cybercrime Index in 2024 further highlights the need to enhance the national cybercrime response mechanisms (Miranda *et al*., 2024).

The advent of Artificial Intelligence (AI) has also transformed the world of cybercrime. Even though AI provides better threat detection and response capabilities, it has also given cybercriminals the power to use advanced automation and social engineering tools (Akinlolu & Jimoh, 2016). It has been reported that phishing attacks have increased by 4000% since the launch of the generative AI tools, and the problem of traditional security and reporting methods has become increasingly inadequate (SlashNext, 2024; Europol, 2024). Although regulatory and enforcement bodies like NITDA, the Nigeria Police Force Cybercrime Unit and EFCC exist, reporting of cybercrime in Nigeria is still ineffective. The current reporting systems are mostly manual, disjointed and inaccessible to many citizens. In Africa, less than one in three countries has operational incident reporting systems, digital evidence repositories, or digital cyber-threat intelligence platforms (Olusola *et al*., 2022; INTERPOL, 2024). The reasons that make victims not report include the complexity of the procedures, fear of stigmatization, privacy, and lack of confidence in the results of enforcement (Van der Hulst & Neve, 2017; Button & Cross, 2017). The law enforcement agencies are also constrained regarding limited training, ineffective tools and lack of resources, which further undermines the capacity of responding to cybercrime (Button & Cross, 2017).

Access this article online

DOI:https://doi.org/10.25271/sjuoz.2026.14.3.1906

**Science Journal of University of Zakho**
**Vol. 14, No. 03, pp. 535-545, July -2026**

Printed ISSN 2410-7549;
Electronic ISSN 2414-6943

In 2024, the Cybercrimes Act in Nigeria was amended, which has enhanced the legal requirements such as the 24-hour reporting of suspicious transactions by financial institutions, which is mandatory. Nevertheless, the reforms have put additional strain on already stressed reporting infrastructures and raised concerns of the population regarding data privacy and surveillance (Sibe & Kaunert, 2024). Conversational AI offers a solution to these problems. Other international programs, including AI-based chatbot reporting systems implemented by law enforcement agencies in India and Singapore, show better accessibility, effectiveness, and citizen involvement in cybercrime reporting (Sinha, 2024). However, there is a lack of empirical studies and system implementation that are specific to the sociocultural, linguistic and technological context of Nigeria. Current systems tend to use fixed web forms, offer little user instructions, and do not have real-time feedback, evidence management, and case tracking features (Dobber *et al*., 2024; Pavaloiu *et al*., 2024).

This paper addresses these gaps by creating a Chatbot Cybercrime Reporting System (CCRS) that is specific to Nigeria. The system proposed is a combination of conversational AI and secure backend architecture to facilitate incident reporting, law enforcement coordination, and centralized data management. The system is expected to enhance the rate of reporting, the quality of the data and the confidence level of the population by addressing the needs of diverse levels of digital literacy and language diversity. The research contributes not only to the theoretical field of conversational AI in law enforcement but also to practice, by offering a scalable cybercrime reporting system for developing nations.

## 2. LITERATURE REVIEW

The rapid growth of digital connectivity has increased cybercrime in the world. In 2024, the FBI received more than 859,000 cybercrime complaints with losses of USD 16 billion or more, which is 33% higher than the 2023 figures (Abdullah *et al*., 2025). This influx is an indication of the growing dependence of society on digital systems as well as the sophistication of cyber threats. Artificial intelligence has also transformed cybercrime, whereby tools capable of cracking ordinary passwords in a month have been developed and have been used in more than 80% of phishing attacks using AI-generated content (Verizon, 2024). Large language models (LLMs) are used by state and non-state actors to advance spear-phishing, reconnaissance, and exploitation of known vulnerabilities (Microsoft Threat Intelligence, 2024). In 2025, global cybercrime-related fraud is estimated to cost businesses USD 1 trillion, especially in the banking, healthcare, and retail sectors (Songsrirote, 2025).

Africa faces unique challenges in this context, including uneven digital infrastructure, limited reporting systems, and limited international cooperation. The number of scam notifications increased up to 3,000 % in some countries, and ransomware and cases of digital sextortion have surged greatly (INTERPOL, 2024). Nigeria being a technological center in West Africa is a target and source of cybercrime. Organizations like the Yahoo Boys use AI-created personas to commit romance scams (Akinlolu & Jimoh, 2016), which result in estimated yearly losses of USD 500 million, particularly in the financial and telecommunications industries (NITDA, 2023). Although the 2024 amendment to the Cybercrimes Act in Nigeria has made it harder to commit cybercrime, the rate of cybercrime has kept pace with enforcement capacity, with 86% of African nations reporting insufficient mechanisms of international cooperation (INTERPOL, 2024).

The two-sided nature of cybersecurity is also apparent in the case of AI: on the one hand, it can be used to detect and protect, but on the other hand, it allows cybercriminals to create advanced and targeted attacks. It has been reported that phishing attacks have grown by 4000 % after the use of generative AI tools such as ChatGPT (SlashNext, 2024; Europol, 2024). These advances highlight the importance of new reporting systems that can be updated to meet the changing threats. AI integration in law enforcement has revolutionized crime detection, prediction, classification and investigation (Jaishankar & Ronel, 2023). As conversational AI agents, chatbots provide an interactive channel through which victims can report crimes and are available 24/7, collect data in a standard format and have a lower reporting latency (Dobber *et al*., 2024). The sophisticated models of NLP enable victims to narrate events using natural language and direct them through investigation-ready forms (Pavaloiu *et al*., 2024). The strategy is a solution to a major problem in crime reporting, which is the transformation of unstructured accounts of the victim into usable intelligence.

A number of jurisdictions have adopted chatbot reporting systems. The Surat Police Cyber Mitra chatbot, which is based on WhatsApp, is used by the Surat Police to offer 24/7 support, whereas the Self-Lodging Police Report Chatbot is used in Singapore to help users write reports and incorporate them into law enforcement databases (Sinha, 2024; Singapore Police Force, 2023). The advantages of these systems include greater accessibility, less apprehension of reporting, and better quality of data. However, the foreign cases are weak. Most of the systems are more oriented on data gathering and lacks complete integration with case tracking, evidence management and investigative procedures. Also, it remains vulnerable to adoption due to language diversity and varying degrees of digital literacy, and cultural attitudes to crime reporting. These issues highlight the need to customize chatbot systems to the local socio-technical settings.

