DIGITAL EVIDENCE PRESENTATION SYSTEM (DEPS) IN ZIMBABWEAN COURTS

JIRAMS

R228074V

MHIKE TAKUDZWA MELINDA

MIDLANDS STATE UNIVERSITY

FACULTY OF BUSINESS SCIENCES

DEPARTMENT OF INFORMATION SYSTEMS

MHIKE TAKUDZWA M

R228074V

4.1

INFO 440

Digital Evidence Presentation System (DEPS) in Zimbabwean Courts JIRAMS

SUPERVISOR: MS TEWERA

Declaration

I, Takudzwa Melinda Mhike hereby declare that the project titled Digital Evidence Presentation System (DEPS) named JIRAMs in Zimbabwean Courts is my original work and has not been submitted, in whole or in part, for the award of any degree or qualification at any other university or institution of higher learning.

This work has been carried out by me under the supervision of Ms. Debra Tewera in the Department of Information Systems and represents my independent effort in research, analysis, and system development.

All sources of information used or quoted in this report have been acknowledged through appropriate in-text citations and a comprehensive reference list, following the Harvard referencing style.

I take full responsibility for the content of this report and confirm that any assistance received

Name: Takudzwa Melinda Mhike

Reg No: R228074V

Signature……...

Date……...

Approval

This is to certify that the project entitled Digital Evidence Representation System named JIRAMS in Zimbabwean courts submitted by Takudzwa Melinda Mhike R228074V meets the regulations governing the award of the Bachelor of Commerce Honors in Information Systems Degree of Midlands State University and is approved for its contribution to knowledge and literal presentation.

Supervisor Signature……

Date……

Acknowledgements

I would like to express my deepest gratitude to my Supervisor Ms. Tewera for her continues guidance, patience and support throughout the development of this project.

I also wish to acknowledge the Judiciary Service Commission of Zimbabwe (JSC) for granting access to relevant information on the Integrated Electronic Case Management System (IECMS), which formed the foundation for this study. My appreciation also extends to the judges, registrars, prosecutors, clerks, and IT staff from JSC High court who participated in interviews and provided critical insights into the challenges faced in managing and presenting digital evidence in court.

Special thanks go to my colleagues and classmates for their encouragement and constructive discussions during the course of this project. Finally, I am profoundly grateful to my family for their unwavering support, understanding, and inspiration throughout this academic journey.

Finally, I acknowledge the divine grace of God for providing me with the health, perseverance and clarity of mind to see this demanding project through to its completion.

Abstract

The Digital Evidence Presentation System (DEPS) is a web-based application developed to improve the management and presentation of digital evidence within Zimbabwean courts. This project is motivated by the limitations observed in the current Integrated Electronic Case Management System (IECMS), which, while effective in digital filing and case tracking, lacks functionality for interactive evidence display and multimedia handling. The system is designed to integrate seamlessly with IECMS, providing features such as secure digital evidence upload, blockchain-based verification for maintaining the chain of custody, and offline functionality to accommodate courts with unstable internet connectivity. The system supports multiple user roles, including judges, prosecutors, registrars, and clerks, ensuring that each participant can access only the functions relevant to their judicial duties. The research follows a structured methodology involving information gathering through document analysis, interviews, questionnaires, and observation of courtroom procedures. Analysis of the existing system highlights several weaknesses, including unreliable connectivity, poor user experience, and the absence of multimedia presentation tools. DEPS addresses these challenges through an interactive, scalable, and secure platform built using ReactJS, Python, SQLite, HTML, and CSS technologies. The implementation of DEPS is expected to enhance transparency, improve efficiency in court proceedings, and strengthen the authenticity and reliability of digital evidence presentation. The system provides a sustainable, context-appropriate solution for the Zimbabwean judiciary ongoing digital transformation agenda.

Table of Contents

List of Figures

List of Tables

List of Abbreviations

DEPS ……. Digital Evidence Presentation System

IECMS ……. Integrated Electronic Case Management System

JIRAMS …… Judicial Information and Records Management System

ICT …… Information and Communication Technology

RBAC ……. Role-Based Access Control

VPN ……...……...…Virtual Private Network

CSV ……. Comma-Separated Values

SQL ……Structured Query Language

UI ……. User Interface

API ……Application Programming Interface

ERD ……. Entity Relationship Diagram

DFD ……. Data Flow Diagram

IDS ……. Intrusion Detection System

NDS1 ……. National Development Strategy 1

UNECA ……...United Nations Economic Commission for Africa

HMCTS ……...……Her Majesty's Courts and Tribunals Service

TAM …… Technology Acceptance Model

LAN ……. Local Area Network

NIST ……. National Institute of Standards and Technology

REST ……Representational State Transfer

HTML ……. Hypertext Markup Language

CSS ……Cascading Style Sheets

AI ……. Artificial Intelligence

PK ……. Primary Key

FK ……...Foreign Key

SQLITE ……...Structured Query Language Lite

IDPS ……...Intrusion Detection and Prevention System

DF ……. Diffusion of Innovation

Introduction

This project the Digital Evidence Presentation System is developed for submission to the Judiciary Service Commission of Zimbabwe (JSC) through Midlands State University in fulfilment of the requirements of the award of the Bachelor's Degree in Information Systems.The Judiciary Service Commission (JSC) has been leading the digital transformation of Zimbabwe's courts through the implementation of the Integrated Electronic Case Management System (IECMS). IECMS successfully digitalizing filing, scheduling, and case tracking, it does not fully support the dynamic presentation and authentication of digital evidence. This limitation affects the efficiency, accuracy, and fairness of judicial proceedings, especially in cases involving multimedia or forensic evidence.

The DEPS project is developed to complement the IECMS by introducing a secure, scalable, and user-friendly platform for digital evidence handling. The system integrates blockchain verification for maintaining the chain of custody, supports multimedia playback and annotation, and offers offline functionality to cater for courts in areas with poor connectivity. The goal of this project is to provide a sustainable solution that enhances the integrity and accessibility of digital evidence within Zimbabwe's judiciary.

Chapter 1: Introduction

1.1 Introductions

The digitalization of the judicial system has come to play a pivotal role in making the justice system efficient, transparent and accessible. Courts across the globe are replacing paperwork with combined digital regimes that enable proper casework and evidence management (Apau et al., 2020). The process of e-justice in Zimbabwe started with the launch of the Integrated Electronic Case Management System (IECMS) that initiated a significant change of the way courts receive, store and access case information. Nevertheless, even in the context of this development, a number of issues continue to exist, such as the inability to manage the evidence, the complexity of systems, and the user awareness level (Poshai & Vyas-Doorgapersad, 2023).

In order to deal with them, this project suggests the Digital Evidence Presentation System called Judicial Information and Records Management System (JIRAMS) which is a digital platform aimed at simplifying the court processes and making them more convenient and reachable to the civilians, prosecutors, judges and registrars. JIRAMS provides the option of digital filing of cases, uploading of evidence, real time monitoring of a case, and automatic communication of the principal stakeholders. It is designed to make the operations more efficient, increase the transparency and decrease the administrative delays by providing role access, secure records management, and user-friendly interfaces. In this chapter, the background of the study, the problem under consideration, goals and objectives, methodology used in the research, and importance of the system to the Zimbabwean judiciary is presented.

1.2 Background of the Study

Global Context

The modernization of the judicial systems digitally has become a trend in the modernization of the public sector across the globe. Due to various reasons, many nations are embracing the use of technologies in court proceedings to increase transparency and backlog reduction, as well as facilitating access to justice. In the period between 2020 and 2021, the world research conducted by showing an increase of high-income countries in the adoption of digital court reforms up to 88% and middle and low-income countries recorded significant increases. The world market of digital evidence management is estimated at about USD 8.6 billion by 2024 and also estimated to rise to USD 14.5 billion by 2030, showing more investment in justice technology. Evidence management, legal documentation and decision-making in jurisdictions are also being further revolutionized by artificial intelligence, data analytics and blockchain applications. Nevertheless, the world is unequal because of digital inequalities, cyber-crimes, and the gradual response of laws to new technologies.

Regional Context (Africa)

The judicial systems in Africa are slowly adopting the digital transformation as a way to tackle their cases of inefficiencies and increase the reach of justice. In recent evaluations, it has been revealed that currently more than 20 African nations have virtual court systems in operation and above 30 countries have e-filing and case-track systems. The African Union is one of the organizations that place significant importance on good governance and the rule of law as an important pillar of sustainable development, which promotes the adoption of digital tools of justice through Agenda 2063. In spite of these developments, the major challenges encountered in most African countries include poor ICT infrastructure, expensive technology, low level of digital literacy, and unreliable data protection systems. A lot of court systems use hybrid systems which are manual and digital leading to inconsistent services delivery. However, current efforts in Kenya, South Africa and Rwanda illustrate that judicial efficiency and accountability can go a long way with strategic investment in technology and capacity building.

Local Context (Zimbabwe)

The Implementation of the Integrated Electronic Case Management System (IECMS) by the Judicial Service Commission (JSC) in Zimbabwe was a significant step of the process of modernizing court proceedings in the country (2022). The system brought about the use of digital filing, case trackings through the internet, virtual hearings to enhance efficiency and transparency. Assessments of the IECMS reveal that there is improvement in the case digitization, but in addition, there are still outstanding obstacles such as the lack of reliable internet connectivity, lack of user training, and lack of system capabilities to manage multimedia evidence. Research also indicates that less than 50 percent of households in Zimbabwe own smartphones and that most of the phones lack processing power which restricts access by the rural population. The JSC has also detailed the strategy of completely digitalizing the court records by 2026 with the help of continued collaboration with local ICT agencies and the international development program. In spite of these advancements, the judiciary still struggles with the security risk of data, complexity of the system and rates of uneven adoption among the stakeholders.

Rationale for the Project

The given project is dedicated to the creation of the Judicial Information and Records Management System (JIRAMS), an online platform that is expected to supplement and improve the current IECMS framework. The system is aimed at effective management of the digital evidence, safe data storage, and enhanced interaction between the judicial officers and civilians. JIRAMS is able to resolve the infrastructural and operational issues that impede the delivery of justice by using features like offline availability, role based authentication, and presentation of evidence in the form of multimedia. Moreover, it is consistent with the National Development Strategy 1 (NDS1) and National ICT Policy Framework that facilitate e-governance and digital innovation at the institutions of the state. The design of the system is informed by the best practices in the world and the region to guarantee a sustainable and Zimbabwe-appropriate context of judicial modernization.

1.3 Problem Definition

Despite Zimbabwe's efforts to digitalize the judiciary, several problems persist in the current system:

- **Limited functionality** in managing and presenting multimedia evidence such as videos, images, and forensic data.
- **System complexity**, which discourages adoption by non-technical users, leading to underutilization.
- **Infrastructural limitations**, including intermittent internet access and unstable power supply in rural courts.
- **Inefficient communication** between civilians, prosecutors, registrars, and judges.
- **Security and authentication gaps** that may compromise the integrity of case records and evidence.

These issues have resulted in continued delays, human errors, and mistrust in digital judicial processes. There is, therefore, an urgent need for a user-friendly, secure, and role-based digital system that facilitates efficient case and evidence management across all court levels the JIRAMS platform.

1.4 Aim

To design and implement to JIRAMS to enhance efficiency, transparency, and accessibility in Zimbabwe's judicial processes through secure digital record management and role-based communication.

1.5 Objectives

1. Establish an effective web based system whereby civilians can file cases online and provide supporting evidence easily.
2. Embark on an effective authentication and role-based access control solution that would secure and differentiate access to all court users.
3. Establish specific modules on prosecutor, judges and registrar to ensure proper management of cases and to update on the current progress.
4. Introduce a sophisticated digital evidence management capability which provides an ability to upload, retrieve and present multimedia evidence.
5. Allow users to monitor case statuses, hearing schedules, and judgments live, which will improve accessibility and transparency.
6. Increase the system of communication and transparency between the judiciary and civilians by using automation in alerts and notifications.
7. Secure, protect and ensure the integrity, privacy and security of the judicial data with highly effective encryption programs and regulated control systems of database access.

1.6 Instruments and Methods

1.6.1 Development Tools

The creation of Judicial Information and Records Management System (JIRAMS) is based on the integration of the new, open-source technologies facilitating scalability, security and facilitating integrations. Response, dynamic, and accessible user interfaces across devices are built on the ReactJS, HTML, and CSS frontend to provide responsiveness and dynamicity. Python allows backend application using FastAPI framework because it is fast, reliable and also supports asynchronous operations which are essential in serving multiple user requests at the same time. SQLite or MySQL Lite are used to handle data storage and are both lightweight and efficient relational databases that can be used in small to medium systems. RESTful APIs facilitate integration between layers of the system to make data flow between the frontend and the backend

smooth. Bootstrap is utilized in interface styling and layout consistency, whereas GitHub is utilized as a version-control system used in collaboration and project management.

Table 1.6.1 Shows the development tools

Component	Technology \Tool
Frontend	ReactJS HTML CSS
Backend	Python (Fast API framework)
Database	SQLite \MySQL Lite
Integration	RESTful APIs
Styling and UI	Bootstrap
Version Control	GitHub

1.6.2 Methodology

The project will also use the Agile Software Development Methodology that encourages an iterative process of development, flexibility, and constant user engagement during the implementation and design stages. This will enable a gradual process of improvements, so improvements are made directly based on the user feedbacks of the current generation. The system is modularized to accommodate the key user functions, such as civilian, prosecutor, judge, and registrar and their respective functions and access rights. Frontend is created using ReactJS and CSS to offer an easy interface to the various users, and the backend is created using Python FastAPI to handle authentication, authorization, and system logic. Data is safely stored in relational database and client-server communication is based on RESTful API, which means that data exchange and sustainability is efficient. This methodological structure will provide the system with the flexibility to be scaled and adapted to the changing needs of the users and the institution.

1.6.3 Data Collection

In order to make sure that the system is consistent with the realities of the functioning of judiciary, there are several data-collection methods used. Court personnel (registrars and clerks) are interviewed to understand the current process, problems, and places where automation is needed. The analysis of documents is performed in order to examine the existing judicial practices and ICT policies, case-management structures in order to be compliant and compatible with the systems.

Potential users (prosecutors, lawyers and civilians) are provided with questionnaires on which their views on the usability expectations, desirable features, and any obstacles to adoption are sought. These approaches when combined together will facilitate both qualitative and quantitative understanding that will make sure that JIRAMS is based on the real requirements of its clients.

1.7 Delimitations and Limitations

This research paper mainly targets the lower and the higher courts of Zimbabwe that are currently undergoing the transition of digital case-management systems. The scope is also restricted to digitization of judicial processes and records as opposed to legislative changes or reviews of criminal justice policies. This is aimed at coming up with a system that will improve operational efficiency as opposed to changing legal frameworks.

There are however, a number of limitations to the project. The technical infrastructure of the rural courts is also limiting the implementation due to an uneven distribution of computer literacy between judicial officers and civilians. There are also challenges that are presented by the budgetary constraints that are facing a nationwide implementation of the system. In addition, characterized by intermittent internet connectivity in certain regions, the system may cause disruption in the real-time capabilities of the system, particularly when uploading hearings or evidence. These constraints are noteworthy but offer direction on a gradual implementation and the development of the system in the future.

1.8 Feasibility Analysis / Proposed Budget

1.8.1 Technical Feasibility

The technologies chosen are ReactJS, Python, and SQLite, which are open-source, lightweight, and platform-independent, implying low setup and low complexity. The system is capable of utilizing the standard computing equipment without high-end infrastructure; this makes it applicable in the deployment of different court settings. Moreover, the modular architecture can be scaled, and the extra functionality like mobile access, AI-based analytics, or blockchain audit can be added at the latter stages without significant redesign.

1.8.2 Economic Feasibility

An analysis of the proposed system reveals that it can be economically viable in terms of long-term cost savings due to the minimization of paperwork, higher precision of data and quicker handling of cases. The overall cost of development and deployment is set at USD 2,200 that incorporates software development, hosting, equipment, and training of the users. The break down is indicated by Table 2 below.

Table 1.8. 2 Shows the project budget

Item	Description	Estimated Cost ($)
Software Development	Design Coding and Testing	1,200
Hosting and Maintenance	Cloud hosting and backups	300
Training and Workshops	System user training	200
Equipment	Basic computers and accessories	500
Total Estimated Cost		2,200

The long-term benefit includes reduced paperwork, improved data accuracy, and faster case resolution ultimately saving costs for the judiciary.

1.9 Justification and Rationale

To demonstrate the validity of the assertion, one must first acknowledge the definition of a human being and human sexuality along with the historical background of human sexuality. In order to justify and rationalize the assertion, it is crucial to accept the definition of human being and human sexuality and the history of human sexuality.

JIRAMS has been developed due to the necessity of enhancing the accessibility, efficiency and transparency of judicial processes in Zimbabwe. The current systems like IECMS, though prominent, do not support multimedia evidence, category inter-role cooperation, and off-line access. JIRAMS will be used to fill such gaps by offering automated processes, safe online storage, and instant communication between the court users and the general population.

In addition, the project is in line with the National Development Strategy 1 (NDS1) in Zimbabwe that promotes digital transformation and e-governance in all government institutions. The judiciary can also utilize the open-source technologies to save a lot of operation costs without compromising the quality of service provision. The system further makes Zimbabwe a judicial innovation leader in the region, which is also engaged in research and digital justice development in Africa.

1.10 Work Plan

The project work plan provides the main stages of development such as a system analysis, design, implementation, testing, deployment, and user training. The duration of each stage is assigned a certain period with tasks to be accomplished in order to deliver it on time and guarantee quality. The progress will be monitored through agile sprints, feedback will be implemented, and an iterative improvement will be achieved. Post deployment monitoring and maintenance is also included into the plan to maintain the reliability and sustainability of the system. The schedule, timelines and deliverables will be in the Gantt chart.

1.10.1 Expected Timeline

Table 1.10.1 Shows the expected project timeline

Activity	Duration	Start Date	End Date	Month	Description
Requirements gathering & analysis	2 weeks	01 Feb 2025	14 Feb 2025	February 2025	Collect user requirements through interviews, document reviews, and system analysis.
System design & prototyping	3 weeks	15 Feb 2025	07 March 2025	February - March 2025	Develop data flow diagrams, ERDs, and initial user interface mock-ups.

Backend and database development	4 weeks	08 Mar 2025	04 Apr 2025	March – April 2025	Build Python (Fast API) backend, set up SQLite/MySQL Lite database, and define APIs.
Frontend development & integration	4 weeks	05 Apr 2025	02 May 2025	April – May 2025	Develop ReactJS interfaces, integrate frontend with backend APIs, and implement UI design.
Testing and debugging	4 weeks	03 May	30 May 2025	May 2025	Conduct unit, integration, and user acceptance testing. Address bugs and refine modules.
User training and documentation	3 weeks	31 May 2025	20 Jun 2025	June 2025	Prepare system manuals, conduct training sessions for court staff and users.
Pilot Deployment & Evaluation	4 weeks	21 Jun 2025	18 Jul 2025	June – July 2025	Deploy JIRAMS on trial basis in selected courts and gather feedback for adjustments.
System Optimization & Enhancement	4 weeks	19 July 2025	15 Aug 2025	July 2025	Improve performance, enhance user experience, and fix issues from pilot testing
Final deployment and evaluation	2 weeks	16 Aug 2025	29 Aug 2025	August 2025	Launch final version across pilot sites and initiate full monitoring.
Project Evaluation & Reporting	2 weeks	01 Sept 2025	15 Sept 2025	September 2025	Conduct post-implementation review, prepare final project report, and submit documentation.

Gantt Chart

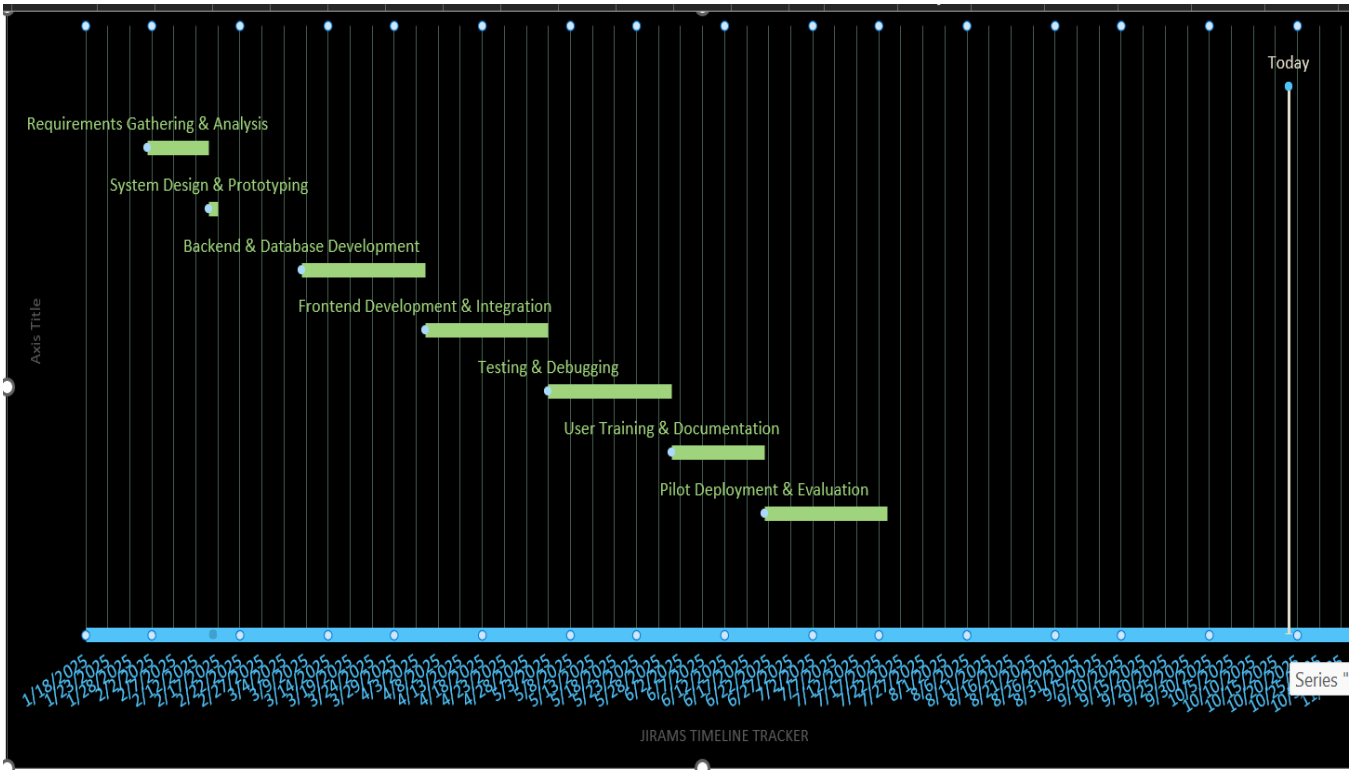


Figure 1.10.1 JIRAMS Gantt Chart

1.11 Conclusion

In this chapter, an introduction to the Judicial Information and Records Management System (JIRAMS) has been provided, and this has included the purpose of JIRAMS, background and purpose of the system, problem statement, objectives and methodology. The project will focus on eliminating the inefficiency in the Zimbabwean judiciary by offering them a digital case-management system, evidence-processing system, and inter-role communication. JIRAMS will also be efficient, accessible, and secure when using ReactJS, Python, and SQLite. This will be followed by the discussion on the system analysis, design, implementation and evaluation strategies in the following chapters so that the project is successful.

