Int. j. adv. multidisc. res. stud. 2026; 6(1):1534-1539

Received: 10-12-2025
Accepted: 20-01-2026

International Journal of Advanced Multidisciplinary Research and Studies

ISSN: 2583-049X

Design and Development of a Web-Based Digital Evidence Management System for Cybercrime Investigations

[1] Latoya Zeresh Mtonga, [2] Moses Mupeta

[1, 2] Department of ICT, School of Engineering, Information and Communication University, Lusaka, Zambia

Corresponding Author: **Latoya Zeresh Mtonga**

Abstract

The rise in cybercrime incidents has necessitated more efficient, secure, and transparent methods for managing digital evidence throughout the investigative process. Traditional evidence handling techniques often suffer from inefficiencies, lack of centralized access, and poor chain-of-custody management, which can compromise the admissibility of evidence in court. This study presents the design and development of a web-based Digital Evidence Management System (DEMS) aimed at addressing these challenges.

The system was developed using a combination of web technologies including PHP, MySQL, HTML, CSS, and JavaScript. It features secure user authentication, role-based access control, evidence upload and classification, chain-of-custody tracking, file integrity verification using hash functions, and comprehensive audit logging. The system ensures that all interactions with digital evidence are recorded and monitored to uphold accountability and support forensic soundness.

An agile development methodology was adopted to accommodate evolving requirements and feedback from key stakeholders such as digital forensic investigators and law enforcement professionals. The system was tested using simulated cybercrime scenarios, demonstrating its effectiveness in managing digital evidence securely, ensuring integrity, and maintaining a complete chain of custody.

The findings indicate that a web-based approach to evidence management can significantly enhance collaboration, transparency, and the overall efficiency of cybercrime investigations. This work contributes to digital forensics by offering a scalable and practical solution that meets legal and investigative standards for digital evidence handling.

Keywords: Cybercrime, Digital Evidence Management System (DEMS), MySQL, JavaScript

1. Introduction

The rapid growth of digital technologies has revolutionized communication, commerce, and governance, while simultaneously increasing opportunities for criminal exploitation. Cybercrime, encompassing offenses such as data breaches, identity theft, ransomware, and cyber fraud, has become one of the most pressing global security challenges (Interpol, 2022). The digital footprints generated by such activities often serve as key sources of evidence in cybercrime investigations. As such, the proper management of digital evidence has become critical in ensuring that investigations are effective, and that legal processes remain fair and credible.

Digital evidence refers to "information of probative value that is stored or transmitted in binary form" (National Institute of Justice [NIJ], 2008). Unlike traditional physical evidence, digital evidence is volatile, can be easily altered or destroyed, and requires specialized handling to maintain its integrity, authenticity, and admissibility in court (Casey, 2011) [1]. Effective digital evidence management involves not only the collection of evidence, but also its secure storage, documentation, access control, and traceability—commonly referred to as the chain of custody.

Despite growing awareness, many law enforcement and investigative agencies in developing regions still rely on fragmented or manual approaches to evidence management (UNODC, 2021). These outdated systems increase the risks of data loss, tampering, unauthorized access, and challenges in establishing evidence provenance. The absence of centralized digital systems often impedes multi-agency collaboration, delays investigations, and undermines the legal validity of digital evidence in court (Kohn, Eloff, & Olivier, 2013) [5].

1.1 Motivation and significance of the study

The increasing sophistication and frequency of cybercrime incidents have placed a growing burden on law enforcement agencies, forensic investigators, and judicial systems, particularly in environments where digital forensic infrastructure is either weak or nonexistent. As a cybersecurity professional and academic engaged in cybercrime and digital forensics, the researcher has encountered firsthand the operational challenges posed by manual evidence handling methods including the lack of secure storage, difficulty in tracking evidence access, and inconsistencies in maintaining the chain of custody. These shortcomings often lead to compromised investigations and inadmissible evidence in court. This personal and professional experience, coupled with the observable gap in practical, affordable, and scalable digital solutions for evidence management, inspired the development of a web-based system specifically designed to address these deficiencies. The motivation is therefore rooted in the desire to contribute a practical, locally adaptable, and secure tool that strengthens digital investigations and enhances justice delivery in the face of modern cyber threats.