Several scholarly articles have been written on the topic of chatbot systems in reporting and public-service settings, providing insight into the design, effectiveness, user interaction, and technical constraints. Vitro *et al*. (2025) examined the impact of chatbot communication styles on the quality of police and user report perceptions. The authors created a chatbot police reporting system and used the online survey experiment involving 950 adults in the U.S. and manipulated the chatbot communication on the dimensions of power and solidarity to observe the impact on report accuracy, willingness to provide contact information, and trust in the system. Findings indicated that high power/high solidarity communication produced much more accurate reports, but there were no differences in trust or desire to provide contact information. The research points out the fact that communication style has an impact on the quality of the report but does not exhaustively cover the barriers to adoption in the real world since the experiment was done using artificial conditions and not real-time reporting information.

Kumukumu *et al*. (2024) created a chatbot that helps people report and handle crimes at the Malawi Police Service, called Kumukumu, which assists the user in formatting and organizing the information to be submitted to the authorities. It is based on a classification model and named entity recognition (NER) to identify structured information, e.g., location, time, and crime type in unstructured text. The methodology is a combination of generative and classification models to enhance usability and accuracy for users who file complaints. Testing was based on system functionality and user interface, and efficiency and organization of information were reported to be better. Nevertheless, the context of this work (Malawi) and the lack of user trust, adoption behaviour, and procedural justice in its analysis, as well as evidence management and follow-up tracking, which are essential to effective reporting systems, limits the work.

In addition to crime reporting, in particular, Zhou *et al*. (Zhou *et al*., 2024) studied the topic of public service chatbots in a metropolitan 311 system, where qualitative surveys and interviews were conducted to evaluate the perceptions of citizens about the design of chatbots. Their results revealed interpretation issues, transparency, and community-oriented design, showing that the current chatbots are too task-oriented without helping to engage the community. The paper has shown that the citizen expectations and socio-contextual considerations should be taken into consideration to improve the effectiveness of chatbots in the context of the public service setting. Although it does not emphasize crime reporting, systematic research offers important methodological background. As an illustration, chatbot security reviews note that data privacy, malicious input, and threat vectors are critical issues to consider in conversational agents, and vulnerabilities can negatively impact user trust and acceptance, which is a key factor to consider when any chatbot is gathering sensitive crime data (Xue *et al*., 2023). Other sources on chatbots in civic systems show that user satisfaction and efficiency can be achieved, although effectiveness is limited by issues like contextual understanding, usability, and metrics of effectiveness (Adam *et al*., 2021).

Overall, although the existing research shows the potential of the chatbot-based reporting systems, there are some gaps in the adaptation of the system in a specific context, especially in developing countries.

Existing systems tend to focus on data collection, but do not include built-in evidence management, real-time interaction, and local socio-cultural and linguistic considerations. This study aims to fill these gaps by developing a context-aware conversational reporting system for Nigeria that incorporates evidence management and usability aspects in one framework.

## Contribution:

Although there has been progress in the technologies of AI and chatbots in reporting crimes, there are still a few gaps. Available chatbot reporting systems are mostly designed and tested in more developed digital settings with little focus on developing nations like Nigeria, where digital literacy, multilingual communication, infrastructure limitations, and socio-cultural aspects play a major role in adoption and effectiveness (Vitro *et al*., 2025; Zhou *et al*., 2024). In addition, existing reporting systems in Nigeria are primarily based on the use of static web forms, and they provide little guidance, no real-time feedback, poor evidence management, and case tracking.

To fill this gap, this paper designed a context-sensitive Chatbot Cybercrime Reporting System (CCRS) that is specific to the Nigerian socio-cultural and technological context. The proposed system involves conversational AI to provide guided interactive, real-time reporting, in-built evidence management, and enhanced case management. The fact that the socio-cultural and technological context of Nigeria is included in this work contributes to the existing literature and demonstrates that context-sensitive conversational AI systems can contribute to much more effective cybercrime reporting in developing nations.

# 3. METHODOLOGY

## Data Collection:

Semi-structured interviews with 25 stakeholders, such as cybercrime law enforcement staff and cybersecurity experts, were used to gather primary data on the system requirements. These interviews were supplemented by a systematic review of the available literature on chatbot-based systems and discussions with law enforcement agencies and the officials of NITDA to identify operational and regulatory requirements. The User Acceptance Testing (UAT) comprised fifteen participants who were cybercrime victims, law enforcement personnel, and IT professionals. The sample population was representative of a wide range of demographic factors such as age, gender, digital literacy, and geographical location, as indicated in Table 1.

**Table 1:** Summary of the User Acceptance Testing (UAT) participants.

| S/N | Category | Subcategory | Frequency (n = 15) | (%) |
|---|---|---|---|---|
| 1 | Stakeholder Group | Cybercrime victims | 5 | 33.3 |
| | | Law enforcement personnel (NPF, EFCC) | 5 | 33.3 |
| | | IT professionals | 5 | 33.3 |
| 2 | Gender | Male | 9 | 60.0 |
| | | Female | 6 | 40.0 |
| 3 | Age (years) | Range | 24–52 | – |
| 4 | Digital Literacy Level | Advanced | 8 | 53.3 |
| | | Intermediate | 5 | 33.3 |
| | | Basic | 2 | 13.4 |
| 5 | Geographic Location | Lagos, Abuja, Ibadan | – | – |

## System Modeling:

The high-level Data Flow Diagram (DFD) in Figure 1 shows the way data is received by the users via the chatbot interface, processed by the backend system, and stored in the database, and accessed by the administrators and law enforcement agencies. Figure 2 illustrates the use case diagrams of the system in terms of user and administrator. The interaction between the user and the system involves registering an account, reporting an incident, tracking of the report, and receiving a notification, whereas the administrator is able to interact with the system in terms of managing the report, updating the case status, generating analytics, and communicating with the user. Figure 3 illustrates the overall system architecture that describes how system components are organized in the presentation, application, and data layers, and embedded security mechanisms. The layered architecture encourages the separation of concerns, which increases the maintainability and scalability of the system. The UML Activity Diagram in Figure 4 shows the end-to-end workflow of the Chatbot Cybercrime Reporting System, including the user authentication process to the chatbot, the subsequent backend processing, the administrative review, and the notification of the law enforcement. Lastly, Figure 5 provides the database design, which describes the data model and relational schema of the system. The database is in the form of core data entities, relationships and access patterns where the data integrity, scalability and optimization of performance were considered.

