International Journal of Artificial Intelligence and Digital Innovation
https://journals.hu.edu.so/index.php/ijaidi

AI-Assisted Cybercrime Management System for Somalia

Salwa Yusuf Hassan[1], Aliya Yusuf Hassan[1], Mohamed Awais Mohamed[1], Adam Ibrahim Abdi[2]*

[1]Faculty of Computer Science and Information Technology, Hormuud University, Mogadishu, Somalia

[2]Faculty of Computer Science, Somali National University, Mogadishu, Somalia

*Corresponding author's email: aadanibraahin@gmail.com

Abstract

The growth of digital services has increased both the scale and complexity of cybercrime, while cybercrime handling in Somalia remains constrained by fragmented reporting and largely manual investigative processes. This paper presents the design, implementation, and evaluation of an AI-powered cybercrime tracking system for centralized reporting, case management, digital-evidence handling, and investigation support in Mogadishu, Somalia. The system was implemented as a full-stack web application using HTML, CSS, and JavaScript for the frontend; Node.js and Express.js for the backend; MongoDB for data storage; and the OpenAI API for AI-assisted case categorization, suspect risk scoring, evidence analysis, victim-statement analysis, similar-case detection, and report generation. The platform provides role-based portals for citizens, analysts, investigators, and administrators, together with JWT-based authentication, SHA-256 evidence integrity verification, IP geolocation records, automated notifications, and PDF case reports. Requirements were informed through observation and interviews, while feasibility was assessed across technical, operational, economic, and schedule dimensions. Functional testing with Postman, verification of evidence hashing and tamper detection, AI-summary testing, and cloud deployment demonstrated the operational feasibility of the implemented platform. The reported evaluation indicates improvements in cybercrime documentation, case organization, and investigation support compared with manual record-keeping. However, quantitative measures of categorization accuracy, response time, false-positive rate, and user acceptance were not collected in this study and are identified as priorities for future evaluation. The study provides a practical, low-cost architecture for AI-assisted cybercrime management in a resource-constrained context and identifies directions for longitudinal evaluation, multi-institutional deployment, and more advanced predictive analytics.

Keywords: Cybercrime tracking, Artificial intelligence, Cybersecurity, Digital evidence management, Case management, Somalia.

1. Introduction

The proliferation of digital services has transformed communication, commerce, and information exchange, but it has also expanded the attack surface available to cybercriminals. Cybercrime activities, including hacking, phishing, online fraud, identity theft, malware, and ransomware, increasingly affect individuals, organizations, and governments, creating significant risks to privacy, financial stability, organizational continuity, and national security

[1]–[3]. As cyber incidents become more frequent and complex, effective cybercrime management requires mechanisms capable of systematically collecting incident reports, organizing case information, preserving digital evidence, identifying relationships among incidents, and supporting timely investigation and response.

In Somalia, cybercrime management remains constrained by reliance on manual record-keeping and basic information systems. Such approaches can make large volumes of case information difficult to organize and can limit investigators' ability to correlate related incidents, analyze digital evidence, monitor suspicious activities, and coordinate investigative activities efficiently [4], [5]. The absence of a centralized workflow connecting citizens, law-enforcement agencies, and the Somalia Computer Incident Response Team (SOMCIRT) further contributes to fragmented reporting and information sharing. These limitations become particularly important in resource-constrained environments, where access to sophisticated forensic infrastructure and specialized cybersecurity technologies may be limited.

Existing cybercrime-management approaches have addressed several aspects of this problem through centralized reporting platforms, digital case-management systems, and electronic evidence-management mechanisms. Centralized reporting can improve the organization of incident information and facilitate coordination among investigative agencies, while digital case-management platforms can support case tracking, assignment, status monitoring, and report generation [6], [7]. Research has also demonstrated the potential of artificial intelligence (AI) and natural language processing to support cybersecurity activities, including incident classification, suspicious-activity analysis, threat assessment, extraction of information from victim statements, and identification of similar cases [8], [9]. However, many existing approaches are designed for relatively well-resourced environments, while comparatively limited research has addressed integrated AI-assisted cybercrime management within the operational context of Somalia. In addition, existing platforms often emphasize incident reporting and information storage without providing a unified workflow that combines centralized case management with practical AI-assisted investigative functions.