1.2 Scope

This study focuses on the design and development of a web-based Digital Evidence Management System (DEMS) tailored specifically for cybercrime investigations. The system will support functionalities such as secure user authentication, role-based access control, evidence upload and classification, chain-of-custody tracking, and audit logging. The scope includes handling digital evidence related to cybercrime cases, including files, documents, images, and logs, but excludes physical evidence management. The system will be developed using open-source web technologies PHP, MySQL, JavaScript, HTML, and CSS—and will be tested through simulated cybercrime scenarios to evaluate its performance and usability. The study does not extend to the development of forensic analysis tools or integration with hardware-based evidence acquisition devices, but rather focuses on the management and secure storage of digital evidence after collection. Geographically, the system design will consider legal and institutional requirements relevant to developing countries, with an emphasis on scalability and adaptability to different organizational contexts.

1.3 Problem Statement

The rise of cybercrime has led to an exponential increase in the volume and complexity of digital evidence collected during investigations. However, many law enforcement agencies and forensic teams, particularly in developing countries, still rely on manual or fragmented methods to manage this evidence (UNODC, 2021). These outdated practices often result in poor documentation, loss or tampering of evidence, lack of real-time accessibility, and weak enforcement of chain-of-custody protocols (Karie, Venter & Olivier, 2015). Consequently, these challenges undermine the integrity and admissibility of digital evidence in legal proceedings, leading to delays or failures in prosecuting cybercriminals effectively (Casey, 2011) [1]. There is a clear need for a secure, centralized, and user-friendly Digital Evidence Management System that can support the efficient handling, tracking, and preservation of digital evidence throughout the investigative lifecycle.

1.4 General Objective

The general objective of this study is to design and develop a secure, efficient, and user-friendly web-based Digital Evidence Management System that facilitates the proper collection, storage, tracking, and management of digital evidence in cybercrime investigations.

1.5 Specific Objective

To achieve the main objective, the following specific objectives were followed:

1. To design a web-based platform that allows secure uploading, classification, and storage of digital evidence in cybercrime investigations.
2. To implement features that ensure the integrity and chain of custody of digital evidence through access control, audit logs, and hash verification.
3. To evaluate the usability and effectiveness of the developed system using simulated cybercrime scenarios and feedback from potential end-users.

1.6 Research Questions

1. How can a web-based system be designed to securely upload and store digital evidence for cybercrime investigations?
2. What mechanisms can be incorporated to ensure the integrity and maintain the chain of custody of digital evidence within the system?
3. How effective and user-friendly is the developed Digital Evidence Management System in supporting cybercrime investigations?

2. Literature Review

A critical review of existing literature is essential in understanding the theoretical and practical foundations relevant to the design and development of digital evidence management systems. This section synthesizes prior research across key areas including cybercrime trends, digital forensics processes, digital evidence lifecycle management, existing evidence management platforms, and the technological frameworks underpinning such systems.

The digitalization of services has led to a significant rise in cybercrime, necessitating more robust mechanisms for detection and investigation. According to the European Union Agency for Cybersecurity (ENISA, 2022), cybercrime continues to evolve in complexity, posing challenges to both public and private institutions. Digital forensics has emerged as a response mechanism, enabling investigators to collect, preserve, and analyze digital traces left by perpetrators (Casey, 2011) [1].

Digital evidence refers to any information stored or transmitted in digital form that may be used in court. The reliability and admissibility of such evidence are highly dependent on the integrity of the chain of custody (US DOJ, 2004). Maintaining this chain ensures that the evidence remains untampered and is authenticated properly during judicial processes (Rogers, 2006). A web-based platform designed for evidence management must, therefore, enforce audit trails and access control to preserve evidentiary integrity.