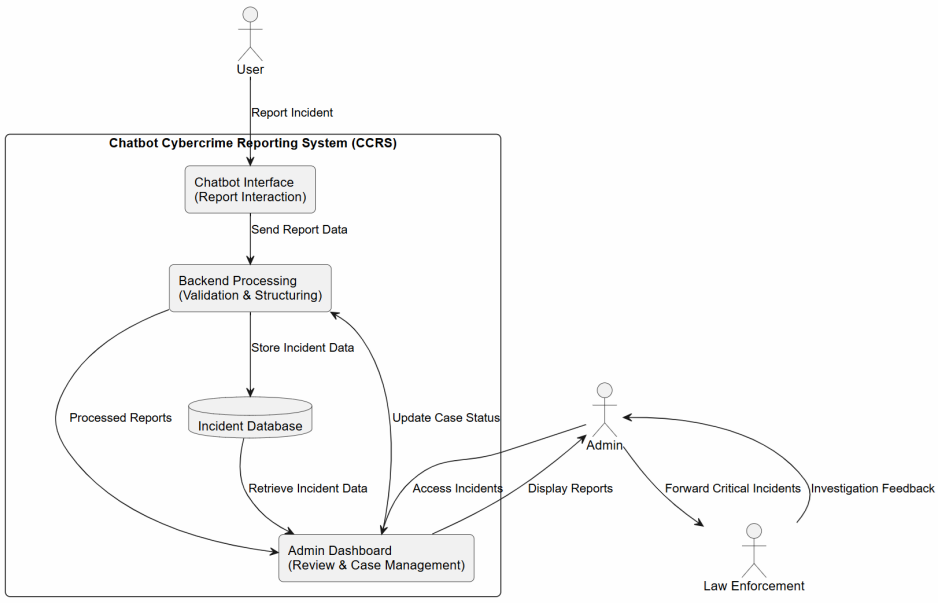


**Figure 1:** Data Flow Diagram of the CRSS.

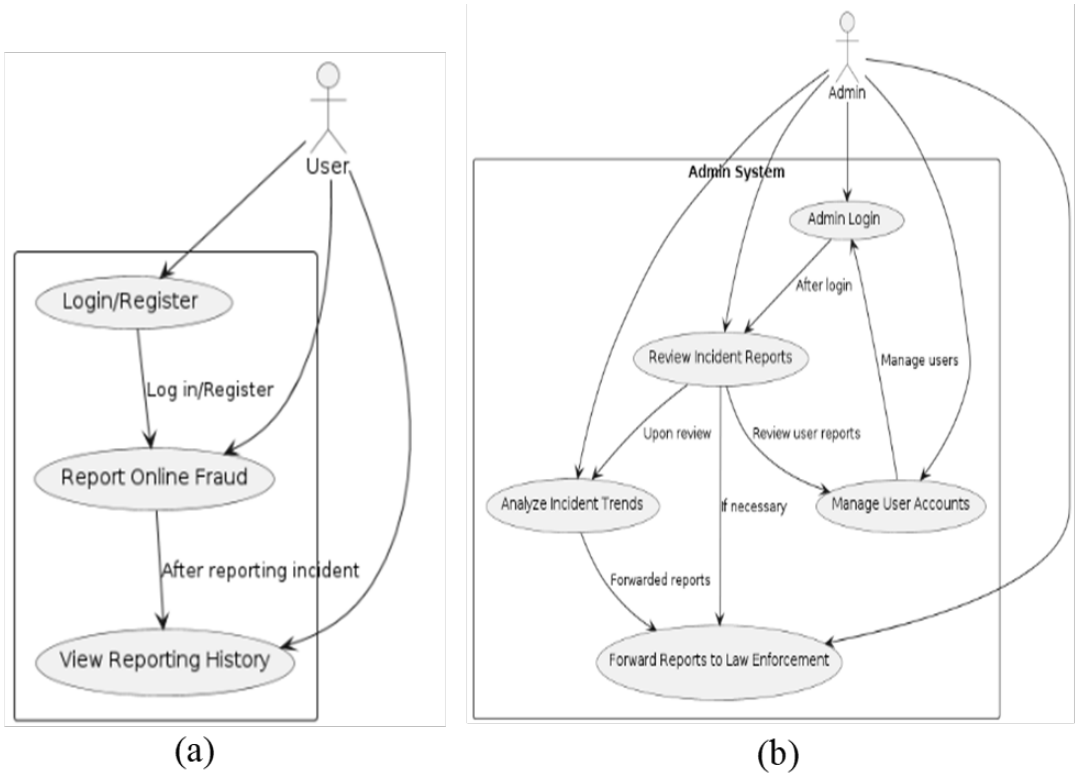


**Figure 2:** Use case diagrams of (a) users and (b) administrators

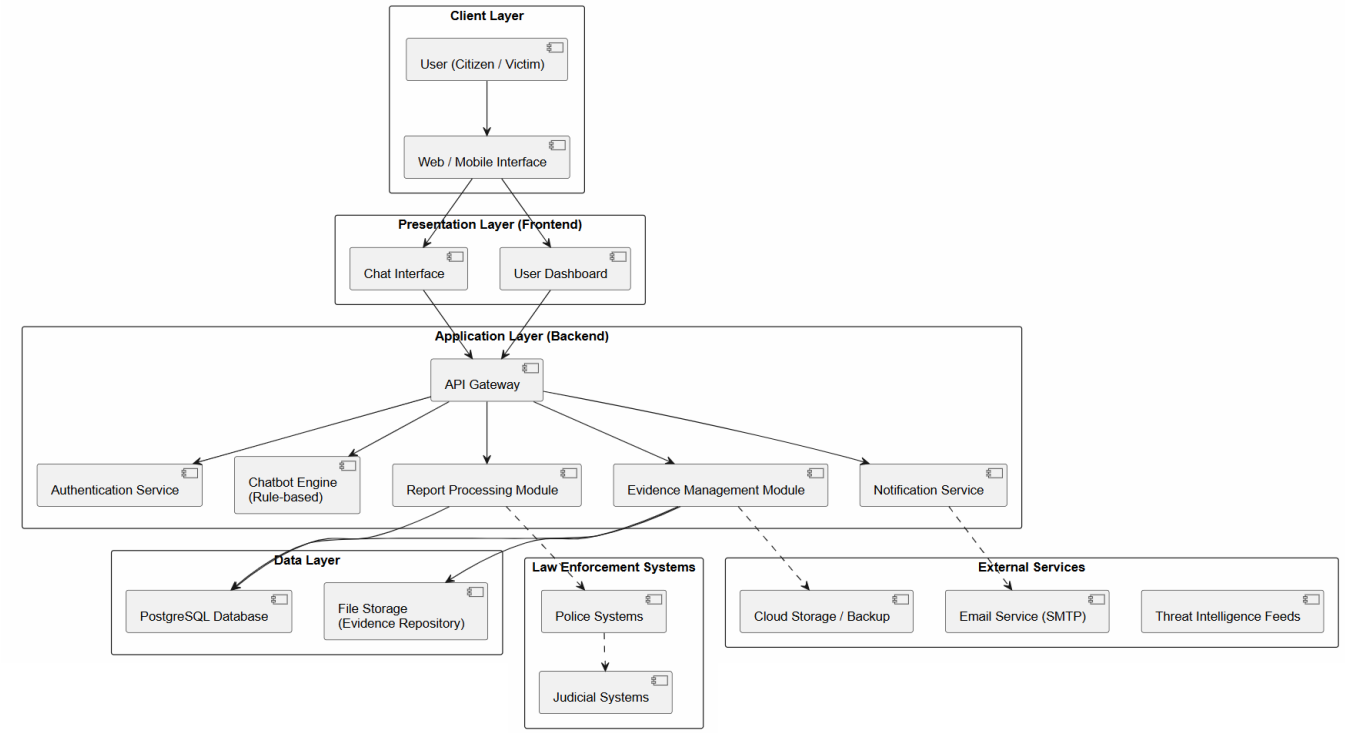


**Figure 3:** System architecture of the CRSS.

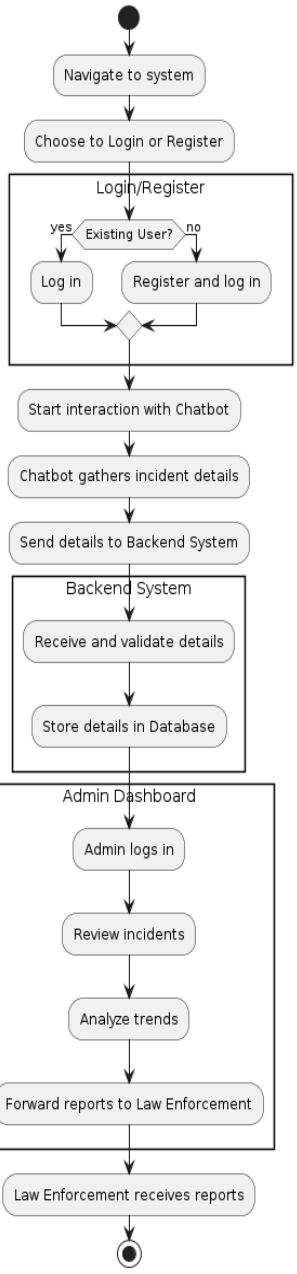


**Figure 4:** UML activity diagram of the CRSS.

### System Implementation:

The implementation step was based on a virtual development environment that applied Python versioning via virtual environments, versioning via Git, isolation of development via Docker, and CI/CD pipeline via automated testing. It had a web framework of Python 3.9 on Flask 2.0, which is a lightweight framework and can be easily combined with AI. SQLAlchemy was employed to provide the object-relational mapping layer, and WTForms was employed to ensure the integrity of the data without errors in the validation of the forms. Flask-Login regulated the user session, and Werzug was used to offer a security mechanism, hash passwords and file protection. The database management system used was PostgreSQL version 13. Visual Studio Code and Postman were the development tools and were used to test the API.

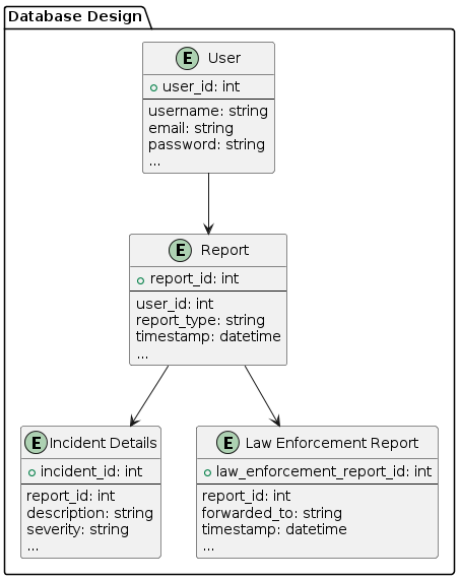


**Figure 5:** Database relational schema of the CCRS.

The chatbot conversation was designed to follow a systematic reporting process, which begins with the identification of the type of incident, followed by the temporal information collection of the incident, i.e. date, time, and duration of occurrence. Users then provide extensive testimonies in their own words, including evidence supporting them in the form of documents, screenshots or communications and assess the impact both in terms of financial loss and emotional impact. All the details about the perpetrators are pre-collected, and the users are obliged to revise and check all the information that they provide. Such a systematic approach ensures that there is comprehensive data collection as well as a conversational interface that reduces anxiety for the user. Data validation is carried out in different stages, wherein there is client-side validation to give instant feedback, server-side validation to guarantee security, and database constraints to validate consistency. The information relayed is encrypted before storing with the AES-256 algorithm and relayed over HTTPS to prevent interception. Uploading files is also scanned against malware and stored with cryptographic hashes, which assure integrity. The system applies Role-Based Access Control (RBAC), such that authorized law enforcement personnel will be allowed to access sensitive information, and any event of information access will be recorded in audit logs.