This gap motivates the development of an AI-powered cybercrime tracking system designed specifically to support cybercrime reporting, investigation, and analysis in Mogadishu, Somalia. The proposed system integrates AI as an investigative-support layer rather than as an autonomous decision-making mechanism. The platform provides automated case categorization, suspect risk scoring, evidence analysis, victim-statement analysis, similar-case detection, and AI-assisted forensic report generation within a centralized case-management environment. By integrating these capabilities with role-based access control, digital evidence integrity verification, notifications, IP geolocation records, and report generation, the system is intended to reduce fragmentation in cybercrime handling and provide investigators with a more structured and efficient workflow.

The objective of this study is to design, develop, and evaluate an AI-powered cybercrime tracking system that improves the reporting, management, investigation, and analysis of cybercrime incidents. Specifically, the system establishes a centralized database for recording and managing cybercrime cases, incorporates AI-assisted functions to support investigation and analysis, and provides mechanisms for identifying cybercrime trends, patterns, and potentially related cases. The study further explores the system requirements and functionality needed to support citizens, analysts, investigators, and administrators within a unified cybercrime-management platform.

The main contributions of this work are fourfold. First, it presents a centralized, role-based cybercrime case-management architecture that integrates public reporting with analyst, investigator, and administrator workflows. Second, it incorporates an AI-assisted investigative layer that supports case categorization, suspect risk assessment, evidence and victim-statement analysis, similar-case detection, and report generation. Third, it integrates SHA-256 hashing

into evidence management to provide a mechanism for verifying the integrity of stored digital evidence. Finally, it demonstrates a comparatively low-cost implementation using a web-based technology stack and cloud infrastructure, providing a practical architecture for AI-assisted cybercrime management in resource-constrained environments such as Somalia.

The study was conducted in Mogadishu, Somalia, from September 2025 to July 2026, with emphasis on public cybercrime reporting, law-enforcement investigation, cybersecurity monitoring, AI-assisted categorization, evidence analysis, and pattern recognition. Overall, this work contributes an integrated and practical framework for AI-assisted cybercrime reporting and investigation, demonstrating how centralized case management and AI-based decision support can be combined to strengthen cybercrime-management capabilities in a resource-constrained national context.

2. Related Work

Centralized cybercrime reporting mechanisms provide a structured channel through which citizens can submit complaints and investigative organizations can coordinate follow-up activities. The Internet Crime Complaint Center (IC3), for example, provides a centralized reporting mechanism for Internet-related crime complaints [6]. Digital reporting mechanisms in East Africa also provide relevant examples for documenting online fraud, mobile-money scams, and phishing.

Digital case-management systems provide functions for recording case details, assigning responsibility, monitoring case status, and generating reports. Even simplified digital platforms can reduce the delays associated with paper-based record keeping, which makes them suitable for resource-constrained environments. Digital evidence management is another critical requirement. Electronic evidence may include emails, screenshots, IP addresses, system logs, and other digital artifacts. Maintaining consistent records of evidence and its integrity can strengthen investigative processes and documentation. In the implemented system, SHA-256 hashing is used to provide a verifiable integrity value for uploaded evidence.

AI is increasingly used in cybersecurity and cybercrime-related tasks. Reported applications include incident classification, suspicious-activity analysis, threat prediction, natural-language processing of victim statements, and similar-case detection [8], [9]. The present system operationalizes these ideas as AI-assisted functions within a case-management workflow rather than as a standalone automated detection engine. Inter-agency coordination and user acceptance are also relevant to system adoption. Integrated information systems can support information sharing and coordination among police, cybersecurity agencies, and other authorities. The Technology Acceptance Model (TAM) and related acceptance research identify perceived usefulness and perceived ease of use as important determinants of technology adoption [10]–[13].