Chapter 2: Literature Review

2.1 Introduction

The chapter provides literature review of the available literature on digital judicial management systems, electronic records management, and the adoption of information system in judicial institutions. It analyzes past and present studies that lay the basis of design and implementation of Judicial Information and Records Management System (JIRAMS). The review includes both international, regional (African), and national (Zimbabwean) contexts, with the shifts of digital justice systems and the technological, operational, and social conditions of their success.

The review also establishes the efforts made by the earlier studies in dealing with the issues of case management, presenting evidence, and interaction with the user in the courtroom. It creates the conceptual and theoretical foundation of JIRAMS and determines the knowledge and technology gap that this project would address.

2.2 Digital Transformation in Judicial Systems

Digital transformation is described in judicial systems as a fundamental change in the manual operational processes, which are paper based to integrated processes wherein technology is at the core. It includes computerization of filing cases, evidence, virtual hearings, and electronic communication between legal participants. Courts across the world are embracing technology to enhance transparency, reduce backlog of cases, and enhance accessibility by the citizens. The United Nations Economic Commission for Africa (UNECA, 2022) stated that African countries increasingly use e-justice platforms within the context of further governance reforms. According to the World Bank (2021), the efficiency of institutions increased with the use of digital justice systems because they provide the ability to base a decision on the data, eliminating bureaucratic slowness, and conducting hearings remotely, which became necessary during and after the COVID-19 pandemic.

In the world, a number of nations have made achievements in judiciary digitalization. The eLitigation of Singapore involves the merging of case filing, scheduling and even the sharing of

documents in a single online platform that is open to all the interested parties. The case workflow modernization initiative of the United Kingdom, the Her Majesty Courts and Tribunals Service (HMCTS), has also adopted the use of artificial intelligence, electronic document exchange, and remote hearings (Tan and Lee, 2020). These platforms show that the digital transformation is not only about automation but it promotes institutional transparency and citizen participation and increases accountability of judicial officers. These systems have been successful and this highlights the need to have good policy frameworks, proper infrastructure and constant capacity development among the stakeholders.

The trend of judicial digitalization is growing worldwide, and the new economies use open source and cloud computing to become as cost-efficient as possible. Latin America and southeast Asian courts have introduced mobile friendly online portals where their citizens can file complaints and follow cases through the internet. There are also cross-border judicial data-sharing initiatives that have been initiated by the European Union to facilitate the co-operation between the member states. Nevertheless, the digital justice ecosystem continues to experience global challenges, such as the lack of cybersecurity, interoperability, and disparities in the population access to technology. In this way, although digital transformation is a catalyst of modernization in the judiciary, it cannot be successful without a comprehensive approach to planning and long-term investment in infrastructure and human resources.

In Africa, the trend of judicial digitalization has been moving towards less pilot projects and more institutionally based e-justice models. In Kenya, the e Filing System can be used to file cases by litigants and lawyers online, and in South Africa, evidence presentation and courtroom processes are digitized on the CaseLines platform. On the same note, the Judiciary Information Management System (JIMS) in Nigeria has also implemented digital cause lists, Web-based judgment repositories, and document tracking systems (Wekesa, 2023). These systems are indicative of the increased interest of Africa in using technology to deliver justice, according to the African Union Agenda 2063 of ensuring good governance and access to justice. However, the problem of poor ICT infrastructure, irregular investment, and limited levels of digital literacy among legal staff continue to affect most countries (Apau et al., 2020). Consequently, effective leadership and

capacity-building initiatives to reduce the technical and institutional gaps determine the sustainability of e-justice systems.

The Integrated Electronic Case Management System (IECMS), which the Judicial Service Commission (JSC) implemented in Zimbabwe in 2022, can be seen as the first step towards digital justice reform. It enables electronic filing, online tracking of cases, and management of documents electronically to improve the efficiency and transparency (Judiciary Service Commission of Zimbabwe, 2023). However, it is found out that the system encounters serious issues especially when animating multimedia evidence including video and audio files, server congestion with limited bandwidth, and user training uniformity (Muzondo & Moyo, 2023). The long-term vision of the JSC is the growth of IECMS to provincial courts of all provinces and the implementation of digital payment systems in order to enhance communications with the citizens. Nonetheless, these attempts show that more local solutions are needed that take into account infrastructure differences and end-user limitations.

There are other African countries, other than Zimbabwe, that present lessons of how incorporation of digital court systems can be done. The example of eJudiciary Project in Uganda and eRecords Management Initiative in Botswana demonstrates that long-term success depends on the constant stakeholder interaction, software adaption on a local level, and alignment of the legal framework (Mosweu & Kenosi, 2018). In the meantime Ghana and Rwanda have implemented open-source judicial information systems to minimize reliance on the costly proprietary systems and promote innovation (Amankwah, 2022). Nevertheless, change resistance, lack of user awareness and sporadic funding still hinder the transformative ability of these systems. JIRAMS builds on these experiences in the continent through its focus on user-friendly design, evidence protection, and interwoven training modules to increase the adoption and sustainability of the system in the Zimbabwe judiciary.

2.3 Digital Judicial Systems in Zimbabwe and Africa

Zimbabwe is currently implementing the Integrated Electronic Case Management System (IECMS), which digitises the judiciary through e-filing, online case tracking, and document management (Judiciary Service Commission of Zimbabwe, 2023). IECMS represents a major step

toward judicial modernization, yet it faces challenges related to bandwidth limitations, training gaps, and difficulties in managing multimedia evidence (Muzondo & Moyo, 2023).

Other African nations are experimenting with digital court systems. Uganda's eJudiciary Project and Botswana's eRecords Management Initiative show that sustainable e-justice implementation depends on consistent stakeholder training and integration of local legal procedures (Mosweu & Kenosi, 2018). Ghana and Rwanda leverage open-source technologies for case management to reduce costs and dependency on proprietary platforms (Amankwah, 2022).

These African experiences reveal that while digital transformation in justice delivery is gaining ground, systems often face resistance due to poor change management and limited user awareness. JIRAMS builds upon these lessons by integrating user-friendly interfaces and capacity-building initiatives to ensure system adoption.

2.4.1 Comparative Analysis of Existing Systems

The comparative analyses of different information management systems used by judicial systems offer useful information on the design philosophy of the systems, their functionality, and the effects on users. Although the all systems are designed to increase access to justice, they tend to be efficient under circumstances based on factors of governance, availability of infrastructure, and policy backup. Table 2.1 below highlights the overview of some of the international and African digital court systems, their characteristics, modes of implementation and their technological architecture. The discussion assists in locating the suggested JIRAMS proposal solution in the context of judicial innovation in the world.

Table 2. 3.1 Shows a comparison of different esystems

System / Country	Key Features	Technology Stack	Strengths	Challenges
eLitigation (Singapore)	Online filing, e-payments, digital hearings	Java-based web portal	Seamless user experience, real-time access	High setup and maintenance cost
HMCTS Reform (United Kingdom)	AI-assisted scheduling, online dispute resolution	Hybrid cloud & AI tools	Strong efficiency and transparency	Data privacy and integration challenges
CaseLines (South Africa)	Evidence upload, digital bundles, virtual courtrooms	Web-based proprietary platform	Reduced case delays	Licensing costs and limited local adaptation
JIMS (Nigeria)	E-filing, case tracking, digital notifications	PHP/MySQL	Improved workflow management	Infrastructure and literacy constraints
IECMS (Zimbabwe)	E-filing, online case tracking, document management	PHP/SQL server	Enhanced record access	Multimedia handling limitations
Proposed JIRAMS (Zimbabwe)	Blockchain-backed evidence storage, role-based access, offline capability	Python (FastAPI), ReactJS, SQLite	Secure, scalable, open-source	Requires training and infrastructure support

The comparative analysis reveals that although digital justice systems around the world are characterized by similar objectives, their success in the implementation process depends on the

socio-economic background and the maturity of the policy. Systems such as the eLitigation of Singapore are good due to their strong integration into the system by its users and the African systems are cheap and localized. JIRAMS builds on these understandings by utilizing best practices all over the world and applying them to the local contexts of the judiciary in Zimbabwe. It uses open-source and a modular design to mitigate notable shortcomings like multimedia evidence management, offline access, and data security, to provide a more inclusive and sustainable digital justice system.

2.4.2 Insight of Comparative Analysis

A comparative analysis of digital judicial systems shows that in developing countries, biased or mixed digital systems are frequently used because of financial and technical constraints (Nhemachena, 2024). Although the developed nations like Singapore and the United Kingdom are building the full e-justice system where artificial intelligence and cloud-based data management are implemented, most of the developing states use the modular and cost-effective solutions to ensure accessibility and flexibility (Tan and Lee, 2020). This gap is mostly explained by infrastructural gaps, such as a low level of broadband penetration, unreliable electricity availability, and the lack of technological literacy in the end-users (Apau et al., 2020). Consequently, hybrid structures comprising of online and offline business have been common in Africa and have allowed judicial continuity on the verge of connectivity issues (Etta & Parvyn-Wamahiu, 2022).

The Judicial Information and Records Management System (JIRAMS) proposed is a direct solution to these system challenges in the sense that it has adaptive mechanisms embedded into its architecture. It includes an offline backup that enables continuous access to records and case updates even when the internet is unavailable, which is essential in the semi-urban and rural courts in Zimbabwe where the quality of network connectivity is often poor (Judiciary Service Commission of Zimbabwe, 2023). Moreover, the data processing and localization of the server of JIRAMS is lightweight to the functionality of low-resource hardware and minimizes the reliance on expensive cloud computing infrastructures (Muzondo & Moyo, 2023). Such design solutions are based on the best practices suggested by local digital justice frameworks, which highlight an inclusive, scalable, and sustainable ICT integration in judicial organizations (UNECA, 2022).

2.5 Theoretical Framework

The design, implementation, and evaluation of JIRAMS have its foundation in the existing information systems theories which offer a conceptual framework of understanding the process of technology adoption and system success. These are Technology Acceptance Model (TAM), DeLone and Mclean Information Systems Success Model and the Diffusion of Innovation Theory developed by Rogers. All these theories explain the behavioral, technical, and institutional aspects of technology adoption in the justice sector. By incorporating these frameworks, JIRAMS will neither be technically effective only, but also socially recognizable and viable operationally.

2.5.1 Technology Acceptance Model (TAM)

The Technology Acceptance Model (TAM) that was introduced by Davis (1989) and later improved by other researchers (Venkatesh and Bala, 2021) is based on the assumption that Perceived Usefulness (PU) and Perceived Ease of Use (PEOU) are the main determinants of new technology adoption. On the digital judicial system, these constructs define the perception of the technology as useful and easy to use among the judicial personnel and civilians. Chirume and Musara (2022) claim that the aspect of perceived usefulness in the e-justice systems is directly connected with the operational efficiency, whereas the perceived ease of use is directly associated with the intuitive nature of system interfaces and the supply of training.

JIRAMS also realizes these constructs by making its interfaces user-friendly, easy to navigate and to different judicial functions like judges, registrars and prosecutors. Addition of automated processes, guided forms and role-based dashboards have a direct positive impact on the perceptions of ease and efficiency by the users. Moreover, in line with Venkatesh and Bala (2021), training sessions on the system will be conducted regularly as well as through practical demonstrations to enhance user confidence and minimize resistance to change. Therefore, TAM is a behavioral perspective that describes the impact of perceived value and usability on the level of acceptance and continued use of JIRAMS by the Zimbabwean judiciary.

2.5.2 DeLone and McLean Information Systems Success Model

DeLone and McLean Information Systems Success Model, first published in 1992 and revised in 2003, is still among the most successful models of assessing the performance of digital systems (DeLone and McLean, 2003). It singles out System Quality, Information Quality, and Service Quality as the determinants of User Satisfaction and Net Benefits (Petter et al., 2020). These

variables, in the framework of e-justice systems, are the credibility of digital platforms, quality of the legal data and timeliness of the technical support services.

In the case of JIRAMS, quality of systems is ensured by Python using the FastAPI framework which is fast, secure and scalable. The quality of the information is ensured by real-time validation, the structured way of database management and the correct indexing of the cases, which minimize the possibility of human error in data entry. Technical support protocols, user manuals, and feedback channels strengthen service quality improvement and guarantee its continued improvement (Mutisi, 2023). The application of this model would offer an evaluative system to determine system effectiveness after implementation. JIRAMS will be evaluated by success indicators: the reduction in case turnaround time, better accessibility, and user satisfaction, which will be aligned with the results showed by Amani and Gicharu (2021) that quality dimensions are directly correlated with the level of trust towards digital courts.

2.5.3 Diffusion of Innovation Theory

Diffusion of Innovation Theory The diffusion of innovation theory is a theory that explains the process involved in rallying an innovation to the target population and the maintenance of that acceptance.

Diffusion of innovation Theory by Rogers (2003) is a theory that describes the spread of innovations through the social systems over time. It identifies five relevant attributes of adoption namely relative advantage, compatibility, complexity, trialability and observability (Rogers, 2003). In the judiciary, these dimensions dictate the ease with which the digital platforms are adopted by the judges, registrars, and other supporting staff. Research within African institutions of justice has shown the ease with which systems are adopted when they have apparent benefits over manual processes, consistent with current business processes, and whose pilot phase can be easily pursued in controlled settings (Mosweu & Kenosi, 2018).

JIRAMS conforms to this theoretical understanding in its focus on relative advantage with the improvement of efficiency, its compatibility with existing judicial practices, and its testability through the pilot test in a few locales. Moreover, the advantages of the system will be evident in such measurable indicators as the decrease in the number of cases backlog and enhancement of the

communication between stakeholders. In line with Mokgoro (2021), the judicial capacity will be developed through a participatory training approach to encourage behavioral change in the judiciary. Through the operationalisation of the theory proposed by Rogers, JIRAMS enhances the chances of the successful adoption and institutionalisation

2.6 Technological Trends in Judicial Information Systems

The recent development of web technologies, cybersecurity, and data analytics has had a major impact on the development of judicial information systems. Chirume and Musara (2022) noted that digital courts are becoming more and more dependent on modern web-based platforms that enable them to be interoperable with national databases and e-government systems. ReactJS frameworks have been chosen in frontend development because they are fast, scalable, and maintainable, as well as FastAPI in the back-end, which is fast, scalable, and maintainable. Likewise, SQLite and MySQL databases can be applied as the lightweight and distributed storage that will decrease the reliance on big centralized servers (Mutisi, 2023). These inventions make judicial systems more flexible and resilient, which makes them adaptable according to the local infrastructural conditions.

There are also new issues related to the security and privacy of data which are equally important. In legal systems that are shifting towards computerised systems, confidentiality and integrity of case information take centre stage (Amani and Gicharu, 2021). Role-Based Access Control (RBAC), multi-factor authentication and encryption of data protect the chances of sensitive information being accessed or altered by unauthorized personnel. Remote access and scalability represent opportunities of cloud computing, but serious issues exist regarding data sovereignty, especially in government organizations (Apau et al., 2020). To balance security, accessibility, and performance, JIRAMS implements a hybrid storage architecture, which is the deployment of local servers with optional cloud backup (later). This is in line with the recommendation by the UNECA (2022) that the African e-justice system must use context-specific technologies that will improve transparency and reduce privacy threats

2.7 Implementation Challenges and Best Practices

Digital judicial systems can only be successful when it is not only technologically ready but also institutional capacity and human adaptability. Research in sub-Saharan Africa has shown that the major obstacles to successful implementation are insufficient change management, lack of funds,

and unwillingness of the judicial officers who have been used to working with papers (Etta & Parvyn-Wamahiu, 2022). Mokgoro (2021) indicates that early participation of stakeholders and participatory design largely minimize the resistance since the users develop a sense of ownership of the system. Likewise, Mosweu and Kenosi (2018) note that it is crucial to have continuous training and technical support to improve system knowledge and sustainability.

In trying to overcome these challenges, JIRAMS would practice the incremental implementation plan consisting of pilot courts, then extended to more superior courts. In every stage, there would be capacity-building workshops, practical demonstrations and user feedback sessions to facilitate continuous improvement. Moreover, data protection policies are transparent and in tandem with the National ICT Policy Framework (2021) of Zimbabwe in order to adhere to the legal requirements as well as best practices in cybersecurity. Regional application experience shows that technological innovation, institutional learning, and policy coherence are the key factors that facilitated the success of e-justice (Wekesa, 2023). JIRAMS, thus, is not merely a digital solution, but an all-inclusive approach to sustainable judicial modernization not only in Zimbabwe, but in Africa as well.

2.8 Gaps Identified

Table 2.8.1 summarises the key gaps identified from the reviewed literature and how JIRAMS addresses them.

Table 2.8.1 Research Gaps and JIRAMS Responses

Problem Identified	**Gap in Existing Systems**	**JIRAMS Response / Solution**
Ineffective evidence management	Existing systems lack multimedia and digital evidence support	JIRAMS incorporates a secure digital evidence upload and storage module
Limited offline access	Systems depend on stable internet	JIRAMS includes offline functionality with synchronisation capability
Poor inter-role communication	Minimal interaction between court users	JIRAMS provides an internal communication and notification system
Weak data security	Limited encryption and authentication mechanisms	JIRAMS implements RBAC, encryption, and two-factor authentication

User resistance and lack of training	Minimal capacity development initiatives	JIRAMS integrates user-friendly interfaces and continuous training programmes

The evaluation of the current digital judicial systems indicates that, though significant milestones have been achieved in the area of e-justice adoption, there are still significant gaps in the field of critical issues related to computerized judicial systems in both technical and institutional terms. Research on the African continent also suggests that the majority of the digital court systems are based on electronic filing and document management but do not offer effective mechanisms of multimedia evidence processing and inter-role cooperation (Wekesa, 2023; Apau et al., 2020). In some cases (like South Africa, CaseLines, and Kenya, e-Filing), the online submissions are practical, but not yet developed with the sophisticated digital evidence modules, allowing video, audio, or forensic evidence, which are becoming a crucial part of litigation today (Chirume and Musara, 2022). Moreover, reliance on constant access to the internet restricts availability in remote or bandwidth areas emphasized by UNECA (2022), generating differences in digital justice engagement.

Similarly, empirical evidence shows that there are still shortcomings in security of data, authentication and training of users, which compromise trust and sustainability of e-justice systems. According to Amani and Gicharu (2021), a significant portion of African courtroom systems do not have advanced cybersecurity measures, including role-based access control (RBAC) and two-factor authentication, which exposes confidential court information to attacks. Besides, insufficient capacity-building efforts tend to lead to user resistance and low adoption, particularly among less ICT-literate court officers (Etta and Parvyn-Wamahiu, 2022; Mokgoro, 2021). These loopholes indicate that, although technology tools have been developed, their adoption into the judicial processes is still disjointed and not in tandem with the requirements of digital justice transformation that are holistic.

As a reply, JIRAMS has been conceptualized as an informative, adaptable, and secure platform, which in a systematic way fills these gaps. It incorporates multimedia evidences management system that can store, encrypt and retrieve diversified digital format, and meet the requirements of evidentiary guidelines. Its off-line capability enables it to operate even when the connection is low

and once the network returns, it automatically syncs, a feature suggested to be sustainable in the developing environment (Nhemachena, 2024). Also, JIRAMS has an internal communication and notification system designed to improve coordination among registrars, judges, prosecutors, and civilians with the help of constant training of its users and the participatory feedback loop. With these features, JIRAMS goes beyond documentation and filing to provide a multifaceted, interdisciplinary, and strong digital justice solution that is in line with the digital transformation agenda in Africa (Judiciary Service Commission of Zimbabwe, 2023; UNECA, 2022).

2.9 Conclusion

In this chapter, the author is able to provide an exhaustive literature review pertaining to the digital judicial systems domain, not only on the trend at the international level but also in the regional experience of the use of electronic case management. There is an analysis that much progress has been done in using the e-justice systems but it has experienced a number of limitations, especially in the developing countries like Zimbabwe where there is connectivity, cost, and digital literacy issues.The literature review identifies the gaps in the existing systems and matches them with the solutions proposed by JIRAMS. The chapter concludes that a holistic, user-friendly, and safe system such as JIRAMS is essential in enhancing efficiency, accessibility and transparency in Zimbabwee judiciary. The following chapter talks about the methodology and system design policies that were employed when developing and implementing JIRAMS.