### Conversational AI and NLP Architecture:

The conversational component of the CCRS was implemented as a structured dialogue management system that integrated rule-based logic with guided input collection. The chatbot has a predefined conversational flow where it responds to users' answers and allows the systematic acquisition of information relative to the incident, including: time and date of the incident, location, description, and supporting evidence. It has the same design as the system workflow: user inputs are sequentially processed and checked in application layers. At the input stage, Natural Language Processing (NLP) was used to translate free-text descriptions given by the user. Some light-weight approaches used in the system involve tokenization, keyword matching and pattern matching for entity recognition and for mapping unstructured narrative to structured reporting formats. This way of working provides uniformity in data capture and usability for non-technical users.

### Data Security and Privacy Compliance:

Due to the sensitivity of reports of cybercrime and associated digital evidence, the CCRS adopted a multi-layered security architec-

ture to ensure that data would be kept confidential, kept intact and available. All data sent from users to the system was secured with the HTTPS protocol, and sensitive data stored in the database was encrypted with AES-256 encryption. All evidence files uploaded were scanned for harmful material before they were saved and received cryptographic hash values to verify integrity and aid in verification. The system implemented RBAC, where only authorized users, such as law enforcement officers, were allowed to view sensitive case data. Furthermore, audit logs were used to log all activities that took place within the system, such as data access and changes, ensuring transparency and traceability. The system allowed for anonymous reporting where user identification information was optional to ensure user privacy. Moreover, the architecture followed the principles of the Nigeria Data Protection Regulation (NDPR), such as data minimization, secure storage, controlled access, and user consent. Together, these guarantee the integrity and legality of the submitted digital evidence while safeguarding the sensitive nature of personal information.

### Evidence Management Mechanism:

In this study, the evidence management mechanism enables users to upload supporting evidence, including transaction receipts, screenshots, and communication records, seamlessly as part of the chatbot experience. All files are given a unique cryptographic hash, which acts as a digital fingerprint to ensure they are accurate and hard to alter. This mechanism helps to maintain evidence admissibility for legal and investigative procedures and addresses chain of custody issues. Evidence files are stored securely on the database infrastructure with the help of a relational schema design and associated incident reports. Data organization and investigative usability are enhanced by the conversational upload process, which maintains the contextual relationships and links between user stories and supporting materials.

