United States International University-Africa

FALL Semester 2025

APT 4900VAB FINAL-TERM PROJECT

Digital Evidence Chain of Custody Management System

BY

Jeremy Kamangara – 667282

Allan Ngugi – 666682

Garnet Githinji – 663183

Supervisor

Dr. Stanley Githinji, PhD

UNITED STATES INTERNATIONAL UNIVERSITY-AFRICA

SCHOOL OF SCIENCE AND TECHNOLOGY

December 18, 2025

This final project report is submitted in partial fulfilment of the requirements of the Applied Information Technology (APT)

Declaration

I declare that this is my original work through my own effort and that it has not been presented in any form for academic or any other reason, to the best of my knowledge. Contributions to this work by any other person or literature have been duly cited.

Students

Name Jeremy Kamangara Reg No 667282

Signature….Jeremy…..... Date……18/12/2025……

Name Allan Ngugi Reg No 666682

Signature……Allan…… Date……18/12/2025……

Name Garnet Githinji Reg No 663183

Signature……Garnet…… Date……18/12/2025……

Supervisor

I confirm that this research project report was carried out by the student under my supervision

Signature……. Date……

Dr. Stanley Githinji, PhD

School of Science and Technology

UNITED STATES INTERNATIONAL UNIVERSITY-AFRICA

.

Acknowledgement

First and foremost, I would like to thank God for giving me the gift of life, health and being with me every step of the way throughout this academic journey, my parents for being there when I needed them, for giving me spiritual, moral and financial support, my friends for their academic and also moral support and all my lecturers especially Dr. Stanley Githinji for guiding me through this unit.

.

Abstract

The management of digital evidence is a large problem for law enforcement agencies all around the world with no exception to the Kenyan sphere where unstandardized procedures reign as one of the major culprits for the judicial rejection of evidence due to a broken chain of custody. This project aims to bridge the gap between traditional, paper-based tracking methods that are prone to tampering & human error as well as the expensive, proprietary international systems that are not necessarily friendly to the Kenyan infrastructure.

Using a systems-oriented research approach along with the Software Development Life Cycle (SDLC) model, this study has successfully led to the design and development of a secure, web-based Digital Evidence Chain of Custody Management (DECCM) prototype. A modern technology stack has been used in the system with Node.js for the backend, MongoDB for data storage as well as HTML5/CSS3 for the frontend. The system has a host of interesting features such as automated evidence logging, cryptographic hashing to ensure file integrity, role-based access controls and the capture of digital signatures for evidence transfer. In order to prevent any data from being altered, the database architecture uses cryptographic linking, whereby each record has a hash of the previous record.

Functional and performance testing results revealed that the Digital Evidence Chain of Custody System prototype does to a great extent improve the reliability and speed of evidence retrieval when compared to manual systems. The findings show that the automated audit trails are able to trace every custody event with user IDs which meets the international courtroom transparency requirements. The study has come to the conclusion that the DECCM system could be a scalable, cost-effective solution for Kenyan law enforcement hence providing a verifiable route from evidence collection to tribunal submission, all the while boosting public trust in the judicial process.

.

Table of Contents

.

.

.

List of tables

.

List of figures

.

List of Abbreviations

Abbreviation	Definition
AES-256	Advanced Encryption Standard (256-bit key length)
API	Application Programming Interface
CISA	Cybersecurity and Infrastructure Security Agency
CSS3	Cascading Style Sheets Level 3
DECCM	Digital Evidence Chain of Custody Management System
HTML5	HyperText Markup Language Version 5
HTTPS	HyperText Transfer Protocol Secure
ID	Identification (user)
IEC 27037	International Electrotechnical Commission Standard 27037
IECMS	Integrated Electronic Case Management System
ISO	International Organization for Standardization
JS	JavaScript
JSON	JavaScript Object Notation
JWT	JSON Web Token
MongoDB	Mongo Database
NIST	National Institute of Standards and Technology
OWASP ZAP	Open Worldwide Application Security Project – Zed Attack Proxy
SDLC	Software Development Life Cycle
SHA-256	Secure Hash Algorithm (256-bit)
SWGDE	Scientific Working Group on Digital Evidence
TLS 1.3	Transport Layer Security Version 1.3
UI	User Interface
UNODC	United Nations Office on Drugs and Crime
VS Code	Visual Studio Code

.

Copyright

.

CHAPTER ONE: INTRODUCTION

According to Cybersecurity and Infrastructure Security Agency (CISA), the chain of custody is defined as a process that is employed to track the movement of assets, evidence, through their lifecycle by documenting every individual or organization that handles said asset. Facts collected include the date and time of each operation as well as the intended purpose of any transfer or collection. Without the chain of custody, digital evidence that is to be presented in court runs the risk of being rendered inadmissible. The chain of custody needs to be complete and unbroken for digital evidence to be admissible in court (CISA, 2023).

Our intention is to build a web application designed specifically for law enforcement that automates the process of evidence collection and preserves the chain of custody throughout the lifecycle of a case.

1.1 Background of the Study

In the worldwide sphere, we have NiCE Evidencentral which was developed by NICE Ltd. an American technology company. It provides a Digital Evidence Management System that supports law enforcement bodies in collecting and managing evidence during their investigations. Through this evidence management system, investigators save quite a bit of time through the automation of manual tasks such as data collection, copying and sharing hence allowing the forensic investigators to put more emphasis on the investigation itself. NiCE Evidencentral allows for automated case building, evidence connections & analytics, evidence sharing, automated video and audio redaction, case performance management as well as community evidence crowdsourcing. Since its launch in 2021, NiCE has supported over five million investigations (*Digital Evidence Management for Law Enforcement | NICE Public Safety & Justice*, n.d.).

We also have Axon Evidence which works as a Digital Evidence Management System offering a centralized, scalable and most importantly, secure platform that can handle and accommodate various forms of digital evidence throughout their entire lifecycle hence preserving the chain of

.

custody. This system was created by Axon Enterprise Inc. which is located in Scottsdale Arizona in the United States. It offers a centralized and secure cloud-based storage platform that can store evidence in the form of videos, images or audio which Axon can transcribe into text. Every upload made is also logged with timestamps hence providing an audit trail. Axon also provides proprietary tools such as body cameras, dashcams and drones to law enforcement authorities.
Data gathered from these devices is automatically uploaded to the system as evidence. Evidence gathered from the use of this system can be shared with other agencies, attorneys and media services (*Digital Evidence Management: The Definitive Guide*, n.d.).

Genetec Clearance is another example of a Digital Management System developed by Genetec Inc. which is headquartered in Montreal Canada. This system allows for the collaboration between various agencies, attorneys, businesses as well as the public. Users of the system including law enforcement are able to request for video evidence crucial to their investigations from the public and get it automatically assigned to their relevant cases hence preserving the chain of custody. Moreover, the system allows for the highest levels of confidentiality through encryption in addition to providing features that lets users set access policies and in turn bar any unauthorized access. Another key feature of the system is that it allows investigators to capture evidence such as audio, video and images directly from their phones and assign it to their case all while ensuring that the chain of custody is secure (*Learn How a Digital Evidence Management System Can Assist in Your Operations | Genetec*, n.d.).

With regards to the African context, the best example to give is South Africa's use of the Hytera Digital Evidence Management Platform. This usage manifests through the use of body worn cameras on police officers, CCTV systems and various other recording devices. This evidence is then gathered in a centralized storage system that uses encrypted connections hence preventing unauthorized access. Hytera records every single operation related to the evidence which helps in preserving a chain of custody (*Hytera UK*, 2025). All that said, Hytera was **not** developed in South Africa but instead in Shenzhen Guangdong Province in China.

In Rwanda, there is the employment of The Integrated Electronic Case Management System (IECMS) that is used by all Justice sector institutions across Rwanda. This system has digitized

.

the case life cycle ranging from the filing of a case to the hearing, appeal process, and eventual closure. It manages any consolidated information hence ensuring that all cases are processed effectively and that decisions and verdicts made are well informed. A bonus is that data moves seamlessly to and from multiple justice sectors hence improving communication. However, it is important to note that despite having features that overlap with traditional digital evidence management systems (DEMS), IECMS is NOT a proper DEMS as it does not track the lifecycle or ensure that the audit trail of evidence is adhered to which are crucial for ensuring chain of custody. Moreover, it was developed by Synergy International Systems, an American company (*Rwanda's Justice Sector Integrated Electronic Case Management System (IECMS)* -, 2024).

In Kenya, the closest example to a digital chain of custody system is the digitization of the Police Occurrence Book (OB). An Occurrence Book is a sort of register that officers use to record everything that occurs within a police station within a given period. This effort made to digitize the process is aimed at reducing cases of record tampering as well as simplifying the reporting of crime so that in time, the performance of these duties runs at an optimum capacity (*Kenyan Police Commence Records Digitisation to Tackle Manipulation*, 2023), (MURAYA, 2020). The issue with this however lies on the fact that this new system deals only with the operations taking place at a station and not the ENTIRE investigative process that happens during forensic investigations. It is hence unlike the chain of custody system that we are proposing to build.

From the discussions above, we have covered the international scene with NICE Evidencentral, Axon Evidence and Genetec Clearance before making our way to the continental setup with the most notable example being that of Hytera. We then analyzed the local situation here in Kenya and it was evident to see that we lack a proper digital evidence management system. As a group, we believe that a DEMS system is crucial to any organization, especially law enforcement. We seek to address the current gap that exists in Kenya through our proposed system that we believe will greatly aid forensic investigators.

.

1.2 Problem Statement

The management of digital evidence represents a sharp challenge to law enforcement agencies all over the world. Digital evidence has been rejected by courts in Kenya and many other countries due to faulty treatment, lack of proper documentation, or failure to meet requirements for chain of custody (Cece, 2019). The problem not only jeopardizes the integrity of investigations but also the judicial process itself. Computer evidence is far more fragile than old- fashioned tangible evidence; and therefore; a minor change, either deliberate or accidental, can render it inadmissible in court. Inadequate documentation, human errors, and non-standardized systems make its credibility even more risky.

Existing procedures for managing the chain of custody of computer evidence are fragmented, non-standard, and in most cases, very labour-intensive. In Kenya, for example, the police will most likely use paper-based methods or general-purpose software to track handling of evidence, which is susceptible to tampering, loss, and unauthorized inspection (Waweru, 2021).
Furthermore, without a central platform that is transparent and tamper-proof, there are opportunities for dispute over the authenticity of evidence during court proceedings. This has led to cases where suspects are unpunished, not because of a lack of facts but because of process failures.

Around the world, advanced jurisdictions began implementing digital chain of custody technology that exploits technology like secure databases, cryptographic hashing, and audit trails to provide integrity. These are, however, expensive, very technical, and not optimized to legal and infrastructural conditions in African countries. This has created a gap in which law enforcement organizations in developing countries, including Kenya, cannot use such systems and thus find themselves disadvantaged in criminal justice procedures.

The problem that this project aims to solve is the lack of a safe, reliable, and simple-to-use digital chain of custody management system specifically designed to be used by Kenyan law enforcement organizations. Our proposed system aims to address this gap through the utilization of web technologies to deliver tamper-proof documentation, auditability, as well as web access to digital
.

evidence records. Through this, the system will enhance accountability, raise the confidence in the decisions of courts, and align Kenya's judicial processes with international best practices in management of digital evidence.

1.3 Project Objectives

1.3.1 Overall Goal

The overall objective of this project is to develop and design a Digital Evidence Chain of Custody Management System for Law Enforcement Agencies in the true spirit of maintaining integrity, accountability, and admissibility of digital evidence in judicial processes.

1.3.2 System Design and Development Objectives

1. To analyze the flaws and deficiencies of existing digital evidence processing procedures of law enforcement agencies.

2. To develop a secure, easy-to-use web-based system that features audit trails, access controls, and automated generation of evidence functions.

3. To compare the performance, usability, and effectiveness of the system outlined herein with the traditional manual and half-digital systems.

4. To optimize transparency and accountability in evidence management, thereby building trust in judicial proceedings.

1.4 Project Questions

1) What are the traditional challenges with the old systems of managing digital evidence?

Traditional systems utilized to manage digital evidence are primarily paper-based tracking forms, manual reports, or non-forensic generic digital applications. They are prone to human errors, record loss, and poor logging of evidence transfer (Waweru, 2021). Most of the manual processes

.

are also not protected by functionality such as encryption, authentication, and tamper- proof audit trails. They are therefore vulnerable to unauthorized access and tampering. The second significant hurdle is the non-existence of central platforms that make it simple for investigators, judicial officers, and prosecutors to communicate freely among themselves. This creates inefficiency, transparency, and high rejection of electronic evidence in court due to poor handling of chain of custody requirements (Cece, 2019).

2) How will the new Digital Evidence Chain of Custody Management System address these challenges?

The proposed system here introduces a web-based, centralized platform specifically for law enforcement agencies. It consists of secure databases, automated evidence logging, and cryptographic hashing to ensure the integrity of digital documents. Access control mechanisms will ensure the right authorization prior to employees being allowed to manage or view the evidence, with audit trails keeping a record of all interaction with the evidence to ensure transparency. As opposed to traditional methods, the system will be easy to use and customized to replicate authentic workflows of the Kenyan law enforcement in order to reduce training costs and adoption burden. Such features directly address concerns of tampering, loss, and poor documentation by providing a traceable, secure, and verifiable chain of custody.

3) How effective is the new system compared to the traditional ones in terms of usability, performance, and scalability?

The new system is expected to be far more effective compared to traditional approaches. Under usability, its intuitive web-based interface allows investigators and prosecutors to easily upload, track, and retrieve evidence records without utilizing paper forms. For performance, the system carries out the most critical procedures such as timestamping, chain of custody tracing, and report generation, which decrease errors and time compared to manual approaches. With regards to scalability, the system needs to be scalable to support growing amounts of digital evidence, compatibility with other law enforcement databases, and future technology needs (NIST, 2020).

.

In combination, these will enhance efficiency, enhance faith in the administration of justice, and align Kenya's evidence management to best practice worldwide.

1.5 Scope of the Project

The project entails developing a fully functional working prototype of a web-based Digital Evidence Chain of Custody Management System for law enforcement in Kenya. The prototype shall showcase systems core functions such as secure user authentication, evidence intake (upload and capture of metadata), automatic timestamping, cryptographic hashing of files, role- based access controls, searchable audit trails recording every handling event, and rudimentary reporting tools with the capability of exporting for court proceedings. The system shall be developed as a standalone application (frontend written in HTML/CSS/JavaScript; backend in Python through FastAPI or Flask; and a relational database for records) to prove the concept, track usability, and confirm technical feasibility.

The study will examine functional and technical considerations to the exclusion of full operational deployment. Integration with and interfacing between national justice-sector systems, for example, the existing case-management platform, and large-scale deployments are considered outside the scope of this project and will be planned for future work. Evaluation will be performed against security features, through several workflows common to investigators, and will compare prototype outputs to traditional paper-based or ad-hoc digital means.

1.6 Limitations of the Study

The following limitations will apply to this work: First, since the project is conducted in the academic environment with little means and infrastructural support, the prototype shall not be deployed in the operational police environment during the study. Second, testing of the system will be carried out with sample data and certain simulated user scenarios, but without the actual case evidence; certain real-world edge cases may not be covered fully (different file formats from specialized forensic tools, very large storage loads, or on cross-agency evidence being moved). The third is that some legal and organizational considerations, procurement rules, policy reform,
.

and user training requirements will be only elaborated on, at a very general level, and left unaddressed in this project. Finally, since the prototype will have core chain-of-custody controls (hashing, logging, access control), key features such as automatic video redaction and full integration with device forensic tools will remain out of scope at this stage.

1.7 Significance of the Study

The project aims to fill the working gap within local handling of digital evidence. By way of demonstration of an auditable, secure, and end-user-oriented custody chain, the work seeks to lessen the rates of chains of rejection of evidence due to procedural errors. The prototype will therefore avail investigators and prosecutors a cleaner, authentic path from collection of evidence to tribunal submission, thus culminating into the strengthening of case determination and public confidence in justice processes (Cece, 2019).

In a general sense, the study supports national development goals as it builds digital infrastructure and institutional accountability. The study is also in concert with Sustainable Development Goals concerning innovation and justice insofar as it places a context-aware solution at the disposal of law enforcement agencies in Kenya for adoption or scaling. Finally, the project constitutes the springboard for further improvements-comprehensive integration with national case management systems, office-wide workflows, and policy recommendations for the governance of digital evidence-which can be addressed in follow-up research, pilot exercises, and capacity-building activities.

1.8 Chapter Summary

From the text above, we have defined and established the importance of the chain of custody. We have proposed the creation of a digital evidence management system that seeks to preserve this chain of custody. Through global, African and local contexts, we have analyzed the existence of systems similar to our proposed platform and have been able to identify a gap especially in the local scene that we aim to address. We have set forth objectives that we feel are relevant to our project in addition to challenging the validity of our system against older and more traditional
.

systems. Furthermore, we have clearly defined our scope as well as stating the limitations that we anticipate coming across during our undertaking of this arduous task. Finally, we have concluded by assessing the significance of our project in relation to the Sustainable Development Goals.

.

CHAPTER TWO: LITERATURE REVIEW

2.0 Introduction

This literature review examines previous works, technologies and systems. It will help us in understanding existing knowledge gaps, identifying successful solutions, and informing the development of new systems. This chapter takes a critical look at and compares the present-day Digital Evidence Management Systems (DEMS) worldwide and in the local context, pointing out their pros and cons. The review also connects to the research objectives by looking into the ways in which these systems have dealt with the challenges of evidence handling and chain of custody.

2.1 Analysis, comparison, and criticism of existing projects

2.1.1 System One: NICE Evidencentral

https://www.nicepublicsafety.com/law-enforcement

NICE Evidencentral, a product of NICE Ltd. in the USA, is a digital evidence management system. It allows police to gather, study, and disseminate digital pieces of evidence in a smooth and quick way. The platform handles uploads of evidence, video/audio redaction, and linking different evidence types to accelerate case building; thus, the developers say that over five million investigations worldwide have benefited from the system (*Digital Evidence Management for Law Enforcement | NICE Public Safety & Justice*, n.d.).

Strengths: Automation, secure sharing, analytics tools, and crowdsourced verification. **Weaknesses**: Expensive to deploy and is designed mainly for well-funded agencies in developed countries.

.

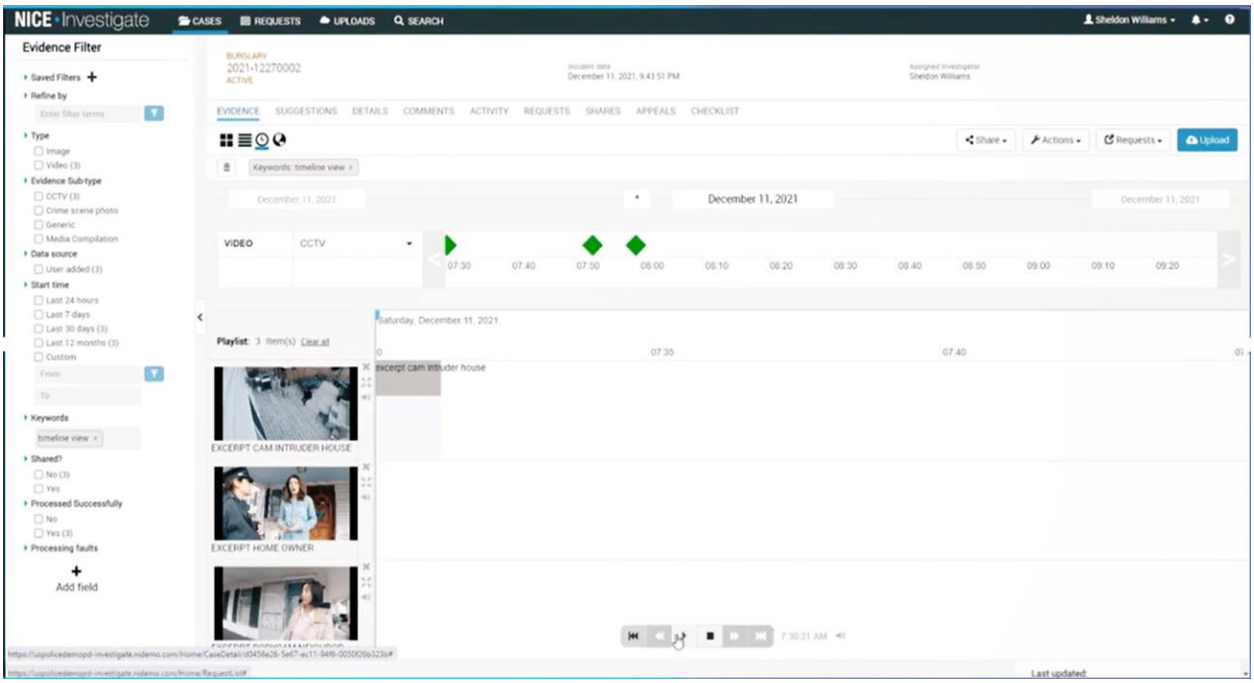


Figure 1: NiCE Evidencentral interface

2.1.2 System Two: Axon Enterprises

https://www.axon.com/resources/digital-evidence-management-guide

The system engineered by Axon Enterprise Inc. offers a trustworthy and centralized solution for the management of digital evidence which involves videos, images, and sound. Its functionality is based on the use of cloud storage and has got audit trails, encryption, and transcription as part of its functionality. The evidence collected by Axon's hardware (e.g. body cams, drones) gets assimilated into the system automatically (*Digital Evidence Management: The Definitive Guide*, n.d.).