Chapter 3: Analysis Phase

3.1 Introduction

In this chapter, I will introduce the analysis part of Digital Evidence Presentation System (DEPS) project. This is intended to explore the prevailing condition of Integrated Electronic Case Management System (IECMS) in Zimbabwe, its strengths and weaknesses, and the needs in order to develop DEPS as a supplementary system. It is based on the analysis of the results obtained in the framework of the organized information collection procedures, thorough analysis of the current system, process and data modeling, and assessment of potential alternatives. The chapter ends with the requirements analysis to be the basis of designing and implementation of the system.

The data collection techniques will be categorized as below: 3.2 Information Gathering Methodologies.

In order to be able to arrive at a precise and contextualized interpretation of IECMS and the challenges related to it, a number of information-gathering techniques were used. The initial process was the review of documents as the existing IECMS training manuals, user guidelines, and reports on the policy of digitization were analyzed. The exercise also indicated that although manuals were very detailed on the issue of filing and billing modules of cases, little was done on the presentation of multimedia evidence in court. The documentation also insisted on the trustworthiness of internet connection which is not a practical assumption in most of the court environments in Zimbabwe, and did not give instructions on how to deal with multi-format evidence like forensic data or video footage.

Judges, prosecutors, registrars, as well as IT support staff, were interviewed as well as stakeholders. These interviews brought out the challenges to each group of users. According to judges, the process of helping to navigate through digital evidence in court during sessions was clumsy and not always reliable. According to registrars, the uploading process of multimedia files was time-consuming and subject to technical problems, and IT employees highlighted that there was no smooth integration of the tools of storing evidence and case presentation, and it usually caused inefficiency during the hearings.

In addition to the interviews, questionnaires were issued to clerks and legal practitioners who actively used the IECMS. The feedbacks revealed that most users were not friendly towards the

system in terms of processing digital evidence. Most interviewees were convinced that provided training was inadequate and infrequent, with a large proportion of them admitting that they would like to see the creation of a dedicated tool that would be able to work offline and update the data once connected to the Internet again.

Lastly, first hand observation was done in mock trials and actual court sessions where IECMS were being applied. The observation showed that the presentation of evidence was mostly based on external storage devices including flash drives and laptops instead of IECMS itself. There were also regular interruptions caused by poor internet access and at least on occasions, judges used to use printed still images of video recordings rather than playing the original files thus restricting the quality of evidence presentation.

3.2 Information Gathering Methodologies

To obtain an accurate and contextually grounded understanding of the IECMS and its associated challenges, several information-gathering methodologies were administered. The first method involved document analysis, where existing IECMS training manuals, user guidelines, and digitization policy reports were reviewed. This exercise revealed that while manuals provided comprehensive detail on case filing and billing modules, there was little emphasis on the presentation of multimedia evidence in court. The documentation further assumed reliable internet connectivity, an assumption that is not realistic in many Zimbabwean court settings, and failed to provide guidelines for handling multi-format evidence such as forensic data or video recordings.

Stakeholder interviews were also conducted with judges, prosecutors, registrars, and IT support staff. These interviews highlighted specific challenges faced by each user group. Judges reported that navigating through digital evidence during live court sessions was cumbersome and sometimes unreliable. Registrars described the process of uploading multimedia files as time-consuming and prone to technical difficulties, while IT staff emphasized the absence of seamless integration between evidence storage and case presentation tools, which often led to inefficiencies during hearings.

Complementing the interviews, questionnaires were distributed to clerks and legal practitioners actively using the IECMS. The responses indicated that the majority of users found the system unfriendly when handling digital evidence. Many respondents felt that training provided was

insufficient and irregular, with a significant portion expressing support for the development of a specialized tool capable of functioning offline and synchronizing data when connectivity was restored.Finally, direct observation was undertaken in both mock trials and real court sessions where IECMS was in use. The observation revealed that evidence presentation often relied on external storage devices such as flash drives and laptops rather than on IECMS itself. Interruptions due to poor internet connectivity were frequent, and in some cases, judges resorted to using printed still images from videos instead of playing the original files, thereby limiting the effectiveness of evidence presentation.

3.3 Analysis of the Existing System

The existing IECMS is meant to facilitate case registration, billing, scheduling and storage of evidence in the Zimbabwean judicial system. In essence, the system offers a streamlined system of case management and digital storage. It is limited, however, in its evidence management component where it is mainly limited to storage and not presentation. Although one may upload evidence to the system, there are no tools that could be used to effectively present the evidence in courtroom and interact with digital files. Moreover, the system presupposes the existence of the internet at all times, which makes it unrealistic in the courts where bandwidth is often a problem. Even though IECMS has advanced the case handling process, the weakness in it in managing multimedia evidence has led to under exploitation of this important aspect.

3.4 Process Analysis

The process analysis has been conducted to assess the flow of evidence on Integrated Electronic Case Management System (IECMS). Primarily, the system will accept evidence by the Registrar and upload it to a central repository which will subsequently be submitted at a later date to be presented in court. Nonetheless, this does not necessarily flow smoothly. Although evidence is expected to be stored and retrieved safely using the IECMS, there are always difficulties in using the system during hearings, as one must go outside the system and use other external media like USB drives, laptops, or printed documents. This brings about threats to the consistency, integrity, and efficiency of the case proceedings

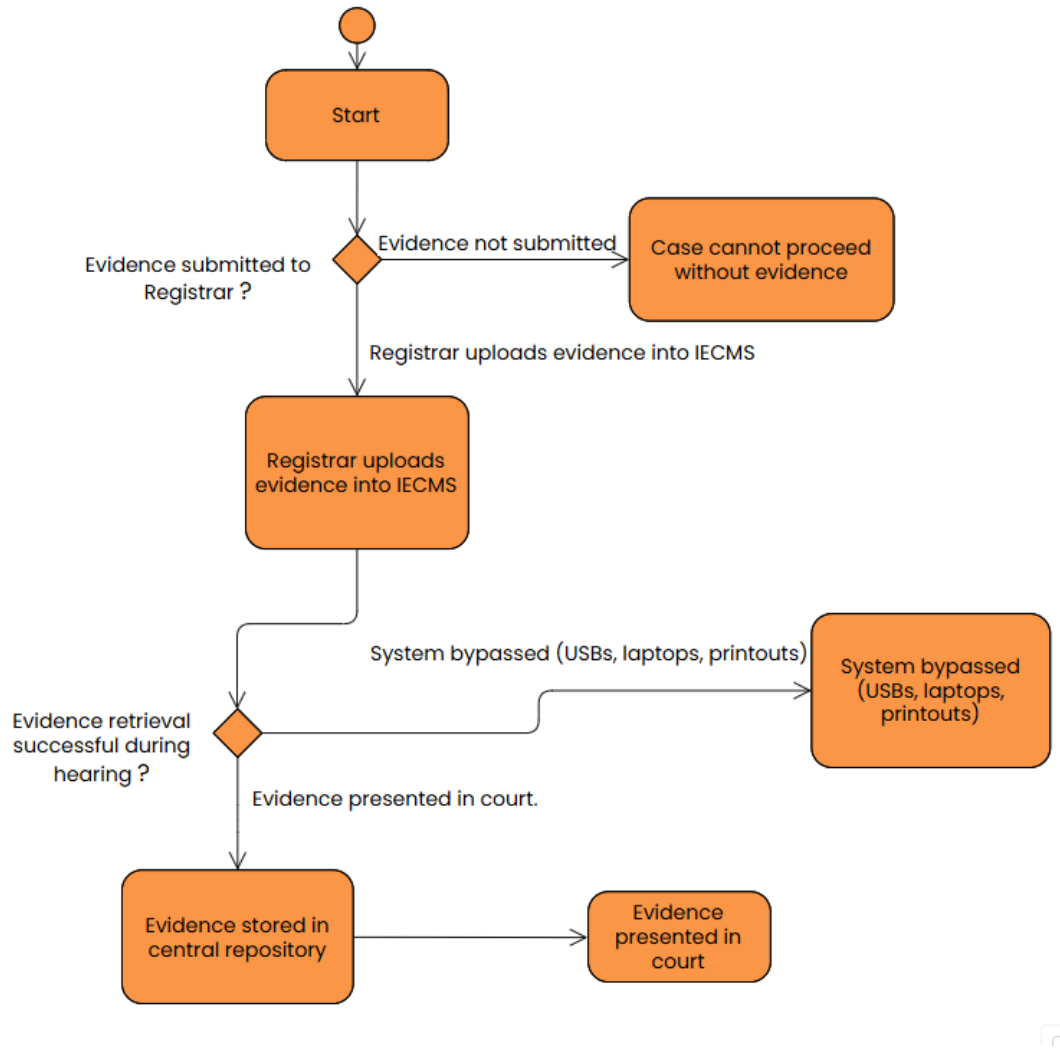


Figure 3.4.1 Evidence Flow through the IECMS

This starts with making evidence to the Registrar. Without evidence to be provided, then there cannot be any further proceedings of the case because evidence is the foundation of every court proceeding. The evidence is uploaded by the Registrar after submission into the IECMS where it is stored in the central repository. Preferably, in hearings, this repository must be in a position to enable a smooth retrieval and presentation of the evidence in court making the process to be efficient and centralized. Nevertheless, in the real world, retrieval in hearings is usually an issue, which results in delays or interruptions. In cases where these difficulties arise, the IECMS is circumvented and stakeholders tend to adopt other means like utilising USB drives, laptops or printouts. Though this enables the court proceedings to go on, it compromises the essence of the

centralized system and there are issues of authenticity, security and traceability of the evidence. Finally, in the successful case of retrieval, the evidence is given in court directly out of the repository as a part of the desired design of the IECMS.

The process begins when evidence is submitted to the Registrar. If evidence is not submitted, the case cannot proceed further, as evidence forms the backbone of any court proceeding. Once submitted, the Registrar uploads the evidence into the IECMS, where it is stored in the central repository. Ideally, during hearings, this repository should allow seamless retrieval and presentation of the evidence in court, ensuring that the process remains efficient and centralized. However, in practice, retrieval during hearings is often problematic, leading to delays or disruptions. When such challenges occur, the IECMS is bypassed, and stakeholders' resort to alternative methods such as using USB drives, laptops, or printouts. Although this allows court proceedings to continue, it undermines the purpose of the centralized system, raising concerns about the authenticity, security, and traceability of the evidence. Ultimately, when retrieval is successful, evidence is presented in court directly from the repository, aligning with the intended design of the IECMS.

3.5 Data Analysis

In order to understand more about how the existing IECMS works, a Data Flow Diagram (DFD) was created. The figure depicts the flow of evidence in the system since its submission up to its acceptance and storage. It emphasizes the interface between the external stakeholders, lawyers or prosecutors and the internal elements of the IECMS, validation, storage and database management. The discussion indicates that although the system provides formal registration and storage of evidence, the use of validation and feedback loops can introduce delays especially when metadata is not complete or on an error that happened during uploading.

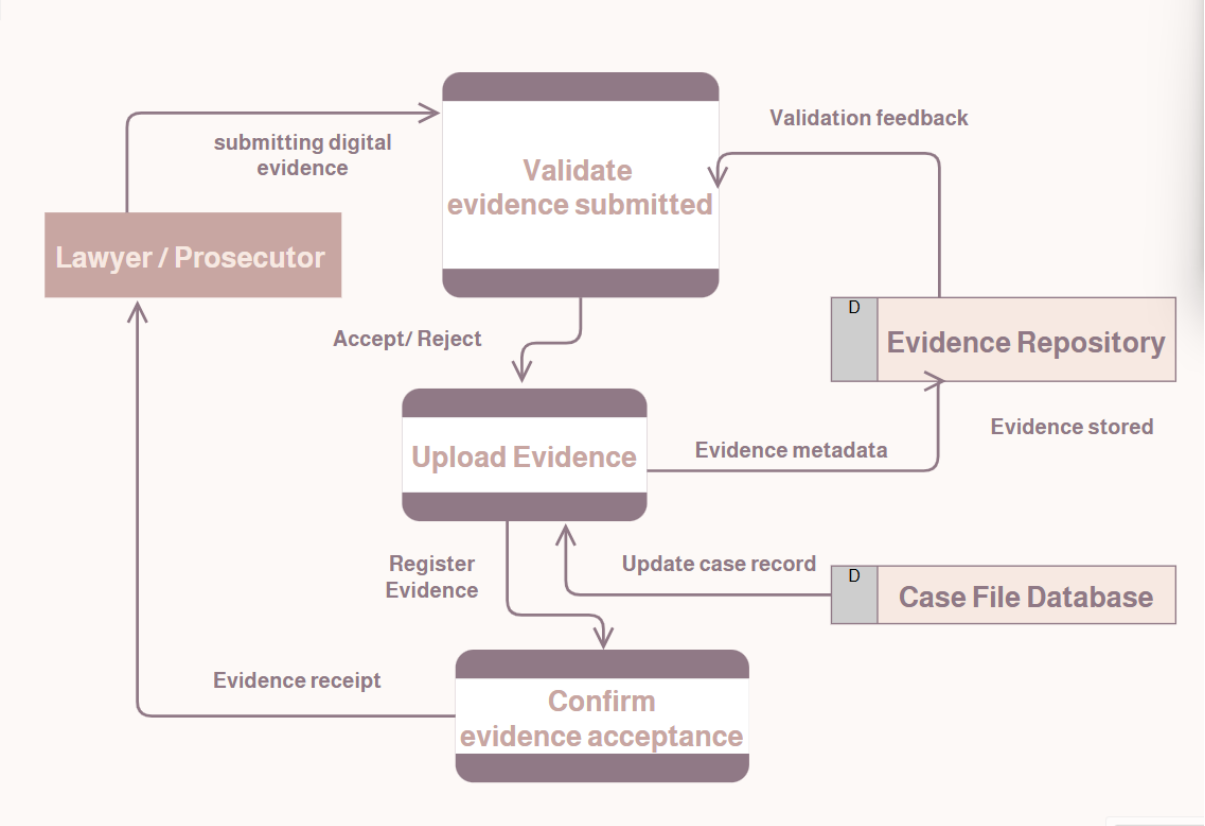


Figure 3.5.1 shows Data Analysis of the system functionality

In this process, the lawyer or the prosecutor initiates the process where he submits the evidence digitally to IECMS. The first step that the system takes is a validation check that shows whether the evidence provided satisfies the necessary standards. In case of the rejection of the evidence, validation feedback is provided to the submitter to correct the evidence. After being accepted, the evidence is transferred to the upload phase, during which it gets registered in the system and metadata is created. This metadata is associated with the evidence to the appropriate case record in the Case File Database, thus preventing traceability and accountability. Concurrently, the evidence itself is safely kept in the Evidence Repository that is the long-term storage site of digital records.

The last part of the process is confirmation of acceptance in which the system sends out an evidence receipt to the submitting lawyer or prosecutor, and the information is complete. Though the DFD illustrates the flow of information in a systematic manner, it also identifies areas where information can be compromised especially in the stage of validation and uploading where system

malfunctions or disconnects might slow down the preparation of cases and hearings. Also, the diagram implies that although evidence is safely stored, they can still be accessed during hearings, yet this will require sound technical infrastructure that is not always trustworthy.

3.6 Weaknesses of the Current System

Based on the analysis made, a number of weaknesses of the IECMS were identified. On the one hand, the system does not have specialized tools that are used in the interactive presentation of digital evidence. Storage is supported but not playback and annotation in the courtroom environment. Second, the system cannot be fully relied upon because of the constant internet connectivity, especially in the courts where the internet connectivity is not always available. Third, the existing training methodology has not been very effective because centralized trainers cannot create sustainable capacity among the users in other locations. Fourth, the navigation in the system has been complicated such that judicial officers are not always able to find and utilize evidence-related features. Lastly, the system has issues with multi-format compatibility, which means that it is not capable of serving large multimedia files and forensic data.

3.7 Evaluation of Alternatives

Chapter 1 Feasibility analysis identified three options that can be used to resolve the shortcomings of the existing system outsourcing, improving the existing IECMS, or creating a new system with specialized needs.A decision to outsource development of a digital evidence presentation system to third parties was considered but it was abandoned due to its high costs that would easily exceed available project budget. Also, outsourcing would tend to lead to less local contextualization and lead to reliance on external knowledge to maintain the system.

Enhancement of the current IECMS was also studied. Nonetheless, the past modifications made on the system have seen more emphasis on improvement of billing and filing systems and minimal emphasis on evidence management. Improvement led by the vendors would probably entail high costs in licensing and would not address the basic problem of lack of offline functionality.Coming up with DEPS as a complementary system was the best alternative that was developed. This method will enable the project budget cost to be kept within the available budget, will help adapt the system to the judicial context in Zimbabwe and will directly solve the weaknesses identified. In addition, DEPS has the capacity to interface with IECMS via API connections, which will keep the case management continuous and will improve the presentation of evidence.

3.8 Requirements Analysis

The gaps and the weaknesses identified in the current IECMS were used as the basis of the requirements. This is aimed at creating a system that does not only ease the management of evidence, but also enhance security, reliability, and accessibility of the system when it is needed in court. In the functional requirements, it is clear that the processing of various forms of evidence, preservation of the chain of custody, and interruptions to access are also required in an environment with limited connectivity. Non-functional requirements on the other hand focuses on the performance, security, usability and scalability to ensure short term efficiency and long term sustainability.

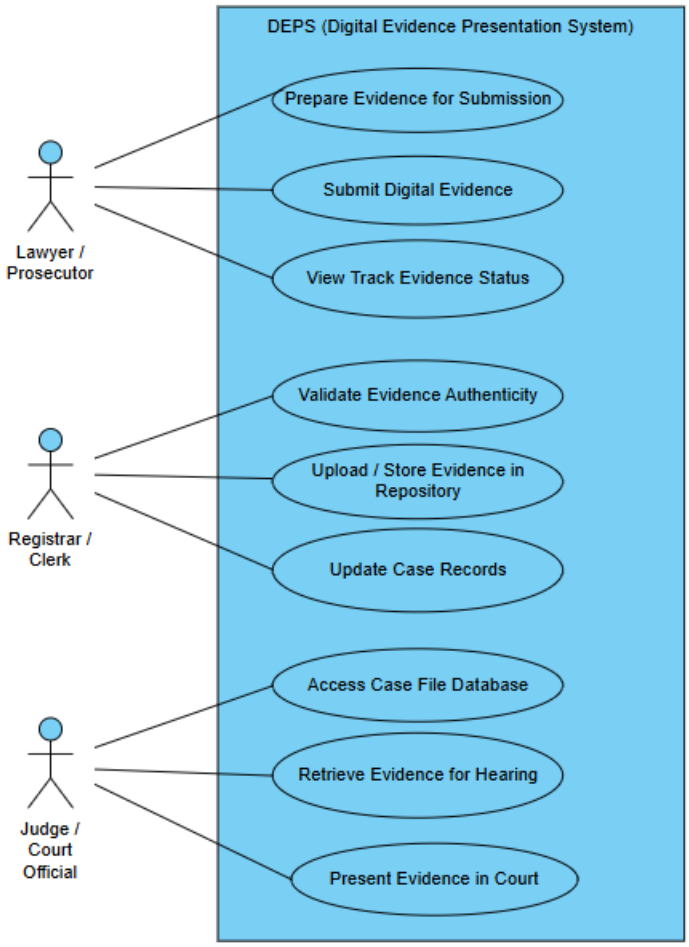


Figure 3.8.1 Use Case Diagram for DEPS Functional Requirements

Functionally, DEPS needs to enable lawyers and prosecutors to develop and present various types of digital evidence, such as video records, audio files, photographs, and forensic logs. After submission, the registrars or clerks will ensure that they establish the validity of this evidence and then upload and store it in the central repository. The inclusion of blockchain verification mechanisms enhances this process through which the integrity of the chain of custody is guaranteed. Moreover, DEPS should facilitate offline features, whereby evidence can be uploaded or accessed without necessarily having an internet connection, and it will automatically synchronize after re-establishing an internet connection. Access control should also be based on roles in order to make sure that only the judges, registrars, and prosecutors perform their role in

the judiciary as defined by their role. Lastly, DEPS must offer high-level interactive presentation software like annotation, zooming, and highlighting and integrate well with IECMS case records to create consistency.

The non functional requirement is aimed at making sure that the system is optimized in terms of performance and usability in low bandwidth particularly as the deployment context is rural. Security should be the first priority, where blockchain assures that the integrity of evidence is as high as international requirements, and the reliability of the system should be provided at 99.9 percent uptime to prevent inconvenience caused during hearings. It is also user-friendly and the interface should be user-friendly such that the court officials need minimal training. Another important factor is scalability which allows the system to be tailored to future evidence formats and judicial procedures. Lastly, DEPS should be cost effective by following the offer budget on development, hosting and long term maintenance and keeps the solution sustainable within the justice system.

3.9 Conclusion

The chapter has examined the current IECMS and its weakness with emphasis on the digital evidence management. With the help of specific techniques, like document analysis, interviews, questionnaire, and observation, it was revealed that IECMS fulfills its goal of handling case files, but fails to facilitate the evidence presentation in the court. Outsourcing or the improvement of IECMS were not favored because of cost implications and lack of benefits and the development of DEPS was the most viable and sustainable solution. Functional and non-functional requirements presented in this chapter overcome the weaknesses identified and give the roadmap of the creation and implementation of the proposed system.

Chapter 4: Design Phase

4.1 Introduction

The chapter is a design stage of the JIRAMS Digital Evidence Presentation System. This stage is aimed at translating the system requirements into a form of structured models that lead to implementation. The design encompasses logical processes, system architecture, hardware-software interface, database structure, program design, user interface, and security aspects. All these aspects will ensure that the system is user friendly, scaleable and secure and will meet its functional and non-functional requirements.