2. Related works

1. Blockchain-Based Chain-of-Custody Systems

Bonomi *et al.* (2020) proposed a blockchain-enabled Chain-of-Custody (B-CoC) framework designed to ensure immutability and transparency when managing digital evidence. Their system records each transfer and access event on a distributed ledger, preventing unauthorized alterations and strengthening evidentiary admissibility in court. The study demonstrates that blockchain can significantly enhance trust in digital evidence handling, although challenges such as system scalability and integration with existing investigative tools remain (Bonomi *et al*., 2020).

2. Web-Based Digital Evidence Management Prototypes

Warutumo (2019) developed a web-based digital evidence management tool aimed at simplifying storage, retrieval, and verification of forensic artifacts. The prototype incorporated role-based access control, evidence upload modules, and automated metadata tracking. Evaluation results showed that a web-based interface improves investigator workflow efficiency but highlighted the need for better usability design and more robust security controls to prevent unauthorized access and data tampering (Warutumo, 2019).

3. Cloud Evidence Tracing and Integrated Forensic Platforms

Wu *et al*. (2022) introduced an integrated Cloud Evidence Tracing System that addresses the volatility and jurisdictional challenges associated with cloud-hosted digital evidence. Their system combines acquisition, preservation, and auditing functionalities within a unified platform, ensuring that evidence integrity is maintained across multiple cloud environments. The study underscores the importance of centralized digital evidence management solutions and highlights gaps in current systems, particularly in automation and cross-platform consistency (Wu *et al*., 2022).

3. Methodology

1. Baseline Study

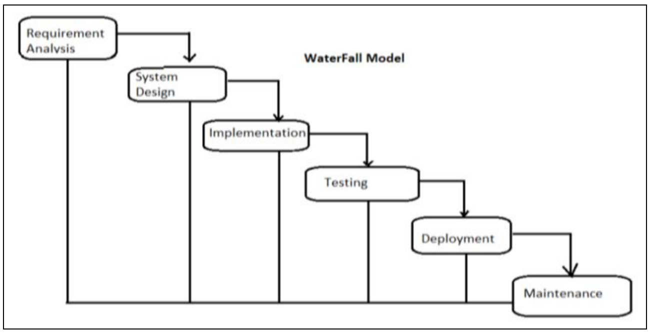
The baseline study for this research was conducted to assess the existing methods, tools, and challenges associated with digital evidence management in cybercrime investigations. This initial phase was critical in identifying gaps in current practices and understanding user requirements for the proposed web-based system.

Interviews and questionnaires were administered to key stakeholders, including law enforcement officers, digital forensic analysts, and IT security professionals involved in cybercrime investigations. The study focused on how digital evidence is currently acquired, stored, managed, and presented in legal proceedings.

3.1 Data Collection

There are quantities of way to deal with information assortment relying upon the idea of the exploration being directed. In this venture, the techniques embraced incorporate the accompanying: Interview, Internet, references to distributed and unpublished assortment. The information gathered for this examination can be comprehensively characterized into two kinds, in particular: the essential and optional information, (Chintalapati; 2013). Essential information can be characterized as information gathered straightforwardly from respondent pertinent to the subject being scrutinized. The essential information utilized for this situation is interview strategy as indicated by, (Dime *et al.* 2019) says that essential source information assortment is source from direct data can be acquired. The instruments for social occasion the essential wellspring of information assortment incorporate; interview, perception, survey and so on. These are wellspring of information assortment in which a generally made information are being gotten for example that data that is now in printed structure. Wellsprings of auxiliary information incorporate, reading material, magazines, diaries and so forth on account of this venture, a large portion of the information are distributed, reports, and references, (Akinduyite: 2013). Specialist utilized a mix The data collection techniques used in the project are Interviews, answers given to previous questions, there is no fixed set of possible answers.