Strengths: Strong integration with proprietary hardware, it involves scalable cloud architecture and secure audit logging.

Weaknesses: High operational costs and heavy reliance on Axon's proprietary devices which may reduce flexibility for agencies with existing equipment.

.

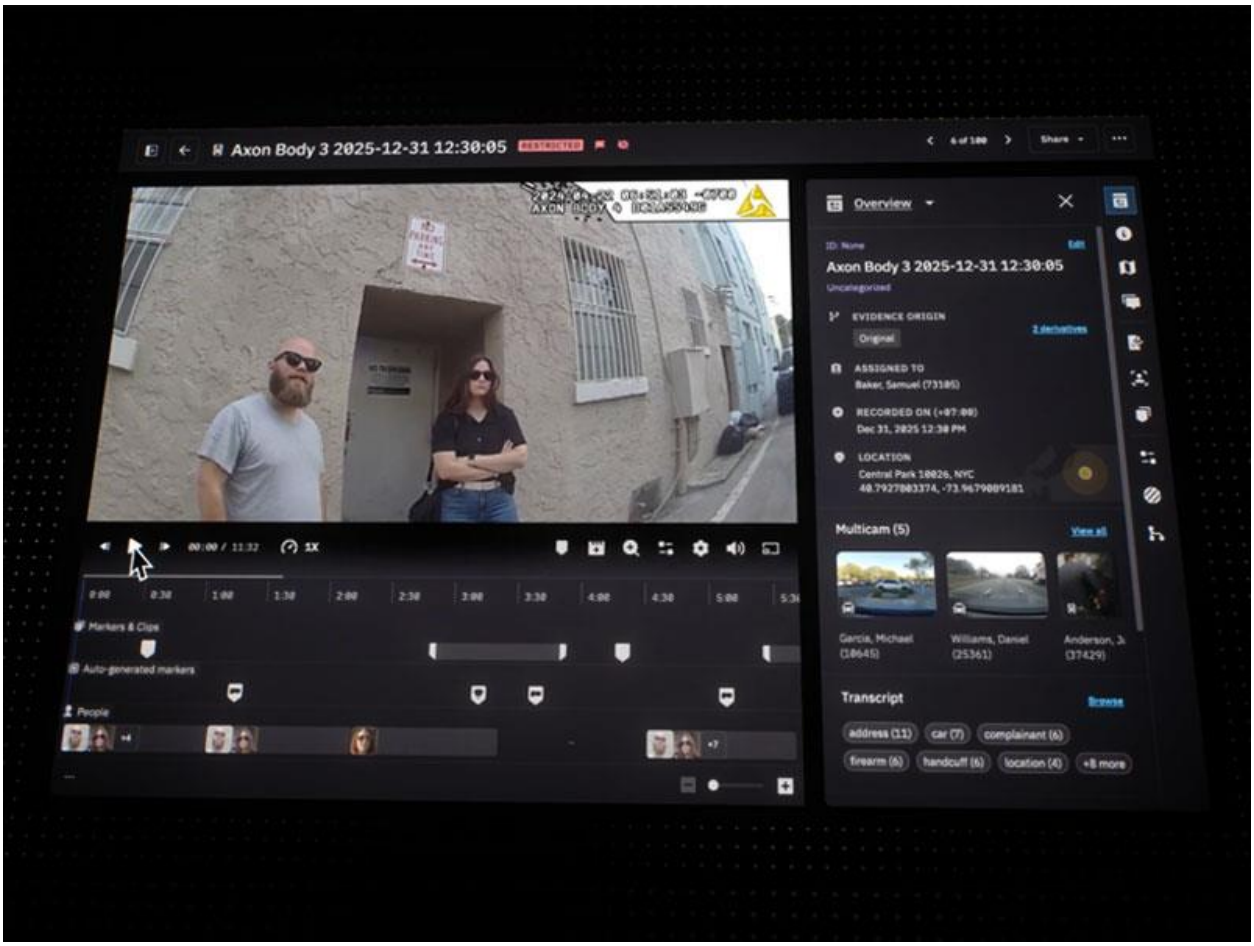


Figure 2: Axon Enterprises system interface

2.1.3 System Three: Genetec Clearance

https://www.genetec.com/products/operations/clearance/case-management

Genetec Clearance is a system that is put into use in Canada and other countries as well, which facilitates teamwork among the police, lawyers, and the public. The setup makes it possible to collect audiovisual evidence securely by means of mobile phones and it comes with very powerful encryption and access control. It makes public submissions easy and promptly assigns them to the corresponding cases, thus aiding in maintaining the custody chain (*Learn How a Digital Evidence Management System Can Assist in Your Operations | Genetec*, n.d.).

Strengths: Secure and flexible. It supports public submission while also supporting mobile- device

.

compatibility.

Weaknesses: it requires reliable internet and may present privacy risks in jurisdictions with weaker data laws.

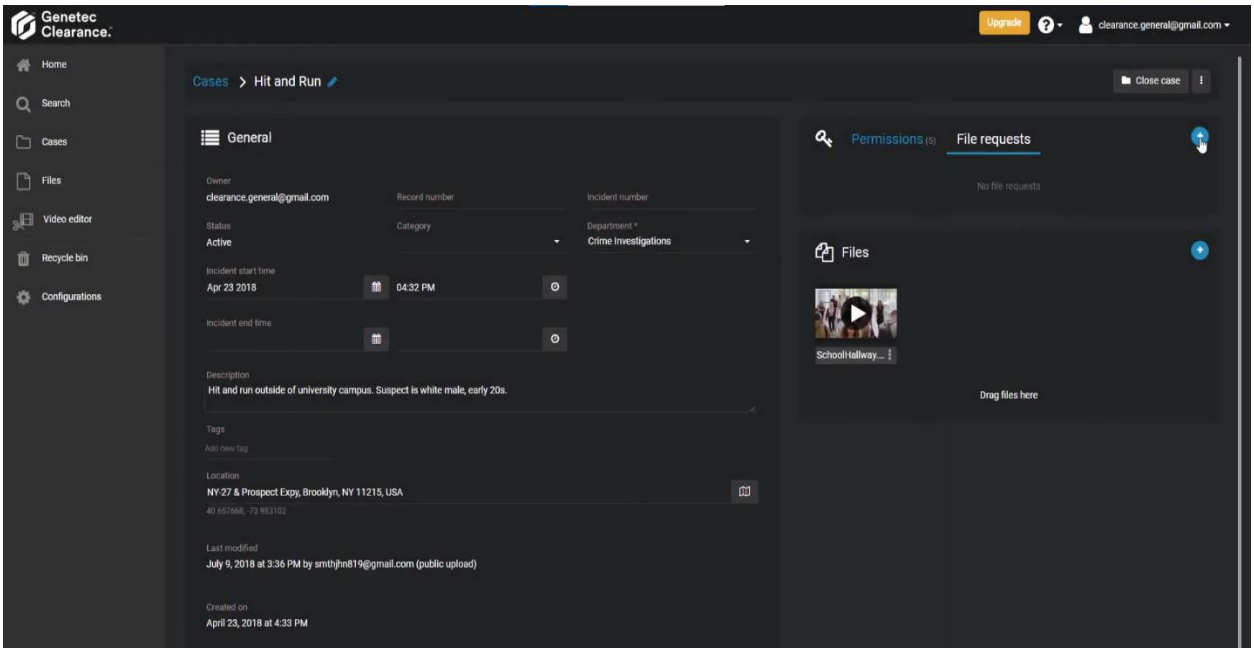


Figure 3: Genetec Clearance System interface

2.1.4 Summary of comparison of the systems

From the three systems mentioned previously, it is clear that all of them were designed to make handling digital evidence easier, faster, and more secure. However, each system has its own strengths and weaknesses depending on where and how it is used.

NICE Evidencentral places a strong emphasis on the automation and swift sharing of evidence, which significantly increases its effectiveness in the case of large investigations. The product incorporates sophisticated tools and analytics designed to speed up the processing of cases by law enforcement personnel. The primary downside is that it is very costly and intended for well- off agencies; therefore, it might not be suitable for countries with tight budgets.

Axon Evidence cooperates seamlessly with hardware of its own like drone and body cameras, and it works with cloud storage to make the data storage very safe. This is a solution that allows all

.

the evidence to be kept securely tracked. On the other hand, heavy reliance on Axon's devices makes it quite expensive and inflexible for those who have already invested in other types of gear.

Genetec Clearance does a great job of fostering collaboration and enables the audience to send video or photo contributions straight from their mobile devices. The system is designed for mobile usage and has solid security measures, but it needs a reliable internet connection which may be difficult to obtain in some regions. There are also questions about privacy when it is implemented in countries with weak data protection laws.

To summarize, the three systems are good at digital evidence management but they are mostly applicable to the context of developed countries with excellent infrastructure and large financial resources. The price of these systems may be a problem for a country like Kenya or they may not be compatible with the local environment. This indicates that there is a genuine requirement for a locally developed system that is economical, secure, and user-friendly for police personnel.

2.2 Literature review based on research objectives

2.2.1 Challenges of old systems

Lack of Standardization

The legal enforcement agencies of Kenya use paper-based systems and digital tools that are not specific for the purpose, which are not backed up by any standard procedure and this in turn is causing the inconsistency in evidence handling.

Poor Security and Tamper Risks

Manual methods promote unauthorized alterations. The guarantee for integrity of evidence cannot be determined effectively without encryption or audit trails.

Limited Accessibility and Transparency

Due to the absence of centralized digital systems, investigators and prosecutors typically work in parallel universes, contributing to delays and mutual misunderstandings.

.

High Risk of Evidence Rejection

One of the reasons that courts might dismiss digital evidence is that they don't trust the chain of custody, that no one has documented the evidence's handling, or that there have been irregularities in the procedure.

(Cece 2019, Waweru, 2021)

2.2.2 Benefits of the new system

Improved Security and Integrity

The proposed system will use cryptographic hashing, access controls, and automatic logging to ensure evidence remains unchanged.

User-Friendly Interface and Accessibility

Designed with local law enforcement workflows in mind, the platform will be intuitive and easy to adopt with minimal training.

Real-Time Auditability

Automatic timestamping and activity logs will provide real-time tracking of evidence which will lead to reducing the chances of procedural errors.

Cost Efficiency and Local Optimization

Built using open-source tools and web technologies, the system avoids vendor lock-in and is scalable to fit local infrastructure and budgets.

.

2.3 Chapter Summary

This chapter has critically examined three major Digital Evidence Management Systems in use globally and while they demonstrate effectiveness in maintaining chain of custody, they are ultimately unaffordable, overly complex, or poorly suited for developing countries in africa such as Kenya in our case. Through our analysis we have identified significant gaps such as high costs, lack of local customization, and infrastructure incompatibility. These findings affirm the need for a locally developed, secure, and simple digital chain of custody system that aligns with the objectives of this research.

.

CHAPTER THREE: RESEARCH DESIGN AND METHODOLOGY

3.0 Introduction

In order to bring our Digital Chain of Custody system to life, we shall adopt a systems-oriented approach in our tailoring of it. This methodological framework will allow us to integrate ourselves in the design, development, testing as well as validation. This will be done through the Software Development Life Cycle (SDLC). We believe that this approach shall ensure that our system functions optimally, is secure, complies with the legal mandates which is also crucial for admissibility in court as well as ultimately being reliable over the long run with regards to its handling of sensitive evidence key in criminal investigations and court proceedings.

3.1 Locality of the Project and Beneficiaries

Our Digital Chain of Custody system is being built with the intention of it aiding in Kenya's criminal justice scene. We aim to aid law enforcement in particular with regards to proper evidence collection, logging and presentation with strict adherence to local and international laws regarding the admissibility of evidence during court proceedings. The specific bodies include the Directorate of Criminal Investigations (DCI), Kenya Police Service Stations as well as any and all forensic laboratories across all the 47 counties. Furthermore, we intend to have a system that works in well-connected urban investigation spaces as well as less connected rural stations that have a limited internet connection.

Key Beneficiaries include:

Evidence collection officers: This refers to the first responders who collect evidence at the scene of the crime.

Forensic Investigators and detectives: These are the personnel who interact with the evidence during their inquiry into what happened with regards to their specific case at hand.

Forensic Analysts: These are the people who examine, analyze and extract information vital to an investigation from digital evidence.

.

Court officials: These are the judicial officers who review evidence submission during trial proceedings and require proof of a clear chain of custody.

Secondary beneficiaries include:

General public: This is in reference to citizens who would benefit from the assurance that evidence regarding any and all cases is carefully handled so that justice is served correctly.

Defense attorneys: These are the legal practitioners who seek transparent access to evidence in order to best serve their client's needs.

3.2 Research Design Approach – Descriptive and Applied

The research adopts a dual research approach that incorporates descriptive and applied methodologies to bridge the theory analysis-practice application gap.

Descriptive Design Component. This method was employed in the critical scrutiny and documentation of the situation of affairs in the management of digital evidence among Kenyan law enforcers. It entailed:

1) Proper scrutiny of current procedures in evidence handling as well as finding procedures that are still manual and require digitization.
2) Documentation of chain of custody-related challenges under current paper-based systems.
3) Finding the international best practice and local implementation reality gaps in documentation.
4) Noting the preconditions for admissibility of evidence under Kenya's Computer Misuse and Cybercrimes Act 2018 and Evidence Act research.

Literature review, available international system analysis (NICE Evidencentral, Axon Evidence, Genetec Clearance) and legal framework analysis with regards to Kenya also aided the descriptive phase in setting up the problem context and setting up rationale for a purpose-driven solution.

Applied Design Component. The applied research methodology aimed at designing and deploying an operational solution to problems. This involved a number of steps.

.

Firstly, there was the *translating theoretical chain of custody requirements into operational system features* as well as *the integration of cryptographic security controls that produce legally authentic evidence integrity*. Moreover, there was the *designing of user interfaces to simplify forensic processes for field officers* in addition to *the integration of legal compliance controls into system activities in an absolute sense*.

The research methodology employed ensures results transcend theory analysis to provide an implementable system capable of meeting real law enforcement needs.

Integration of Methods: Integration of the descriptive and applied methods offers a converging approach to research. Descriptive analysis defines what has to be solved and for what purposes whie applied implementation defines how the solution operates in practice. Integration ensures the resulting system is theoretically correct as well as operational.

3.3 Software Development Life Cycle (SDLC) Approach

Since our Digital Evidence Chain of Custody System has been developed using a systematic System Development Life Cycle (SDLC) model, systematic progression from conceptualization to implementation has been made possible. Moreover, our chosen model has allowed for iterative improvement with clear phase boundaries.

Phase 1: Planning – Project Foundation

Objectives Definition

1) Establish project objectives: Construct a legally compliant, secure and user-friendly Digital Evidence Management System.
2) Define success metrics: Confirmation of evidence integrity, documentation of chain of custody in full, admissibility of evidence in court.
3) Constraints Identification: Budget limitations in favour of open-source technologies, unpredictability of internet connection, dependence on digital literacy from our intended users.

.

Scope Determination

For the items that were **in scope**, we had: Evidence intake, chain of custody tracking, cryptographic integrity verification, forensic examination utilities as well as presentation interfaces for courts.

For **out of scope**, there was: Physical evidence handling management, integration of lab equipment and case management external to general evidence management.

Our **proposed future enhancements** would be: AI-supported evidence analysis, native mobile apps and finally Inter- Operable Criminal Justice System (ICJIS) integration.

Resource Allocation

Technology Stack: Node Server.js for the backend, CloudMongoDB as the database side, HTML5/CSS3/Bootstrap for the frontend and finally JavaScript for interactivity.

Infrastructure: Local host infrastructure with future enhancements incorporating cloud host solutions (AWS, Azure, and local data centres), developing/testing/production environments.

Human Resources: Development staff (us), compliance verification through legal advisors (deep compliance research) and workflow validation by law enforcement consultants (also through research and observance of other systems).

Phase 2: Analysis – Requirements Gathering

Identification of Functional Requirements

Having an intake of evidence with auto-extracted metadata such as file hash, date/time and geolocation.

Capturing of digital signatures for the verification of evidence transfer.

.

Having role-based access controls (for example profiles for: an evidence Officer, a forensic analyst, a legal officer, a court user and finally the administrator themselves).

The presence of live chain of custody status reporting.

Having hash verification applications for the integrity verification of evidence.

Having report generation with embedded digital certificates.

Lastly, having an improved search function with filters.

Non-Functional Requirements

Security. End-to-end encryption, cryptographic hashing (SHA-256), audit trail immutability.

Performance. Upload of evidence in 30 seconds for files of up to 100MB, search results in 2 seconds.

Usability. Easy-to-use interface with minimal training, mobile-responsive design.

Reliability. 99.5% uptime target, automated backup procedures.

Compliance. Kenya Computer Misuse and Cybercrimes Act 2018 and The Data Protection Act 2019 adherence.

For the user workflow analysis, we noticed that mapping existing evidence handling processes in detail revealed a host of issues that included:

1) Manual chain of custody forms being vulnerable to human error and loss.
2) Poor evidence integrity verification controls.
3) Difficulty in the access of evidence between multiple investigation teams.
4) Court preparation and evidence presentation being a time-consuming phase.

.

3: Design – System Architecture

With regards to the database design, we proposed having:

MongoDB. This would have the normalized database structure with independent tables for Users and Evidence Items with possibility of Chain of custody transfers, Audit logs, Cases and Reports.

Cryptographic Linking. Hash of previous record appended to each database entry creating blockchain-like immutability.

Indexing Strategy: Performance-tuned indexes on majority of queried fields (for example: case number, evidence ID, timestamp).

Backend Architecture:

For the backend design, we opted for a Node Server.js backend with a logic that executes:

- User authentication and authorization.
- Role-based access control (admin, officer, analyst, court clerk).
- Evidence creation, retrieval and status updates.
- Automatic logging of chain-of-custody for every action related to evidence.
- Every custody event (upload, transfer, access) is documented with a time and the user who did it.

Frontend Design:

With regards to planning for our frontend graphical user interface look, we opted for:

Progressive Enhancement. Integral functionality without JavaScript as well as enhanced features for newer browsers.

Evidence Upload Interface. HTML5 drag-and-drop regions with progress bars.

Digital Signature Canvas. HTML5 Canvas API for capturing officer signature on evidence transfer.

.

Authorization Testing:

In order to ensure that there is a strict adherence to admin defined roles, we chose to take the steps below to ensure that through the following testing approaches.

Role-Based Access Control. Verify that evidence collection officers are not able to see forensic analysis tools, forensic analysts are not able to edit chain of custody forms they did not author and legal officers have read-only access appropriate for preparation for court.

Horizontal Privilege Escalation. Check and see if we can access evidence for cases not assigned to the test user.

Vertical Privilege Escalation. Trying administrative operations with non-admin accounts.

API Endpoint Security. Verify direct API calls which bypass frontend authorization checks.

With regards to the actual test methods, we opted for manual testing on various user accounts.

Our success criteria hinges on unauthorized access being impossible, all privilege escalation attempts logged and blocked as well as having authentication tokens that cannot be forged or hijacked.

.