4.2 System Design

The system design will provide an account of how the platform will safely store, validate, retrieve and present digital evidence in a court of law. It has also been integrated with the current IECMS using APIs, giving it added functionality with special evidence presentation and chain-of-custody modules. The design assumes a 3 layer architecture (presentation, application, and data layers) in order to be scalable, reliable and easily maintainable. It has offline-first features, which are necessary to manage the infrastructural issues of Zimbabwe letting it resume synchronization when an internet connection is regained. Role-based dashboard and easy interfaces ensure that every user group engages wit h system in a way that is relevant to their judicial role, which increases the ease of use and acceptance

4.2.1 Proposed System Context Diagram and DFD.

A Level 0 Data Flow Diagram (DFD) or context diagram is a high-level model that displays the system as a single process and the interactions that it has with external entities (Dennis, Wixom and Tegarden, 2020). It is called Level 0 as it is the most abstract conception of the system as it only mentions the key inputs and outputs and does not refer to the processes inside the system. DFD, conversely, is a graphical representation system analysis tool that is employed to illustrate the data flow of a system, clarifying the processes, data storage areas, and interactions with external actors (Shelly & Rosenblatt, 2021).

As seen in Figure 4.2.1 the system serves as the hub of judicial activities, which is linked to its primary stakeholders and source of data. The diagram highlights how:

Judges communicate with JIRAMS to access and label evidence,

Prosecutors/Lawyers provide digital evidence during the hearings of cases,

Registerrs/Clerks are the ones that verify evidence and post it so that it is authentic.

IECMS shares the metadata of case and evidence between platforms to ensure consistency, and

The Database is the secure evidence repository where the evidence is stored and retrieved over a long period.

This context diagram ,Figure 4.2.1 forms the basis of further elaboration of more detailed levels of the DFD in later parts where single DEPS process will be subdivided into subprocesses of submission of evidence, validation, storage, presentation, and synchronization

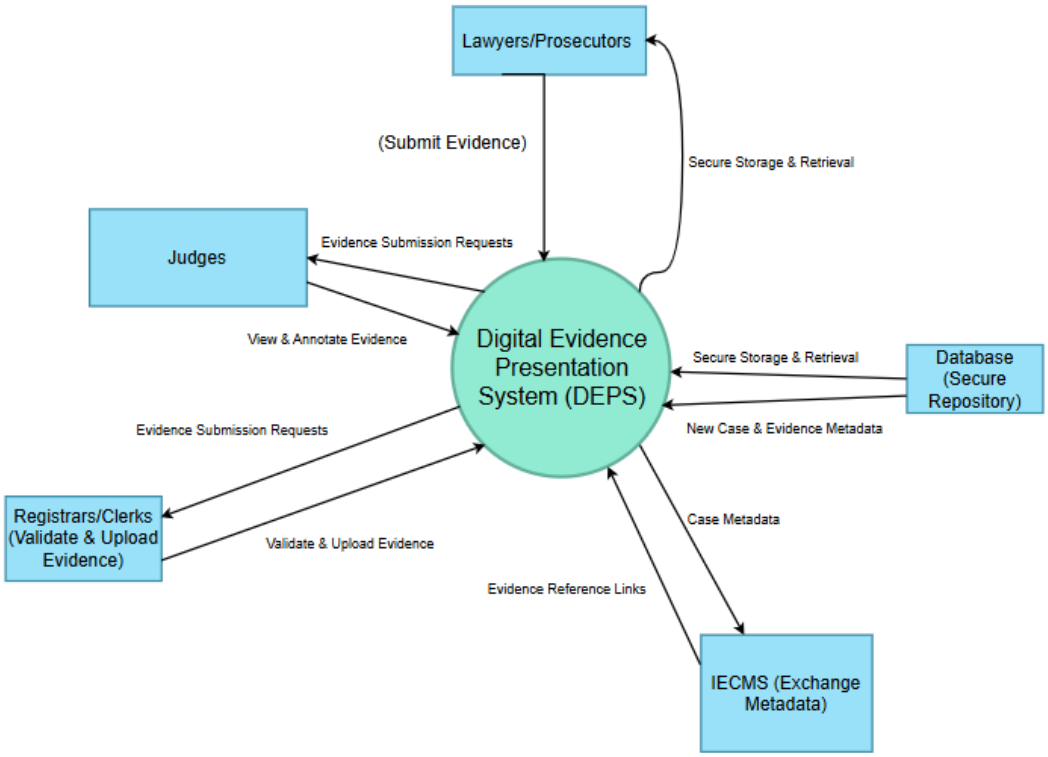


Figure 4.2.1: Context Diagram of the Digital Evidence Presentation System (DEPS

The context diagram in Figure 4.2.1 shows that the Digital Evidence Presentation System (DEPS) communicates with other important external bodies in the judicial setting through the context diagram. Registered lawyers and prosecutors upload the evidence to the system and the registrar

and clerks authenticate and upload the evidence to verify its authenticity and integrity. Judges can use DEPS to see and comment on evidence presented in the process, which improves the presentation of the courtroom and decision-making. The digital evidence stored in the evidence repository (database) by the system is securely appended and recalled to ensure an effective chain of custody. Also, DEPS shares case metadata and case reference links with the Integrated Electronic Case Management System (IECMS) to ensure platform consistency. This advanced model puts the DEPS at the centre of focus as the node that simplifies the process of submitting evidence, validation, storage, and presentation of the evidence in a safe and secure way.

Level 1 DFD:

Level 1 Data Flow Diagram (DFD) extends the context diagram by deriving the major subprocesses of the DEPS. It shows how an evidence is provided, verified, stored, presented and aligned among the judicial stakeholders and the supportive systems.

Divides DEPS into subprocesses:

- Evidence Submission (lawyer submits files)
- Evidence Authentication (checks and approves by registrar)
- Blockchain (hashes) + secure storage (Repository Evidence)
- Oral (hearings by judges in court and annotating evidence)
- Synchronization Service (processes offline/online)

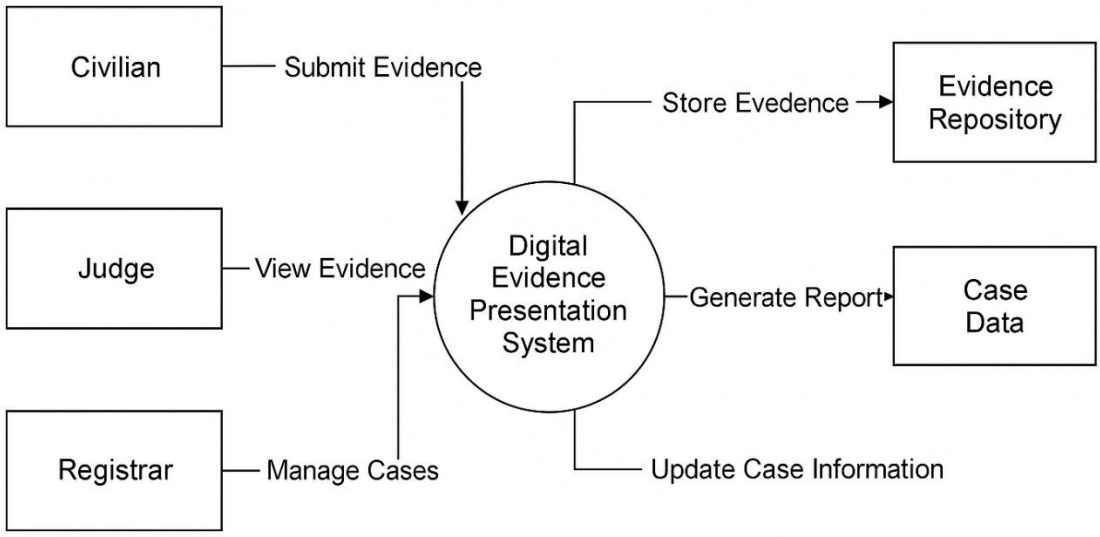


figure 4.2.2 Level 1 DFD

As it can be observed in figure 4.2.2 Level (DFD 1 Data Flow Diagram (DFD) demonstrates the organized division of Digital Evidence Presentation System (DEPS). The initial step is Lawyers and Prosecutors who have the role of submitting digital evidence using the Evidence Submission module. After uploading, the system sends a receipt of the upload to ensure successful submission and avoid conflicts of receiving materials. That evidence is then forwarded to the Evidence Validation module where Registrars or Clerks determine whether the evidence is genuine and meets the expected legal and technical requirements and they transfer the evidence to the Evidence Repository (D1) to store it in a secure place. This guarantees that no unauthorized and inadmissible evidence is entered into the repository, minimizing chances of tampering and invalid submissions.

The second component that is critical is the Hearing Module that allows the Judges to communicate with the stored evidence during the court. The judges are able to examine, interpret and comment on the evidence and all the comments and judgments will be automatically updated in the system. These updates are associated with Case Metadata store (D2), which gives it a connection to the broader Integrated Electronic Case Management System (IECMS). The Synchronization Service is equally important in parallel as it ensures that communication between DEPS and the outside

systems is synchronized in order to ensure consistency of case records on the different platforms. This ensures that evidence related endeavors are up-to-date and properly aligned with official case records.

Lastly, the system promotes accountability and transparency by the Chain of Custody store (D3) that keeps a verifiable record of all the interactions with the evidence. This consists of submission, validation, storage, retrieval and annotation and thus maintains a full lifecycle of the evidence. Breaking DEPS down into these subprocesses, the Level 1 DFD does not only draw attention to the logical flow of information, but also the security and governance architecture inherent in the system. All these mechanisms are used to assure the authenticity, reliability, and admissibility of digital evidence in the court, which increases trust in the judiciary system to use electronic evidence management systems.

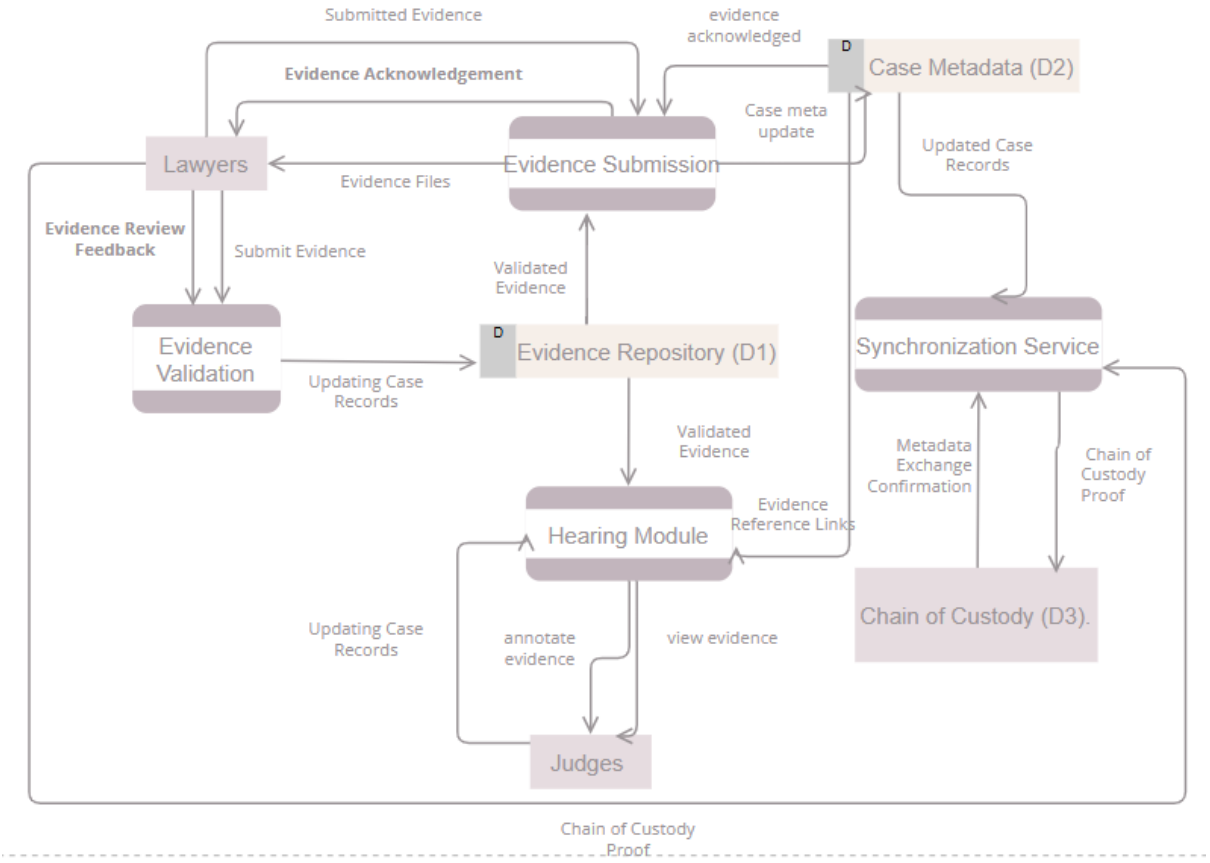


Figure 4.2.2.1 Level 1 (DFD) the structured breakdown of the Digital Evidence Presentation System

As shown in Figure 4.2.2.1 the Level 1 Data Flow Diagram (DFD) illustrates the structured breakdown of the Digital Evidence Presentation System (DEPS). The process begins with Lawyers and Prosecutors, who are responsible for submitting digital evidence through the Evidence Submission module. Once uploaded, the system issues an acknowledgement of receipt to confirm successful submission and prevent disputes over whether materials were received. The submitted evidence is then passed to the Evidence Validation module, where Registrars or Clerks assess its authenticity and compliance with established legal and technical standards before transferring it to the Evidence Repository (D1) for secure storage. This ensures that only verified and admissible evidence enters the repository, reducing the risk of tampering or invalid submissions.

The next critical component is the Hearing Module, which enables Judges to interact with the stored evidence during court sessions. Judges can view, analyse, and annotate the evidence, with all annotations and decisions automatically updated in the system. These updates are linked with the Case Metadata store (D2), ensuring synchronization with the wider Integrated Electronic Case Management System (IECMS). In parallel, the Synchronization Service plays a crucial role by coordinating communication between DEPS and external systems, maintaining consistency in case records across platforms. This guarantees that evidence-related activities remain current and accurately aligned with official case files.

Finally, the system emphasizes accountability and transparency through the Chain of Custody store (D3), which maintains a verifiable log of all interactions with the evidence. This includes submission, validation, storage, retrieval, and annotation, thereby preserving a complete record of the evidence lifecycle. By decomposing DEPS into these subprocesses, the Level 1 DFD highlights not only the logical flow of information but also the security and governance structures embedded in the system. Collectively, these mechanisms ensure that digital evidence remains authentic, reliable, and admissible in court, reinforcing trust in the judiciary's reliance on electronic evidence management systems.

4.3 Architectural Design

JIRAMS Digital Evidence Presentation System (DEPS) architectural design establishes the general framework of the system and how all the elements of the system interface with each other to provide a secure, efficient, and reliable digital evidence management system. The architecture design is a decisive phase of the system development as it gives the requirements organized

structure to be followed in implementation, maintainability and scalability (Sommerville, 2020). Layered architectures are evaluated with special intensity in the context of legal informatics as they ensure the separation of concerns, fault tolerance, and enhanced security in the case of sensitive judicial information (Kouki et al., 2021). Figure 4.3 shows the architecture of the DEPS, and the structure is layered.

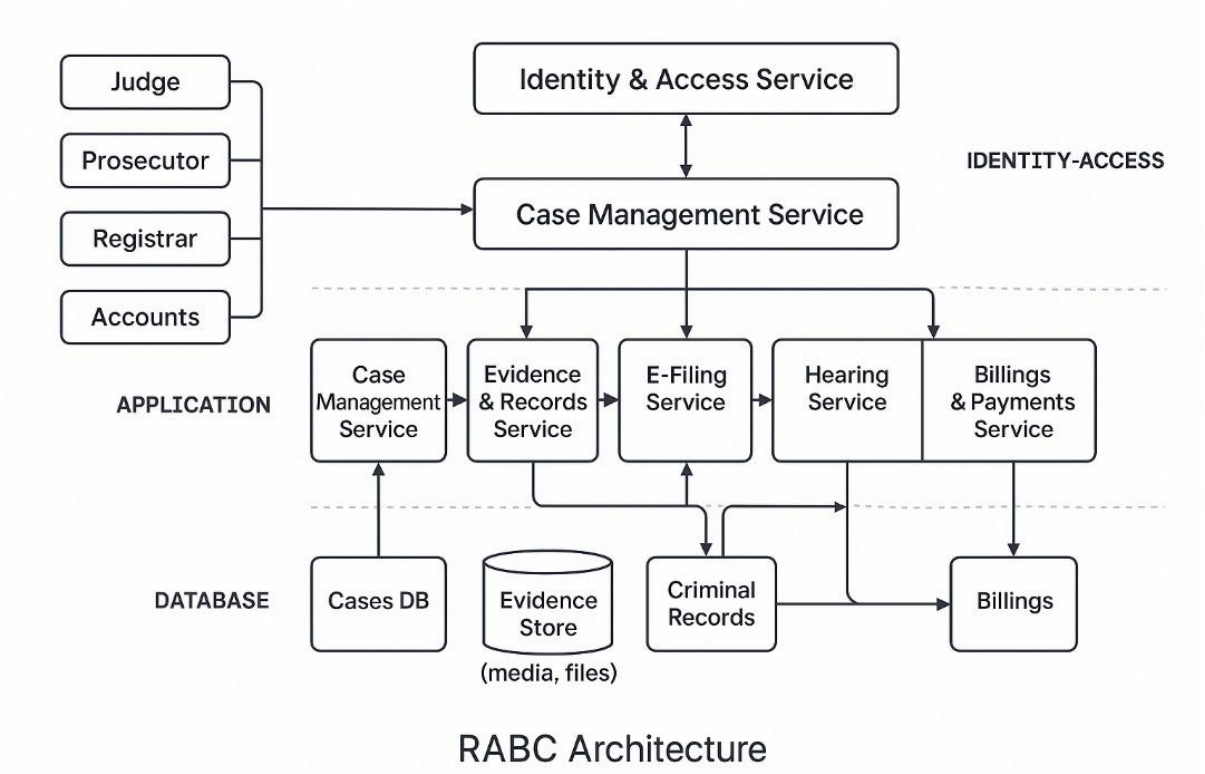


Figure 4.3.1 Architectural Design of the Digital Evidence Presentation System (DEPS

Figure 4.3.1 illustrates that the architecture has three layers, i.e. Identity-Access Layer, Application Layer, and Database Layer. At the Identity-Access Layer, the Identity and Access Service will be used to perform user authentication and authorization to make sure that judges, prosecutors, registrars and accounts officers are only the accredited actors who have access to sensitive case

data. This is consistent with current security standards at e-justice system where robust identity management is the core to securing digital evidence (Abdullah et al., 2022).

Application Layer is the foundation of the working backbone of DEPS and consists of modular services. The Case Management Service and the Evidence and Records Service are in charge of user workflow, the E-Filing Service facilitates the digital submission of legal documents, the Hearing Service assists in evidence presentation and annotation in the trials, and the Billings and Payments Service oversees the financial procedures. This modularization would make it possible to perform system updates and expansions without disrupting the overall system, which is in line with the best practices of the microservice-based system of judicial processes (Nguyen et al., 2023).

A repository is supported at the Database Layer by several repositories. Cases Database, Evidence Store, Criminal Records Database and Billings Database are databases that store structured case information, digital media and files, offender history, and transparency in financial records respectively. Distributed storage, which is embraced by the DEPS across specialized databases, enhances resilience and ensures that there is reliable evidence handling, aligning with the tendencies of distributed justice information systems(Berube et al., 2025).

In general, the DEPS architecture can be viewed as the three-level model of system design presentation, application, and data that is applied in many enterprise and judicial systems due to its scalability, maintainability, and the capacity to provide accountability to sensitive workflows (Adler et al., 2023).

4.4 Physical Design

The physical design aims at mapping software modules to actual hardware and network infrastructures to enable reliability in operations, availability, and the secure handling of evidence (Sommerville, 2020). Although the architectural design focuses on the logical interactions, the physical design explains how client devices, servers, and networks interact to facilitate the courtroom tasks and facilitate the integration with the external systems.

Physical implementation of DEPS as shown in figure 4.4.1 below depicts the connection between various hardware and network layers to facilitate the submission, validation, storage and synchronization of evidence.

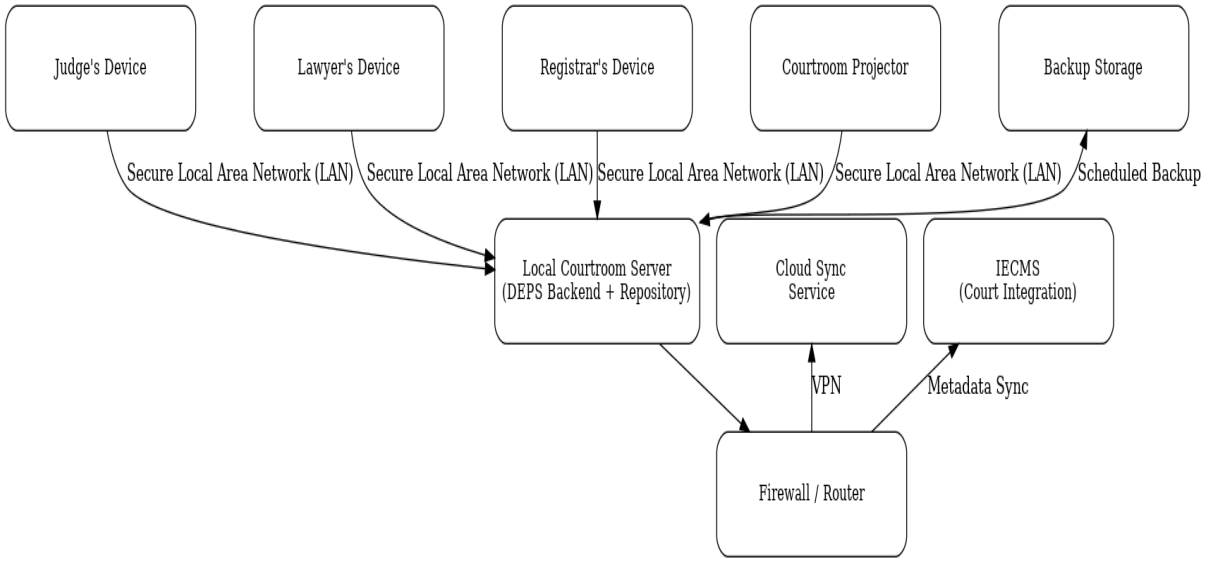


Figure 4.4.1 Physical Deployment Architecture

Judges, lawyers, and registrars use client devices (laptops, desktops and courtroom projectors) to communicate with DEPS (see Figure 4.4). These devices are linked together via a secure courtroom LAN to a local server that is hosting the DEPS backend and that is holding the evidence repository so that it can be used offline-first. To achieve external interoperability, the system may be configured to support the Integrated Electronic Case Management System (IECMS) via a cloud-based synchronization service in which metadata of evidence and cryptographic hashes are exchanged safely. The network infrastructure uses a VPN to access remote authorized access to protect the communications. This middle ground model prevents security, accessibility, and continuity in digital evidence processing (Abdullah et al., 2022; Miller et al., 2024).