2.1 Research Gap

Three related gaps can be identified. First, relatively little published work addresses cybercrime-management systems in low-resource settings such as Somalia, particularly within the operational context of Mogadishu. Second, many systems emphasize reporting and storage but provide limited AI-assisted investigative support. Third, some approaches assume access to advanced forensic infrastructure that may not be readily available to local institutions. The proposed system responds by combining centralized case management, evidence integrity controls, and practical AI-assisted investigation features within a comparatively low-cost web architecture.

3. Methodology

A descriptive research design was used, supported by observation and interviews with intended users to inform functional and non-functional requirements [14], [15]. UML-based system

analysis and an operational workflow were used to model the process from incident submission through case management and resolution.

Table 1: Development Environment and Technology Stack

Layer / Tool	Technology	Purpose
Frontend	HTML5, CSS3, JavaScript	Citizen and staff interfaces
Backend	Node.js, Express.js	API services, authentication, case management
Database	MongoDB / MongoDB Atlas	Document-oriented case and evidence data
AI	OpenAI API	Categorization, analysis, risk scoring, similar-case detection, report support
Modeling	StarUML	System analysis and UML modeling
Testing	Postman	API, authentication, authorization, and error-handling tests
Deployment	DigitalOcean	Cloud application deployment
Reporting	PDFKit	PDF case-report generation

The development and technology stack of the system is summarised in Table 1. The development environment consisted of a laptop with an Intel Core i7 processor, 16 GB RAM, and 512 GB SSD, running Windows 11 Pro with Visual Studio Code. Stable Internet connectivity was used for cloud database and OpenAI API communication.

3.1 Feasibility Analysis

Technical, operational, economic, and schedule feasibility were assessed; the economic feasibility is summarised in Table 2. The selected software stack was considered adequate for the required web and AI functions. The design was intended to minimize disruption to investigative workflows. The reported development cost was approximately USD 113, covering hosting, Internet data, domain registration, publishing, transport, and incidental expenses. The project was completed within the planned project period.

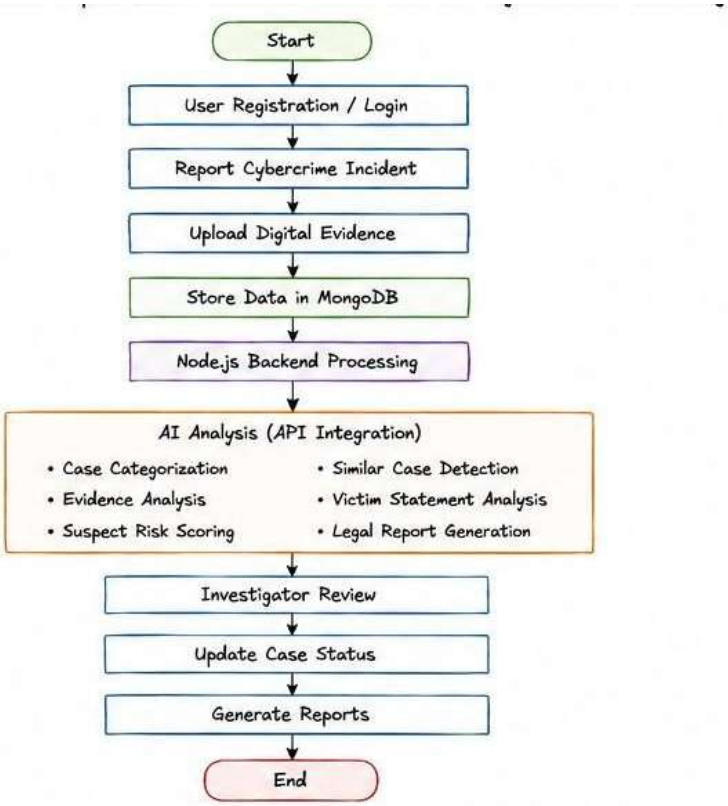
Table 2. Economic feasibility summary.