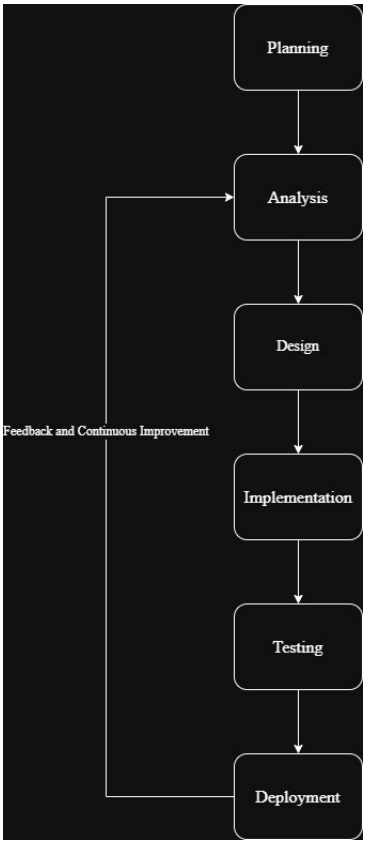


Figure 4: A diagrammatic representation of the SDLC of our Digital Evidence Chain of Custody Management System

3.4 System Testing Plan

Testing will be a very important stage of the development of the Digital Evidence Chain of Custody Management System. It will guarantee that every component of the system operates as designed and that it is as described in the functional and non-functional requirements determined during system design. Since the system will be handling digital evidence that can later be used as evidence in court cases, its accuracy, reliability, and security will be a top priority.

The phase of functional testing will validate that all modules, including evidence intake, custody transfer, authentication, and reporting, function as expected. This will ensure that users are able to upload, track, and obtain evidence without errors or system failures. Performance testing will then validate the stability and scalability of the system under a range of loads. For instance, multiple concurrent users will be duplicated to test if the platform accommodates multiple

.

investigators opening or uploading digital proof at the same time. Usability testing will confirm if law enforcement agents and forensic examiners are able to use the interface seamlessly and accomplish their work without any technical proficiency. Lastly, compatibility testing will check the performance of the system on different browsers, resolutions, and operating systems to guarantee availability from different law enforcement devices.

Testing will be carried out using a dedicated environment that replicates the real situation but with simulated data for confidentiality purposes. Automated testing software such as Apache JMeter and OWASP ZAP will be applied to ensure the process is efficient and produces consistent results. Systematic testing, according to Sommerville (2020), has the ability to detect defects early and ensure that software meets user and technical needs. In this project, there will be such an approach in order to confirm the reliability of the system prior to moving toward full

implementation.

3.5 Security Testing

As digital evidence is sensitive, security testing will be prioritized to ensure that the system maintains confidentiality, integrity, and availability of information stored. The main objective will be to identify and eliminate any vulnerabilities that would render digital evidence inadmissible in court.

The process will begin with the vulnerability scans meant to identify weaknesses in the layers of authentication, data storage, and transmission. Automated tools such as Burp Suite and OWASP ZAP will be utilized to simulate probable cyber-attacks such as SQL injection, cross-site scripting, and privilege escalation. Penetration testing will be conducted to simulate actual intrusion attempts, attempting to determine how secure the system is from unauthorized use or manipulation.

Due regard will be given to access controls and encryption. There will be three user roles—investigator, evidence custodian, and auditor—to which specific functions will be made accessible so that users cannot view data that is not relevant to their work. Evidence files and metadata will be secured with AES-256 encryption, while communication between the server and client will be

.

made by means of TLS 1.3. This will ensure that although interceptions of data are taking place, they remain unintelligible to unauthorized staff (Kumar & Patel, 2023). Audit trails will be examined as well to make sure that any action taken by a system is tracked with an immutable timestamp and not detectably altered.

Finally, the system will be compared with industry cyber-security standards such as ISO/IEC 27001 and NIST (2020) guidelines on integrity for digital evidence. These standards constitute a basis for assessing compliance against industry best practice. The outcome will indicate that the application will be resistant to common vulnerabilities, safeguard sensitive data, and ensure traceability over the entire lifecycle of the evidence.

3.6 Data Handling and Analysis

Data analysis for this project will be purely system-generated log and test metric-driven and not survey or interview user-based. Data including performance metrics, system logs, and error reports collected during functional and security testing will be used. These data sets will be utilized to evaluate the efficiency, responsiveness, and integrity of the system.

The data will be processed based on the best practices in digital forensics throughout. Every evidence record will be assigned an individual cryptographic hash (SHA-256) for authenticity checking and against concealed tampering. On receiving a manipulated file upload, the system will identify a mismatch between stored and recalculated hash values. This method follows guidance from the National Institute of Standards and Technology (NIST, 2020), which emphasizes cryptographic hashing as being the critical underpinning of trustworthy evidence management systems.

The test data will be utilized to determine system response time, error rates, and reliability of audit logs. The optimization areas will be determined by the analysis, such as database indexing and caching, that will be optimized to execute the system in an accelerated mode. Backups and encryption at rest will also prevent data loss and unauthorized access. These measures are aligned with digital security best practice by Kumar and Patel (2023), which states the importance of redundancy and encryption in maintaining the availability and confidentiality of digital evidence.

.

Through this approach, not only will global standards compliance during the process of dealing with the data be guaranteed, but the validity of results during the testing phase will be enhanced. This will guarantee that the system will perform as desired in an actual law enforcement environment.

3.7 Ethical Considerations

Moral considerations form a part of the design and evaluation of the Digital Evidence Chain of Custody Management System. As a result of the legal nature of digital evidence management, the project upholds stringent confidentiality, transparency, and accountability standards.

To begin with, anonymity will be maintained by using anonymized and simulated data during testing. There will be no processing of genuine proof or personal data, thus maintaining privacy and data protection laws. Throughout the duration of penetration and vulnerability tests, ethical practices will be followed so that no harm is caused and unauthorized data exposure takes place. Every process of modification of systems or testing will be documented, promoting transparency and traceability of all activities of the project.

The project also adheres to the moral principle of non-repudiation, where all actions within the system are held responsible to specific individuals. In alignment with the National Institute of Justice (NIJ, 2023), distinct responsibility lines must be maintained intact in forensic systems to have the confidence and legal evidence. All the activities in the system—uploading, transferring, and updating evidence—will automatically be logged with user ID and timestamp.

In addition to this, intellectual integrity will be maintained through proper referencing of all open-source libraries and frameworks used in developing the system. Ethical responsibility will also be exercised on the anticipated real-world application of the system. Access control will be implemented such that only the specified law enforcement officers are able to tamper with evidence, minimizing misuse to the minimum. Lastly, data protection and human rights will be considered in the project such that data of individuals would only be retrieved when necessitated by law and properly recorded.

Generally, these practices ensure that not just will the system be made to function but also comply
.

with legal, ethical, and professional standards for the management of digital evidence in law enforcement.

3.8 Chapter Summary

This chapter described the research design and methodology framework employed for designing the Digital Evidence Chain of Custody Management System for Law Enforcement. It applied descriptive and applied research designs in order to analyze the gaps in evidence management that exist currently and translate theoretical outcomes into a usable, functional system. The descriptive approach provided insight into the manual processes and regulatory requirements of Kenya, while the applied approach led the system development through the Software Development Life Cycle (SDLC) so that each phase—from planning and analysis to design, testing, and implementation—was carried out systematically.

Moreover, the chapter established the most important technical, ethical, and security concerns critical to system success. It encompassed complete functional and security testing, data handling procedures in accordance with NIST and ISO/IEC standards, and moral processes that ensure confidentiality, accountability, and legislations compliance. Implementing strong encryption procedures, audit trails, and role-based access controls, the plan made the system integrity-oriented, transparent, and acceptable as court evidence. Overall, the methods applied are adequate enough to allow one to develop a secure, safe, and locally optimized digital evidence management system for the Kenya law enforcement community.

.

CHAPTER FOUR: SYSTEMS ANALYSIS AND SYSTEM DESIGN

4.0 Introduction

This chapter covers the design, testing, and implementation process of the Digital Evidence Chain of Custody Management System for Law Enforcement. This touches on how the system is to be structured, tested, and implemented to ensure that it is functional, secure, and easy to use. The designed framework should be modular, have integrity, and, importantly, be scalable to ensure that digital evidence management by law enforcement is effectively, securely handled.

The chapter also describes the methods of testing to be applied in determining whether it will meet functional and non-functional requirements. Finally, the implementation plan is a representation of how the system will be deployed into the existing operational environments. In summary, these stages ensure that the system meets its intended purpose of maintaining authenticity, confidentiality, and traceability throughout the lifecycle of any digital evidence (Laudon & Laudon, 2022).

4.1 System Requirements

Definition

System requirements define what features, functionalities, and constraints are required from the Digital Evidence Chain of Custody Management System for Law Enforcement. The system requirements specify how a system treats, acts, and interfaces with users and other components.

Purpose

Defining the system requirements provides a perfect understanding of what the system must achieve. It ensures that the focus of the development process remains in a way intended by users and organizational goals; it also sets standards concerning security. Well-defined requirements avoid ambiguity, reduce design errors, and provide a solid foundation for future enhancements (Pressman & Maxim, 2020).

.

4.1.1 Functional Requirements

Definition

Functional requirements define what the system must accomplish: its actions, processes, and operations to achieve the users' and organizational objectives. These describe the core capabilities of the system, such as inputting data, processing, and generating output.

Purpose

These functional requirements define what the main features are and what functions need to be performed by the system to support users. Having these functionalities well-identified helps ensure that the system supports tracking evidence efficiently, securely stores it, and provides proper chain-of-custody management.

ID	Functional Requirement	Description
FR1	Evidence registration	The system shall allow officers to add new digital evidence into the system, including metadata such as case ID, date, and collector.
FR2	User Authentication	The system shall ensure that only authorized personnel can access the system using secure login credentials.
FR3	Evidence Transfer Module	The system shall enable custodians to record and approve evidence transfers between officers or departments.

.

FR4	Audit Trail Generation	The system shall keep an immutable log of every user action to allow audit trails for traceable accountability.
FR5	Report Generation	The system shall prepare case summaries, evidence logs, and transfer histories for legal and administrative use.
FR6	Search and Retrieval	The system shall allow users to quickly locate digital evidence using filters including, but not limited to, case number or file type.
FR7	Role-Based Access Control	The system shall differentiate between modules and their accessibility according to user function-investigator, custodian, administrator.

Table 1: Functional Requirements

4.1.2 Non-Functional Requirements

Definition

Non-functional requirements describe how the system performs its functions rather than what it does, and include quality attributes such as performance, security, usability, and maintainability.

.

Purpose

While non-functional requirements do concern performance benchmarking and setting standards that ensure reliability, scalability, and satisfaction of the users, they present how efficient the system will be under various conditions and during failures (Sommerville, 2020).

ID	Non-Functional Requirement	Description
NFR1	Security	The system shall leverage AES-256 encryption and TLS protocols to secure the confidentiality and integrity of data.
NFR2	Usability	The system shall implement an interface that is intuitive and easy to use, reducing training needs among law enforcement officers.
NFR3	Reliability	The system shall perform predictably and automatically recover from slight failures.
NFR4	Scalability	The system architecture shall support additional users, cases, and data volume without degradation in performance.
NFR5	Performance	The system shall process user requests and database

.

		transactions within acceptable time limits, such as less than 2 seconds.
NFR6	Maintainability	The system shall use Modular code, (*(PDF) The Impact of Digital Tools and Online Learning Platforms on Higher Education Learning Outcomes*, n.d.)which shall allow updates and troubleshoot issues with ease.
NFR7	Availability	The system shall ensure that at least 99% of the time, the digital evidence is available.

Table 2: Non-Functional Requirements

4.2 Stakeholders

Definition

These are individuals, groups, or organizations that may have an interest in the design, development, deployment, or operation of the Digital Evidence Chain of Custody Management System for Law Enforcement. The stakeholders will also contribute to the definition of the requirements, validation of functionalities, and successful system adoption.

Purpose

It characterizes all stakeholders involved, defines their roles, and ascertains how they will communicate with each other. Understanding the needs of stakeholders helps to design a system for meeting operational needs and promotes user acceptance and accountability (PMI, 2021).

.

Stakeholder	Role	Interest
System Developers	Design, develop, and maintain the functionality and architecture of the system.	Ensure that the system is technically sound and meets design specifications.
Project Manager	Oversees the planning of projects, resource allocation, and timely delivery of system milestones.	Ensure completion of projects within scope, time, and budget.
Law Enforcement Officers	Use the system to register, transfer, and manage digital evidence.	Allow for efficient and secure evidence tracking.
Evidence Custodians	Ensure that the evidence within the system is properly stored, handled, and documented.	Ensure evidence integrity and that chain-of-custody rules are followed.
Forensic Analysts	Gather and analyze evidence to aid investigations and the judicial process.	Ensure access to valid and verifiable evidence to analyze.
System Administrators	Manage user accounts, monitor performance, and ensure data integrity.	Ensure operational stability and security of the system.
Legal Authorities	Review system-generated reports and ensure compliance with legal chain-of-custody analysis.	Preclude the admittance of unreliable evidence in court.

Table 3: Stakeholders

.

4.3 System Models

A system model refers to the creation of a structured representation of interconnected hardware and software components that is developed during the system analysis and design phase. This representation aids in communicating various aspects of a system among team members and system users. It also serves as documentation for any future developers (Satzinger et al., 2010, Mishra et al., 2016).

4.3.1 System Architecture

System architecture refers to the specifications of a class of systems. It consists of connections, constraints and interfaces that specify the components of the system as well as how these components interact (Luckham, Vera, & Meldal, 1996).

For our proposed system, we chose a three-tier architecture. This architecture sorts applications into logical, physical and computing layers. It has a presentation layer which is the interface the user interacts with, an application layer where data processing takes place and finally a data layer that manages and stores the application data (IBM, 2021).

.

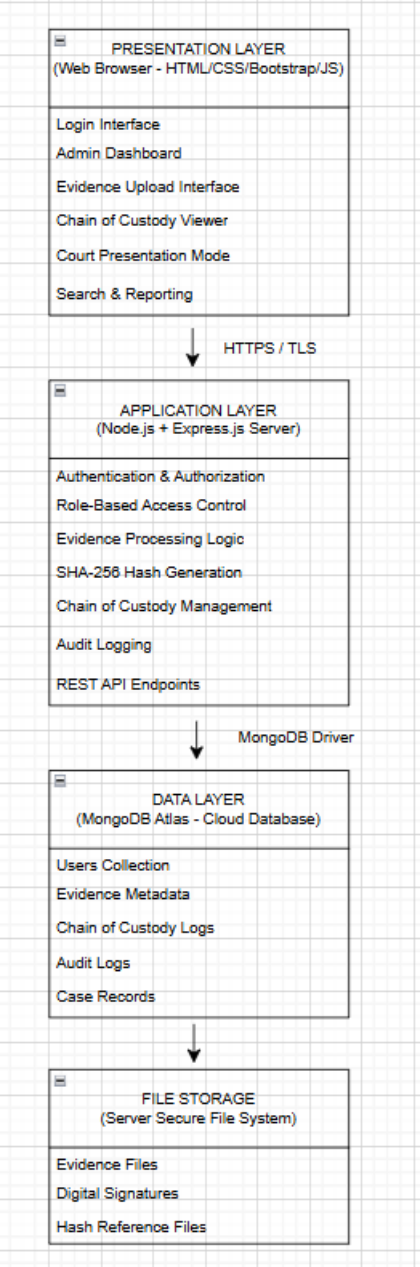


Figure 5: Three-Tier System Architecture

4.3.2 Use Case Diagram

A use case diagram refers to a visual representation used to derive the requirements of a system with focus to both external and internal influences. It helps to establish which parties (actors) will be interacting with the system and the nature of those interactions (relationships) (Waykar, 2015).

.

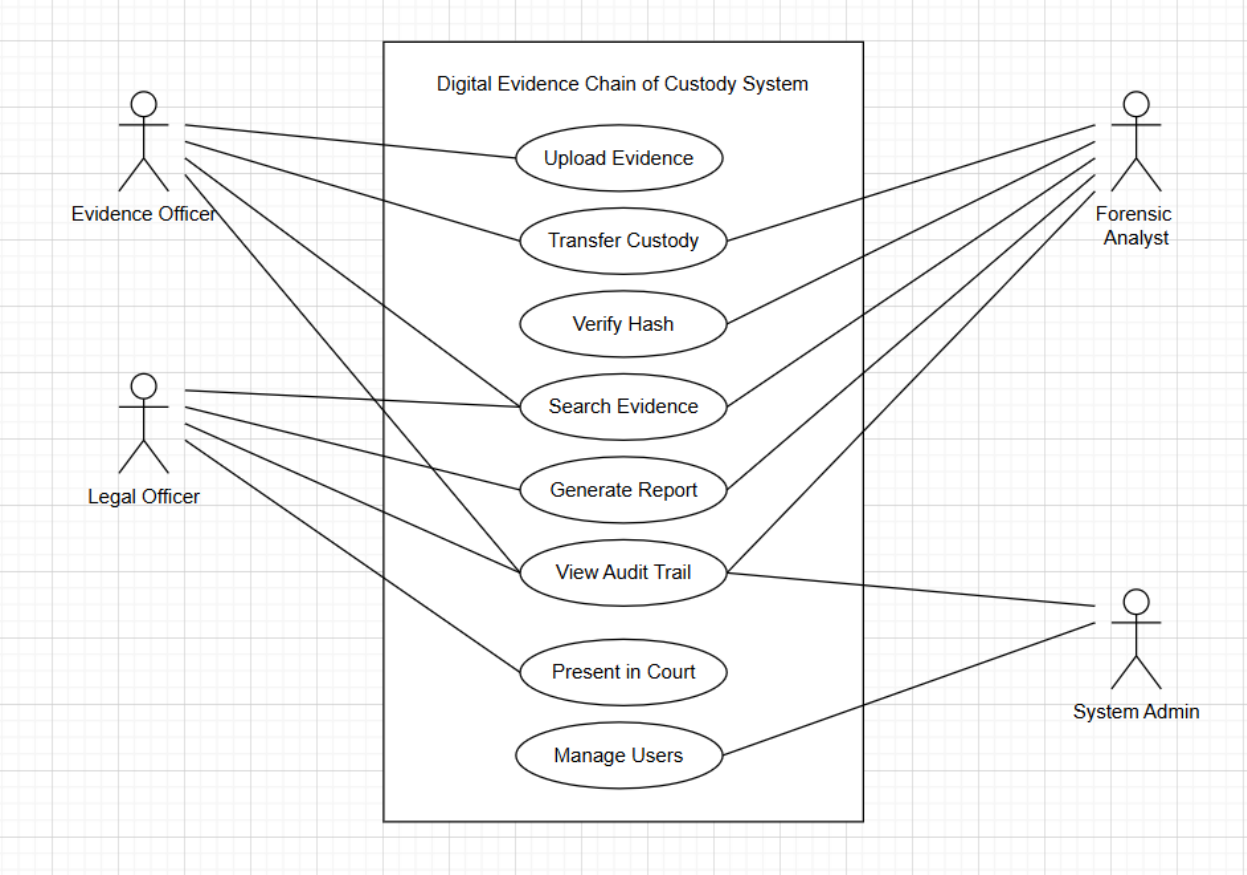


Figure 6: Use Case Diagram

4.3.3 Flowchart

This flowchart shows the steps taken when a user uploads digital evidence. It starts with login, then the system checks if the file and details are valid. If everything's fine, the system saves the evidence and records it in the audit log, then notifies the custodian. If something's wrong, it rejects the upload and shows an error. The flowchart helps make it clear how data moves and how evidence integrity is kept at each step.

.