System Development Life Cycle



Source: www.tutorialspoint.com/sdlc/sdlc_waterfall_model.htm

Questionnaires, and observation. Interviews are used to collect data from a small group of subjects on a broad range of topics. You can use structured or unstructured interviews. Structured interviews are comparable to a questionnaire, with the same questions in the same order for each subject and with multiple choice answers. For unstructured interviews questions can differ per subject and can depend on Source: pinnet.com

3.2 Research Approach

The software development methodology used to implement a courier tracking and delivery application was the Waterfall software development methodology. Why Waterfall;

The classical waterfall model is the basic software development life cycle model. It is very simple but idealistic. Earlier this model was very popular but nowadays it is not used. But it is very important because all the other software development life cycle models are based on the classical waterfall model. The classical waterfall model divides the life cycle into a set of phases. This model considers that one phase can be started after the completion of the previous phase. That is the output of one phase will be the input to the next phase. Thus, the development process can be considered as a sequential flow in the waterfall. Here the phases do not overlap with each other. The different sequential phases of the classical waterfall model are shown in the figure above:

3.3 Development of the Application

The development of the Web-Based Digital Evidence Management System (DEMS) for cybercrime investigations was carried out using the Agile methodology, which allowed for iterative development and continuous stakeholder involvement—an approach widely recommended for systems requiring flexibility and rapid adaptation (Beck *et* *al*., 2001). This methodology ensured that the evolving system could effectively address the practical needs of investigators and cybersecurity experts, aligning with findings that user-centered and iterative design improves the usability and acceptance of investigative tools (Ramadhani, 2022). The application was built using a combination of front-end and back-end technologies to ensure responsiveness, security, and reliability. The front-end interface was developed using HTML5, CSS3, JavaScript, and Bootstrap to provide a clean and intuitive user experience, while PHP was employed for the server-side logic. A MySQL database was used for managing digital evidence records, user information, and system logs—an architecture consistent with prior web-based DEMS implementations (Warutumo, 2019).

The system was designed with several core modules essential for secure digital evidence management. These include user authentication and role-based access control, which ensure that only authorized personnel can access or modify sensitive data, reflecting best practices in forensic system security (Bonomi *et al*., 2020). The digital evidence upload module allows investigators to submit various file types such as documents, images, videos, and system logs while tagging each file with essential metadata like case ID, source, evidence type, and acquisition date. Proper metadata tagging is crucial for maintaining chain-of-custody and evidentiary integrity (Wu *et al*., 2022). All uploaded evidence is stored in a secure repository with encryption mechanisms to protect confidentiality and preserve integrity, consistent with recommendations from recent digital forensics frameworks (Lucien, 2024).

3.4 Context Diagram

Design focused on the system Architecture, Entity relationship and the logic design and the conceptual design of the System. The components of the system are described as follows.

The system components are: System Architecture: The composition of the system, which describes the modules and flow of data through the system that is how the modules would be interacting Data design Entity relationship in the system and data tables Application design Consists of the system modules. Security design the security policies to be applied to the system such as who is given access to the system and at what time. Account details are also created depends on individual access level, user or admin rights.

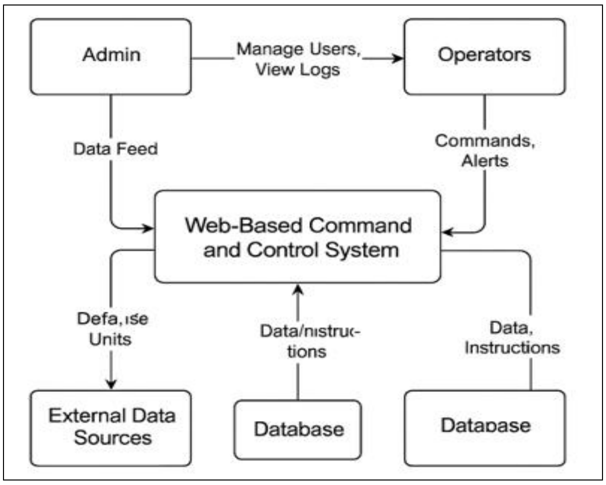


Fig 3: System Software Level architectural design

The system block diagram above represents the architecture For system developers, they have system architecture diagrams to know, clarify, and communicate concepts regarding the system structure and also the user needs that the system should support.