## RESULTS

The implementation of the Chatbot Cybercrime Reporting System (CCRS) presented an operationally secure web-based system, with three integrated modules that are user dashboard, the conversational chatbot interface and the administrative dashboard. These modules are combined to enhance end-to-end reporting on cybercrime, submission of evidence, tracking of cases, and administrative analysis.

### User Dashboard Interface and Usability:

The secure login interface is the entry point to the system, and it is a multi-factor authentication where the identity of the user is verified. Once an authentication occurs, users will be redirected to a personalized dashboard, as demonstrated in Figure 6, where they can view their reporting history, track the status of reported items and view previous interactions with the chatbot. The design is inspired by a philosophy of minimalism to make sure potentially stressed-out victims do not need to think too deeply, presenting only the information they need with easy visual hierarchies and common navigation patterns.

The usability testing of some of the data showed that the dashboard was well accepted by the users with the 87% of those participating stating that the dashboard was intuitive or very intuitive, with an average time of completing the first task being estimated at 1.8 minutes. The card-based design, which was considered clean, helped take certain cognitive load off of customers reporting distressing events, and the participants commented positively on how easy it was to comprehend the status indicators, which included: Pending, Under Review, and Resolved.

### Chatbot Reporting Performance:

The key invention of the system is a conversational chatbot interface that simply transforms the experience of being able to report a crime more conventionally. Unlike a conventional fixed format that may be overwhelming and even intimidating, a chatbot will be used to initiate a natural conversation with the user, which will build up the necessary information through a set of questions. Figure 7 illustrates that the chatbot asks some specific, programmed questions, which are focused on creating a comprehensive background about the cybercrime event and not judgmental or critical. The interface is also well integrated to allow evidence collection and users can add supportive evidence (screenshots, transaction receipts, email heads and other documentation) directly into the conversation. This will eliminate the act of uploading files individually and will maintain the contextual thread of the reporting session, which will enhance user experience and quality of the data.

The performance review revealed that the mean length of conversation was 15.3, the mean time of report completion was 2.1 minutes and the rate of report completion was 94.2. The users could add as many as ten files with a size limit of 25 MB each directly into the chat program and accept many different file formats, such as JPEG, PNG, PDF, DOCX, and email files, MSG, EML. User content was positive (4.6/5.0) and 93% of the users were more satisfied with the chatbot than traditional forms as it was clear, guided and possessed the sense of a real person. The interface was observed to be less challenging, user friendly and provided a clear guideline on what to include in qualitative feedback.

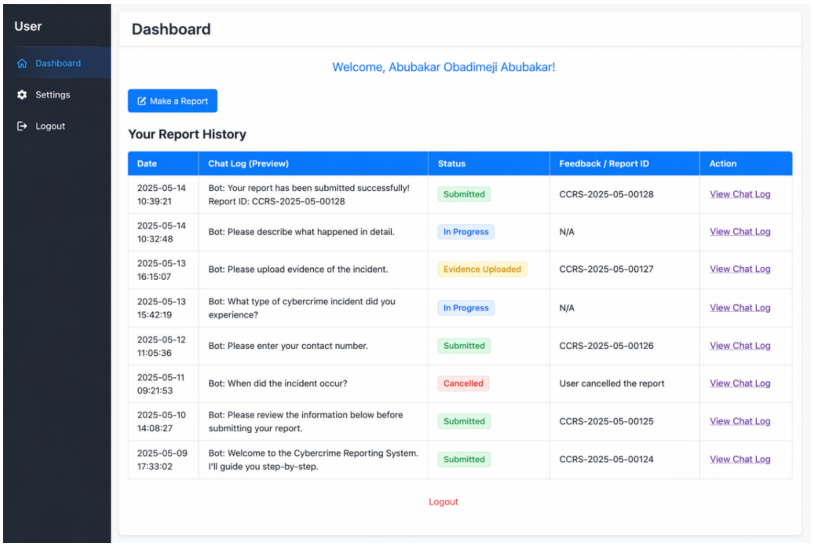


**Figure 6:** User Dashboard showing reporting history and status.

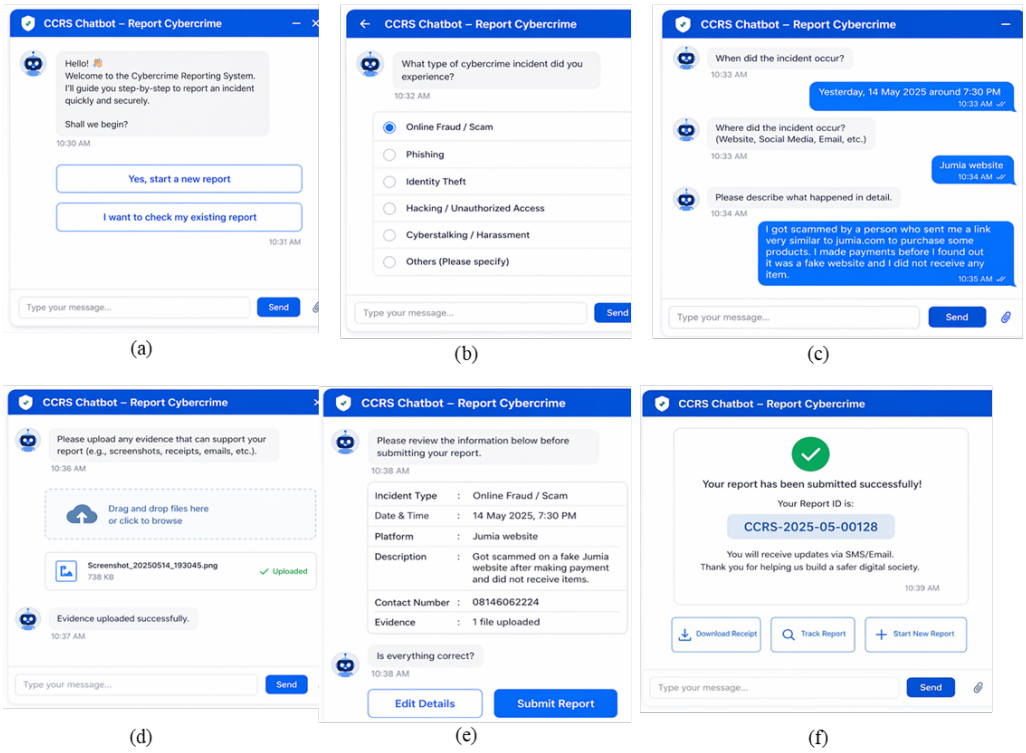


**Figure 7:** Conversational chatbot interface of the CCRS illustrating the cybercrime reporting workflow: (a) Welcome / Start Conversation, (b) Incident Type Selection, (c) Details Collection through (Guided Questions), (d) Evidence Upload, (e) Review & confirm report, and (f) Report submitted (Confirmation).