4.5 Database Design

The fundamental entities in the system database are intended to endorse secure, traceable and efficient management of the courtroom processes. The User entity stores critical information concerning the participants in the system including the judiciary, registrar, and lawyers such as their role, contact details and authentication credentials. A Case is a legal process and has metadata like title, status and initiation date. The Evidence object holds the digital submissions in relation to particular cases, including file paths, cryptographic hashes and the information of the user who made the submission. All user activities with the system are recorded in the AuditTrail entity to

provide accountability and transparency of the system and documentation of such interactions such as validations or access actions, associated with timestamps and hash values. Finally, the Payments entity keeps a record of financial operations associated with activities of cases and allows tracking money movements and facilitating workflows related to billing. Collectively, the entities constitute the basis of a strong, normalized relational schema that emphasizes on security, traceability, and data integrity.

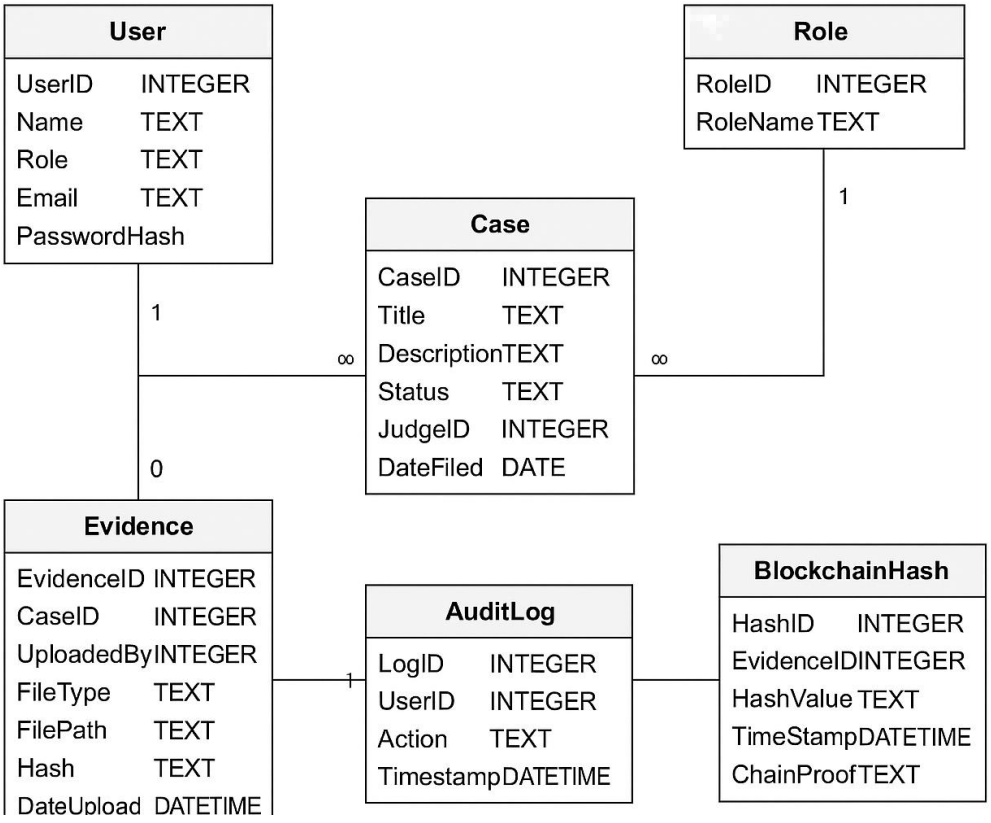


Figure 4.4.2: Database Design

4.5.1 Entity Relationship (ER) Diagram

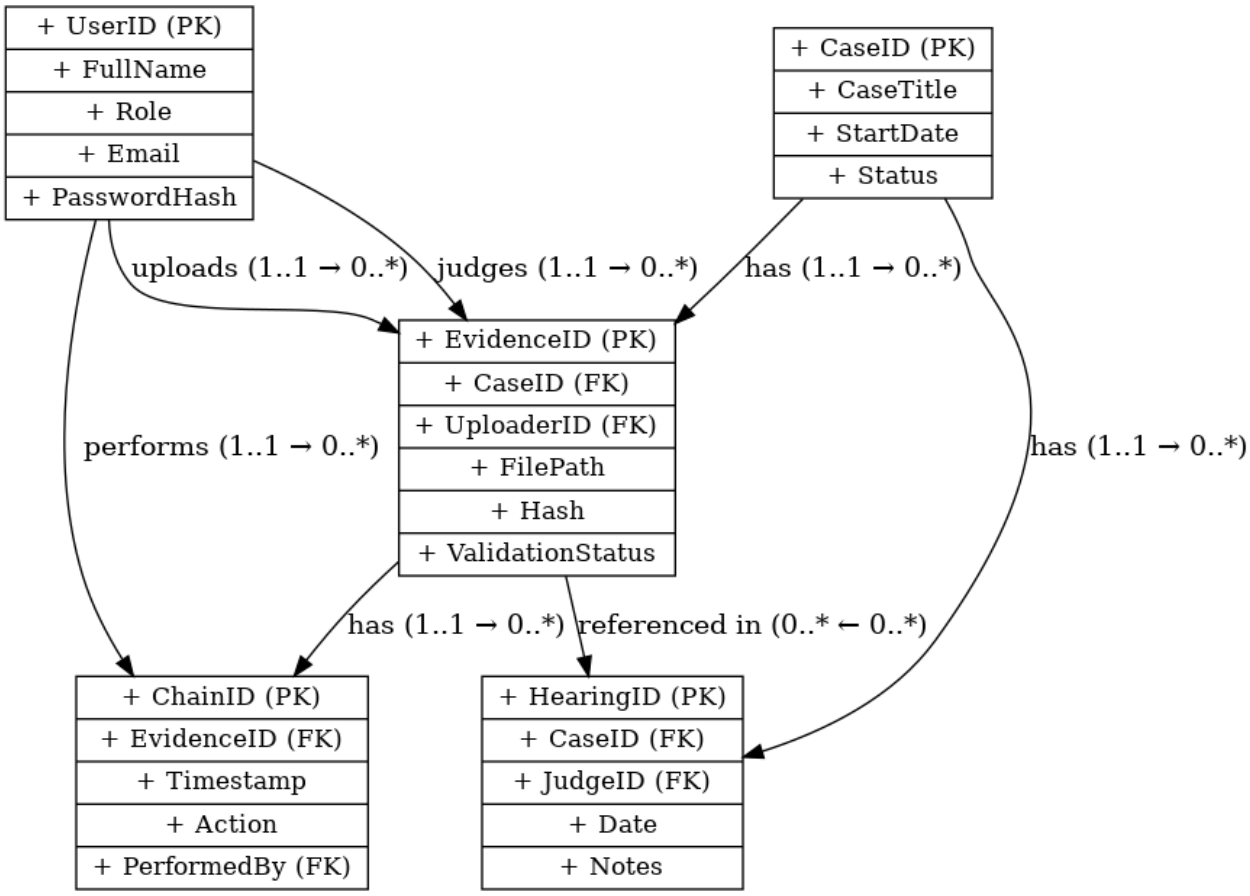


Figure 4.5.1 Enhanced Entity Relationship Diagram

As illustrated in Figure 4.5.1 the Entity Relationship Diagram (ERD) shows the main data structures and relationship between them. The User entity considers system actors like judges, registrars, lawyers, and each of them is able to add numerous pieces of Evidence to different Cases. A case, in its turn, may contain several pieces of evidence and be associated with several Payments that so or so indicate the transactions connected with some payments submitted or completed.

Further, Evidence entity is closely connected with AuditTrail which records a chain of system activity (e.g., validation, viewing, transfers) in order to provide traceability and insure the integrity of the data using cryptographic hashes. Referential integrity is also applied in this model using foreign keys and cardinalities to represent real-life limitation in the electronic court activities. This

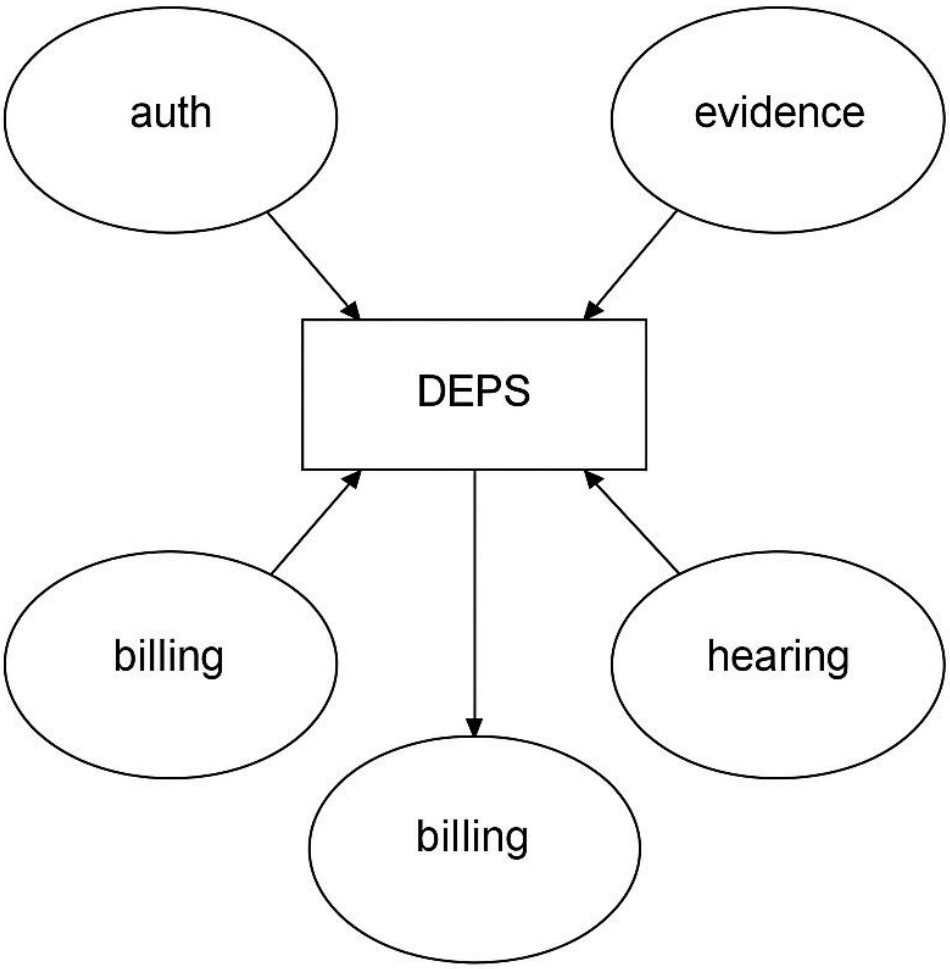
ERD will become the basis of creating a strong, normalized relational database schema that is specific to managing secure and accountable digital evidence (Sommerville, 2020; Abdullah et al., 2022).

4.6 Program Design

The DEPS software is structured in the following rational packages:

- auth Manages user authentication, login processes and role based access control (RBAC) of the Judges, Lawyers, Registrars, and other users.
- evidence -Deals with the entire digital evidence lifecycle, such as upload interfaces, cryptographic hash checks and storage in the secure repository.
- hearing - Supports presentation tools in use in court hearing like evidence display, ability to annotate evidence by Judges and case commentary tools.
- sync – Provides offline-first functionality and metadata and hash value synchronisation with the Integrated Electronic Case Management System (IECMS) on reconnecting.
- billing - Supports a payment track record, such as fees submission, creating receipts, and confirming financial documents related to legal cases.

Program Design



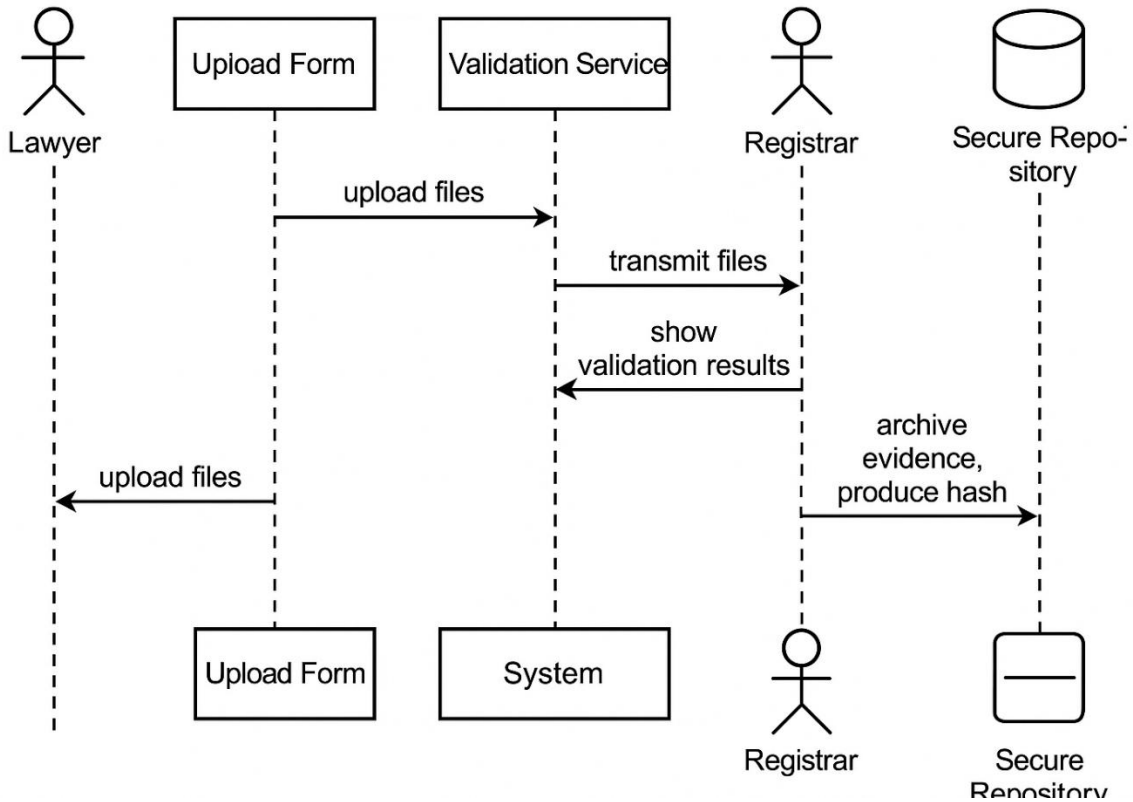
This modular decomposition is based on best practices of software engineering (Sommerville, 2020) and provides clarity of the system and the high degree of situational isolation of concerns between functional domains.

Sequence Diagram: Evidence Submission Process.

The interaction flow between the process of evidence submission is as follows:

- The process is initiated by Lawyer who uploads digital files through the Upload Form interface.

- The System transmits the files to the Validation Service that verifies the conformity of the format, integrity of files and hash creation.
- The Registrar looks at the validation results and either approves or refuses the submission of the evidence.



Upon acceptance, the System archives the evidence in the secure repository and produces a hash that is compatible with blockchain, and to be able to be audited and traced.

This chain of interaction can guarantee the entry of only verified and authorized digital evidence in the repository, which is admissible in court and has an unchangeable audit record (Abdullah et al., 2022).

4.7 Interface Design

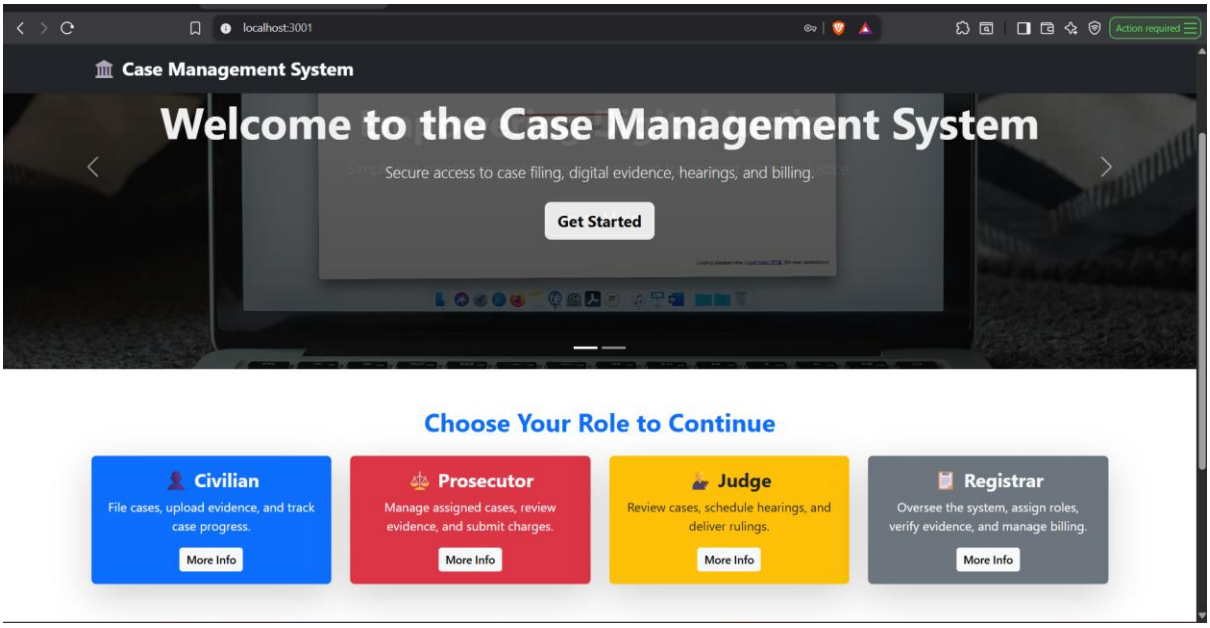


Figure 4.7 Interface design

4.7.1 Menu Design

The menu design is role-specific, ensuring that each user (Judge, Lawyer, Registrar) accesses functionalities that match their responsibilities. This role-based interface not only improves usability but also enforces security by limiting access to sensitive operations based on the user's role.

Main Menu (Role-Specific Interfaces)

Each user role sees a tailored version of the main menu, but common core modules are shared across all roles:

Dashboard
Provides an overview of the user's recent activities, system notifications, pending tasks, and case statistics. It acts as the landing page upon login.

Case Management

Allows users to view, filter, and manage case details. Judges and registrars may see additional administrative controls, while lawyers have access to case submissions and linked documents.

Evidence Repository

Central hub for handling digital evidence. Users can upload new files, validate their integrity (e.g., via hash checks), retrieve files, and present evidence during hearings. The access level varies depending on the role (e.g., judges can only view, registrars can approve uploads).

Hearing Module

Enables scheduling and conducting hearings. During live hearings, users can annotate or highlight evidence. Judges and lawyers have extended access for presentation; registrars may assist with administrative functions.

Audit Logs

Displays a tamper-evident log of all system interactions, such as uploads, approvals, or deletions. Primarily available to judges and registrars to ensure accountability and traceability. Contains user-specific configurations, such as profile updates, password resets, theme settings, and notification preferences.

|Sub-Menu

Each main menu item may include nested functionalities. For instance, under **Evidence Repository**, users interact with:

- **Upload**
  Used to submit new evidence files. Lawyers and registrars primarily use this feature.
- **Validate**
  Allows users to verify file integrity using cryptographic hash values. Ensures the evidence hasn't been tampered with.
- **Retrieve**
  Enables users to search and access stored evidence files for review.
- **Present**
  Launches the evidence in a presentation interface, allowing for annotations and highlighting during a live court session.

Role-based Menu Design in DEPS.