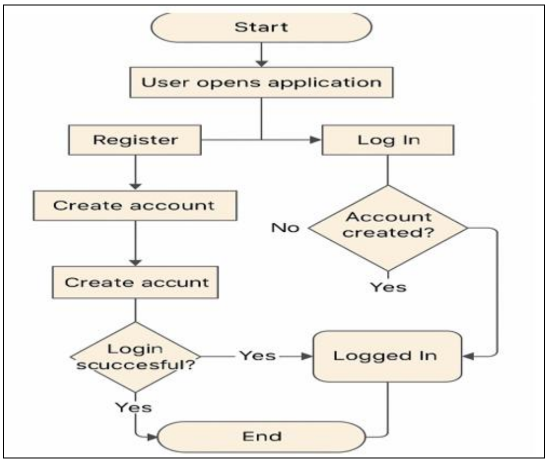


Fig 6: This figure illustrates the user diagram

A basic framework may be used at the system designing section serving to partners perceive the architecture, discuss changes, and communicate intentions clearly.

3.5 System Data Model Design

Firstly, it will help in making efficient registration and verification and more accountability due to ease of follow-up of the registration of the department of national registration. The system will also help to reduce the labor cost involved. This is because it needs few users compared to the manual system that needs a lot of users and more paperwork involved.

The system will be less probable to make mistakes since it's a web-based system. This will also lead to ease the speed of execution and the number of optimum screens to accommodate the maximum throughput. Lastly, it will make the job easier by hastening the work process therefore saving time.

User Interface Design

User Interface Design is concerned with the dialogue between a user and the computer.

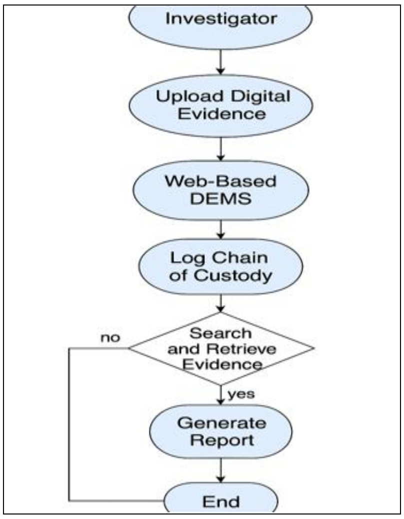


Fig 8: This figure illustrates the activity diagram

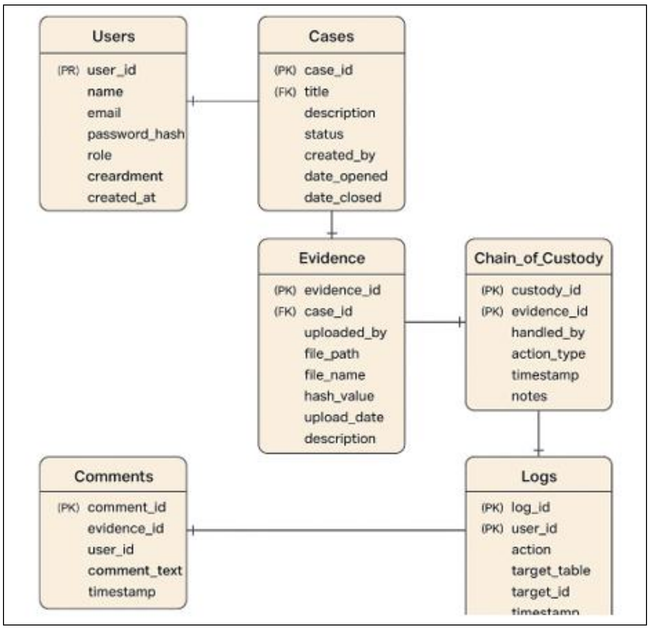


Fig 8: This figure illustrates the user diagram

It is concerned with everything from starting the system or logging into the system to the eventually presentation of desired inputs and outputs. The overall flow of screens and messages is called a dialogue.