## Case Management and Administrative Dashboard:

Besides the components to be used by the user, the administrative dashboard provides law enforcement officers and system administrators with convenient tools to handle cases and analyze data. The advanced administration system is presented in Figures 8 and 9, and enables authorized users to view, filter and navigate through all the reports submitted using a handy control panel. The dashboard will support high-resolution data visualization features to present the critical data, such as the number of reports received, the rate of case resolution, the distribution of cases based on their types and time trends in the trends of cybercrime. These analytical functions transform raw incident data into actionable intelligence, which can be used to make evidence-based decisions and allocate resources, as well as enable administrators to identify new patterns of threats and track the utility of investigation activities.

The administrators documented an average of 8.7 minutes on an average case review per new report, a mean of 4.2 days on average following submissions to case closure and accuracy of reports in their classification at 96.8%. The filtering and search features of the dashboard facilitated effective management of cases with the administrators having the option of sorting and filtering the reports based on date range, type of crime, status, level of severity, and geographic location. The dashboard also included communication tools that made direct contact with reporters to seek clarification or request further information. The general satisfaction of the administrators was 4.4 out of 5.0, with the feedback focusing on the usefulness of visualization tools and the efficiency of the case assignment workflow.

## System Testing and Performance:

Reliability and accuracy of the system were tested. Eleven-unit test cases were successfully passed (Table 2), and the integration testing was 100 % successful in authentication, database operations, file uploads, and frontend-backend communication. The success rate of the tasks in User Acceptance Testing (n 15) was 94.2%, and the error rate was 5.8%, with 89% of the users being comfortable in sharing sensitive information. These six-week performance measures showed that the company was highly stable in its operations (Table 3). The system was documented to have 99.50 % uptime, average server response time of 234 ms, average database query time of 42 ms and 98.7 % file upload success rate. Load testing ensured that it supported 150 simultaneous users without deterioration of performance.

## Security Validation:

No vulnerabilities were detected during security audits and penetration testing in SQL injection, cross-site scripting, authentication bypass, session hijacking, or malicious file uploads. All the data was encrypted during transit and at rest, which confirms the strength of the multi-layered security architecture.

## Comparative Evaluation:

CCRS performed much better than the traditional methods of reporting, as seen in Table 4. The average reporting time decreased by 15-30 minutes to 2.1 minutes (86-93% decrease), and the completion rates rose by 45-60% to 94.2% (57-109% improvement). Continuous availability, instant recognition, organized data capture, and built-in evidence management were also presented by the system, which proves the usefulness of conversational AI in reporting cybercrime in Nigeria.

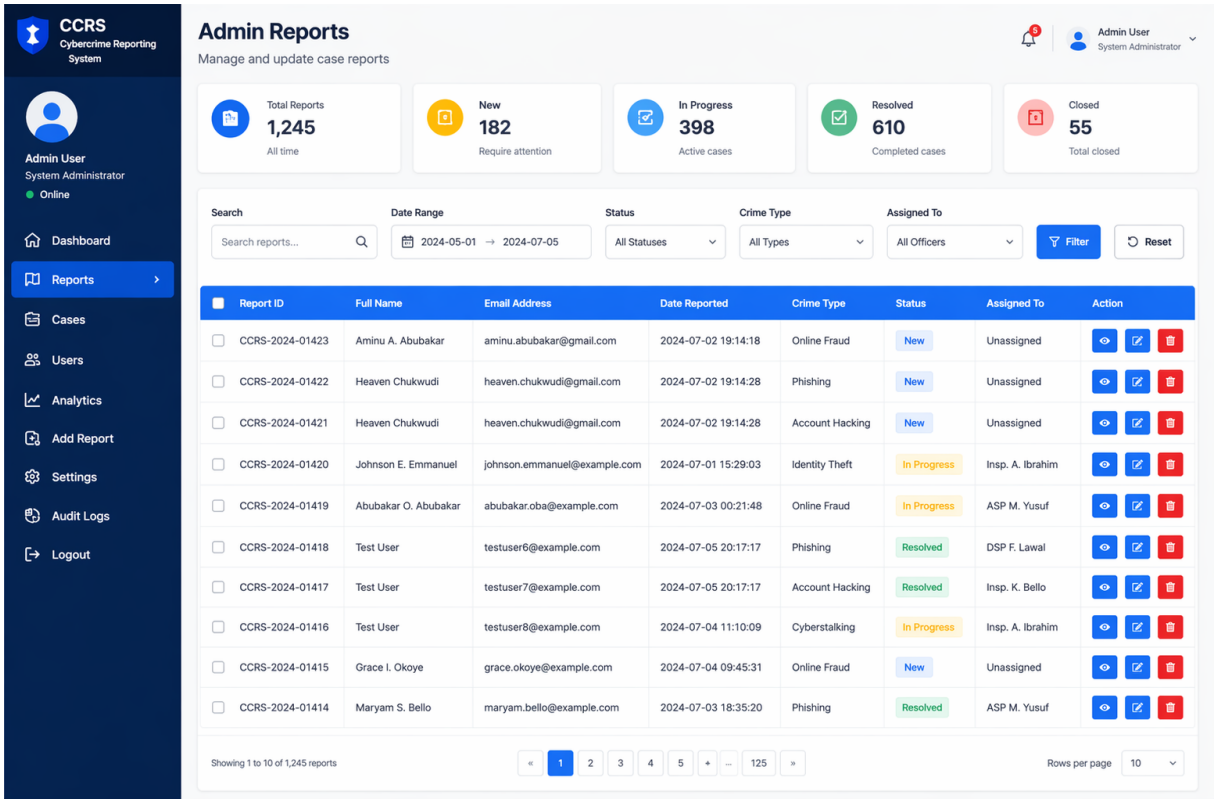


**Figure 8:** Admin Reports Interface for managing and updating case status.


**Figure 9:** Admin dashboard displaying case management tools and crime trend analytics.

**Table 2:** Unit Test Results for User Dashboard.

| S/N | Category | Subcategory | Frequency (n = 15) | (%) |
|---|---|---|---|---|
| 1 | Stakeholder Group | Cybercrime victims | 5 | 33.3 |
| | | Law enforcement personnel (NPF, EFCC) | 5 | 33.3 |
| | | IT professionals | 5 | 33.3 |
| 2 | Gender | Male | 9 | 60.0 |
| | | Female | 6 | 40.0 |
| 3 | Age (years) | Range | 24–52 | – |
| 4 | Digital Literacy Level | Advanced | 8 | 53.3 |
| | | Intermediate | 5 | 33.3 |
| | | Basic | 2 | 13.4 |
| 5 | Geographic Location | Lagos, Abuja, Ibadan | – | – |

All test cases (n=11) passed successfully, demonstrating robust core functionality.