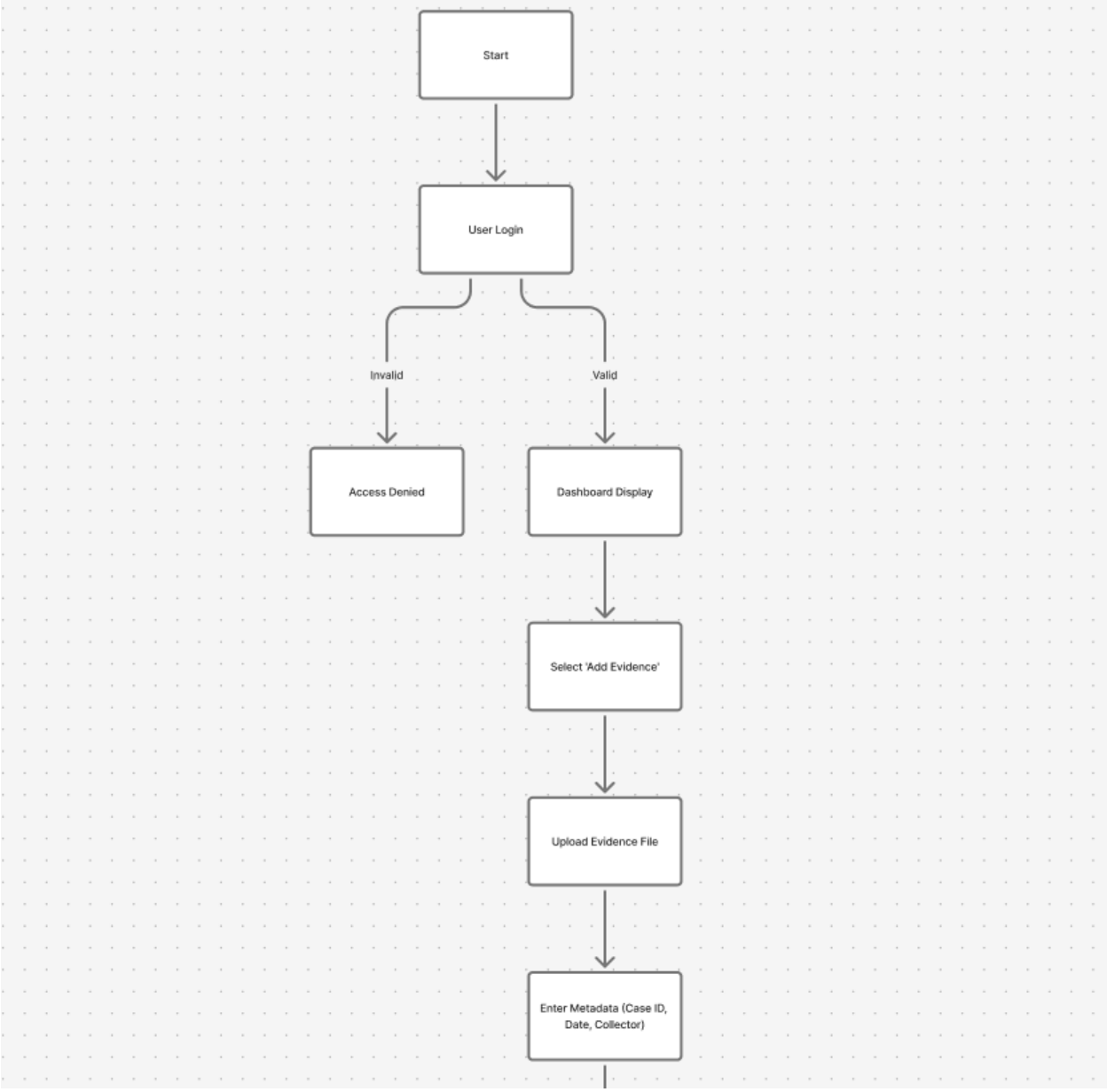


Figure 7: First part of the system flowchart

.

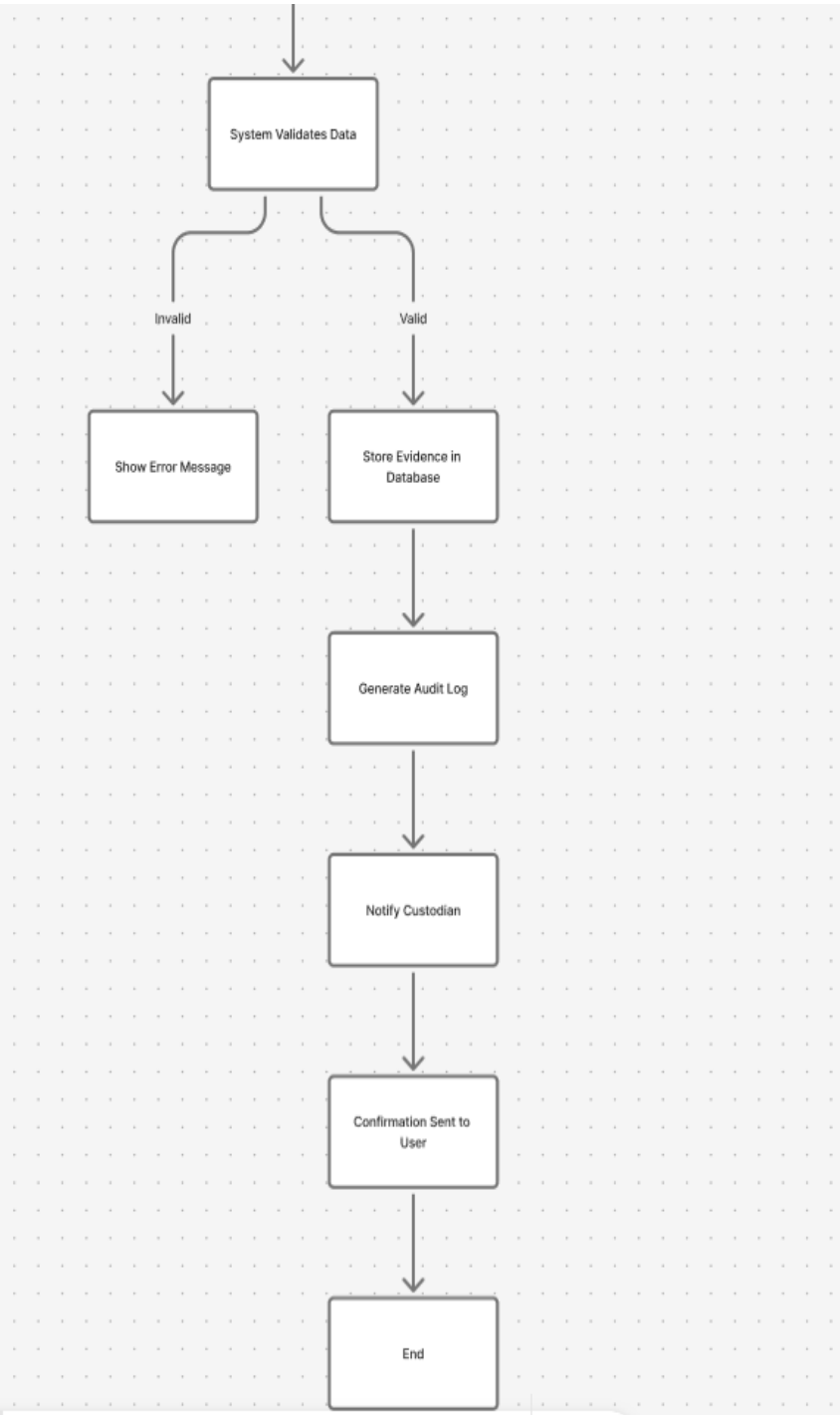


Figure 8: Second part of the system flowchart

.

4.3.4 Class Diagram

A class diagram is a representation of the static view of an application or system. They are employed when visualizing, describing and documenting the various features of a system. This representation is also useful when embarking on the construction of the application's executable code (Yashwant Waykar, 2014).

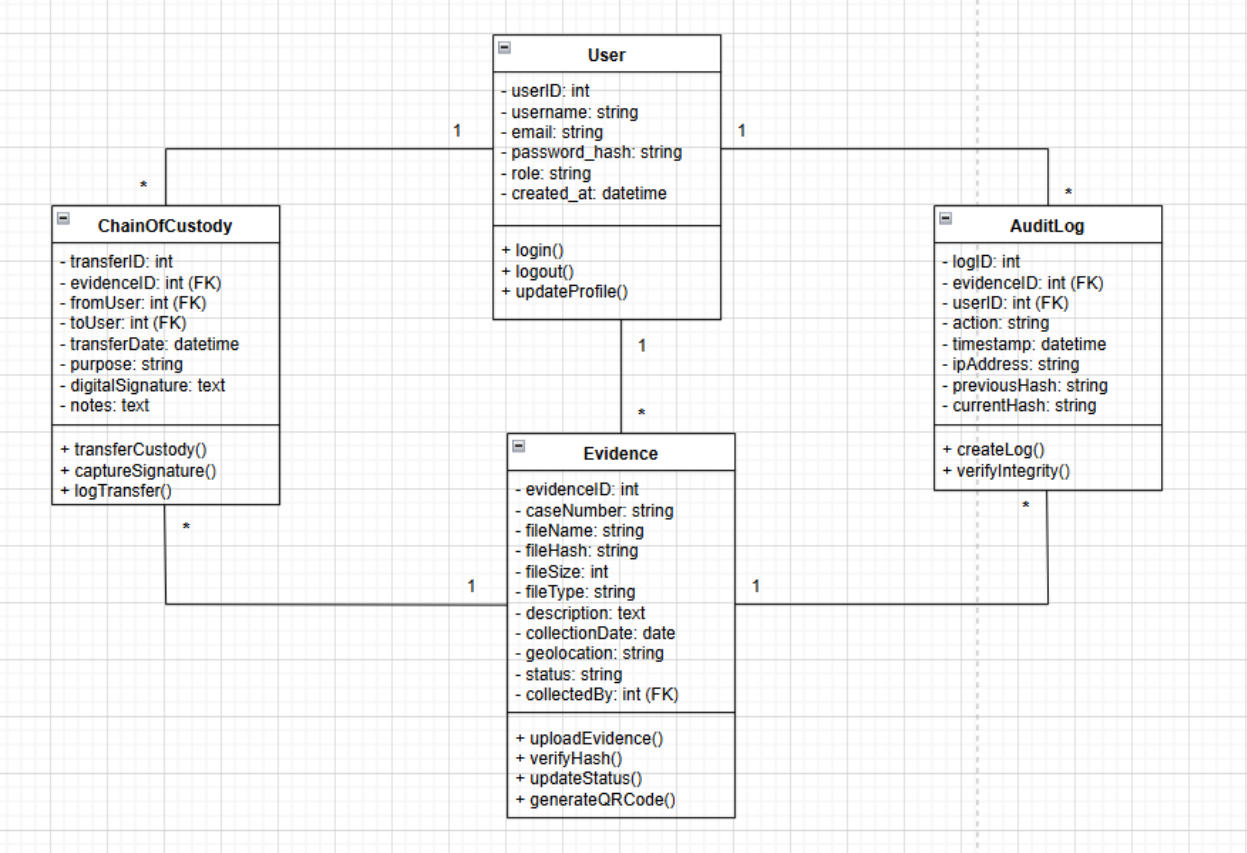


Figure 9: Class Diagram

4.3.5 Data Flow Diagram (DFD)

The DFD shows how data moves through the system and how different users and components interact. It helps to understand what info goes in, how it's processed, and what comes out. The diagram breaks down the system into simple steps like uploading evidence, storing it in the database, and logging every action. This makes it easier to see how data flows between users, the system, and storage, and ensures everything stays organized and traceable.

.

4.3.5.1 Context Diagram (Level 0)

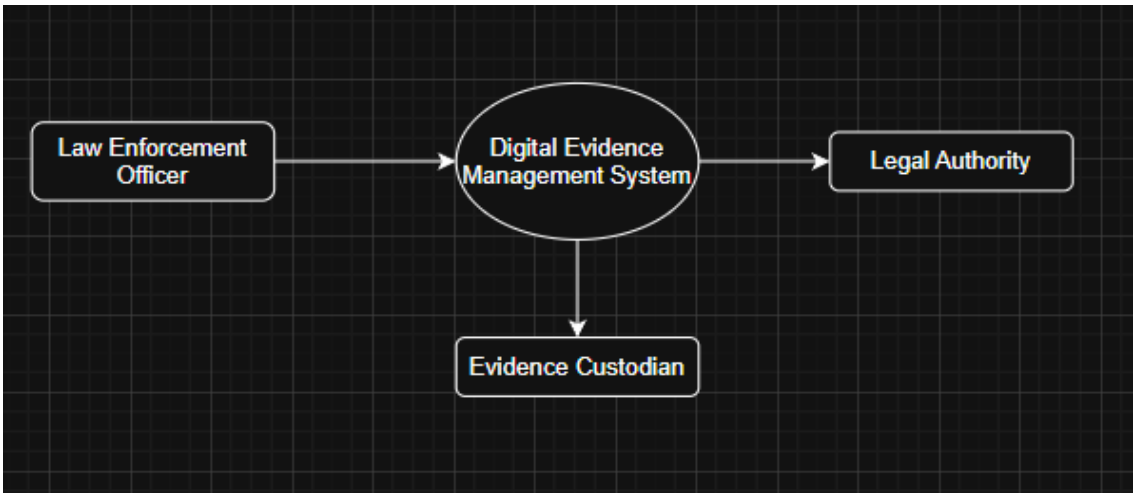


Figure 10: Level 0 Context Diagram

4.3.5.2 Level 1 Diagram

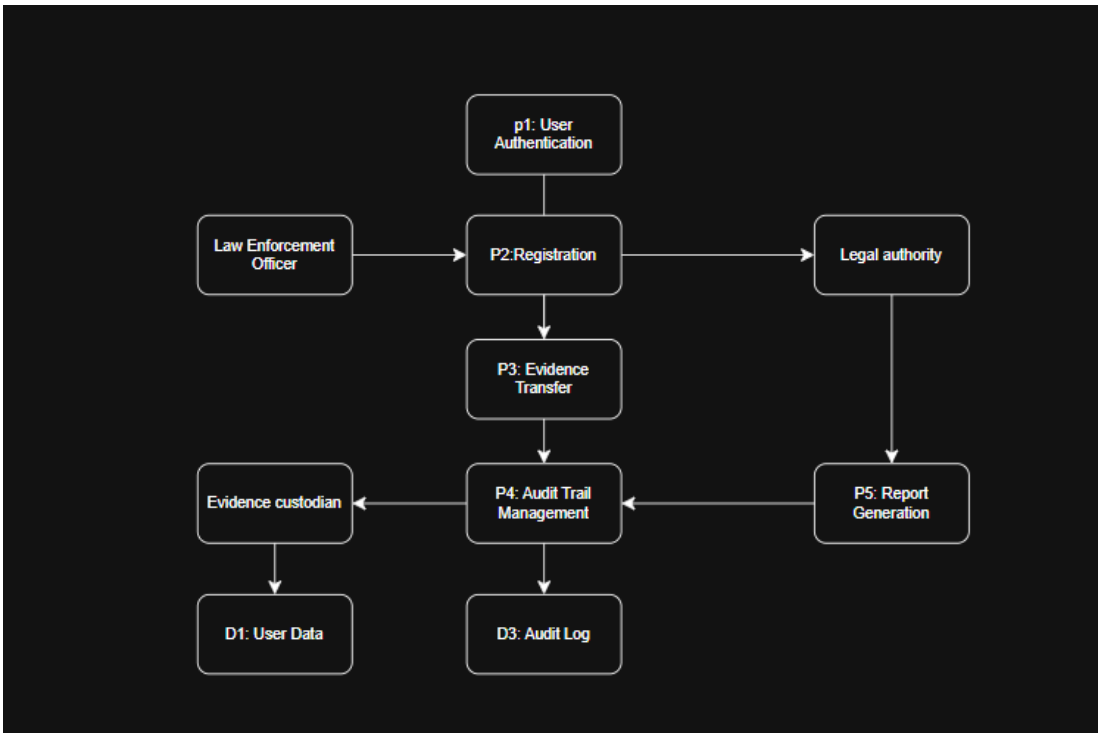


Figure 11: Level 1 Context Diagram

.

4.3.5.3 Level 2 Diagram

This level 2 diagram focuses on the process: "**P2: Evidence Management**"

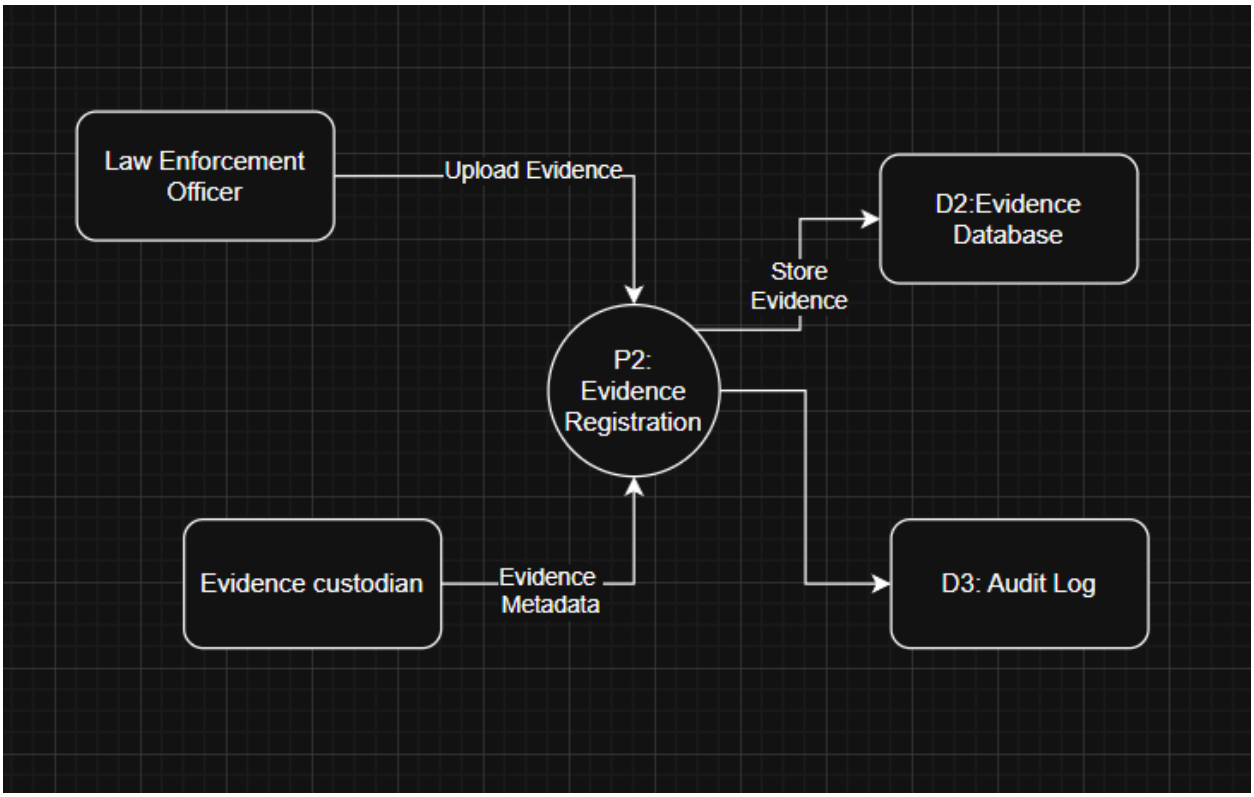


Figure 12: Level 2 Context Diagram

4.3.6 Entity Relationship Diagram (ERD)

An Entity-Relationship Diagram is a graphical depiction of the real-world data environment that is being modeled. This representation aids in database design with regards to the identification of data and rules that will be employed in creation of the database (Il-Yeol Song & Froehlich, 1995).

.

.

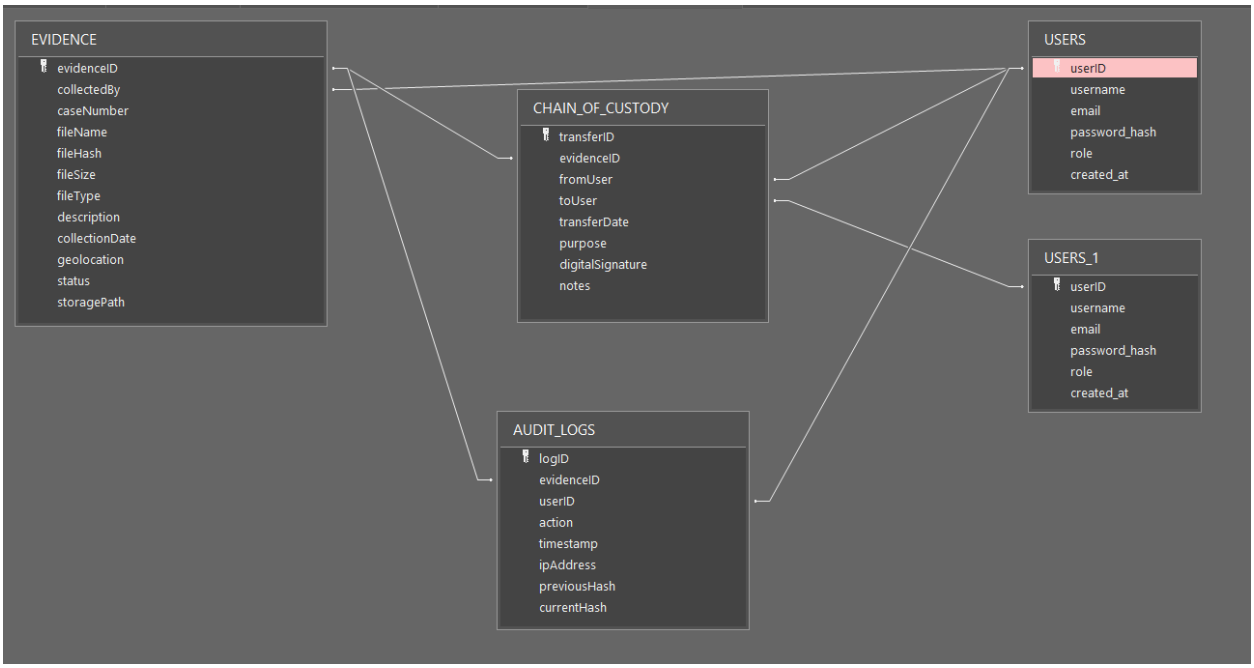


Figure 13: Entity Relationship Diagram

4.3.7 Sequence Diagram

The sequence diagram shows how users and the system talk to each other step by step. It helps explain the order of actions, like logging in, uploading evidence, or getting confirmation from the system. By showing how messages move between users, the database, and the audit log, it makes it easier to see what happens first and what follows next. This helps understand the flow of activities in a more visual and simple way.

