**EVIDENCE PROTECTION SYSTEM USING**

**BLOCKCHAIN TECHNOLOGY**

**Project Stage-II (CS851PC)**

***Submitted***

*in partial fulfilment of the requirements for*

*the award of the degree of*

**BACHELOR OF TECHNOLOGY**

*in*

**COMPUTER SCIENCE AND ENGINEERING**

*by*

**MOHAMMED ZAID**

**[Reg. No. 21261A0537]**

*and*

**UZMA BEGUM**

**[Reg. No. 21261A0563]**

**Under the guidance of**

**Dr. V. Subba Ramaiah, Assistant Professor**

**Dr. A. Ratna Raju, Assistant Professor**

**DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**MAHATMA GANDHI INSTITUTE OF TECHNOLOGY ( A)**

**HYDERABAD-500075, TELANGANA**

**MAY-2025** `



**CERTIFICATE**

This is to certify that the report entitled “Evidence Protection System Using Blockchain Technology” being submitted by Mr. MOHAMMED ZAID bearing Reg.No. 21261A0537 and Ms. UZMA BEGUM bearing Reg.No. 21261A0563 in partial fulfilment for the award of Bachelor of Technology (B.Tech.) in Computer Science and Engineering to the Department of CSE, Mahatma Gandhi Institute of Technology (A), Hyderabad-500075, Telangana, is a record of bonafide work carried out by them under our guidance and supervision, at our organization/institution.

The results embodied in this report have not been submitted to any other University or Institute for the award of any degree or diploma.

Signature of Supervisor 1 Signature of Supervisor 2

**Dr. V. Subba Ramaiah Dr. A. Ratna Raju**

Assistant Professor Assistant Professor

Head of Department

**Dr. C.R.K Reddy**

Professor, Dept.of CSE

**EXTERNAL EXAMINER**

**DECLARATION**

We hereby declare that the work described in this report, entitled **“Evidence Protection System Using Blockchain Technology”** which is being submitted by us in partial fulfilment for the award of **Bachelor of Technology** (**B.Tech.)** in Computer Science and Engineering to the **Department of CSE,** **Mahatma Gandhi Institute of Technology (A)**, **Hyderabad-500075, Telangana,** is the result of investigations carried out by us under the guidance of **Dr. V. Subba Ramaiah** and **Dr. A. Ratna Raju**.

# The work is original and has not been submitted for any Degree/Diploma of this or any other university.

Place: Hyderabad

Date:

Signature:

Name of the Student: **MOHAMMED ZAID**

[Reg.No: **21261A0537**]

Signature:

Name of the Student: **UZMA BEGUM**

[Reg.No: **21261A0563**]

# ACKNOWLEDGEMENT

The satisfaction that accompanies the successful completion of any task would be incomplete without the mention of people who made it possible because success is the abstract of hard work and perseverance, but steadfast of all is encouraging guidance. So, we acknowledge all those whose guidance and encouragement served as a beacon light and crowned our efforts with success.

We would like to express our sincere thanks to, **Prof G. Chandra Mohan Reddy, Principal, MGIT**, for providing the working facilities in college.

We wish to express our sincere thanks and gratitude to **Dr. C.R.K Reddy, Professor and HoD,** **Department of CSE, MGIT,** for all the timely support and valuable suggestions during the period of project.

We are extremely thankful to **Dr. V. Subba Ramaiah, Assistant Professor, Department of CSE, MGIT and Ms. M. Mamatha, Assistant Professor, Department of CSE, MGIT,** MajorProjectCoordinators for their encouragement and support throughout the project.

Finally, we would also like to thank all the faculty and staff of the CSE Department who helped us directly or indirectly in completing this project.

**MOHAMMED ZAID**

[Reg.No: **21261A0537**]

**UZMA BEGUM**

[Reg.No: **21261A0563**]

# ABSTRACT

The proposed Evidence Protection System (EPS) represents a paradigm shift in evidence management by combining the strengths of blockchain technology with advanced cryptographic measures. The decentralized nature of the system ensures that evidence records are distributed across multiple nodes, making them inherently resistant to tampering or unauthorized modifications. Each record is secured with a timestamp and verified through consensus mechanisms, ensuring the authenticity and chronological order of the data. The integration of smart contracts further enhances the system's functionality by automating critical processes, such as logging evidence transactions, verifying user permissions, and managing access rights. These contracts eliminate reliance on manual interventions, reducing human error while enforcing strict custody chains that are transparent and auditable. To safeguard sensitive information, the EPS incorporates cryptographic techniques, such as encryption to protect confidentiality and hashing to verify data integrity, enabling users to confirm that evidence has not been altered. By addressing key vulnerabilities in traditional evidence handling, EPS delivers a robust, secure, and trustworthy framework that minimizes risks of tampering, unauthorized access, and data breaches, making it a vital tool in modern evidence protection.