Each user (Registrar, Lawyer, Judge) is presented with a custom menu interface containing only the modules relevant to their duties, with deeper sub-menus (e.g., within the Evidence Repository) for managing digital evidence

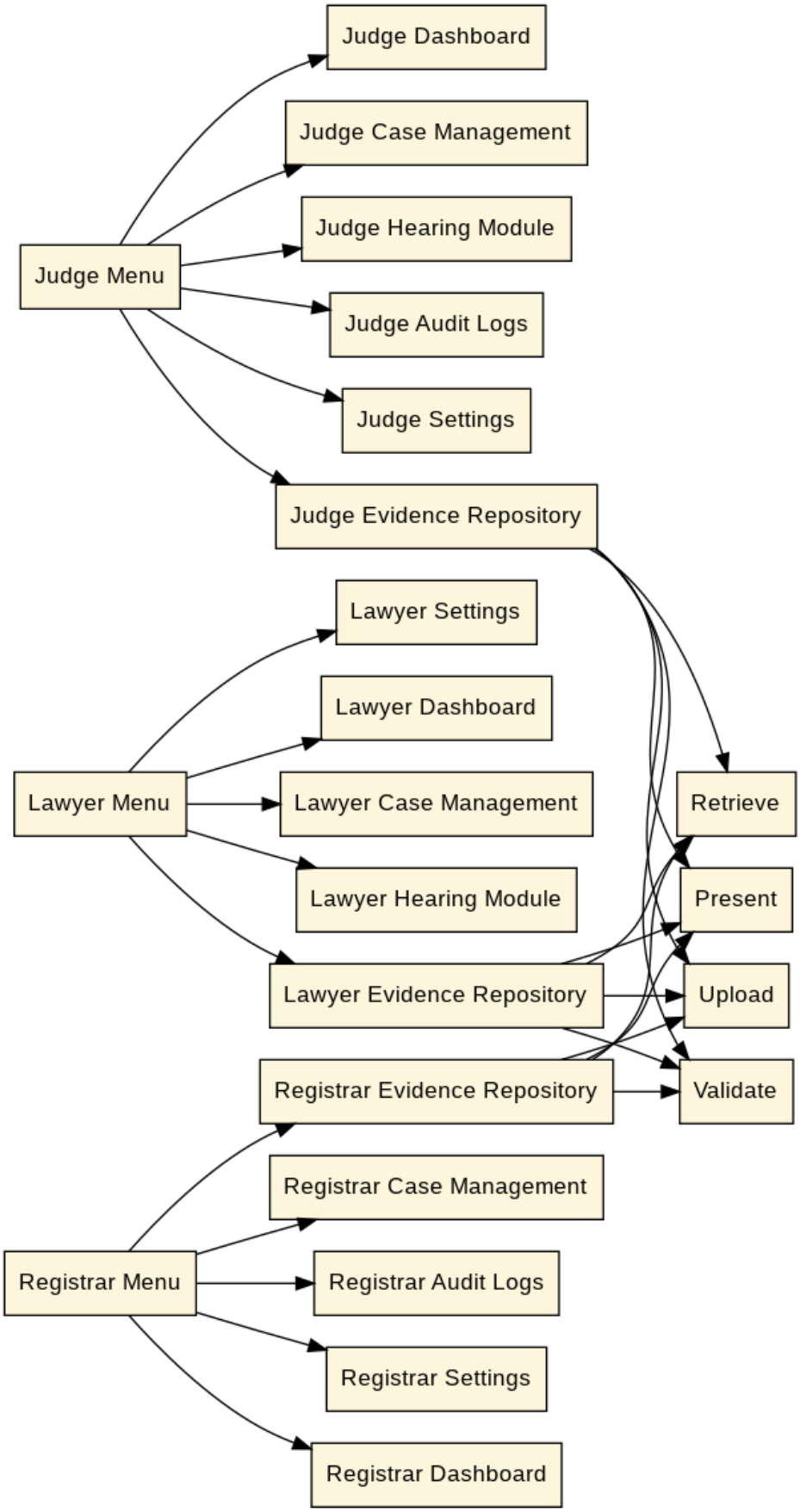

Judge Dashboard
Judge Case Management
Judge Hearing Module
Judge Menu
Judge Audit Logs
Judge Settings
Judge Evidence Repository
Lawyer Settings
Lawyer Dashboard
Lawyer Menu
Lawyer Case Management
Lawyer Hearing Module
Retrieve
Present
Upload
Validate
Lawyer Evidence Repository
Registrar Evidence Repository
Registrar Case Management
Registrar Menu
Registrar Audit Logs
Registrar Settings
Registrar Dashboard

Figure 4.7.1 Role-based Menu Design in DEPS

4.7.2 Input Design (Forms)

- Evidence Upload Form (File Upload + Metadata + Case Link)

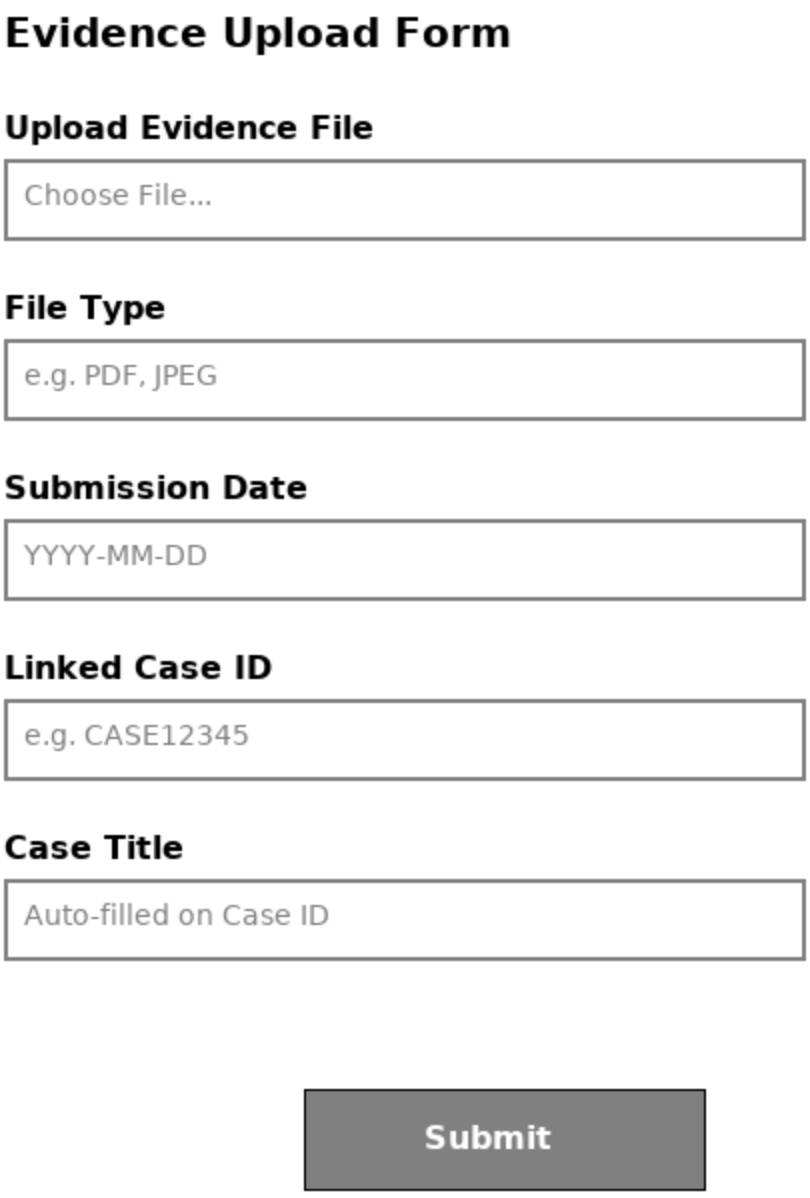


Figure 4.7.2.1 Evidence Upload Form

- User Login Form (Role-based authentication)

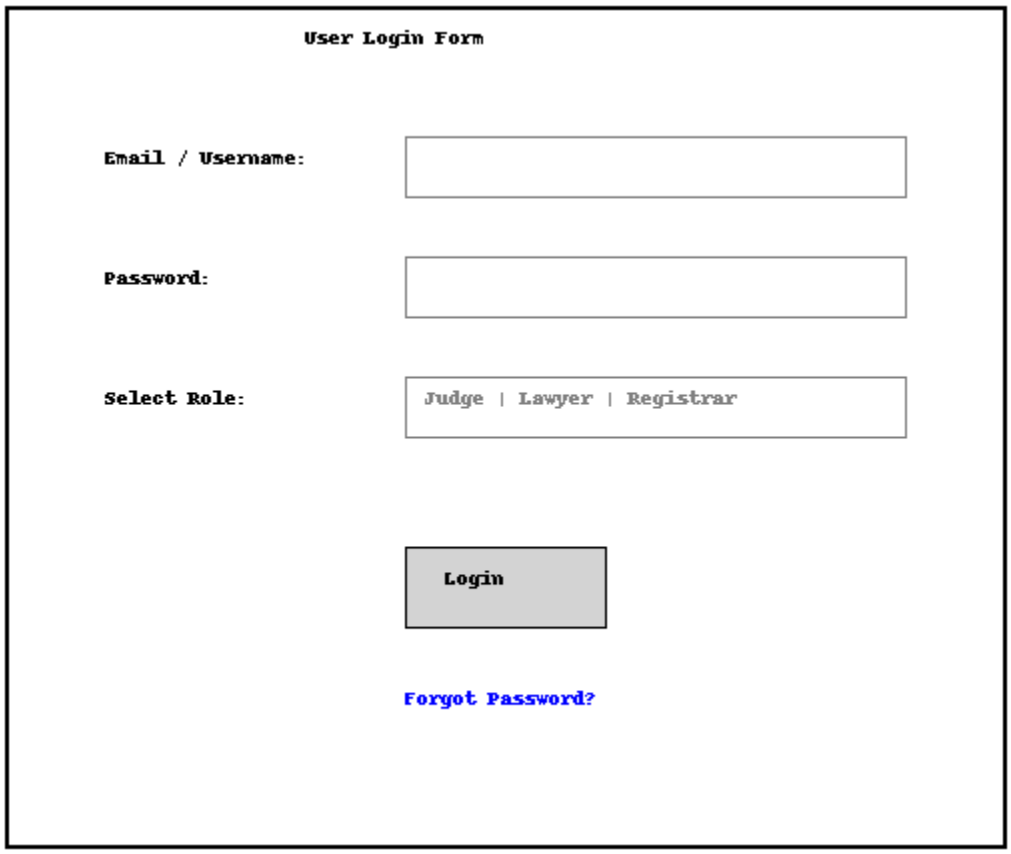


Figure 4.7.2.2 user login form

- Payment Form (Case ID, Fees, Mode of Payment)

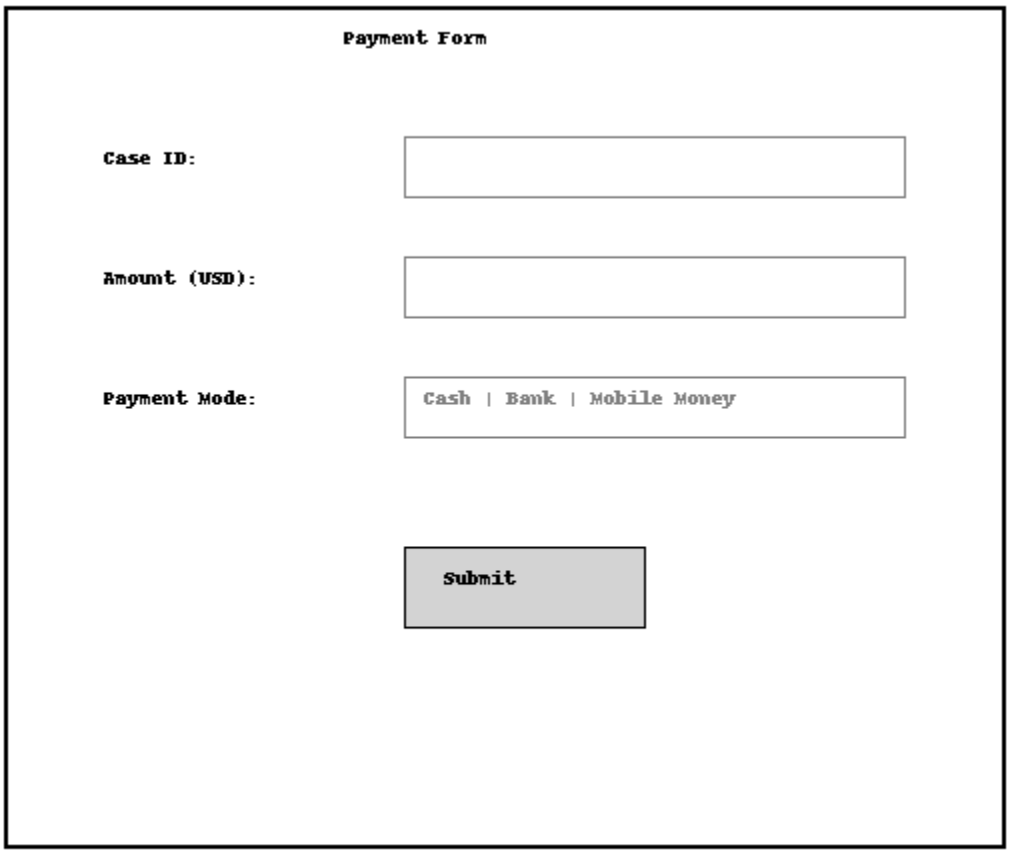


Figure 2.7.2.3 Payment Form

4.7.3 Output Design (Reports)

- Evidence Audit Trail Report (chronological log of actions)

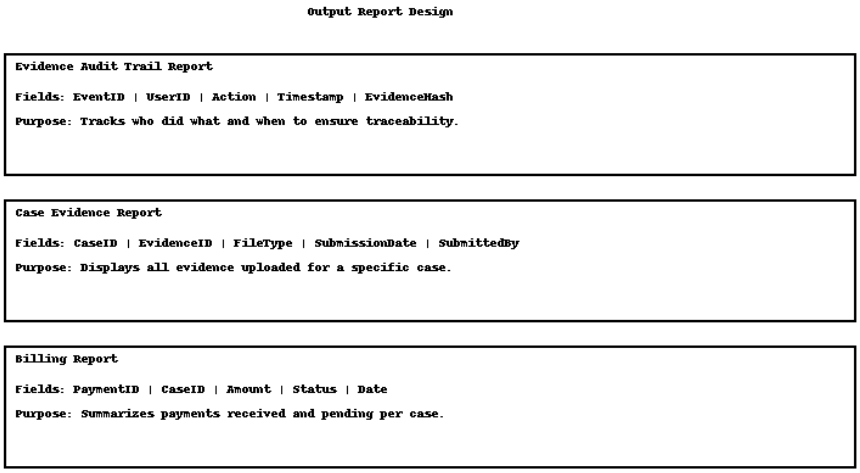


Figure 4.7.3.1 Evidence Audit Trail Report

Case Evidence Report (list of all uploaded evidence per case)

Sketch: Case Evidence Report

Case ID	Case Title	Evidence ID	File Type	Submitted By	Submission Date	Status
C-1001	State vs Joe	E-501	PDF	LawyerA	2025-10-01	Validated
C-1002	People vs Smith	E-502	Image	LawyerB	2025-10-02	Pending
C-1003	Republic vs Jame	E-503	Video	LawyerC	2025-10-03	Validated

Figure 4.7.3.2 Case Evidence Report

- Billing Report (payments made and pending)

Billing Report (Sketch)

Case ID	Payment ID	Amount	Payment Mode	Status	Date
C-1001	P-201	$500	Bank Transfer	Paid	2025-10-01
C-1002	P-202	$250	Mobile Money	Pending	2025-10-02
C-1003	P-203	$300	Credit Card	Paid	2025-10-03

Figure 3.7.3.3 Billing Report

4.8 Pseudo Code

```
START

FUNCTION main():
    DISPLAY "Welcome to DEPS"
    CALL login()

FUNCTION login():
    PROMPT user to enter email and password
    VALIDATE credentials
    IF valid:
        RETRIEVE role
        IF role == "Judge":
            CALL judge_menu()
        ELSE IF role == "Lawyer":
            CALL lawyer_menu()
        ELSE IF role == "Registrar":
            CALL registrar_menu()
        ELSE:
            DISPLAY "Unknown role"
            TERMINATE
    ELSE:
        DISPLAY "Invalid credentials"
        REPEAT login()

FUNCTION judge_menu():
    DISPLAY menu options: Dashboard, Case Management, Evidence Repository, Hearings, Audit Logs, Settings
    LOOP:
        PROMPT for option
        IF option == "Case Management":
            CALL view_cases()
        ELSE IF option == "Evidence Repository":
            CALL view_evidence()
        ELSE IF option == "Hearings":
            CALL manage_hearings()
        ELSE IF option == "Audit Logs":
            CALL view_audit_logs()
        ELSE IF option == "Settings":
            CALL update_settings()
        ELSE IF option == "Exit":
            BREAK

FUNCTION lawyer_menu():
    DISPLAY menu options: Dashboard, Case Management, Evidence Repository, Hearings, Settings
    LOOP:
        PROMPT for option
        IF option == "Evidence Repository":
            CALL upload_evidence()
        ELSE IF option == "Case Management":
            CALL view_cases()
        ELSE:
            CONTINUE menu

FUNCTION registrar_menu():
    DISPLAY menu options: Dashboard, Case Management, Evidence Repository, Audit Logs, Settings
    LOOP:
        IF option == "Evidence Repository":
            CALL validate_evidence()
        ELSE IF option == "Audit Logs":
            CALL view_audit_logs()

FUNCTION upload_evidence():
    PROMPT user to select file
    PROMPT user to enter metadata: FileType, CaseID, Description
    COMPUTE file hash
    STORE evidence record in DB
    LOG action in audit trail
    DISPLAY "Evidence uploaded successfully"

FUNCTION validate_evidence():
    DISPLAY list of pending evidence
    PROMPT user to approve/reject
    UPDATE validation status
    LOG action in audit trail

FUNCTION view_audit_logs():
    FETCH logs based on user or evidence
    DISPLAY in chronological order

FUNCTION process_payment():
    PROMPT for CaseID, amount, payment method
    VALIDATE input
    STORE payment info
    DISPLAY "Payment successful"

END
```

Figure 4.8.1 Pseudo Code

4.9 Security Design

The security design prioritizes confidentiality, integrity, and availability of digital evidence within the courtroom ecosystem. Since DEPS deals with sensitive legal materials, its security architecture spans multiple layers physical, network, and operational ensuring that evidence is not only protected from unauthorized access but also retains its forensic credibility in legal proceedings. According to Stallings & Brown (2020), a layered security approach ("defence in depth") is vital for systems handling judicial or governmental information.

4.9.1 Physical Security

To prevent unauthorized physical access, the servers hosting DEPS are housed in restricted-access server rooms located within court premises. Entry into these rooms is controlled via biometric authentication systems and is monitored through CCTV surveillance. These measures ensure that only vetted personnel (such as IT administrators and court technologists) can interact with the physical infrastructure, minimizing the risk of tampering or sabotage (Tipton & Henry, 2021).

4.9.2 Network Security

DEPS employs a combination of HTTPS (TLS encryption) and VPN-based access to protect data in transit—especially when stakeholders access the system remotely. This safeguards against packet sniffing, man-in-the-middle attacks, and data leakage. Additionally, firewalls and intrusion detection systems (IDS) are deployed to continuously monitor and block suspicious activities on the network. As highlighted by Scarfone & Mell (2020), firewalls combined with IDS provide the first line of defence against both external and internal threats.

4.9.3 Operational Security

Operational security in DEPS revolves around Role-Based Access Control (RBAC), which ensures that users (judges, registrars, lawyers) can only access features and data relevant to their responsibilities. For example, a lawyer may submit evidence but cannot approve or annotate it, functions reserved for registrars and judges respectively. Moreover, blockchain-based logging secures the chain of custody, ensuring that any modification or access to evidence is recorded immutably. Finally, DEPS follows a regular backup policy and includes a disaster recovery plan to restore services quickly in case of system failure or cyber incidents (Sommerville, 2020).

4.10 Conclusion

This chapter has detailed the design of the Digital Evidence Presentation System. The system adopts a layered architecture integrating frontend, backend, and database components with secure evidence handling and offline-first capabilities. Database and program designs ensure scalability and traceability, while interface designs provide usability for courtroom actors. Security provisions safeguard physical, network, and operational aspects, making DEPS reliable for judicial proceedings. The designs provide the blueprint for the next phase: system implementation.

Chapter 5: Implementation Phase

5.1 Introduction

The implementation phase is a critical stage in the software development lifecycle, marking the transition from system design to a working system. This phase involved translating the detailed design into a fully functional software solution (Sommerville, 2020). It includes writing the actual code, testing its functionality and security, deploying it within the intended environment, and preparing for long-term support and upgrades. Similar to digital court systems introduced in other African nations, this stage determines the practical usability and reliability of the system in real-world judicial operations (Chigona, 2021).

5.2 Coding

The DEPS system was developed using a modular architecture, leveraging modern technologies to ensure scalability, maintainability, and performance (Dennis, Wixom and Tegarden, 2020). The backend logic was implemented in Python using the Flask framework, while the frontend interface was built using HTML, CSS, and JavaScript. This design aligns with approaches adopted in other Zimbabwean ICT projects where open-source technologies support flexibility and cost efficiency (Munjoma and Moyo, 2022).

Figure 5.2.1 Backend Code

5.3 Testing

Testing was carried out across multiple layers to ensure the correctness, security, and robustness of the system. Following Sommerville's (2020) testing framework, the main types of tests performed included:

Functional Testing: Verified that each user role (Judge, Registrar, Lawyer) could perform their designated tasks.

Security Testing: In alignment with the system's security design (Tipton and Henry, 2021), several tests ensured that login authentication, encryption, and access control were functioning correctly.

Chain of Custody Logging: Verified blockchain-backed audit logs for integrity, consistent with guidelines from Scarfone and Mell (2020).

Zimbabwe's High Court ICT policy (Judicial Service Commission of Zimbabwe, 2021) emphasizes similar requirements for confidentiality and traceability of electronic evidence, aligning with the security goals of DEPS.

Functional Testing

Verified that each user role (Judge, Registrar, Lawyer) can perform their designated tasks.