.

4.3.7.1 Admin Sequence Diagram

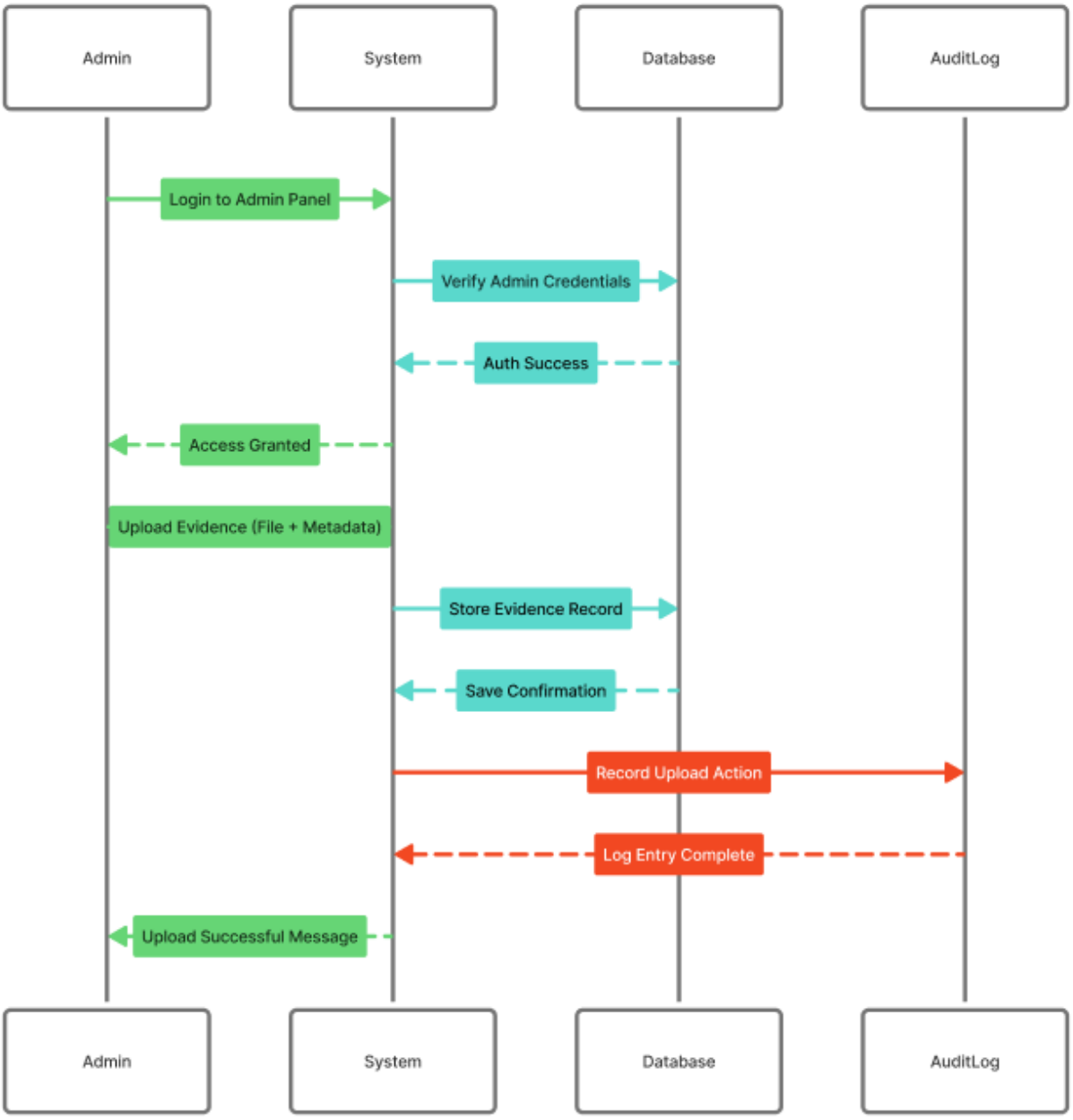


Figure 14: Admin Sequence Diagram

.

4.3.7.2 User Sequence Diagram

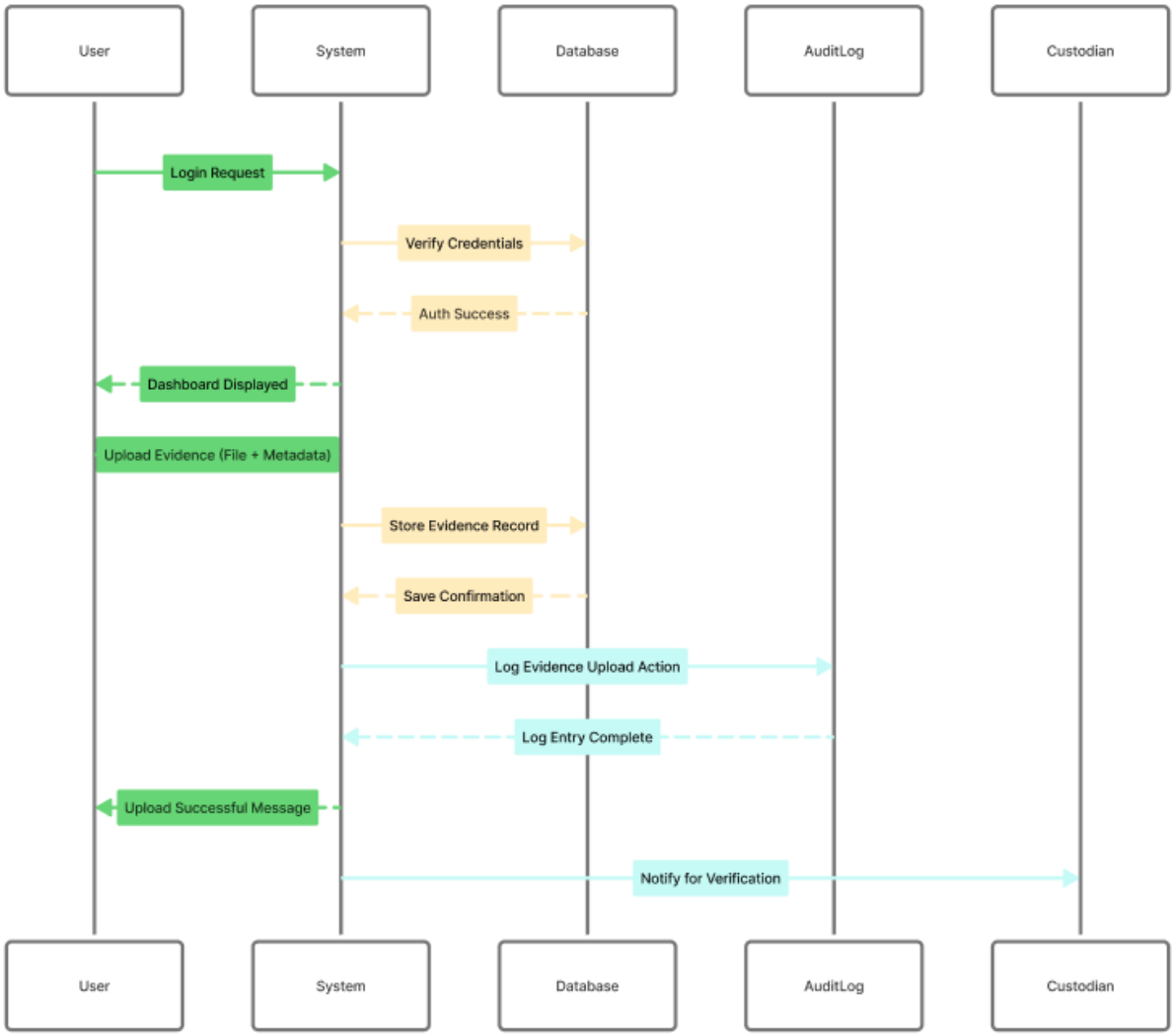


Figure 15: User Sequence Diagram

4.4 Chapter Summary

In this chapter, we presented the design, testing and the implementation framework for our Digital Evidence Chain of Custody Management System. We started by defining the system requirements through functional requirements such as evidence registration and user authentication to non-functional requirements like usability, reliability and availability. Moreover, we identified the various stakeholders who would interact with the system based on their roles and interests.

.

Furthermore, we created various models in a bid to illustrate the structure and functionality of our system. These models include the system architecture, use case diagram, flowchart. class diagram, data flow diagrams, entity relationship diagram, and sequence diagrams. These illustrations provide a comprehensive understanding of our system and provide us with a foundational framework to use during the system development phase.

.

CHAPTER FIVE: SYSTEM IMPLEMENTATION AND RESULTS

5.1 Introduction

In this chapter, we shall examine the manner in which we implemented stated functionalities into a cohesive and user-friendly system as well as analyzing the results from said implementation. We shall restate our objectives through the system overview and analyze which problems exactly our system aims to solve and how we have solved them. We shall also look at our system architecture with regards to the technologies we used, the physical and logical components that our system is composed of, as well as the description of the modules and the interaction between them. Lastly, we shall display the results and outputs of our system as well as the discussion of these results.

5.2 System Overview

The purpose of creating this system is to provide an application to law enforcement that helps preserve the chain of custody that is imperative in ensuring that digital evidence is rendered admissible in court. Our goals are mostly aimed at fixing the flaws and deficiencies in the current digital evidence processing procedures within Kenya's law enforcement agencies.

We aim to tackle this issue through two primary objectives which are:

1. To develop a secure and easy to use web-based system that features audit trails, access controls and an automated generation of evidence functions.
2. To optimize transparency and accountability in evidence management hence building trust in judicial proceedings within our country.

We also aim to tackle these objectives as well:

3. To analyze the flaws and deficiencies of existing digital evidence processing procedures of law enforcement agencies.
4. To conduct a study comparing the system's performance, usability and effectiveness to that of the traditional manual and half-digital systems.

There are a host of issues with the old paper-based systems in use by Kenya's law enforcement

.

agencies that our system aims to solve. These include:

A lack of standardization brought about by the lack of a ubiquitous standard procedure hence bringing about inconsistency in evidence handling.
Limited accessibility and transparency due to the lack of a centralized digital system that both investigators and prosecutors can work through which ultimately brings about delays and mutual misunderstandings.

High risk of evidence rejection through the lack of strict adherence to digital chain of custody protocols regarding evidence handling.

Poor security and tamper risks through the use of paper-based systems which can be easily altered and forged due to a lack of digital encryption methods and audit trails.

With regards to the targeted users of our system, these key beneficiaries are:

- **Forensic investigators and detectives** who are the personnel responsible for interacting with the evidence to gain insight into exactly what transpired within a specific case.

- **Evidence collection officers** who are the first responders at the scene of the crime and are responsible for the collection of evidence.

- **Forensic analysts** who examine, analyze and extract information vital in an investigation.

- **Court officials** who review the submitted evidence during trial proceedings with a keen emphasis on the adherence to chain of custody protocols.

With regards to deployment, our system employs the use of a hybrid cloud architecture that balances local application hosting with managed cloud database services. We have employed the use of Node.js and the Express.js framework to construct the backend. This runs on local host port 3000 or port 4000. We have also utilized MongoDB Atlas as our database environment. For the

frontend environment, we are using a static web server setup where express serves the HTML, JavaScript as well as the CSS files directly from the public/ directory.

For our system, we have a relatively straightforward sequence of the chain of events. This follows a Request-Response pattern that links the frontend, backend and database in the accomplishment of specific tasks.

Firstly, we have the request orchestration (client to server). This process is initiated when the admin creates a user. The frontend (JS) captures the input then sends a fetch request with JSON data to API endpoint /api/admin/users/create.

Processing and validation then take place where the express server acts as the orchestrator and captures the request using middleware to translate the data. It then uses route logic to validate the data by checking for things such as if the user being created already exists and if all the fields in the input forms are presently there.

Lastly, we have the state management (server to database) where the server communicates with the MongoDB Atlas cluster so as to persist the data. The server uses the async/await logic to ensure that freezing does not take place when waiting for the cloud database to respond which ultimately allows it to handle multiple requests. This is basically asynchronous handling.

5.3 System Architecture

Overall System Architecture

The Digital Evidence Chain of Custody Management System architecture is structured into three layers:
Presentation Layer (Frontend)
Application Layer (Backend)
Data Management Layer (Database)

The communication between the frontend and backend occurs via secured HTTP requests and the backend covers all aspects of the user authentication, the application of business logic, and

performing database operations.

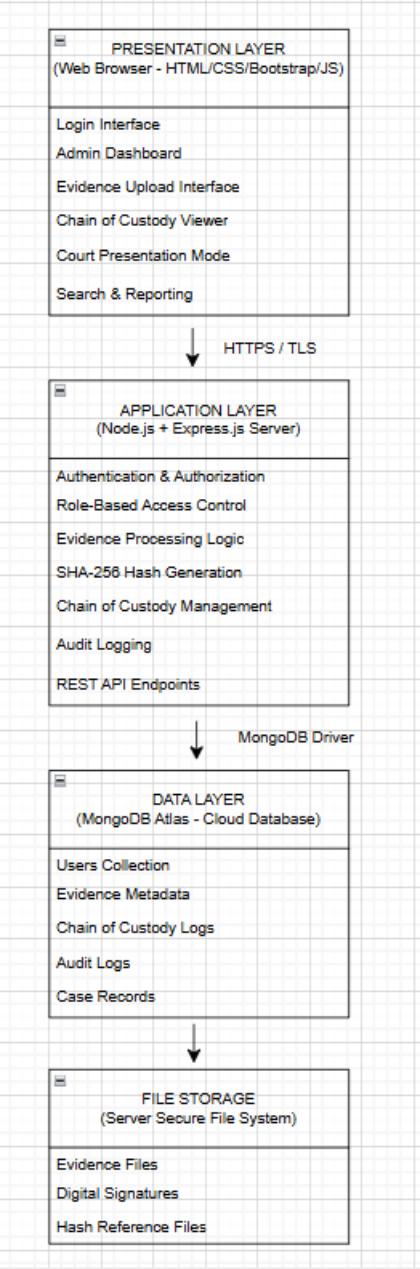


Figure 16: System architecture diagram.

Logical and Physical Components

Frontend: A user interface that is built with HTML, CSS, and JavaScript;

Backend: A node server.js backend

Database: A MongDB database.

.

Module Interaction

Firstly, the users log in through the login interface. JWT tokens are then used for validating authenticated requests. An automatic chain-of-custody logging is then triggered by evidence actions. Lastly, storage happens whereby all records are kept securely.

Technology Stack

Frontend: HTML5, CSS3, JavaScript

Backend: Node Server.js

Database: MongoDB

Authentication: JWT-based authentication

Development Tools: Visual Studio Code

5.4 System Implementation

This part illustrates how the Digital Evidence Chain of Custody Management (DECCM) System was put into effect. The discussion on the implementation is done by dividing the system into its functional layers which are the User Interface Layer, application logic layer, data management layer and lastly the deployment environment.

5.4.1 User Interface Layer

The User Interface (UI) layer serves as the interactive, graphical interface which is based on roles and allows the users to work with the DECCM System. The four dashboards are distinct and the system implements each one specially designed for the user role.

GUI Layout and Dashboards

Administrator Dashboard:

This dashboard grants system management possibilities such as user creation, role assignment, and tenant management. In addition, administrators are allowed to get an overview of the system's overall activity at the same time.

.

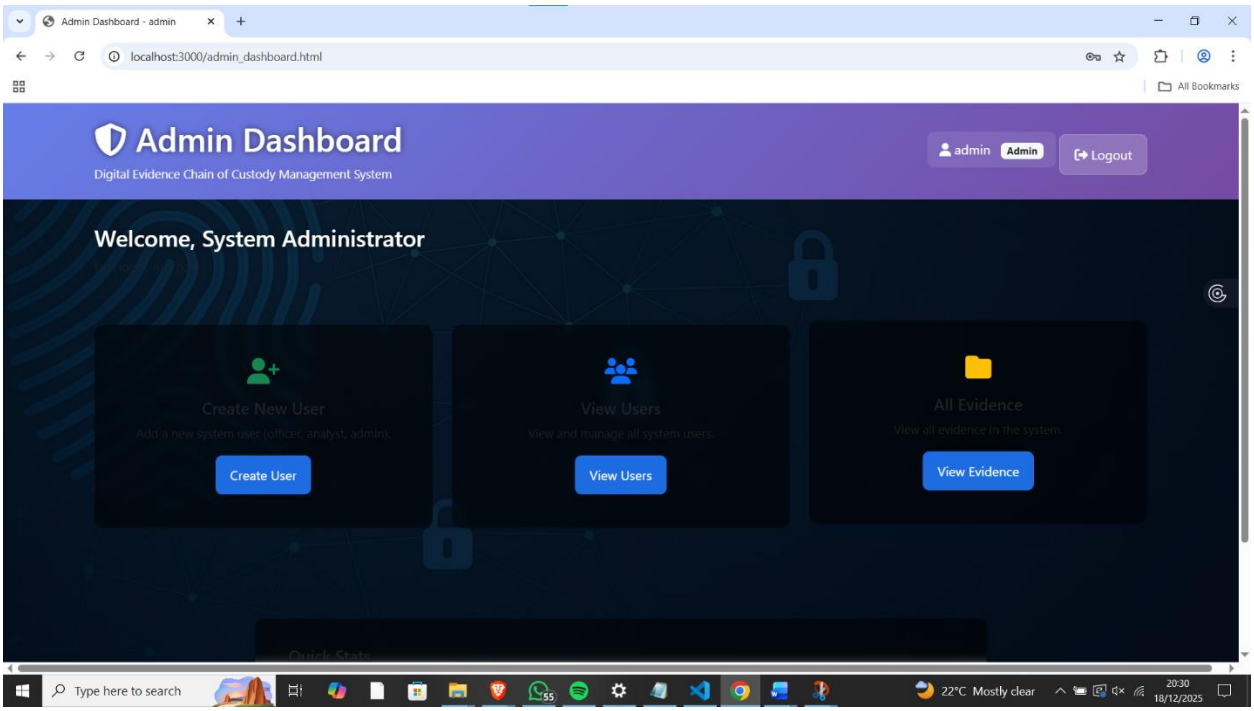


Figure 17: Admin Dashboard

Officer Dashboard:

This dashboard is in place for the evidence officers to be able to record and register the digital evidence. Moreover, this dashboard includes the evidence submission forms and views whereby one can track the submitted evidence.

.