Cost Item	Frequency	Cost (USD)
Web hosting	31	5
Internet data	18	64
Book publishing	2	10
Domain name	1	18
Data gathering / transport	2	8
Food and drinks	6	8
Total	—	113

3.2 System Design and Implementation

The implemented system is a full-stack web application with a public-facing citizen portal and role-based internal portals for analysts, investigators, and administrators. These components communicate with a MongoDB data layer and an AI service layer. Fig. 1 summarizes the operational framework of the system.

Fig. 1. Operational Framework of the AI Cybercrime Tracking System.



3.3 Database Design

The database comprises eight documented collections: Users, Cases, Victims, Suspects, Evidence, IpRecords, Notifications, and Reports as reported in Table 3. Users supports role-based access and account status. Cases stores unique case numbers, crime categories, and case status. Victim and suspect records provide case-specific entities, while Evidence stores evidence metadata and integrity information. IpRecords captures suspicious IP information and geolocation data; Notifications supports user alerts; and Reports stores generated analytical outputs.

Table 3. Database collections and functions.

Collection	**Primary Function**
Users	Accounts, roles, hashed passwords, and account status
Cases	Case number, category, status, and core incident information
Victims	Victim-related case information
Suspects	Suspect-related case information and risk-related attributes
Evidence	Evidence records and integrity metadata
IpRecords	Suspicious IP records and geolocation information
Notifications	System and case notifications
Reports	AI-generated summaries and exported report content

3.4 Backend and Security

The backend was implemented with Node.js [16] and Express.js. JWT-based authentication and role-based authorization control access to staff functions. Evidence handling uses SHA-256 hashing to provide an integrity check for uploaded files. IP tracking records geolocation information. Environment variables are used to protect database credentials, JWT secrets, and API keys during deployment.

For AI-assisted analysis, an analyst can request a summary of an existing case. The system aggregates associated case information, including victim, suspect, and evidence records, and sends the relevant content to the OpenAI GPT model. The returned structured analysis includes a case summary, key findings, and recommended next steps. The result is stored in the Reports collection and incorporated into PDF output. A mock fallback response is used when the API quota is exceeded. The AI-assisted investigative functions of the system are summarised in Table 4.

Table 4. AI-assisted investigative functions of the system.

AI Function	Role in the Documented System
Case categorization	Supports classification of reported cybercrime cases.
Suspect risk scoring	Provides an AI-assisted risk assessment for investigative support.
Evidence analysis	Analyzes associated evidence information supplied to the AI workflow.
Victim-statement analysis	Extracts or summarizes investigative information from statements.
Similar-case detection	Supports identification of related or previously investigated cases.
Report generation	Produces structured AI-assisted analysis for inclusion in case reports.

3.5 Frontend and Role-Based Workflows

The frontend uses vanilla HTML5, CSS3, and JavaScript. The public experience provides a home page and citizen portal with incident reporting, case-status access, notifications, profile functions, and support contact. After authentication, staff are directed according to role. Analysts receive dashboards with crime-trend analytics and reports; investigators manage assigned cases, evidence, and status updates; administrators manage users, investigator assignments, case oversight, and system settings.

3.6 Testing and Deployment

Testing covered API endpoint behavior, error handling, authentication, and role-based access control using Postman. Evidence integrity was tested by uploading files and checking generated hash values, while AI summary generation was tested using real case data. The application was deployed to a DigitalOcean cloud server, with MongoDB Atlas used as the production database. The frontend was served as static files through the DigitalOcean App Platform.

4. Results and Evaluation

The evaluation in this study is primarily functional and qualitative rather than statistically quantified. The implemented platform successfully provides the documented combination of citizen reporting, role-based case management, evidence integrity verification, IP geolocation records, notifications, PDF reporting, and AI-assisted case analysis.

4.1 Functional Outcomes

The proposed system contributes to cybercrime management by centralizing the collection, organization, and analysis of case information, thereby addressing the fragmentation associated with manual record-keeping. It provides role-based access through separate workflows for citizens, analysts, investigators, and administrators, allowing each user group to interact with the system according to its operational responsibilities.