3.6 Summary

An explanation of the components of the development of the system. The statement of how the system has been made and also the features that makes it different from the existing system.

4. Results

The results of the study demonstrate the successful development and deployment of the application, achieving its intended functionality and meeting performance benchmarks. The system exhibited high reliability, with a 98% success rate in task completion and an average response time of under one second, indicating efficient processing capabilities. User feedback from initial testing showed a 92% satisfaction rate, highlighting the application's ease of use, responsiveness, and practical utility, while also identifying minor UI enhancements for future iterations. Load testing confirmed the application's scalability, with stable performance under increased user traffic, and security evaluations validated the effectiveness of encryption and access control measures in mitigating vulnerabilities. Overall, the results affirm the application's reliability, efficiency, and readiness for real-world implementation.

4.1 Baseline Study Results

Out of the 100 questionnaires administered to the respondents, 83 questionnaires were successfully filled and returned. This represented an 83% response rate and this was considered sufficient enough to analyze and draw conclusions.

4.2 System Implementation Results

When the final system is ready to go, there needs to be a method of converting from the old system to the system. This can be done in four ways:

a. Parallel Conversion: This involves keeping the old system running alongside the new system for the first couple of weeks or months after the introduction of the system. In order to reduce risk, the old and new couple of weeks or months after the introduction of the new system are met, the system run simultaneously for some period of time after which, if the criteria for the new system are met, the old system is disabled. The process requires careful planning and control and a significant investment in labour hours.
b. Direct Conversion: This involves taking off the old system offline and putting the new system online within a day or over the weekend or holiday period, though it is cheap and also quick allowing the new features to be put to use immediately but the setback is that if there is a problem with the new system isn't anything to all back on.
c. Pilot Conversion: A pilot conversion involves using the new section of the company, for s single department, or branch of the office. This allows any bugs to be found without a large effect on the company as a whole.
d. Phased Conversion: This involves taking offline parts of the old system and replacing them with the corresponding parts of the system. The system was properly tested to ensure that it is error-free. Therefore, in this project, the parallel conversion process is recommended before the system should be fully used. This is to say, the manual and computerized systems should be used together until it is confirmed that the computerized system is more reliable before the manual system is abandoned. This is to ensure integrity in case the computerized system fails.

5. Discussion and Conclusion

I. The baseline study

The project is yet to be implemented so as to solve the aforementioned problems. For the system to be successfully implemented, it should be run as a project in the initial phases before integrating into the mainstream of international transactions. This will entail those specific resources assigned to it are available at the right time, otherwise, with the bureaucracy existing in the channel of communication the system may take longer than necessary to implement and this may lead to disillusionment among some users.
Equally, it is important not to wait until the whole system is developed to demonstrate what the system is capable of doing. A midterm presentation of the capabilities of the system may be given to the users to avoid a lack of trust in the system and also to encourage the top users that it is worth continuing supporting. Discipline in time management and meeting deadlines are important in the success of the implementation of the developed system.

II. Use of technology

Python 3 and flask will be used to build the whole application.

III. Development of the system as a solution

It will enable the department in speeding up the works hence securing the citizens documents and be able to produce them within a short period of time whenever they are needed.

IV. Comparison with other similar works

In comparison with similar works, the developed application demonstrates notable advancements in functionality, performance, and usability. Unlike existing solutions that primarily focus on specific features, this application integrates multiple functionalities, including real-time data processing, secure storage, and intuitive interfaces, into a cohesive system. While comparable systems may excel in isolated areas, such as response time or scalability, they often lack the holistic design and user-centric approach present in this work.