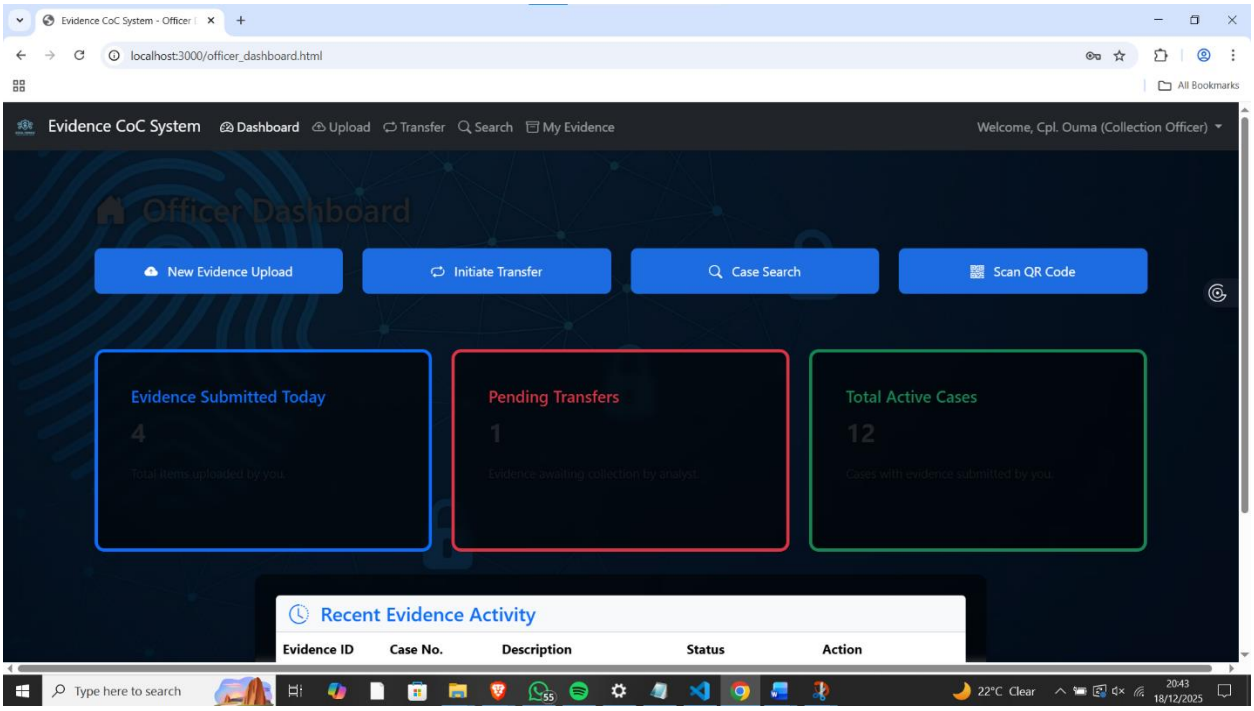


Figure 18: Officer Dashboard

Analyst Dashboard:

This dashboard enables forensic analysts to receive the submitted evidence for analysis. The analysts can then note their findings and change the evidence status without losing the original data.

.

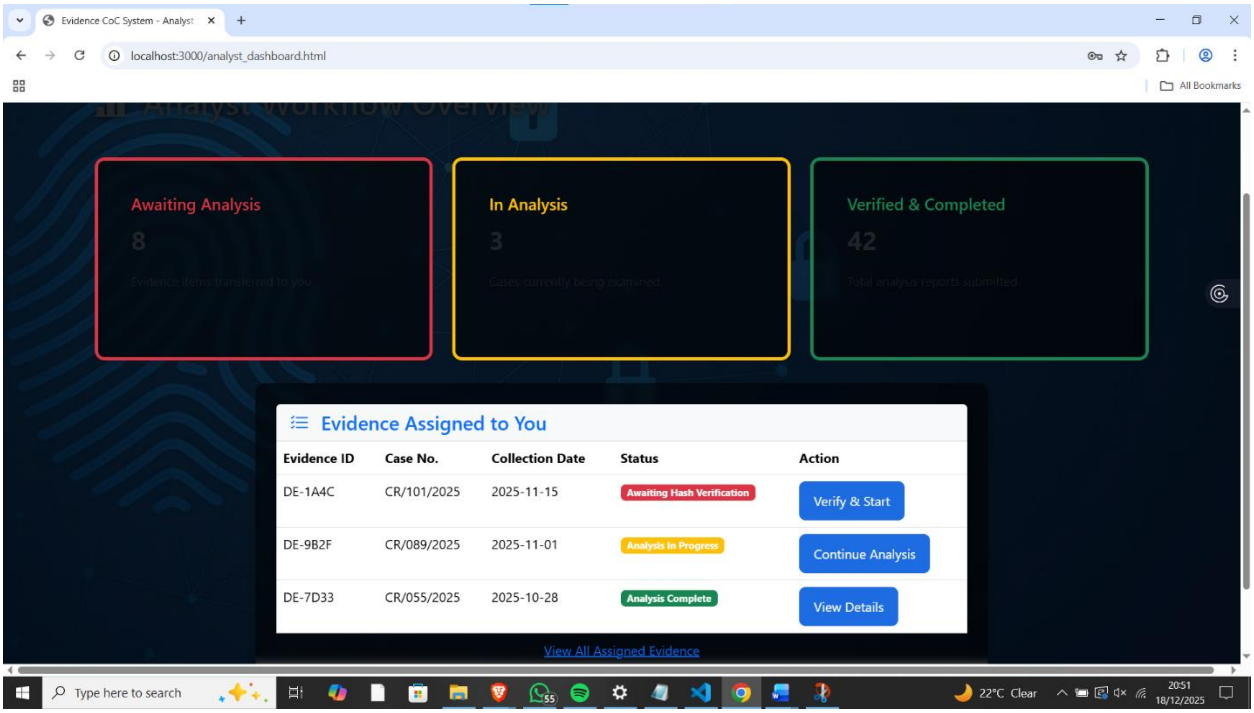


Figure 19: Analyst Dashboard

Court Clerk Dashboard:

This dashboard gives access to the finalized evidence and the complete chain-of-custody records that are for reading only. The court clerks can see if the evidence is ready and approve it for court presentation.

.

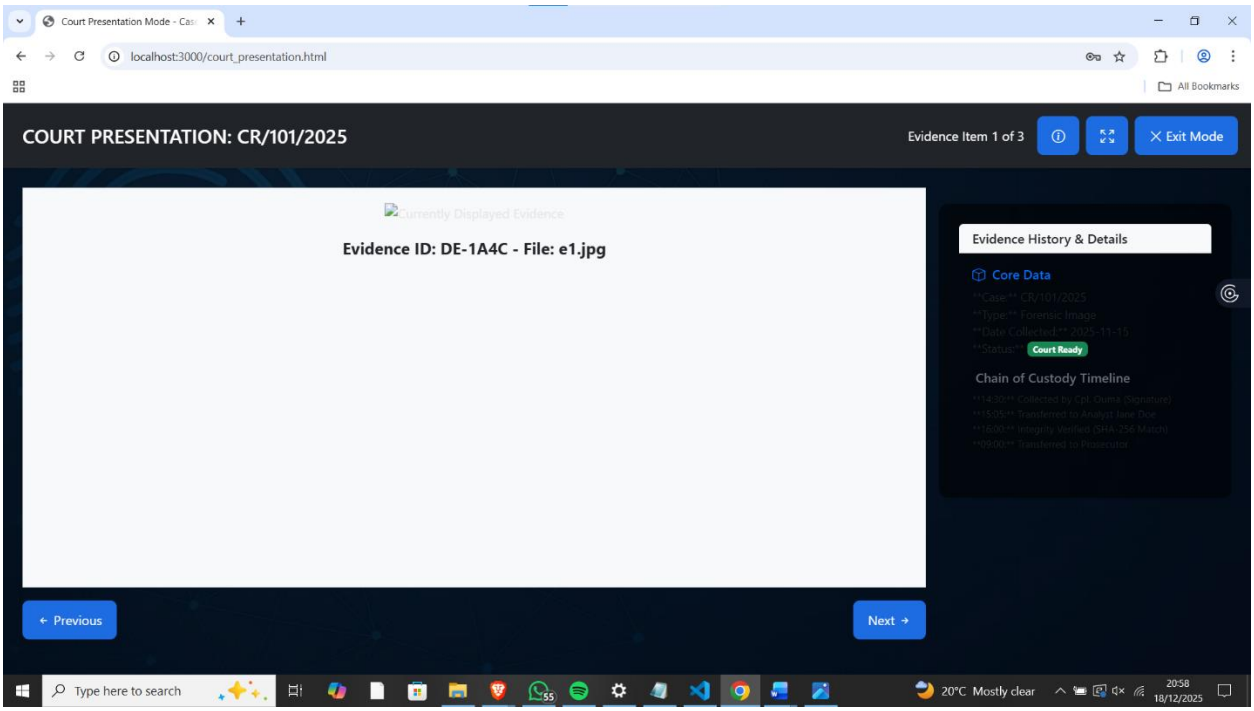


Figure 20: Court Presentation Dashboard

Input Forms and Screens

Structured input forms are included in the UI for:

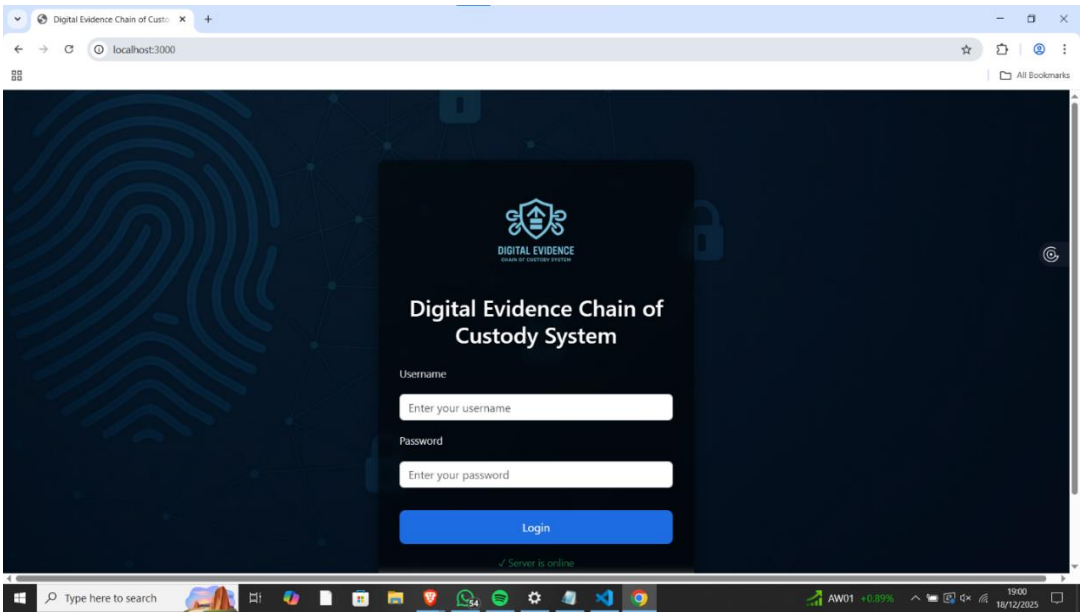


Figure 21: User authentication (login page) above.

.

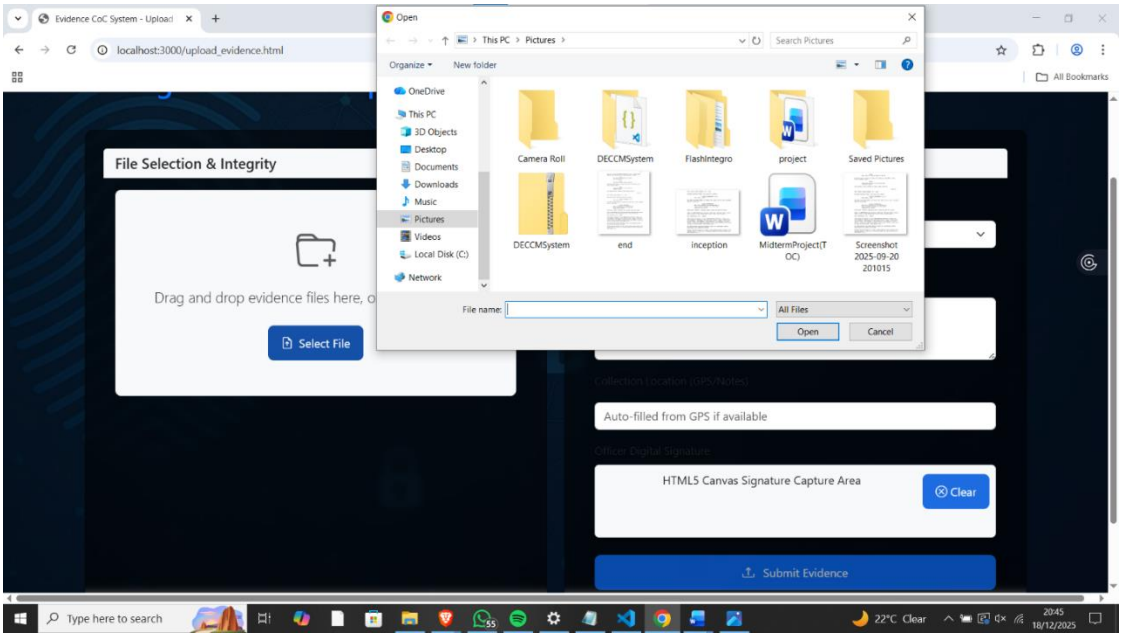


Figure 22: Digital evidence submission whereby users can upload and submit evidence.

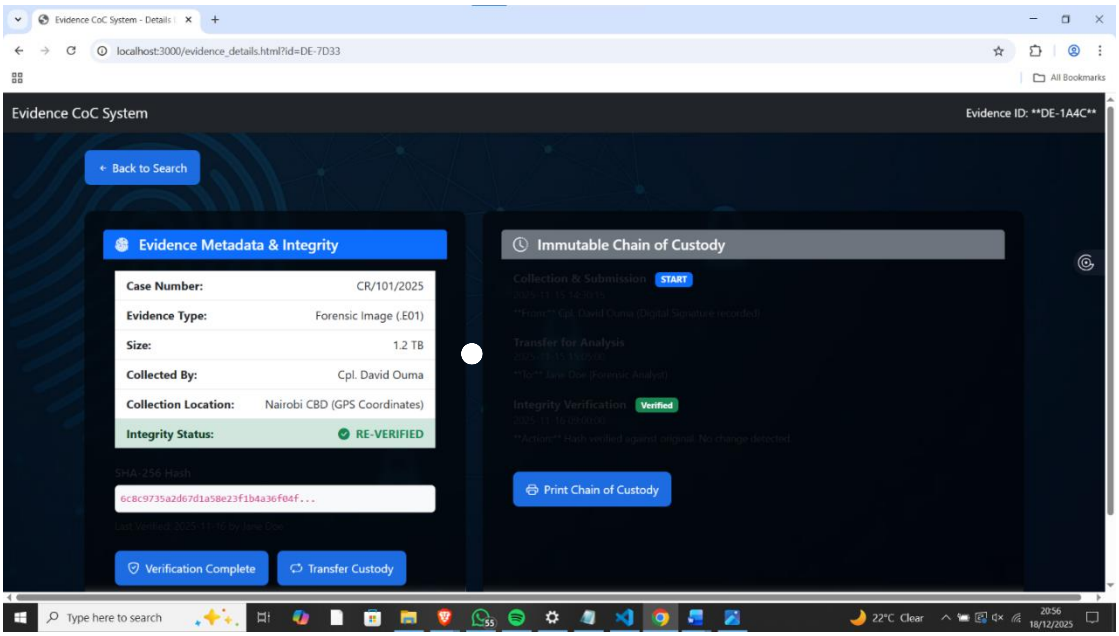


Figure 23: Evidence review and analysis whereby one is afforded a brief overview of the evidence they have.

.

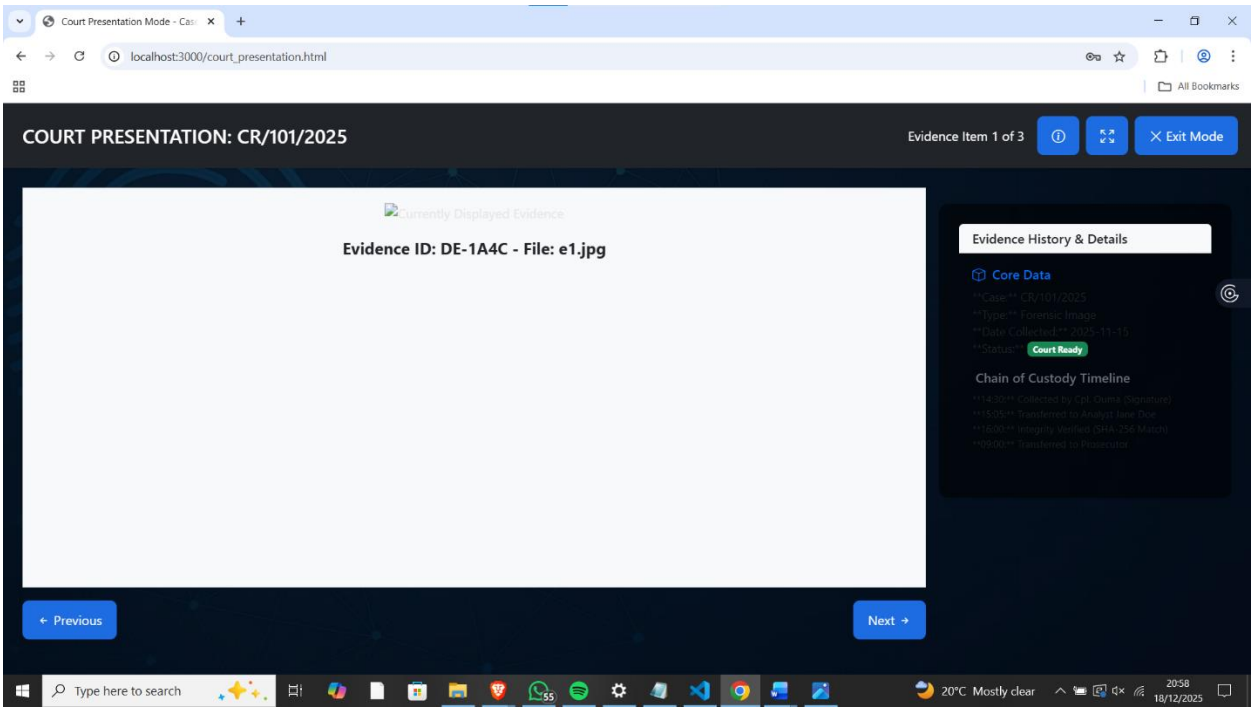


Figure 24: Verification of court readiness whereby one can make presentations for court.

5.4.2 Application Logic Layer

The backend application logic executes:

- User authentication and authorization
- Role-based access control (admin, officer, analyst, court clerk)
- Evidence creation, retrieval and status updates
- Automatic logging of chain-of-custody for every action related to evidence

Every custody event (upload, transfer, access) is documented with a time and the user who did it.

.

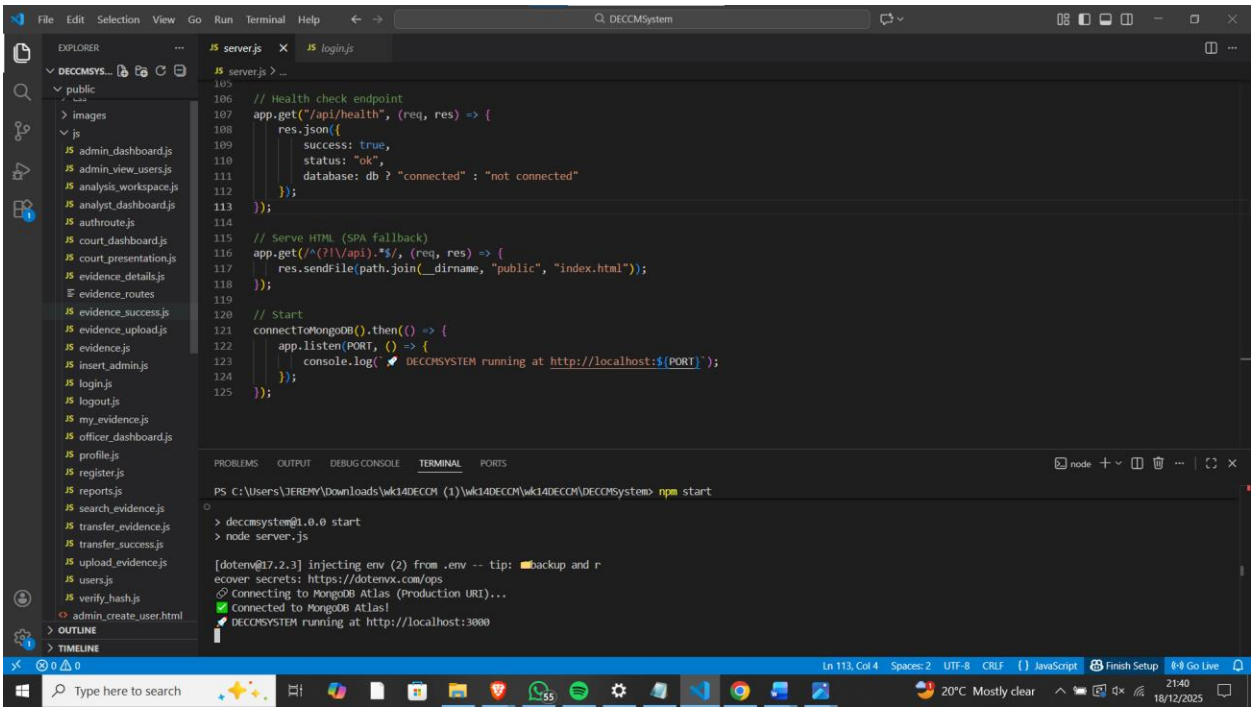


Figure 25: VSCode Schema

In the above screenshot we get a glimpse of our Visual Studio Code schema. On the extreme left we have the tree that has all of our JavaScript files containing the system logic in this case. Below them and slightly hidden we have the HTML files responsible for our user interface. On the center most part, we have the server.js code which is crucial in launching our system.