# TABLE OF CONTENTS

# CHAPTER PAGE NO.

# 

[Certificate](#_CERTIFICATE)  i  
[Declaration ii](#_DECLARATION)

[Acknowledgement ⅲ](#_ACKNOWLEDGEMENT) [Abstract ⅳ](#_TABLE_OF_CONTENTS)

Table of Contents ⅴ

List of Tables vi

[List of Figures](#_LIST_OF_ABBREVIATIONS)  vii

[List of Abbreviations viii](#_ABSTRACT)

**CHAPTER 1** [**INTRODUCTION 1**](#_INTRODUCTION)**-3**

* 1. [Problem Definition 1](#_1.1_Problem_Definition)
  2. [Existing Applications 2](#_1.2_Existing_Applications)
  3. [Proposed System 2](#_1.3_Proposed_Application)
  4. [Requirements Specification 3](#_1.4_Requirements_Specification)

**CHAPTER 2 LITERATURE SURVEY 4-14**

2.1 [Literature Survey Table](#_S.No)  11

**CHAPTER 3 METHODOLOGY 15-17**

3.1 Technologies Used 15 3.2 [Development Process 16](#_3.2_Development_Process:)

**CHAPTER 4 DESIGN OF EVIDENCE PROTECTION SYSTEM 18-30**

* 1. Design 18

4.2 [Process Flow Diagram 21](#_4.2_PROCESS_FLOW)

4.3 System Architecture 23

4.4 UML Diagrams 24

4.4.1 Use case diagram of Evidence Protection system 24

4.4.2 Class diagram of Evidence Protection system 25

4.4.3 Activity diagram of Evidence Protection system 26

4.4.4 Sequence Diagram of Evidence Protection System 27

4.4.5 Collaboration diagram of Evidence Protection System 28

4.4.6 Component diagram of Evidence Protection System 29

4.4.7 Deployment diagram of Evidence Protection System 30

[**CHAPTER 5 IMPLEMENTATION 31-40**](#_IMPLEMENTATION)

* 1. [Technology Stack 35](#_5.1_TECHNOLOGY_STACK)
  2. Features 35
  3. Implementation Details 37
  4. User Interface 38

**CHAPTER 6 RESULT 41-48**

6.1 User Signup Interface 41

6.2 User Registration Page 41

6.3 User Signup Confirmation (1) 42

6.4 User Signup (2) 43

6.5 User Signup Confirmation(2) 43

6.6 User login 44

6.7 Add Information and Evidence 42

6.8 User Signin 45

6.9 Checking information and Displaying 48

6.10 Ganache Screen 49

6.11 Metamask Screen 50

6.12 Test cases table 51

**CHAPTER 7 CONCLUSION AND FUTURE SCOPE 52**

7.1 Conclusion 52

7.2 Future Scope 52

References 53

Appendix: A Source code 55

**LIST OF TABLES**

|  |  |  |
| --- | --- | --- |
| Table No. | Description | Page No. |
| Table 2.1 | Literature Survey Table | 11 |

Table 6.12 Test cases and results 51

# LIST OF FIGURES

|  |  |  |
| --- | --- | --- |
| **Figure No.** | **Description** | **Page No.** |
| 4.1 | Design of Evidence Protection system | 18 |
| 4.2 | Process flow Diagram of Evidence Protection system | 22 |
| 4.3 | Detailed System Architecture of Evidence Protection system | 23 |
| 4.4.1 | Use Case Diagram of Evidence Protection system | 24 |
| 4.4.2 | Class Diagram of Evidence Protection system | 25 |
| 4.4.3 | Activity Diagram of Evidence Protection system | 26 |
| 4.4.4 | Sequence Diagram of Evidence Protection system | 27 |

4.4.5 Collaboration diagram of Evidence Protection System 28

4.4.6 Component diagram of Evidence Protection System 29

4.4.7 Deployment diagram of Evidence Protection System 30

6.1 User Signup Interface of Evidence Protection System 41

6.2 User Registration Page of Evidence Protection System 42

6.3 User Signup Confirmation of Evidence Protection System 37

6.4 User Signup (2) of Evidence Protection System 43

6.5 User Signup Confirmation (2) of Evidence Protection System 44

6.6 User login of Evidence Protection System 44

6.7 Add Information and Evidence of Evidence Protection System 46

6.8 User Signin of Evidence Protection System 48

6.9 Checking information and Displaying 49

6.10 Ganache Screen of Evidence Protection System 49

6.11 Metamask Screen of Evidence Protection System 50

# LIST OF ABBREVIATIONS

|  |  |  |
| --- | --- | --- |
| S.NO | ABBREVIATIONS | FULLFORM |
| 1. | HTML | Hypertext Markup Language |
| 2. | CSS | Cascading Style Sheets |
| 3. | i5 | Intel Core i5 |
| 4. | GB | Gigabytes |
| 5. | GAN | Generative Adversarial Network |
| 6. | UAT | User Acceptance Testing |

# CHAPTER 1

# INTRODUCTION

In contemporary society, managing and preserving evidence is critical for fostering trust and accountability in areas such as legal proceedings, supply chain management, financial transactions, and intellectual property disputes. The integrity and authenticity of evidence form the foundation of fair decision-making and justice, yet traditional evidence management practices often struggle to meet these high standards. Centralized storage systems are particularly vulnerable to tampering, unauthorized access, and human errors, which can compromise the credibility of the evidence. These shortcomings underscore the urgent need for innovative solutions capable of ensuring the security, transparency, and reliability of sensitive information. Blockchain technology, with its decentralized and immutable characteristics, has emerged as a promising alternative to address these challenges effectively.