The system also supports digital evidence integrity through SHA-256 hashing, which generates an integrity value that can be checked against uploaded evidence records. In addition, its AI-assisted analysis capabilities support case categorization, suspect risk scoring, evidence and victim-statement analysis, similar-case detection, and AI-assisted report generation. Operational monitoring is further supported through IP geolocation records, notifications, cloud-based dashboards, and report export functions. Finally, the system demonstrates deployment feasibility through cloud infrastructure using MongoDB Atlas and protected environment variables.

4.2 Evaluation Scope and Boundaries

During implementation, improved documentation, faster case triage, stronger evidence handling, positive user feedback, and near-real-time monitoring were observed. However, this study did not collect numerical measurements, sample sizes, baseline-versus-system timing data, confusion matrices, precision/recall/F1 scores, false-positive and false-negative rates, or formal user-acceptance scores. Accordingly, these observations are reported as qualitative outcomes rather than quantitative performance claims.

A stronger empirical evaluation would require documented test counts, case or dataset composition, AI evaluation criteria, response-time measurements, categorization accuracy, false-positive/false-negative analysis, and a defined user-evaluation protocol; these are identified as priorities for future work.

5. Discussion of the Results

The principal value of the implemented system is its integration of reporting, case management, evidence integrity, and AI-assisted analysis in a single workflow. Rather than requiring separate tools for citizen reporting, investigation, evidence tracking, and report generation, the architecture places these activities within a common application and database. This directly addresses the fragmentation identified in the problem statement.

The use of SHA-256 hashing provides a practical integrity mechanism for a low-cost prototype. It does not, by itself, establish complete forensic chain-of-custody compliance; rather, it supplies a cryptographic value that can be used to detect changes to stored evidence. Likewise, AI-generated analyses should be interpreted as decision-support outputs rather than authoritative investigative or legal conclusions.

The architecture is also appropriate to the resource constraints emphasized in the study. Its use of a web application, document-oriented database, cloud deployment, and API-based AI service reduces the need for specialized local infrastructure. Nevertheless, this introduces dependencies on Internet availability, cloud services, API quotas, and the quality and privacy of information supplied to external AI services.

Finally, the observations about user acceptance and improved operational efficiency should be treated cautiously because this study did not include a formal user study or quantitative acceptance instrument. The reported outcomes are useful as an initial system evaluation, but multi-institutional and longitudinal studies are needed before generalizing them.

5.1 Limitations and Future Work

Despite the successful implementation of the proposed system, several limitations should be acknowledged. The evaluation was conducted within a limited environment and using a limited dataset, which restricts the generalizability of the findings, while the relatively short evaluation period limits assessment of long-term system reliability and operational performance. The availability of cybercrime data also constrained systematic training and testing of the AI components. Furthermore, dependence on Internet connectivity and third-party services, particularly cloud infrastructure and AI APIs, may affect operational continuity. The AI-assisted categorization and analysis functions may produce false-positive or false-negative outputs, and the study does not provide numerical error rates or sufficient quantitative evaluation to establish their accuracy under operational conditions. Although positive usability and acceptance outcomes were reported, no formal quantitative user-acceptance study was documented. Finally, while SHA-256 hashing provides a mechanism for verifying digital-evidence integrity, it does not by itself constitute a complete forensic chain-of-custody framework; therefore, the current system should be regarded as a functional prototype and decision-support platform rather than a fully certified forensic or law-enforcement system.

Future research should focus on strengthening the empirical evaluation and operational applicability of the proposed system through longitudinal evaluation using documented cybercrime datasets and repeatable performance metrics, as well as deployment across multiple institutions to assess generalizability and interoperability. The AI components should be evaluated using appropriate quantitative metrics, including precision, recall, F1-score, confusion matrices, and task-specific validation procedures. Advanced machine-learning and predictive-analytics techniques could also be investigated to support proactive threat forecasting and improve identification of emerging cybercrime patterns. Integration with external threat-intelligence platforms and stronger evidence-provenance mechanisms, such as blockchain-based evidence records, could further strengthen investigative capabilities and evidence management. In addition, mobile and cross-platform versions could be developed to improve accessibility for citizens and investigators, while future implementations should establish appropriate governance and privacy mechanisms, human-review procedures, and auditable decision-making processes for AI-assisted law-enforcement activities. These improvements would help transition the current prototype toward a more robust, scalable, and operationally suitable cybercrime-management platform.