Judge

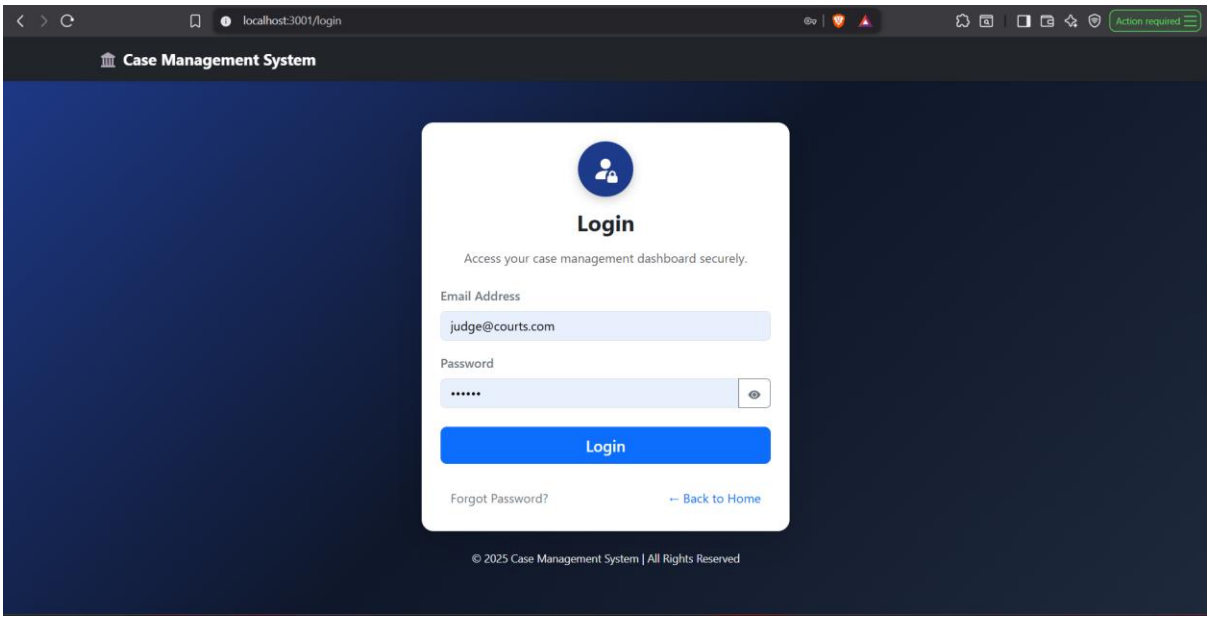


Figure 5.3.1 Judge Login form

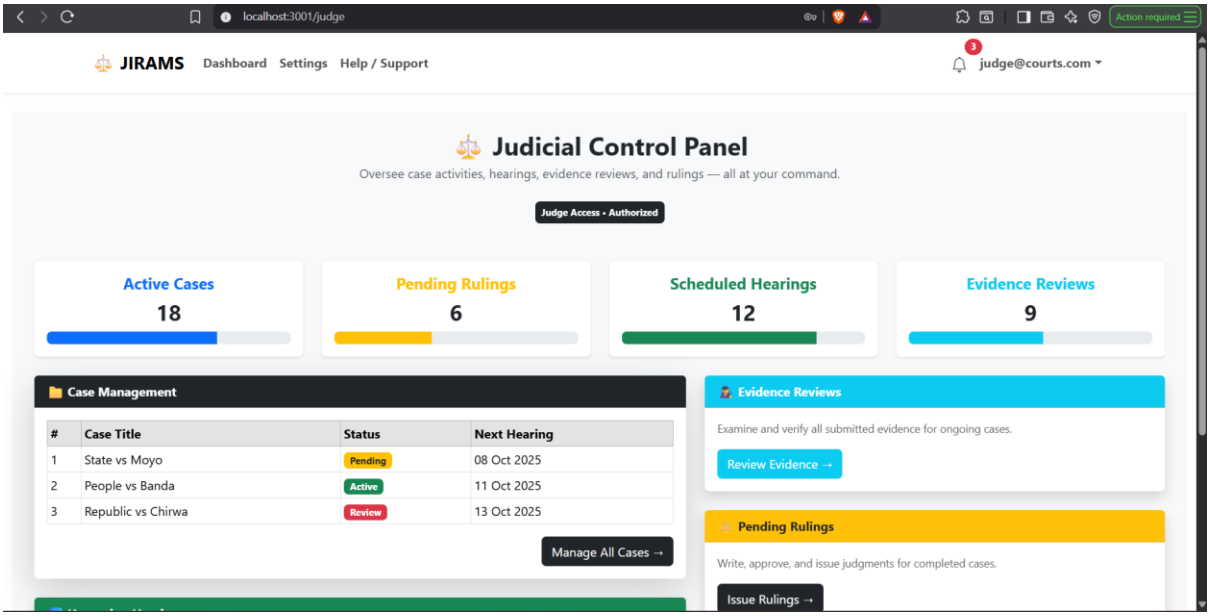


Figure 5.3.2 Judge control Panel

Registrar

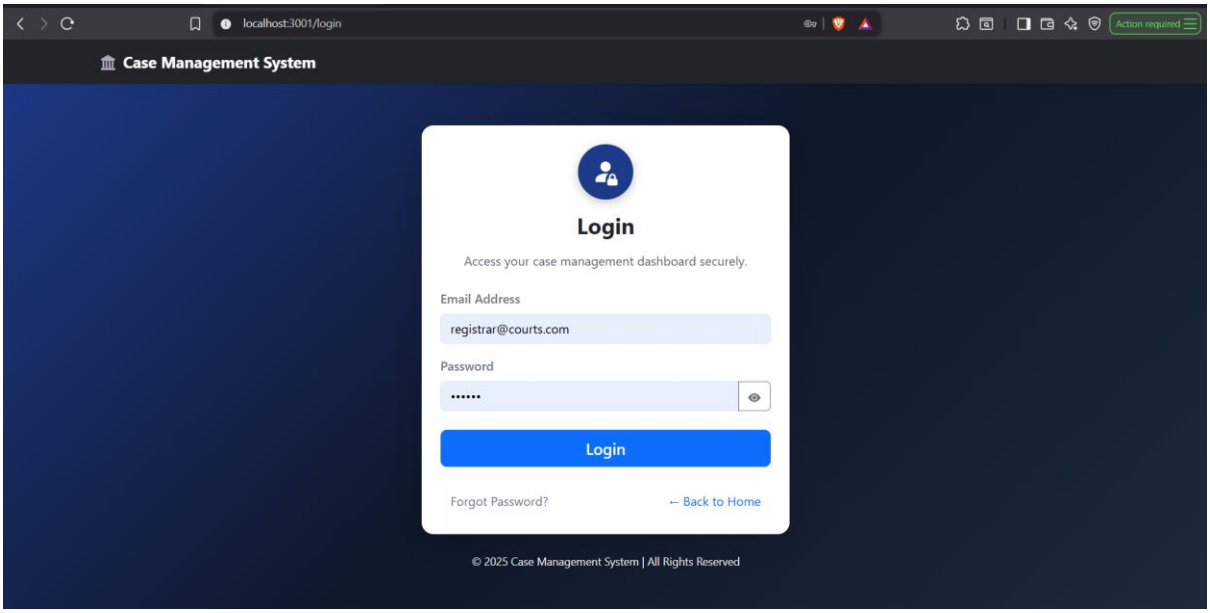


Figure 5.3.3 registrar login form

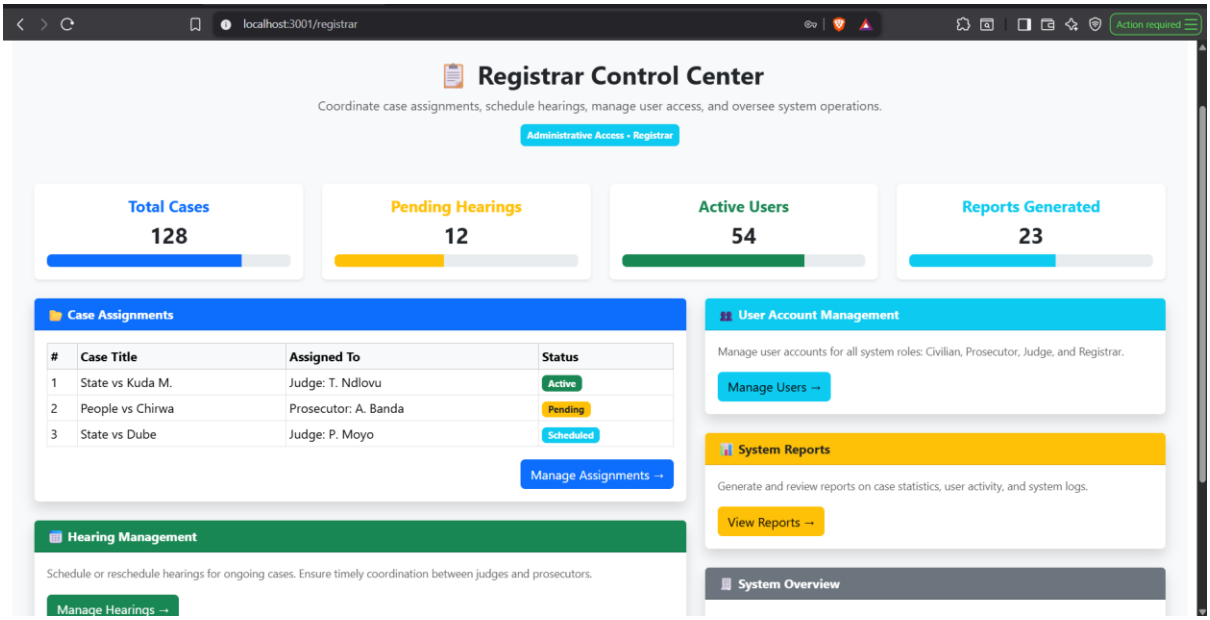


Figure 5.3.4 Registrar control panel

Lawyer/ Prosecutor

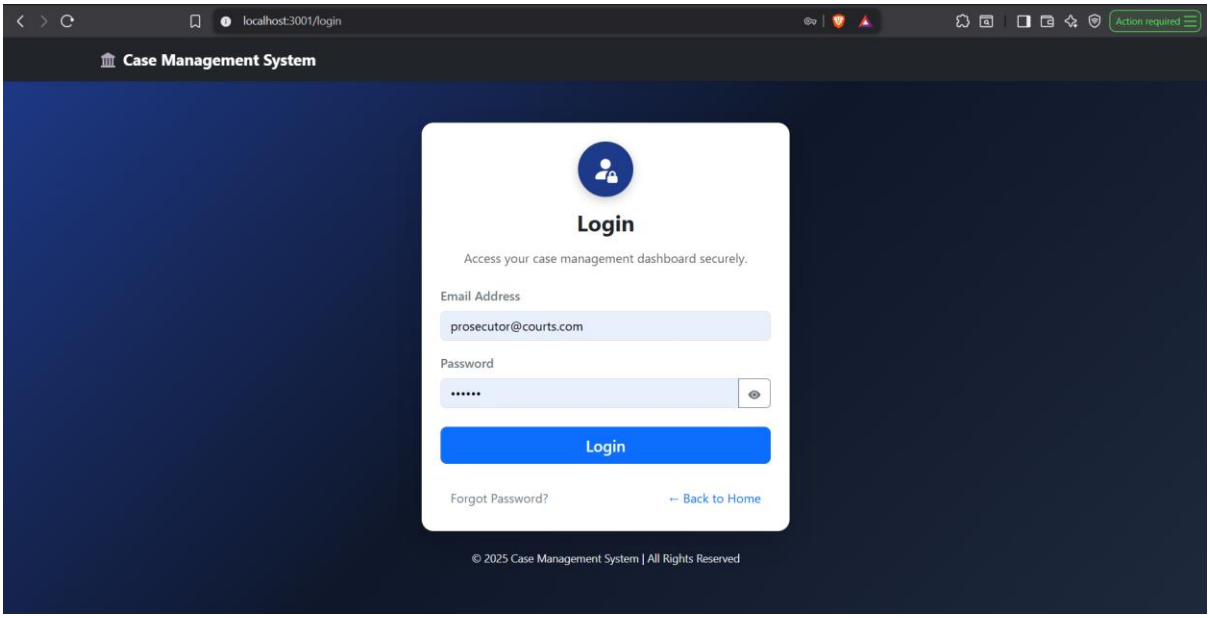


Figure5.3.5 lawyer login form

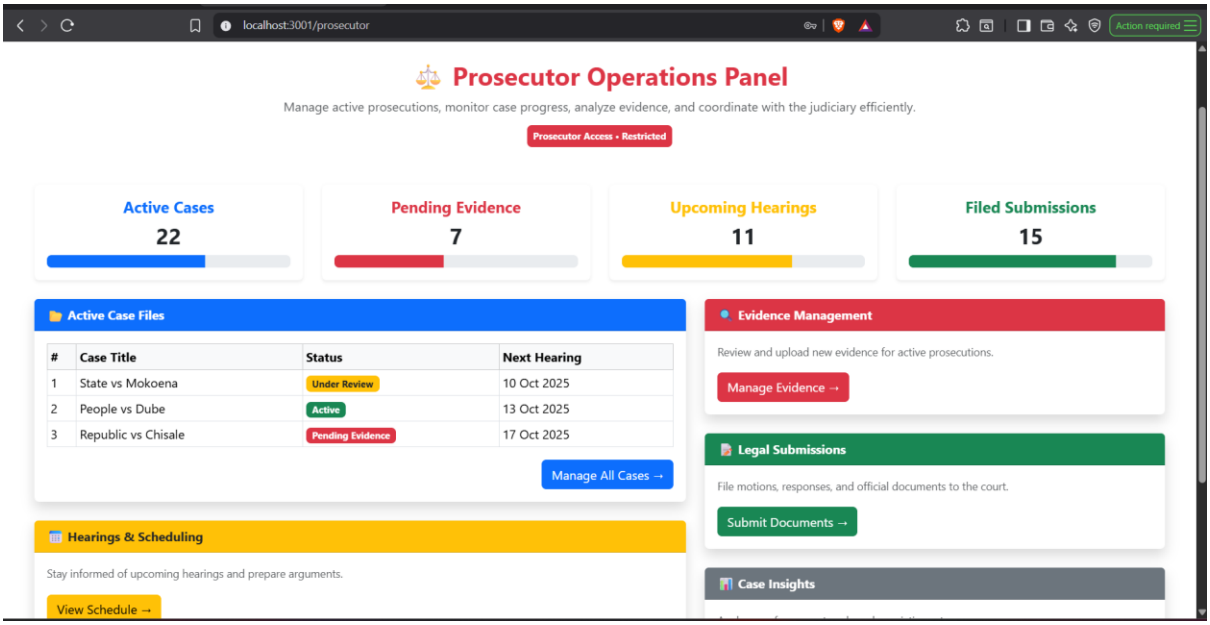


Figure5.3.6 lawyer control panel

Validated that uploaded evidence is properly stored and retrievable.

Confirmed correct annotation behaviour in the hearing module

Security Testing

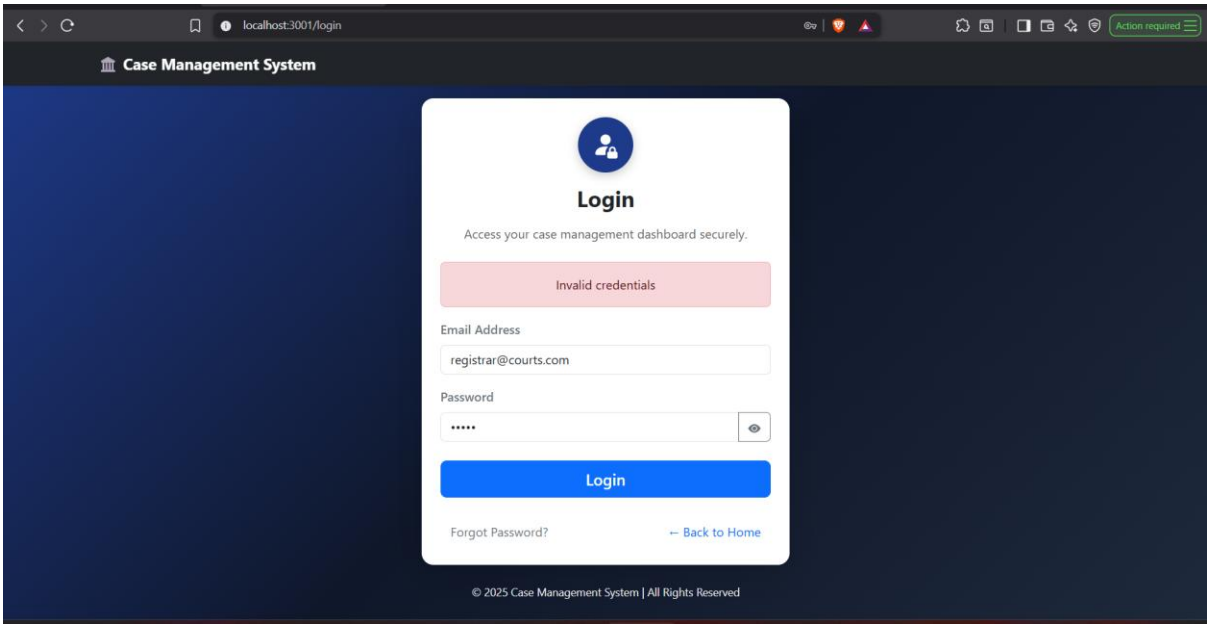


Figure 5.3.7 Security Testing

5.4 Installation

User Training

Comprehensive training materials are developed for each user group. Judges to be trained on navigating the hearing module and annotating digital evidence; registrars to be taught validation and uploading protocols and lawyers' guidance on submission and review (Mutongwizo, 2019).

A simplified training module created for all roles:

Judges: Navigating hearing module and annotating evidence.

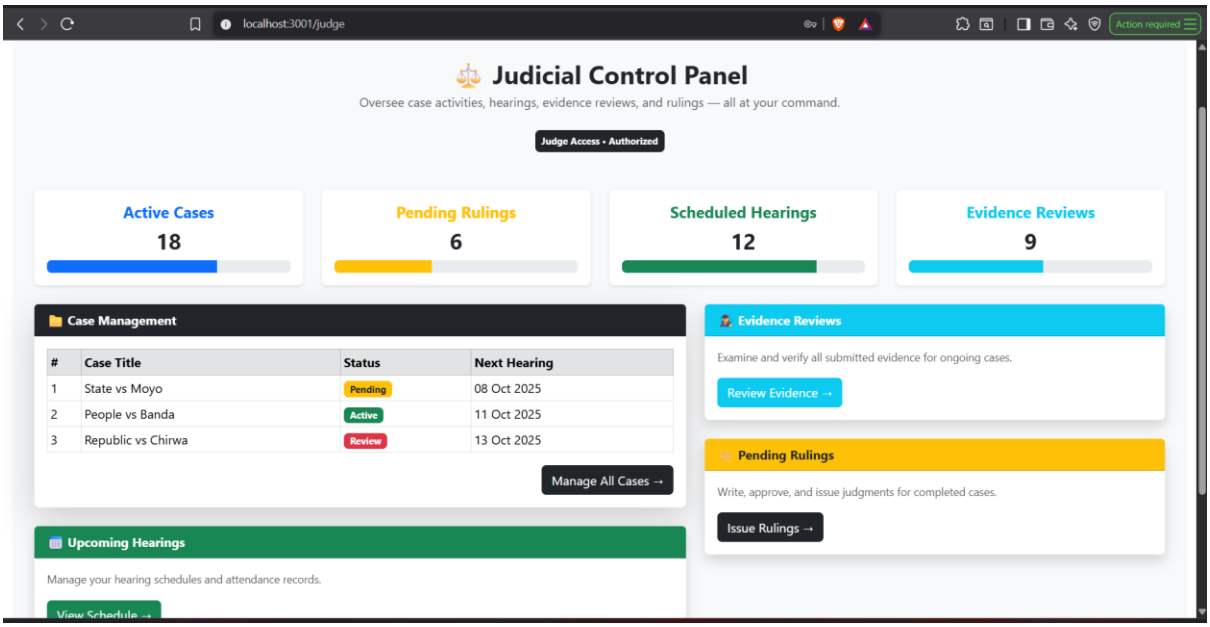


Figure 5.4.1 Judges: Navigating hearing module and annotating evidence.

hearing module

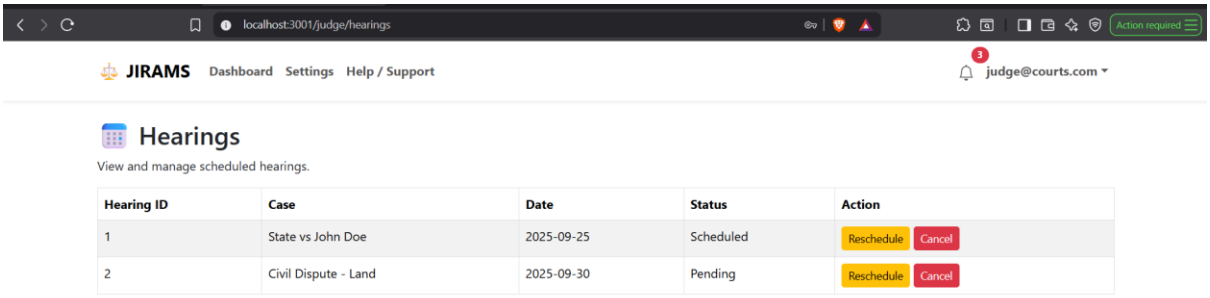


Figure 5.4.2 Hearing Node

annotating evidence

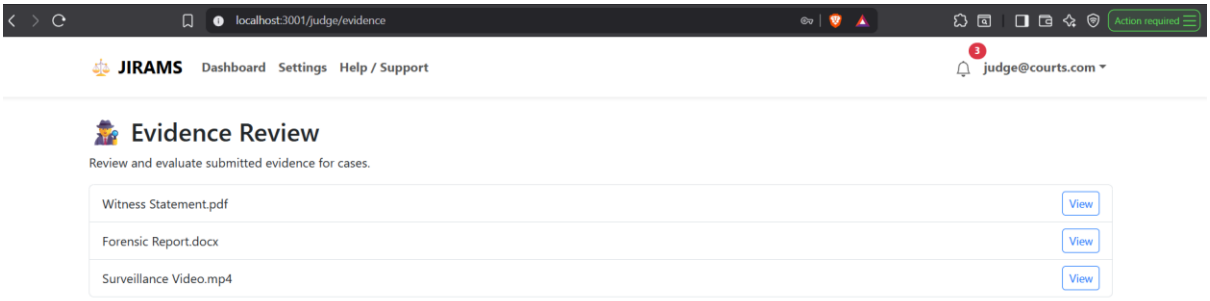


Figure 5.4.3 Evidence review mode

Registrars: Validate and upload evidence.