**Table 3:** System Performance Metrics (6-Week Testing Period).

| Performance Indicator | Measured Value | Standard/Target |
|---|---|---|
| System operational uptime | 99.50% | $>$ 99.0% (Met) |
| Average report completion time | 2.1 minutes | $<$ 5 minutes (Met) |
| Average server response time | 234 ms | $<$ 500 ms (Met) |
| Database query execution time | 42 ms | $<$ 100 ms (Met) |
| Concurrent user capacity | 150 users | $>$ 100 users (Met) |
| Report completion rate | 94.2% | $>$ 80% (Met) |
| Chatbot interaction rate | 100% | $>$ 90% (Met) |
| File upload success rate | 98.7% | $>$ 95% (Met) |
| User satisfaction rating | 4.6/5.0 | $>$ 4.0 (Met) |
| Active user engagement rate | 80% | $>$ 70% (Met) |

All performance metrics exceeded minimum operational standards.

## 4. DISCUSSION

The findings of this study align with earlier studies showing that conversational interfaces can enhance user experience and data accuracy over traditional form-based systems. Previous research has demonstrated the effectiveness of structured conversational interaction to decrease cognitive load and improve reporting experience. The CCRS builds on prior work by combining conversational reporting with evidence management and case tracking in a single system, overcomes some of the challenges faced in previous implementations, and extending the work to a new context. This mix is a major step forward from approaches that have been done to date, which are mostly based on data collection without support for end-to-end reporting.

The Chatbot Cybercrime Reporting System (CCRS) was tested and measured relative to traditional reporting methods with benchmarks based on previous research on online form-based systems. The CCRS had a higher 97.4% report completion rate than the typical range reported for traditional systems (45-60%) in the online form performance studies conducted in a number of industries (Zuko Analytics, 2025; pdfFiller, 2026). In the same way, the average reporting time of conventional systems was decreased from around 15-30 minutes to 2.1 minutes, representing significant efficiency gains.

The feedback of the users shows that 93% of them liked the chatbot, and they found it less intimidating and felt like talking to a person, which is the key to the success of the system in terms of controlling the emotional component of reporting. CRRS had an actual high uptime at 99.5 %, a mean response time of 234 ms and 150 parallel users, which confirms its suitability for city-wide implementation. The error rate of 5.8 %, mostly because of the ambiguous inputs, implies that NLP models (e.g., BERT, RoBERTa) should be used in the future to enhance the understanding of context and flexibility. It can be compared to other international applications like Cyber Mitra in India or a self-lodging chatbot in Singapore that show that CCRS is in line with the international trends of streamlining reporting and adjusting to local limitations, including bandwidth restrictions, fluctuating digital literacy, and complicated evidence management. The concept of file uploads in conversation flows is a viable innovation that would help solve these Nigeria-specific issues.

In addition to technical validation, the way to the actual implementation of the CCRS is fraught with serious non-technical challenges and the need to align with the national digital policies. To move a research prototype to a national utility, one will need to deal with the recurrent expenses of maintaining cloud infrastructure and the ongoing training of law enforcement officers to operate the integrated administrative dashboard successfully. Moreover, the large-scale adoption is conditional on the intensive publicity campaigns to address the current cultural distrust and procedural fears of crime reporting in Nigeria. Policymaking-wise, the incorporation of such a system into the official channels is a strategic opportunity for synergy with agencies such as the National Information Technology Development Agency (NITDA) and the Nigeria Police Force (NPF) Cybercrime Unit. With the CCRS being aligned to the 2024 amendments to the Cybercrimes Act, the system can be used as a uniform portal of mandatory reporting, with data privacy and surveillance issues being resolved through open, AI-controlled structures. This would not only consolidate national cyber-threat intelligence but also make sure that the system keeps pace with the overall digital governance and security agenda of Nigeria.

The study was carried out in the Nigerian context, which is peculiar to socio-cultural, technological and regulatory environment. This enhances the relevance, but the system architecture is flexible and can be replicated in other settings, where integration with the legal framework in the region and alignment with the local reporting procedures are relevant. The CCRS uses a rule-based conversational structure to facilitate structured data collection, reliability and deployment in resource-limited environments. It guarantees consistency of report generation and controlled interaction according to investigative needs.

While the CCRS shows good usability and performance benefits, it is not as sophisticated as more complex conversational systems using machine learning and LLM for dynamic interactions and richer context understanding. Recent systems, such as LLM-based reporting frameworks, provide enhanced flexibility and semantic interpretation capabilities. The CCRS, on the other hand, employs a rule-based conversational approach for structured data collection, reliability, and ease of deployment in resource-constrained environments. What makes the proposed system so strong, however, is the combination of conversational reporting along with evidence management and case tracking, which aren't necessarily fully covered by the current implementations. The hybrid approach of rule-based workflows and advanced NLP models would be an interesting future research area to explore, as it would enhance adaptability while maintaining the data structure and reliability.

### Limitation:

The study is limited by the relatively small sample size (n = 15) used in the User Acceptance Testing, which restricts the statistical reliability and generalizability of the findings. While appropriate for prototype evaluation, larger and more representative samples are required to strengthen empirical validity. Also, descriptive statistics such as completion rates, mean reporting time and user satisfaction rates were used to evaluate the system. Limited sample size prevented the study from using inferential statistical tests such t-tests and confidence interval estimation. Future studies should include a more in-depth statistical analysis to confirm the differences observed and to determine the significance of system performance improvements.

## 5. CONCLUSION

The foregoing results indicated that SAMNUT 24 and SAMNUT 25 responded positively to fertiliser application, most importantly, the inorganic fertilisers. The inorganic fertilisers (NPK and SSP) had a marked influence on both pod and seed yield, protein content, fat, and energy values when compared to the organic fertiliser (Super GRO), where the latter promoted higher vegetative growth and carbohydrate accumulation. However, fertilizer application is still necessary when other essential nutrients needed for improving the quality and productivity of the seeds are limited in the soil. The cultivation of these varieties under inorganic fertilisers should be encouraged where there is low soil fertility.

**Table 4:** Comparative Analysis - CCRS vs Traditional Reporting Methods.

| Performance Metric | Traditional Methods | CCRS | Improvement |
|---|---|---|---|
| Average reporting time | 15–30 minutes | 2.1 minutes | 86–93% reduction |
| User completion rate | 45–60% | 94.2% | 57–109% increase |
| 24/7 availability | No | Yes | Full availability |
| Immediate acknowledgment | No | Yes | Instant feedback |
| Data collection quality | Variable | Consistent | Standardized |
| Evidence upload process | Separate/manual | Integrated | Streamlined |
| User satisfaction | 2.8–3.2/5.0* | 4.6/5.0 | 44–64% improvement |

*Literature-based satisfaction scores of traditional methods.