5.4.3 Data Management Layer

The structure of the database schema entails the following:

- Users: Actors responsible during a forensic investigation.
- Evidence: Digital artifacts being investigated
- Chain of Custody Logs: Non-editable event documentation

Interconnections among entities make sure the isolation of evidence between tenants and also uphold referential integrity.

.

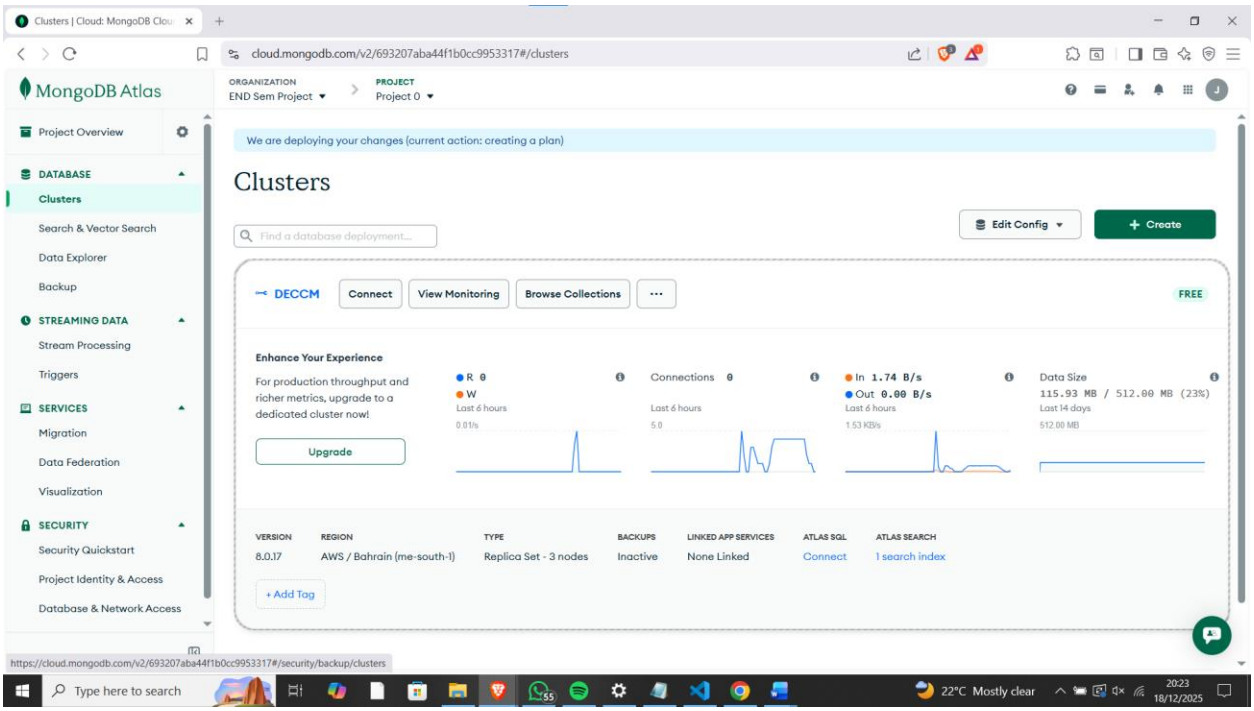


Figure 26: Cloud MongoDB section showing performance metrics

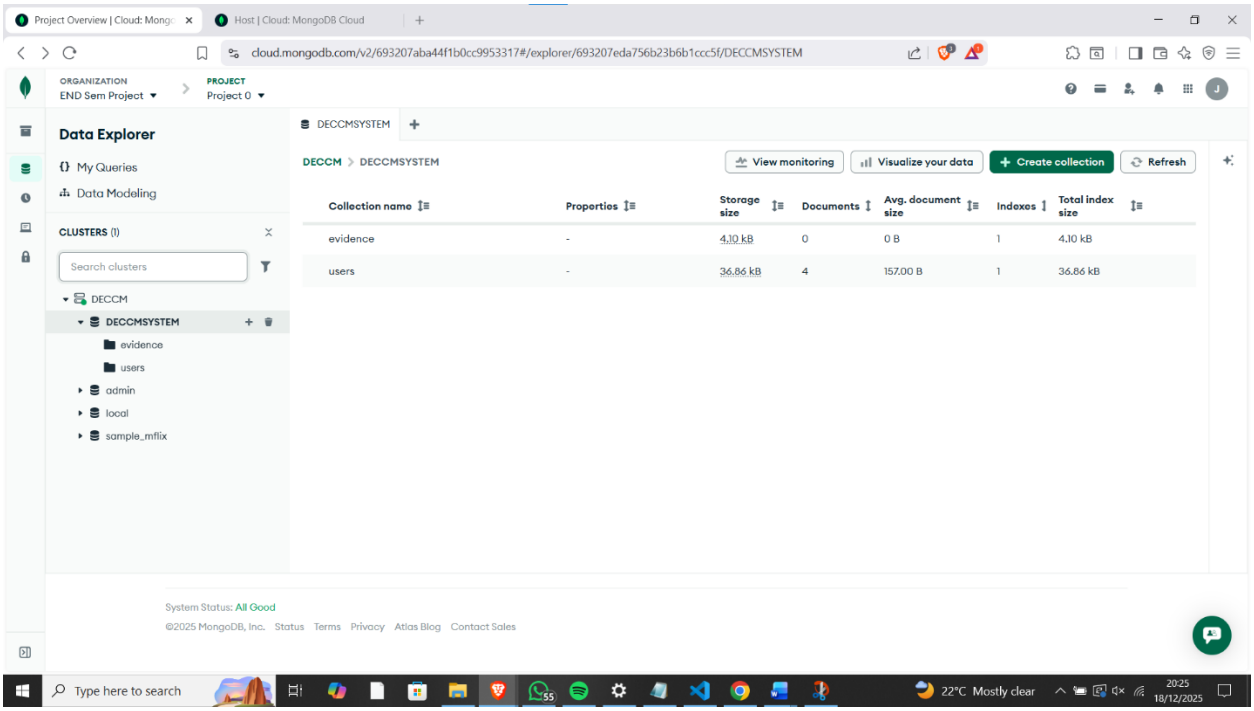


Figure 27: Collections taking place within our backend

.

5.4.4 Deployment Environment

The deployment of the system took place on a local development server with the help of:

- Uvicorn for executing the FastAPI backend
- Python HTTP server for serving the frontend
- Swagger UI for API testing and documentation

The REST API endpoints of the backend are accessible to the frontend.

5.5 Key Functionalities of the Application

Function (Module)	**Description**	**Output**
User Authentication	Secure login using JWT tokens	Login confirmation
User Management	Assign users and roles	User table
Evidence Management	Upload and register evidence	Evidence records
Chain of Custody	Automatic logging of evidence actions	Audit logs

Table 4: Key functionalities

.

5.6 Sample Results and Outputs

The following are among the sample outputs produced by the system:

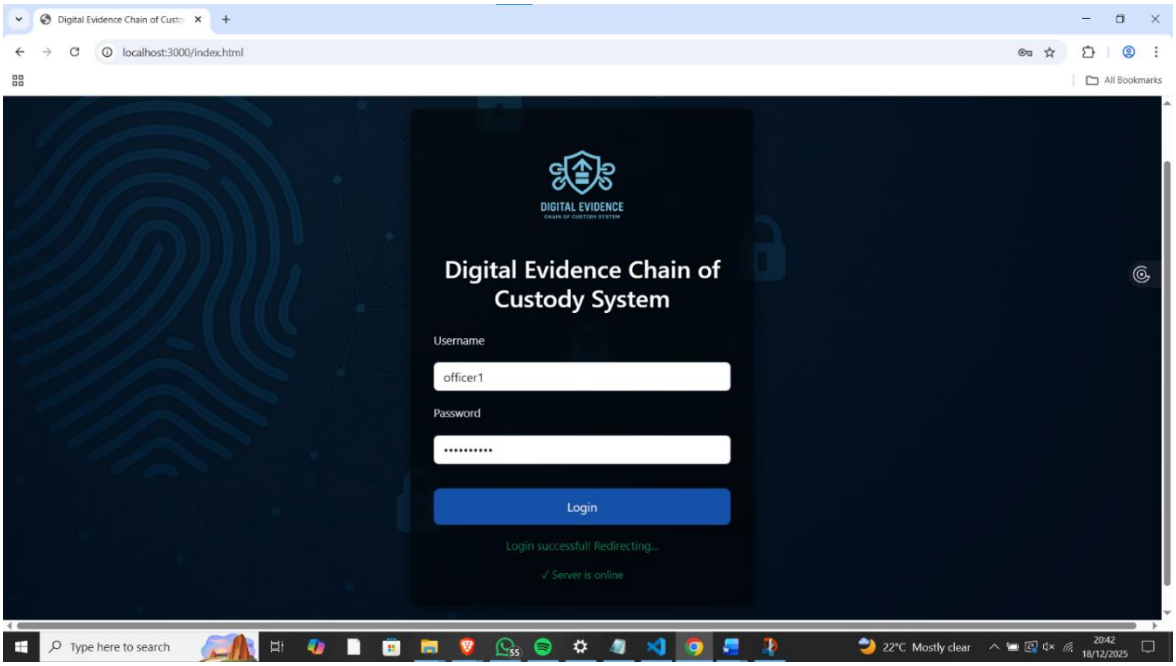


Figure 28: Login confirmation and loading

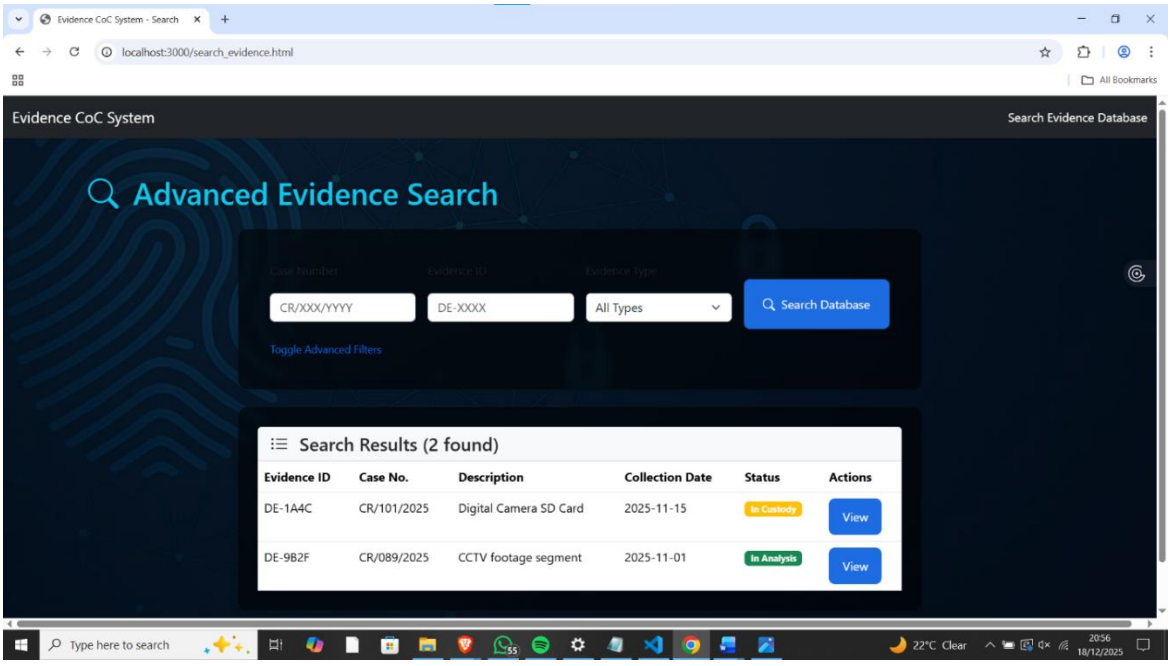


Figure 29: Dashboard featuring evidence records (above)

.

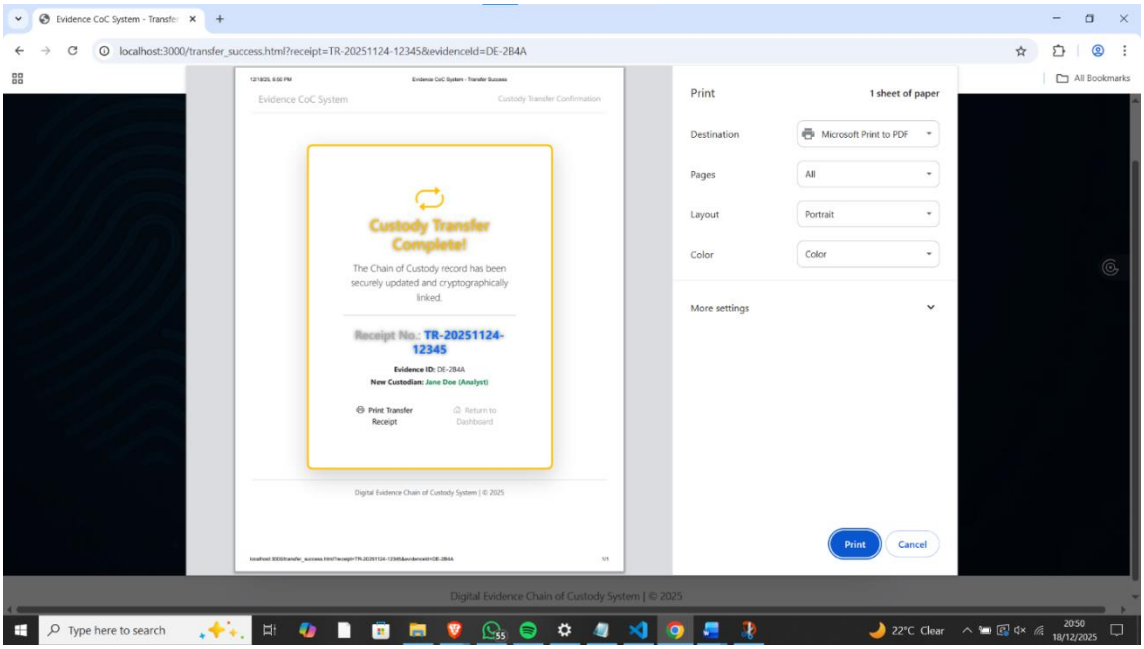


Figure 30: Evidence Transfer

As we can see from the screenshot above, we can see exactly who the evidence was transferred to hence supporting chain of custody requirements.

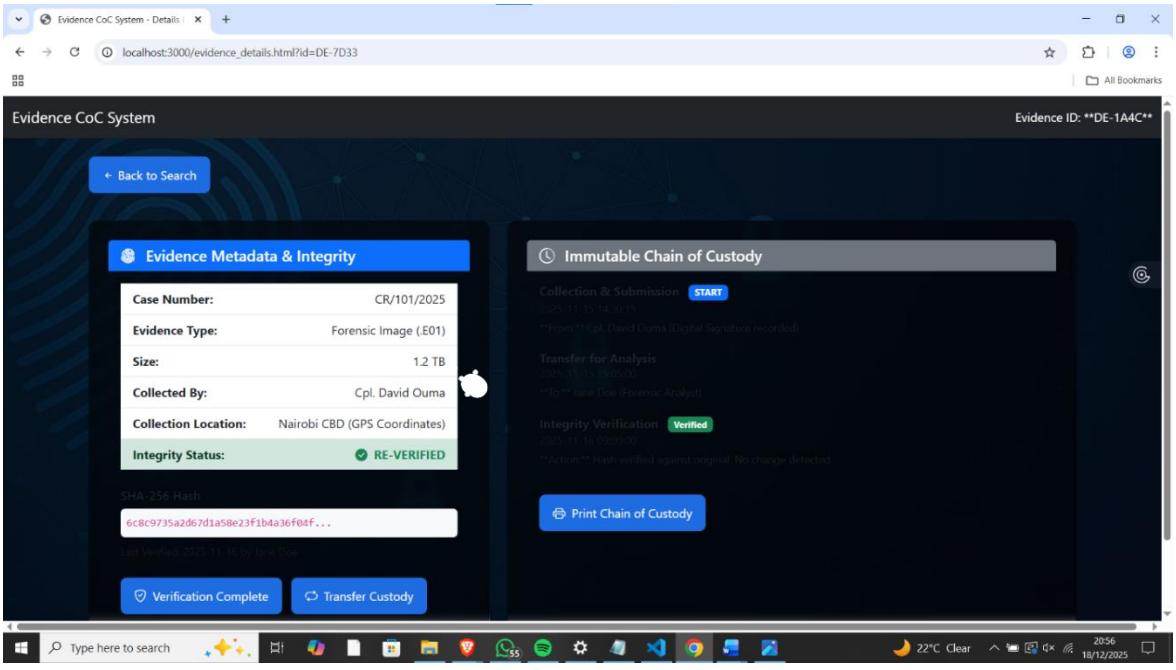


Figure 31: Evidence details - audit trail

.

We can also see a glimpse of the audit trail within the evidence details section.

The accurate tracking and transparency of evidence handling are proved by these outputs.

5.7 System Testing and Evaluation

5.7.1 Functionality Testing

Test Case	Expected Result	Actual Result
User Login	Successful authentication	Passed (as shown in screenshots above)
Evidence Upload	Evidence saved and logged	Passed (as shown in screenshots above)
Role Restriction	Unauthorized access blocked	Passed (as shown in the screenshot below)
Custody Logging	Action recorded automatically	Passed (as shown in screenshots above)

Table 5: Functionality testing

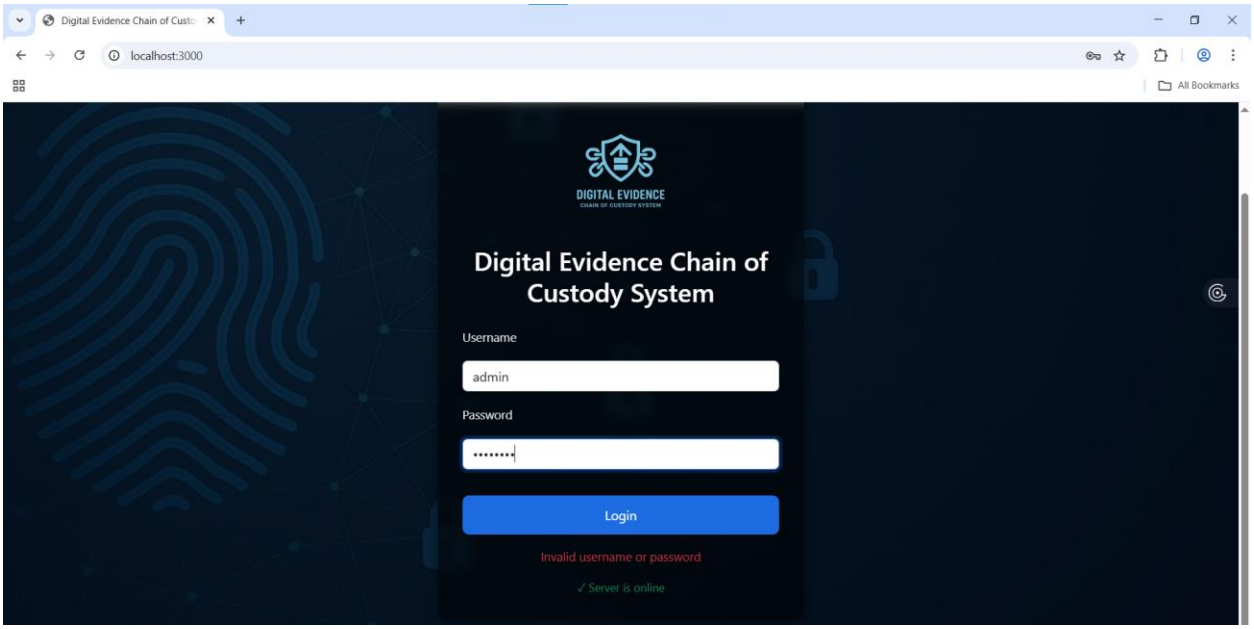


Figure 32: Failed Login

.

Login attempt with wrong credentials. Demonstrates success through failure of getting into the system.