6. Conclusion

This paper presented an AI-powered cybercrime tracking system designed to centralize cybercrime reporting, investigation, evidence management, and analytical support in Mogadishu, Somalia. The implemented platform combines a citizen reporting portal with role-based staff workflows, MongoDB-based case storage, JWT authentication, SHA-256 evidence integrity checking, IP geolocation records, notifications, PDF reporting, and AI-assisted investigative functions.

The system demonstrates the technical feasibility of integrating these capabilities into a comparatively low-cost web-based platform for a resource-constrained context. Its main contribution is not a new standalone AI model, but an integrated application architecture that embeds AI assistance within a cybercrime case-management workflow. The available evaluation supports functional feasibility and reported operational benefits, but the absence of detailed quantitative measurements limits claims about detection accuracy, response-time improvement, and user acceptance. Future empirical studies should address these gaps through reproducible datasets, defined evaluation metrics, longer deployments, and multi-institutional testing.

Conflict of Interest

The authors confirm that there is no conflict of interest related to this manuscript.

References

[1] INTERPOL, Global Cybercrime Programme: Cybercrime Threats and Trends, Lyon, France: International Criminal Police Organization, 2024.
[2] European Union Agency for Law Enforcement Cooperation (Europol), Internet Organised Crime Threat Assessment (IOCTA) 2024, Luxembourg: Publications Office of the European Union, 2024.
[3] INTERPOL, African Cyberthreat Assessment Report 2024, Lyon, France: INTERPOL, 2024.
[4] Federal Government of Somalia, Ministry of Communications and Technology, Somalia National Cybersecurity Policy, Mogadishu, Somalia, 2023.
[5] Somalia Computer Incident Response Team (SOMCIRT), Cyber Incident Response and National Cybersecurity Information Publications, Mogadishu, Somalia, 2024.
[6] Federal Bureau of Investigation, Internet Crime Report 2023, Washington, DC, USA: Internet Crime Complaint Center (IC3), 2024.
[7] Europol, Online Fraud Schemes: A Web of Deceit, The Hague, Netherlands: Europol, 2023.
[8] M. Schmitt, "Securing the Digital World: Protecting Smart Infrastructures with AI-Enabled Malware and Intrusion Detection," arXiv preprint, 2024.
[9] European Union Agency for Law Enforcement Cooperation (Europol), ChatGPT: The Impact of Large Language Models on Law Enforcement, The Hague, Netherlands, 2023.
[10] F. D. Davis, "Perceived usefulness, perceived ease of use, and user acceptance of information technology," MIS Quarterly, vol. 13, no. 3, pp. 319–340, 1989.
[11] F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, "User acceptance of computer technology: A comparison of two theoretical models," Management Science, vol. 35, no. 8, pp. 982–1003, 1989.
[12] V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view," MIS Quarterly, vol. 27, no. 3, pp. 425–478, 2003.
[13] V. Venkatesh, J. Y. L. Thong, and X. Xu, "Unified Theory of Acceptance and Use of Technology: A synthesis and the road ahead," Journal of the Association for Information Systems, vol. 17, no. 5, pp. 328–376, 2016.
[14] J. W. Creswell and J. D. Creswell, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, 6th ed. Thousand Oaks, CA, USA: SAGE Publications, 2023.
[15] M. Saunders, P. Lewis, and A. Thornhill, Research Methods for Business Students, 9th ed. Harlow, UK: Pearson, 2023.
[16] OpenJS Foundation, Node.js Documentation, OpenJS Foundation, 2025.