Future directions are to extend the coverage of crimes beyond online fraud, add support for multiple languages, flexible conversation management through machine learning and advanced NLP, linking with law enforcement databases, and secure evidence management. Such improvements would also increase the scalability, usability, and effectiveness of the system on the cybersecurity infrastructure of Nigeria. The current CCRS is basically a rule-based conversation system in the lines of structured reporting workflows. Further research is needed to incorporate sophisticated models for NLP, such as transformer-based systems, to improve the contextual understanding and adaptability of these systems. Also, the introduction of multilingual support, such as Nigerian Pidgin and major local languages, to enhance accessibility and user engagement among various populations is essential. In general, CCRS confirms the possibility of conversational interfaces to enhance citizen-government interactions and evidence-based approaches to crime prevention and response, as well as trust and accessibility in digital governance.

## Acknowledgment:

The authors extend their gratitude to everyone who contributed to the system's testing and evaluation phases.

## Ethical Statement:

The study did not require ethical approval as it involved neither human nor animal subjects.

## Conflict of Interests:

Conflict of Interest

## Funding:

This research did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors. The work was carried out using personal and institutional resources of the authors.

## Author Contributions:

A.O.A., E.R.J., A.H.A., A.O.Ab., & M.M.E., Design and Implementation of the Project, Software Development, Experimental Works, Data Analysis, and Writing.

## 6. REFERENCES

Abdullah, M., Nawaz, M. M., Saleem, B., Zahra, M., Ashfaq, E. B., & Muhammad, Z. (2025). Evolution Cybercrime-Key Trends, Cybersecurity Threats, and Mitigation Strategies from Historical Data. *Analytics*, 4(3), 25. DOI:https://doi.org/10.3390/analytics4030025

Adam, M., Wessel, M., & Benlian, A. (2021). AI-based chatbots in customer service and their effects on user compliance. *Electronic Markets*, 31(2), 427–445. DOI:https://doi.org/10.1007/s12525-020-00414-7

Akinlolu, A. O., & Jimoh, R. G. (2016). Detection of online phishing attacks using a transparent proxy system. *Elixir Network Engineering*, 100, 43375–43378.

Asoquo, A., Adewale, O., & Obinna, E. (2020). The multifaceted challenge of cybercrime in Nigeria: An urgent call for concerted mitigation efforts. *African Journal of Cybersecurity*, 12(3), 145–162.

Button, M., & Cross, C. (2017). *Cyber frauds, scams and their victims*. Routledge. DOI:https://doi.org/10.4324/9781315679877

Dobber, T., Metoui, N., & Lavorgna, A. (2024). Chatbot cops: How design features of police chatbots impact the quality of reports and perceptions of procedural justice. *Computers in Human Behavior*, 150, 108004. DOI:https://doi.org/10.1016/j.chb.2023.108004

Europol. (2024). *Internet organised crime threat assessment (IOCTA) 2024*. European Union Agency for Law Enforcement Cooperation.

He, X., Xu, G., Han, X., et al. (2025). Artificial intelligence security and privacy: a survey. *Sci. China Inf. Sci.*, 68, 181101. DOI:https://doi.org/10.1007/s11432-025-4388-5

INTERPOL. (2024). *African cyberthreat assessment report 2024*. INTERPOL Global Cybercrime Programme.

Jaishankar, K., & Ronel, N. (2023). *Global criminology: Crime and victimization in a globalized era* (2nd ed.). CRC Press.

Kumukumu, F., Medi, C., & Chatola, F. (2024). Development of an intelligent crime reporting chatbot for the Malawi police service. *International Journal of Computer Applications*, 186(22), 1–8. DOI:https://doi.org/10.26634/jse.18.3.20631

Lewis, J. A. (2018). *Economic impact of cybercrime: No slowing down*. Center for Strategic and International Studies.

Microsoft Threat Intelligence. (2024). *Microsoft digital defense report 2024*. Microsoft Corporation.

Miranda, M. Q., Tissot, P., & Esteves, J. L. (2024). The global cybercrime industry: A world cybercrime index. *PLOS ONE*, 19(4), e0297312. DOI:https://doi.org/10.1371/journal.pone.0297312

National Information Technology Development Agency. (2023). *Nigeria's 2023 general elections: Cyber threat assessment report*.

Olusola, F., Adeleke, T., & Oluwaseun, A. (2022). The absence of robust cybersecurity infrastructure and its implications: A case study of Nigeria. *International Journal of Information Security*, 21(4), 789–804. DOI:https://doi.org/10.1007/s10207-022-00583-0

Pavaloiu, A., Grigorescu, O., Mara, D. A., & Dobre, C. (2024). CrimeGPT: Leveraging large language models for enhanced cybercrime reporting and investigation. *Expert Systems with Applications*, 238, 121858. DOI:https://doi.org/10.1016/j.eswa.2023.121858

pdfFiller. (2026). *Online form statistics and completion rate insights*.

Sibe, R. T., & Kaunert, C. (2024). Cyber crime in Nigeria—reviewing the problems. In *Cybercrime, Digital Forensic Readiness, and Financial Crime Investigation in Nigeria* (pp. 19–55). Springer Nature Switzerland. DOI:https://doi.org/10.1007/978-3-031-54089-9_2

Singapore Police Force. (2023). *Annual report 2023: Innovation and community engagement*. Ministry of Home Affairs.

Sinha, S. (2024, October 16). Surat police launch AI chatbot to combat rising cybercrime. *Times of India*.

SlashNext. (2024). *The state of phishing 2024: AI-powered threats and defense*.

Songsrirote, N. (2025). Socioeconomic Determinants of Cybercrime Costs: A Panel Data Analysis of OECD Countries. *Asian Journal of Applied Economics*, 32(1), 30–57.

Van der Hulst, M., & Neve, R. J. M. (2017). High-tech crime, soorten criminaliteit en hun daders: Een literatuur-inventarisatie. *Tijdschrift voor Criminologie*, 59(1), 3–22. DOI:https://doi.org/10.5553/TvC/0165182X2017059001001

Verizon. (2024). *2024 data breach investigations report*. Verizon Business.

Vitro, C., Kearns, E. M., & Elson, J. S. (2025). How chatbot communication styles impact citizen reports to police. *Law and Human Behavior*, 49(1), 42–57. DOI:https://doi.org/10.1037/lhb0000613

Zhou, J., et al. (2024). Understanding citizen perceptions of government chatbots. In *Proceedings of the 2024 CHI Conference on Human Factors in Computing Systems* (pp. 1–16). DOI:https://doi.org/10.1145/3613904.3642398

Zuko Analytics. (2025). *Form conversion rate benchmarking data*.