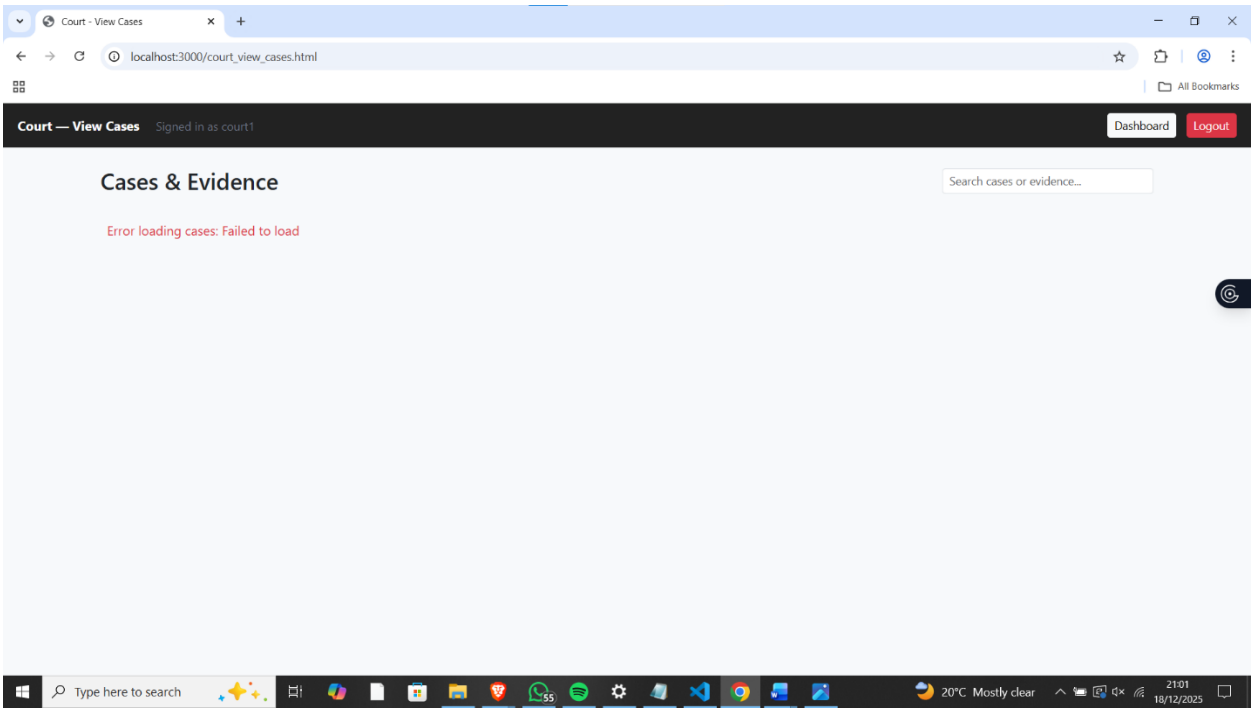


Figure 33: View cases - court dashboard above

All was not smooth however as when we tested one of our court cases sections within our court dashboard section, we encountered errors in that things did not seem to fully work as intended – the evidence was not viewable. This was a partial failure.

5.7.2 Performance Testing

The tests were conducted on the system using moderate load conditions. We simulated logging in functionality across different machines simultaneously and experienced the same speed output as doing it one one machine alone. Moreover, our system was almost always up which demonstrated a satisfactory level of uptime. The output demonstrated:

- Quick response times for API calls.
- Performance remained stable with several simultaneous users connected.
- Database activities were consistent and there was no loss of data.

.

There was however a matter of concern in that logging out took a while across most if not all user profiles (30 seconds on average). This is definitely something that we could improve upon.

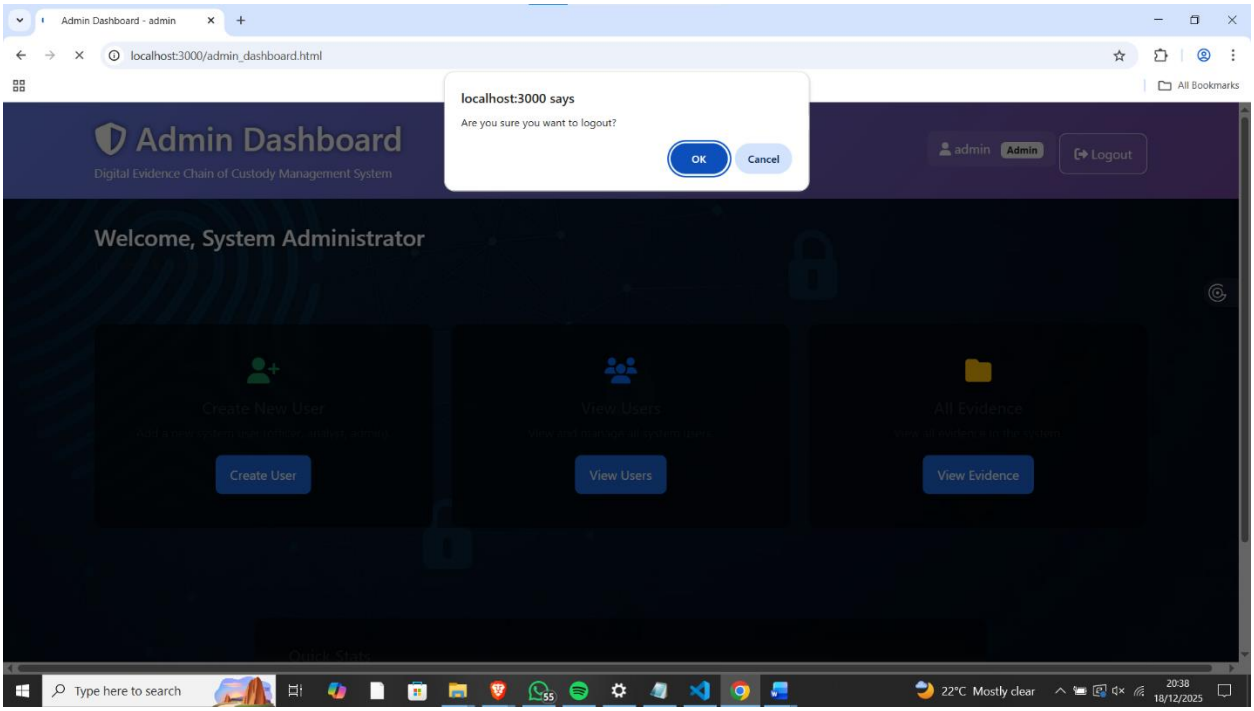


Figure 34: Logout delay

5.8 Discussion of Results

The findings of the study suggest that the Digital Evidence Chain of Custody Management System does an overall great job in terms of its design objectives. Transparency is enhanced with automated custody logging, and security is guaranteed with role-based access and multiple users and parties can be created using this system. In general, the system proves to be relatively consistent and appropriate for practical forensic settings.

5.9 Chapter Summary

The chapter outlined the system implementation, architecture, features and evaluation findings. The Digital Evidence Chain of Custody Management System has been successful in automating the management of digital evidence without compromising its integrity or accountability. The testing has verified the system's efficiency and performance, thus providing a solid base for the

.

future improvements that we have planned.

.

CHAPTER 6: CONCLUSION AND RECOMMENDATIONS

6.1 Introduction

This chapter summarizes the results of the research, demonstrates how the work accomplished the goals that we set when embarking on this project, points out the academic and practical contributions of the research, mentions the limitations that we encountered and provides solid recommendations for future research and deployment.

6.2 Achievement of Chapter 1 Objectives — Key findings & outputs

Objective 1 — To create a web-based system that is secure and easy to use and that possesses features such as audit trails, access controls and automated generation of evidence functions.

Achievement & outputs: The DECCM prototype generated a web-based role-based interface (admin, officer, analyst, court clerk), JWT-based authentication, role-specific dashboards, full automation, no-write custody logs as well as forms for evidence upload & metadata acquisition. Our deliverables are our working prototype, screenshots proving the same, API endpoints, and logged custody timelines.

Objective 2 — To enhance the credibility of judicial proceedings by establishing a system of transparency and accountability in the handling of evidence.

Achievement & findings: The automated audit trails that keep track of time, user involved and specific actions taken for each custody event have made it possible to trace and hold accountable all individuals within a forensic investigation which in turn has made evidence more likely to meet chain of custody demands. The architecture and outputs (audit logs, custody timelines) meet the courtroom transparency and chain-of-custody requirements as stated in international guides.

.

Objective 3 − To analyze the flaws and deficiencies of existing digital evidence processing procedures of law enforcement agencies.

Achievement & findings: The study recorded the major shortcomings in the traditional and half-digital procedures still in use within many law enforcement agencies across Kenya. With the old systems, there is a lack of proper standards, non-existent or poor-quality control measures, inaccessibility of evidence to certain parties and the easy loss or alteration of the chain of custody due to a high risk of tampering and carelessness (Cece 2019, Waweru, 2021). These weaknesses were taken into consideration during the system requirements stage and directed the design choices (standardized forms, mandatory metadata, tamper-evident logs) that we used.

Objective 4 — To conduct a study comparing the system's performance, usability and effectiveness to that of the traditional manual and half-digital systems.

Achievement & findings: Through functional test cases and moderate-load performance tests, the system showed enhanced reliability (less human omission errors), faster evidence retrieval and easy-to-follow custody events compared to equivalent manual counterparts (handwritten). The role of the user was highlighted in a qualitative manner by the role workflow screenshots and in a quantitative manner through the accepted test cases. Though not a complete field trial, the controlled comparisons point out significant improvements in process reliability and user task completion.

6.3 Contributions of the Study

Academic contributions

The paper highlights how such principles of forensic chain-of-custody can be practically applied in a web system which is in conformity with ISO standards for the handling of digital evidence.

Offers design patterns and a reference implementation that can be easily replicated and enhanced by future researchers.

.

Practical contributions

Creates a tested prototype that mostly solves; standardization, evidence tampering, restricted access and centralized logging problems that law enforcement faces within their workflows.

Gives procedures for testing and expected results that are appropriate for inclusion in the procurement or pilot projects of the agency.

Industry / Policy contributions

Provides the agencies with a plan for the migration from paper-based systems to controlled and auditable digital evidence management consistent with the NIST and international best practices (NIST, 2025).

6.4 Recommendations for Future Work

1. Pilot deployment in a live law-enforcement environment

Conduct a supervised trial in one or more agencies to evaluate real-world performance, user acceptance, legal admissibility outcomes and operational constraints that could not seen or replicated in our lab testing.

2. Integrate immutable provenance (blockchain) for higher trust

Try a hybrid method where the custody metadata (hashes, timestamps, custody events) is linked to a permissioned blockchain to boost tamper resistance and auditability. Previous literature has pointed out the potential of this but also mentioned the drawbacks (latency, cost) and the need to conform to standards.

3. Conformance with international standards and guidelines

By extending system workflows and documentation to ISO/IEC 27037 (digital evidence handling) and NIST guidance for evidence preservation and acquisition, it is possible to improve the admissibility of the evidence and facilitate its interoperability (ISO, 2012, NIST, 2025).

.

4. Cloud-scale, secure multi-agency deployment design

Investigate secure cloud architectures (multi-tenant isolation, encryption-at-rest, key management) and federated identity so that the system could be used nationwide or inter-agency-wise while data separation and privacy are still guaranteed.

5. Mobile evidence capture and edge ingestion

Design, develop and secure mobile clients for on-site captures that create signed metadata and hashes at the moment of collection hence shortening the time between collection and logging whilst still facilitating early preservation. The NIST and SWGDE guidelines for cloud and collection practices should be the basis for the design (NIST, 2025).

6. Advanced integrity & analytics tools

Introduce the tools of hash verification, access pattern analysis and reporting dashboards so that auditors and prosecutors could rapidly determine the authenticity of the evidence and the integrity of the chain-of-custody.

7. Legal and policy alignment study

Further research on legal stakeholders (prosecutors, judges) should be done in order to ascertain what system outputs and documentation are enough for the courtroom to accept the evidence as fully admissible. This will guide required audit formats and retention policies. UNODC and other legal handbooks can provide guidance in this regard which helps bridge the technical-to-legal gap (Afernand, n.d.).

6.5 Limitations

Controlled environment testing. Evaluation was made in a development/test environment and under moderate simulated load. The production-scale performance and inter-agency integration are still unknown.

No live field deployment. Real-world limitations (connectivity at the places, officers performing their tasks, and legal regulations across jurisdictions) were not entirely put to test.

.

Dataset and scope constraints. The prototype was limited to core custody logging and management. No connections with specialized forensic analysis tools and long-term archival systems were made.

Blockchain and advanced features not implemented. Suggestions such as blockchain anchoring and mobile clients are still in the proposal stage to be verified in future work.

Time. It was rather challenging to gather as a group regularly to push the envelope on everything that could be done with this system. This was as a result of the rigorous semester especially with this being our final learning semester for all of us. Nonetheless, we appreciate your deadline extensions and flexibility as they proved vital to our moderate successes with the project.

Learning curve. This is mostly in relation to PostgreSQL as well as the python flask web server. A major factor contributing to this was as stated above, time.

6.6 Final Conclusion

This project accomplished the set objectives by identifying existing process shortcomings, developing automated chain-of-custody logging, producing a secure, role-based web prototype as well as showing measurable enhancements in the reliability and traceability of investigative processes as compared to manual or semi-digital options. Our Digital Evidence Chain of Custody System prototype bolsters transparency and accountability in the handling of evidence and establishes a practical, standards-aware basis for further deployment and research. Large-scale adoption, supported by pilots and compliant with standards such as (ISO/IEC 27037, NIST guidance) while also having legal validation, would almost fully guarantee the chances of the digital evidence handled by our system as being fully admissible in court hence fulfilling our ultimate goal (ISO, 2012).

.

References

Cece, S. (2019, July 21). *Why courts have grown cautious of electronic evidence*. Daily Nation; Nation. https://nation.africa/kenya/news/why-courts-have-grown-cautious-of-electronic-evidence-188180

National Institute of Standards and Technology (NIST). (2020). *Digital evidence integrity and chain of custody best practices.* U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-86

Waweru, J. (2021). Digital forensics challenges in Kenya's criminal justice system. *African Journal of Criminology and Justice Studies, 14*(1), 55–70.

CISA. (2023). *Chain of custody and critical infrastructure systems*. https://www.cisa.gov/sites/default/files/publications/cisa-insights_chain-of-custody-and-ci-systems_508.pdf

Digital Evidence Management for Law Enforcement | NICE Public Safety & Justice. (n.d.). NICE. https://www.nicepublicsafety.com/law-enforcement

Digital Evidence Management: The Definitive Guide. (n.d.). Axon.com. https://www.axon.com/resources/digital-evidence-management-guide

Learn how a digital evidence management system can assist in your operations | Genetec. (n.d.). Www.genetec.com. https://www.genetec.com/products/operations/clearance/case-management

Hytera UK. (2025). Hytera South Africa. https://hytera.co.za/communication-applications/evidence-management

Rwanda's Justice Sector Integrated Electronic Case Management System (IECMS) -. (2024, March 13). Synergy International Systems | Empowering Impact-Driven Organizations. https://www.synisys.com/case-studies/rwandas-justice-sector-integrated-electronic-case-management-system-iecms/

.

Kenyan police commence records digitisation to tackle manipulation. (2023, July 3). Technext. https://technext24.com/2023/07/03/kenya-digital-occurence-books-police/

MURAYA, J. (2020, August 3). *Kenya's National Police Service goes digital*. Capital News. https://www.capitalfm.co.ke/news/2020/08/kenyas-national-police-service-goes-digital/

Kumar, S., & Patel, R. (2023). Implementing advanced encryption techniques for digital forensic systems. Journal of Information Security and Applications, 75(1), 103-118.

National Institute of Justice (NIJ). (2023). Law 101: Legal guide for the forensic expert – Chain of custody and admissibility. U.S. Department of Justice. https://nij.ojp.gov/nij-hosted-online-training-courses/law-101-legal-guide-forensic-expert/pretrial/pretrial-motions/chain-custody

National Institute of Standards and Technology (NIST). (2020). Digital evidence integrity and chain of custody best practices (NIST Special Publication 800-86). https://doi.org/10.6028/NIST.SP.800-86

Laudon, K. C., & Laudon, J. P. (2022). *Management information systems: Managing the digital firm* (17th ed.). Pearson. https://doi.org/10.1017/9781292403272

Pressman, R. S., & Maxim, B. R. (2020). *Software engineering: A practitioner's approach* (9th ed.). McGraw-Hill Education.

Project Management Institute (PMI). (2021). *A guide to the project management body of knowledge (PMBOK® Guide)* (7th ed.). Project Management Institute.

Sommerville, I. (2020). *Software engineering* (10th ed.). Pearson Education.

Satzinger, J., Jackson, R., & Burd, S. (2010). *SYSTEMS ANALYSIS AND DESIGN I N A C H A N G I N G W O R L D FIFTH EDITION*. https://sif.uin-suska.ac.id/wp-content/uploads/2024/02/RPLL-Analisis-Design-Sistem-edisi-7-1.pdf

Mishra, S., Neeraj Kumar Singh, & Rousseau, V. (2016). SoC Design Fundamentals and Evolution. *Elsevier EBooks*, 1–11. https://doi.org/10.1016/b978-0-12-801630-5.00001-3

Luckham, D., Vera, J., & Meldal, S. (1996, August). *Three concepts of system architecture*.
.

Stanford University; Mostly Sunny LLC. https://www.researchgate.net/publication/2820026_Three_Concepts_of_System_Architecture

IBM. (2021, October 18). *Three-tier architecture*. Ibm.com. https://www.ibm.com/think/topics/three-tier-architecture

Waykar, Y. (2015, January). *(PDF) role of use case diagram in software development*. ResearchGate. https://www.researchgate.net/publication/322991847_role_of_use_case_diagram_in_software_development

Yashwant Waykar. (2014). Significance of class diagram in software development. *MANAGELIZATION*. https://www.researchgate.net/publication/322991881_Significance_of_class_diagram_in_software_development

Il-Yeol Song, & Froehlich, K. (1995). Entity-relationship modeling. *IEEE Potentials*, *13*(5), 29–34. https://doi.org/10.1109/45.464652

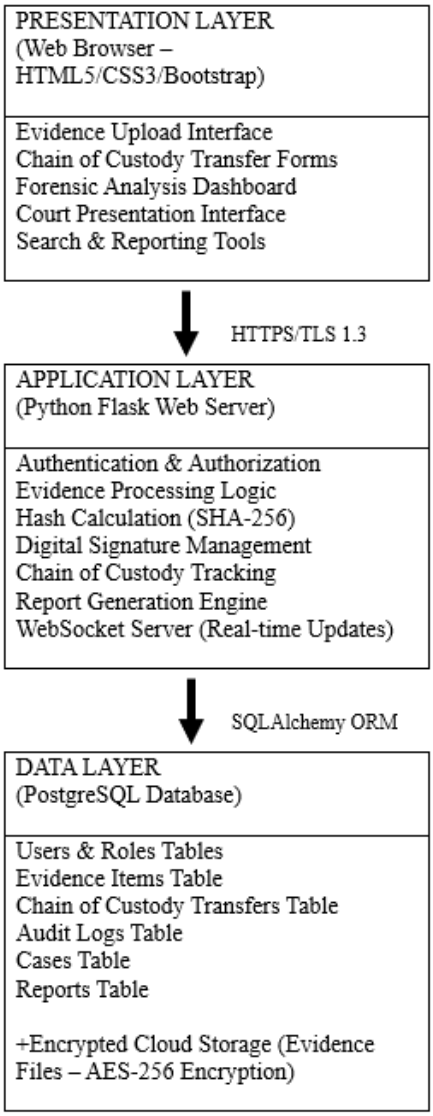
ISO. (2012). *ISO/IEC 27037:2012*. ISO. https://www.iso.org/standard/44381.html

Afernand. (n.d.). *Guidelines for identification, collection, acquisition, and Preservation of Digital evidence*. https://www.unodc.org/e4j/data/_university_uni_/guidelines_for_identification_collection_acquisition_and_preservation_of_digital_evidence.html?lng=en&match=guidelines%20for%20identification

SWGDE: 23-F-004-1.1 Best Practices for Digital Evidence Acquisition, Preservation, and Analysis from Cloud Service Providers | NIST. (2025, April). NIST. https://www.nist.gov/standard/3351

.

Appendices



Old Three-Tier System Architecture diagram.

We opted to switch to node.js + exress.js for the server and MongoDB Atlas for the cloud Database mostly due to time-constraints and learning curve.

.