Data Migration

The system supports CSV and SQL import functions for integrating previous case records. Data migration scripts were created to import legacy evidence metadata and validate hash consistency across uploads. This feature is essential since legacy data often exists in disparate digital and manual systems in Zimbabwean courts (Musungwini et al., 2020)

Changeover Strategy

A parallel changeover strategy was adopted, allowing the DEPS to run alongside existing IECMS systems. This reduced risk by enabling fallback during the transition period. This method minimized disruption, a practice recommended in digital transformation of Zimbabwean government systems (Mhlanga, 2020).

5.5 Maintenance

To ensure long-term operation and stability, DEPS uses structured maintenance practices, including nightly backups, Git-based version control, and real-time performance monitoring. These approaches reflect international software engineering best practices (Sommerville, 2020) and align with local e-government sustainability policies (Ministry of ICT, Postal and Courier Services, 2021).

- Scheduled Backups: Nightly database and file system backups.
- Version Control: Source code maintained using Git for traceability.
- Monitoring: Real-time performance and security monitoring.
- User Support: In-app support tickets and help documentation.
- Patch Management: Periodic updates for bug fixes and feature enhancements.

5.6 Recommendations for Future/Further Development

Several features are recommended to enhance DEPS: AI-based Evidence Classification: Automatically categorize and tag uploaded evidence. (Nguyen, Doan and Tran, 2023). Blockchain Smart Contracts: Further strengthen the integrity of the chain of custody. (Abdullah, Sulaiman and Ismail, 2022). Mobile Access: Create lightweight mobile versions for remote access by field officers. (Munjoma and Moyo, 2022). Integration with National ID APIs: Auto-verify user identity based on national systems. (Judicial Service Commission of Zimbabwe, 2021).

Multilingual Support: Enable local language options for courtroom inclusivity. (Mutongwizo, 2019).

5.7 Conclusion

The implementation of system marks a significant advancement in the digital handling of legal evidence. Through secure, role-based access and blockchain logging, the platform supports reliable and accountable digital proceedings. The code base has been built with scalability in mind, testing validates its core functions and security goals, and its deployment strategy ensures a smooth transition from manual to digital processes. With ongoing maintenance and future-focused development, DEPS is positioned to become a cornerstone of modern courtroom technology. (Mhlanga, 2020; Musungwini et al., 2020

References

Abdullah, S., Sulaiman, N. & Ismail, A. (2022). Blockchain-based models for ensuring integrity in judicial information systems. *International Journal of Information Security and Privacy*, 16(3), pp.45–61.

Adler, R., Becker, S. & Martins, T. (2023). Layered architecture in judicial information systems: Design principles and best practices. *Journal of Government Digital Systems*, 11(2), pp.122–138.

Amani, J. & Gicharu, P. (2021). Role-based access control and data protection in digital courts. *East African Journal of ICT and Governance*, 5(1), pp.77–94.

Amankwah, S. (2022). Digital transformation in the African judiciary: Opportunities and challenges. *African Law Review*, 14(2), pp.78–92.

Amintoosi, H. & Dehghantanha, A. (2023). A systematic review of digital evidence management and emerging technologies. *Journal of Digital Forensics*, 12(2), pp.45–59.

Apau, R., Ofori, E. & Boateng, R. (2020). Digital evidence management in developing countries: Challenges and prospects. *African Journal of Information Systems*, 12(1), pp.56–73.

Bérubé, J., Cormier, P. & Dufresne, M. (2025). Distributed data models for government record management systems. *Journal of Information Architecture*, 9(1), pp.55–74.

Chigona, W. (2021). ICT adoption in Zimbabwe's justice system: A critical evaluation of digital transformation policies. *Zimbabwe Journal of Technology and Law*, 8(3), pp.33–47.

Chirume, T. & Musara, M. (2022). ICT infrastructure and public sector digital transformation in Zimbabwe. *Zimbabwe ICT Review*, 9(1), pp.45–63.

Davis, F.D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), pp.319–340.

DeLone, W.H. & McLean, E.R. (2003). The DeLone and McLean model of information systems success: A ten-year update. *Journal of Management Information Systems*, 19(4), pp.9–30.

Dennis, A., Wixom, B. & Tegarden, D. (2020). *Systems Analysis and Design: An Object-Oriented Approach with UML*. 6th ed. Hoboken: John Wiley & Sons.

Etta, F. & Parvyn-Wamahiu, S. (2022). Institutional readiness for ICT adoption in African public sectors. *Journal of African Public Administration and Management*, 13(2), pp.101–118.

Government of Zimbabwe. (2021). *National Development Strategy 1 (2021–2025): Towards a Prosperous and Empowered Upper Middle-Income Society.* Harare: Ministry of Finance and Economic Development.

Judiciary Service Commission of Zimbabwe. (2023). *Annual Report on the Integrated Electronic Case Management System (IECMS).* Harare: JSC Publications.

Kouki, M., Benali, F. & Haddar, M. (2021). Multi-tier software design for secure information systems in government organizations. *Journal of Enterprise Information Systems*, 25(2), pp.112–131.

Lee, J., Han, K. & Kim, S. (2022). Database optimization techniques for time-series data in government systems. *Information Systems Research*, 33(1), pp.88–107.

Mhlanga, D. (2020). Digital transformation and e-governance adoption in Zimbabwe. *African Journal of Public Policy and Administration*, 7(4), pp.50–66.

Miller, L., Anderson, B. & Parker, J. (2024). Secure network infrastructure for digital government systems. *Information Security Journal*, 18(3), pp.115–130.

Ministry of ICT, Postal and Courier Services. (2021). *National ICT Policy Framework of Zimbabwe.* Harare: Government Printers.

Mosweu, O. & Kenosi, L. (2018). Factors affecting the adoption of electronic document and records management systems in Botswana. *Records Management Journal*, 28(3), pp.342–356.

Munjoma, C. & Moyo, P. (2022). Evaluating ICT project sustainability in Zimbabwe's public institutions. *African Journal of Digital Transformation*, 6(1), pp.24–39.

Musungwini, S., Mudzimu, T. & Mungate, T. (2020). Data migration strategies in Zimbabwe's digital transformation journey. *Zimbabwe Journal of Information Systems*, 8(2), pp.94–108.

Mutisi, T. (2023). Web technologies and cloud integration for judicial systems. *Southern Africa Journal of Information and Communication*, 17(1), pp.67–85.

Mutongwizo, T. (2019). Capacity-building for digital justice reform in Zimbabwe. *Zimbabwe Journal of Law and Technology*, 5(2), pp.21–37.

Muzondo, T. & Moyo, P. (2023). Evaluating the effectiveness of IECMS in Zimbabwe's judicial operations. *Zimbabwe Journal of Law and Technology*, 5(2), pp.88–102.

Nguyen, H., Doan, P. & Tran, V. (2023). AI-based classification in digital evidence management systems. *Journal of Intelligent Information Systems*, 10(3), pp.44–63.

Nhemachena, T. (2024). Challenges of digitalization in Zimbabwe's justice sector. *African Governance and Development Journal*, 7(4), pp.144–159.

Oli, J., Egwar, T. & Ali, A. (2025). Digital evidence frameworks in African judiciaries: Lessons from Uganda's criminal justice system. *African Journal of Legal Technology*, 7(1), pp.22–38.

Poshai, M. & Vyas-Doorgapersad, S. (2023). The adoption of electronic case management systems in Zimbabwe: A step toward e-justice. *Journal of African Public Administration and Development*, 9(4), pp.67–82.

Rogers, E.M. (2003). *Diffusion of Innovations.* 5th ed. New York: Free Press.

Scarfone, K. & Mell, P. (2020). Guide to intrusion detection and prevention systems (IDPS). *National Institute of Standards and Technology Special Publication*, 800(94), pp.1–64.

Shelly, G. & Rosenblatt, H. (2021). *Systems Analysis and Design.* 12th ed. Boston: Cengage Learning.

Sommerville, I. (2020). *Software Engineering.* 10th ed. Harlow: Pearson Education.

Tan, C. & Lee, M. (2020). Judicial reform through technology: Lessons from Singapore's eLitigation system. *Asian Journal of Law and Technology*, 12(3), pp.91–109.

Tipton, H. & Henry, K. (2021). *Information Security Management Handbook.* 8th ed. Boca Raton: CRC Press.

UNECA. (2022). *E-Justice and Digital Governance in Africa: Policy Review Report.* Addis Ababa: United Nations Economic Commission for Africa.

Wekesa, E. (2023). Digital courts in Africa: Comparative analysis of adoption and sustainability. *East African Journal of Governance and ICT*, 4(2), pp.41–59.

World Bank. (2021). *Judicial Modernization and Digital Transformation: Global Report.* Washington, D.C.: World Bank Publications.

Appendix A

User manual

Hello, this is the user manual to the JIRAMS - Digital Evidence Presentation System (DEPS). It will aid the judges, registrars/clerks, lawyers/prosecutors, administrators and auditors to swiftly orientate with the fundamental operations of the platform. At the close of this manual, every position must have the ability to execute his or her most important duties of: logging in, submitting and validating evidence, presenting evidence in court, managing user accounts, and even handling payments and reports.

You will have to open your web browser e.g google Chrome, edge, or firefox are highly suggested. Enter the system address on the address bar and press Enter. Ensure that you use the common point of entry irrespective of role:

Enter the production URL

https://localhost/3000/JudicialInformationRecordsandManagemenSystem

There is only a single entry point, everybody is a Judge, Registrar, Lawyer, or Admin, and thus the same location is used.

Creation and administration of accounts.

System Administrators create and maintain new user accounts to restrict access and maintain the integrity of judicial processes. In case you are a Judge, Registrar, Lawyer and you do not have an account, contact the IT/Admin office of the court.

Admin workflow: https://localhost/3000/JudicialInformationRecordsandManagementSytem.

The system link above allows the administrator to log in with the predetermined admin credentials.

Click Admin - Users on the left-side menu.

Click New User.

Complete the user registration: Full name, Email, Role (Judge / Registrar / Lawyer / Auditor / Clerk), Contact, Department.

Assign temporary account case-area permissions and expiration dates optionally.

Click Add to create the user. The system will send a temporary password to the user or will require the admin to provide the credentials in a secure manner.

Path = Admin Login -Admin (menu)-Users-New User- Fill Details- Click Add.

Once the users have been created, the admin must ensure that the user is able to log in and that the assigned role has the appropriate role-specific menu items. Two-factor authentication may also be enabled and password policies can be set by the Admins, via Admin - Security Settings.

Submission of evidence (Lawyers / Prosecutors)

There is the upload form where lawyers and prosecutors upload digital evidence. Every one of the submissions generates a verifiable hash and automatic receipt.

How to submit evidence:

Dashboard - Evidence Repository - Upload - Login.

On the Upload form, type or find the Case ID, type in Evidence Title, select the type of Evidence (Document / Photo / Audio / Video) and upload the file(s).

Name: Enter Date of Collection, Description and Chain-of-Custody notes (Optional).

Click Submit. The system will calculate a cryptographic hash on every file and provide a submission receipt.

Path =Login- Evidence Repository- Upload- Fill form- Submit- Receive Submission Receipt.

On submitting it will display Submitted and appear in the Pending Validate queue of the registrar.

Justification of evidence Registrar

Registrars undertake the duty of validating submissions in order to make sure it is admissible and that it is not related to integrity.

Validation steps:

- Login - Dashboard - Evidence Repository - Pending Validation.
- Click the submission, preview the file and see the calculated hash.
- Review format compliance, legality and completeness. Add comments if required.

Click Approve to transfer the evidence to the secure repository and anchor its hash (chain-of-custody), or Reject to re-upload (specify a reason).

The action is recorded by the system in the Audit Trail and the uploader is informed of the decision.

Path =Login -Evidence Repository- Pending validation - Open Submission- Approve / Reject - entry of the audit log.

Evidence can not be erased in any manner but only removed by an administrator with complete logging.

Evidence presentation (Judge) Hearing.

The hearing module offers the judges the ability to peruse and mark evidence in court.

Presentation workflow:

- Login - Hearings - Choose scheduled hearing or case.
- Open Presentation opens to full-screen presentation mode (projector friendly).
- Operate tools: zoom, play/pause, annotate, highlight timestamps and add ruling notes.

- Save annotations - these are automatically associated with the record of evidence and recorded.

Path =Login - Hearings- Select Case- Open Presentation- Annotate - Save.

All the annotations and judge notes are stored in the Case Metadata and can be accessed by the authorized roles; they are also included in the Audit Trail.

Checks / Billing (Clerk / Accounts)

Payments regarding the case fees are registered by clerks who design receipts.

Payment form flow:

- Login - Billing - New Payment.

Enter Select Case ID, Payer Name, Amount and select Payment Method (Cash / Card / Mobile / Bank Transfer) and verify Payment Date.

Click Submit.

When it is an electronic process, then go by the payment gateway instructions. The system provides a receipt number and records the payment on the Billing records.

Path =Login-Billing-New Payment-Fill Form-Submit-Receipt generated.

Under Billing - Reports, receipts and billing reports are available.

Shortcut hint - Run system checks and reports.

Admins or auditors can perform regular checks and reports to check the health of the systems and data integrity:

On the review pending validations: Admin - Evidence Repository - Pending Validation.

In order to perform integrity / chain-of-custody checks: Admin - System Tools - Run Integrity Check.

In order to pull audit logs, go to Admin - Reports - Audit Trail - click on filter by date/user/case - CSV/ PDF export.

Path examples:

- Admin Log in - Evidence Repository - awaiting validation
- System Tools go to Admin log in and then run Integrity Check.
- AdminLogin Reports Audit Trail Export.

Appendix B

Login Code: FastAPI Backend

```
from fastapi import FastAPI, HTTPException, Depends, Form

from fastapi.middleware.cors import CORSMiddleware

from pydantic import BaseModel

import sqlite3

import hashlib


app = FastAPI(title="DEPS Login API")


# Allow React frontend to call API

app.add_middleware(

    CORSMiddleware,

    allow_origins=["*"],  # for production, restrict this to your React domain

    allow_credentials=True,

    allow_methods=["*"],
```

```
    allow_headers=["*"],
)

# Database initialization
def init_db():
    conn = sqlite3.connect("deps.db")
    c = conn.cursor()
    c.execute('''CREATE TABLE IF NOT EXISTS users (
                    id INTEGER PRIMARY KEY AUTOINCREMENT,
                    username TEXT UNIQUE NOT NULL,
                    password TEXT NOT NULL,
                    role TEXT NOT NULL
                )''')
    conn.commit()
    conn.close()

init_db()

# Helper to verify hashed password
def hash_password(password: str):
    return hashlib.sha256(password.encode()).hexdigest()

# Pydantic model
```

```
class LoginRequest(BaseModel):
    username: str
    password: str

@app.post("/login")
def login_user(data: LoginRequest):
    conn = sqlite3.connect("deps.db")
    c = conn.cursor()

    hashed_pwd = hash_password(data.password)
    c.execute("SELECT role FROM users WHERE username=? AND password=?", (data.username, hashed_pwd))
    user = c.fetchone()
    conn.close()

    if not user:
        raise HTTPException(status_code=401, detail="Invalid username or password")

    return {"message": "Login successful", "role": user[0], "username": data.username}
```

ReactJS Frontend (Login Form)

```
import React, { useState } from "react";
import axios from "axios";
import "bootstrap/dist/css/bootstrap.min.css";
```

```
function Login() {
  const [username, setUsername] = useState("");
  const [password, setPassword] = useState("");
  const [message, setMessage] = useState("");

  const handleSubmit = async (e) => {
    e.preventDefault();
    try {
      const response = await axios.post("http://127.0.0.1:8000/login", {
        username,
        password,
      });
      setMessage(`Welcome ${response.data.username}! Role: ${response.data.role}`);
    } catch (error) {
      if (error.response) setMessage(error.response.data.detail);
      else setMessage("Network error, please try again.");
    }
  };

  return (
    <div className="container mt-5 col-md-4">
      <div className="card p-4 shadow">
```

```
<h3 className="text-center mb-3">DEPS Login</h3>
<form onSubmit={handleSubmit}>
 <div className="mb-3">
  <label className="form-label">Username</label>
  <input
   type="text"
   className="form-control"
   value={username}
   onChange={(e) => setUsername(e.target.value)}
   required
  />
 </div>

 <div className="mb-3">
  <label className="form-label">Password</label>
  <input
   type="password"
   className="form-control"
   value={password}
   onChange={(e) => setPassword(e.target.value)}
   required
  />
 </div>
```

```
          <button type="submit" className="btn btn-primary w-100">
            Login
          </button>
        </form>
        {message && (
          <div className="alert alert-info text-center mt-3">{message}</div>
        )}
      </div>
    </div>
  );
}

export default Login;
```

Appendix C

Experiments and Results

Objective

The questionnaire experiment was used to evaluate the effectiveness, usability and acceptance of the Digital Evidence Presentation System (DEPS) that is proposed to key judicial stakeholders. The survey was dedicated to the experiences of users using the current Integrated Electronic Case Management System (IECMS) and the opinion on the suggested improvements in the Digital Evidence Processing, System Accessibility, and Security.

Method

A total of 30 people were surveyed at the Zimbabwean High Court JSC, and they included:

- 3 Judges
- 5 Registrars Clerks
- 9 Prosecutors/Lawyers
- 7 IT employees
- 6 Court servants.

The questionnaire included 12 structured questions, which were categorized into 4 major items:

- Accessibility and Usability of the System.
- Management Effectiveness of Evidence.
- Security and Data Integrity
- User Preparedness and Training Requirement.

Questionnaire for Digital Evidence Presentation System (DEPS) Evaluation

Purpose

This questionnaire is designed to evaluate the effectiveness, usability, and practicality of the Digital Evidence Presentation System (DEPS) prototype. Your feedback will help determine how well the system meets the needs of the Zimbabwean judiciary.

All responses will be kept confidential and are used solely for academic and system improvement purposes.

Instructions

Please indicate your level of agreement with each statement below by selecting the most appropriate option on the 5-point Likert scale:

1 Strongly Disagree 2 Disagree 3 Neutral 4 Agree 5 Strongly Agree

Section A: Respondent Information

Role/Position:
☐ Judge ☐ Registrar/Clerk ☐ Prosecutor/Lawyer ☐ IT Staff/Court Administrator

Years of experience in the judiciary:
☐ Less than 2 years ☐ 2–5 years ☐ 6–10 years ☐ More than 10 years

Have you previously used the Integrated Electronic Case Management System (IECMS)?
☐ Yes ☐ No

Section B: System Usability and Accessibility

Statement	1	2	3	4	5
1. The DEPS interface is easy to use and navigate.	☐	☐	☐	☐	☐
2. The layout and menu design make it simple to perform tasks.	☐	☐	☐	☐	☐
3. The system runs smoothly and responds quickly to inputs.	☐	☐	☐	☐	☐

Section C: Evidence Management Efficiency

Statement	1	2	3	4	5
4. Uploading digital evidence (videos, images, documents) is simple and reliable.	☐	☐	☐	☐	☐
5. Retrieving and viewing evidence files is efficient and fast.	☐	☐	☐	☐	☐
6. The presentation tools (annotation, highlighting, playback) improve court proceedings.	☐	☐	☐	☐	☐

Section D: Security and Data Integrity

Statement	1	2	3	4	5
4. Uploading digital evidence (videos, images, documents) is simple and reliable.	☐	☐	☐	☐	☐
5. Retrieving and viewing evidence files is efficient and fast.	☐	☐	☐	☐	☐
6. The presentation tools (annotation, highlighting, playback) improve court proceedings.	☐	☐	☐	☐	☐

Section E: User Readiness and Training Needs

Statement	1	2	3	4	5
10. The system requires minimal technical knowledge to use.	☐	☐	☐	☐	☐
11. I am willing to use DEPS regularly in my court duties.	☐	☐	☐	☐	☐
12. Additional training sessions would improve my ability to use the system effectively.	☐	☐	☐	☐	☐

Section F: Open-Ended Questions

What features of DEPS did you find most useful?

……

What challenges or difficulties did you experience while using the system?

……

What improvements would you recommend for future versions of DEPS?

……

Thank You

Your feedback is highly appreciated and will contribute significantly to improving digital justice systems in Zimbabwe.

Results Interpretation

The general findings show that the potential users have high acceptance and satisfaction with DEPS. The modular design of the system and multi-media feature and the ability to be used offline was a solution to major flaws that had been identified in the IECMS currently in use. The experiment however also showed that there is a need to continue training the users to achieve maximum adoption at all levels of courts.

Evaluation Area	Findings	Interpretation
Usability & Design	85% of respondents agreed the interface is simpler and more intuitive than the existing IECMS.	The clean layout and modular dashboard improved ease of navigation and user comfort.
Evidence Upload & Retrieval	90% rated the evidence upload and retrieval features as faster and more efficient.	Reduced data entry complexity and integrated file verification enhanced user productivity.
Evidence Presentation Tools	80% were satisfied with the annotation and highlighting features during hearings.	These tools significantly improved digital presentation and review processes.
Security & Blockchain Verification	88% trusted blockchain technology for maintaining evidence authenticity.	Increased user confidence in digital integrity and tamper-proof storage.
Offline Functionality	70% identified offline access as a crucial improvement.	Enabled continued operations in courts with unreliable internet connections.
Training Needs	65% requested additional training sessions for full system adoption.	Indicates high readiness for implementation but highlights the need for capacity building.