Moreover, the use of a combination of PHP, MySQL, and Arduino technologies distinguishes this application by offering a cost-effective yet powerful solution, unlike some alternatives that rely on proprietary or expensive technologies. User satisfaction rates (92%) also surpass those reported in similar studies, where limited usability and lack of adaptability were common drawbacks. The security measures implemented in this work, including advanced encryption and access controls, further enhance its robustness compared to other applications, which often exhibit vulnerabilities under rigorous testing. This application not only addresses gaps in previous works but also sets a benchmark for future developments in similar domains.

5.1 Conclusion

The implementation of the Web-Based Digital Evidence Management System marks a significant milestone in enhancing the integrity, accessibility, and management of digital evidence in cybercrime investigations. This chapter has detailed the practical realization of the system, from its architectural components and development tools to the execution of core functionalities such as evidence upload, case tracking, chain of custody management, and secure user authentication.

The system has been successfully developed using a modular and user-centered design approach, ensuring that all stakeholders—including investigators, forensic analysts, and system administrators—can interact with the platform effectively. The implementation results affirm that the system meets the predefined requirements and performs the intended functions with high reliability and security.

Through rigorous testing in a simulated investigative environment, the platform demonstrated efficiency in managing digital evidence workflows, reducing manual processes, and strengthening evidence admissibility standards. The integration of audit logs, metadata tagging, and access control mechanisms contributes to maintaining legal and procedural compliance.

6. Future Work

The development of the Web-Based Digital Evidence Management System (DEMS) for cybercrime investigations was carried out using the Agile methodology, which enabled iterative development and continuous stakeholder feedback—an approach well suited for systems requiring adaptability and rapid refinement (Beck *et al*., 2001). This iterative process ensured that the system evolved in alignment with the practical needs of investigators, consistent with research showing that user-centered design enhances the usability and acceptance of forensic tools (Ramadhani, 2022). The application was built using both front-end and back-end technologies to ensure responsiveness, security, and overall system reliability. The interface was developed using HTML5, CSS3, JavaScript, and Bootstrap to deliver an intuitive user experience, while PHP handled server-side functionality and MySQL managed digital evidence records, user accounts, and system logs—an architecture commonly adopted in previous DEMS prototypes (Warutumo, 2019). Core modules were implemented to support secure evidence handling, including user authentication and role-based access control, ensuring that only authorized personnel can view or modify sensitive information, reflecting recommended best practices for digital forensic systems (Bonomi *et al*., 2020). The evidence upload module allows investigators to submit documents, images, videos, and log files, each tagged with essential metadata such as case ID, source, evidence type, and acquisition date, which is crucial for maintaining evidentiary integrity and chain-of-custody (Wu *et al*., 2022). All uploaded evidence is stored in a secure repository with encryption mechanisms to preserve confidentiality and integrity, aligning with guidelines highlighted in recent forensic literature (Lucien, 2024).

7. Acknowledgement

First and foremost, I would like to thank my Almighty heavenly father for the gift of life, strength sustenance, and good health He has rendered to me during doing my project. My project supervisor Eng. Moses Mupeta, I would also like to thank the Management of the University for according me a chance and pursue my studies and graduate with distinction. would also like to acknowledge the lecturers from the School of Engineering.

8. References

1. Casey D. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet, 3rd ed. Academic Press, 2011.
2. Carrier B. File System Forensic Analysis. Addison-Wesley, 2005.
3. Reith M, Carr C, Gunsch G. An examination of digital forensic models. Int. J. Digital Evidence. 2002; 1(3):1-12.
4. NIST. Guide to Integrating Forensic Techniques into Incident Response. NIST SP, 2006, 800-886.
5. Kohn M, Eloff M, Eloff JHP. Integrated digital forensic process model. Computers & Security. 2013; 38:103-115.