# 1.1 PROBLEM DEFINITION

Existing systems for evidence management in legal and investigative processes often face various drawbacks, impacting their efficiency, security, and overall effectiveness. Many traditional systems rely on centralized databases, making them vulnerable to hacking, unauthorized access, and manipulation. Traditional systems may lack robust security measures to protect sensitive information. Without advanced encryption and access controls, the risk of data breaches and unauthorized disclosure of evidence remains high.Some existing systems may face challenges in handling a large volume of evidence or adapting to the increasing complexity of legal cases.

**1.2 EXISTING SYSTEM**

The existing work is a conceptual model called "EvidenceChain" that utilizes blockchain technology to prevent spoliation of evidence in South Asian countries. The model allows citizens to anonymously upload digital evidence, which is then stored in an immutable and indestructible distributed repository. The ownership of evidence is transferred from authorities to ordinary citizens, which can minimize spoliation of evidence and human rights abuse. The model is theoretically tested against high-profile spoliation of evidence cases from four South Asian developing countries.

# 1.3 PROPOSED SYSTEM

The Evidence Protection System (EPS) presented in this paper harnesses the unique attributes of blockchain technology to create a secure, tamper-proof, and transparent environment for safeguarding evidence across a spectrum of applications. The system offers a comprehensive set of features that address the challenges associated with evidence tampering, data manipulation, and unauthorized access, while also promoting efficient evidence handling and verification. The proposed Evidence Protection System introduces a paradigm shift in evidence management by harnessing the capabilities of blockchain technology. Its robust architecture ensures the integrity, authenticity, and accessibility of evidence, while its automation and security features streamline evidence handling processes. With applications across various domains, the EPS holds the potential to redefine how evidence is protected, shared, and trusted in our increasingly digital and interconnected world.

# 1.4 REQUIREMENTS SPECIFICATION

Requirement Specifications describe the arti-craft of Software Requirements and Hardware Requirements used in this project.

**Software Requirements**

**1) Software :** Python IDE (3.7.0), Node Js, Visual Studio, Community Version, Ganache, MetaMask-Chrome Extension

**2) Primary Language :** Python

**3) Frontend Framework :** Flask

**4) Back-end Framework :** JavaScript ,Python

**5) Front-End Technologies** : HTML, CSS, JavaScript, Bootstrap4

**Hardware Requirements**

**1) Operating System :** Windows Only

**2) Processor :** i5 and above

**3) Ram** : 8gb and above

**4) Hard Disk :** 25 GB in local drive

# CHAPTER 2

# LITERATURE SURVEY

# 1.“Blockchain-Powered Forensic Evidence Storage: A New Approach to Data Security” [1] byA. Sangekar, V. Gumalwad, S. Khillare, K. Warbhog, S. Hadbe and U. Tupe.

The paper *"Blockchain-Powered Forensic Evidence Storage: A New Approach to Data Security"* by A. Sangekar et al. explores the use of blockchain technology to enhance the security, transparency, and integrity of forensic evidence storage. It proposes a decentralized system that prevents tampering and ensures traceability of evidence throughout the investigation process. The approach aims to eliminate single points of failure and unauthorized access. By leveraging blockchain’s immutability and smart contracts, the system enhances trust and reliability in forensic data handling.

**2.“Implementation of Blockchain and IPFS to safeguard evidentiary data”** [2]byS. Srivastava, G. Kaur, Himank and S. Singla.

The paper "Implementation of Blockchain and IPFS to Safeguard Evidentiary Data" by S. Srivastava et al. presents a secure framework combining Blockchain and InterPlanetary File System (IPFS) to protect digital evidence. The system ensures data immutability, decentralized storage, and secure access control. Blockchain is used to store metadata and hash values, while IPFS handles the actual data storage. This hybrid approach enhances the integrity, traceability, and resilience of evidentiary data against tampering or loss.

**3.“A Framework for Digital Forensics Using Blockchain to Secure Digital Data”** [3]by J. Jacob and S. Kumar.

The paper "*A Framework for Digital Forensics Using Blockchain to Secure Digital Data*" by J. Jacob and S. Kumar proposes a blockchain-based framework to enhance the security and reliability of digital forensic data. The system ensures tamper-proof logging, transparent evidence tracking, and secure chain of custody. Blockchain's decentralized nature helps maintain data integrity and authenticity throughout investigations. The framework supports real-time verification and promotes trust in digital forensic processes.

**4.“A hybrid framework for secure data transfer for enhancing the Blockchain Security”** [4]by P. Batta, S. Ahuja and A. Kumar.

The paper *"A Hybrid Framework for Secure Data Transfer for Enhancing the Blockchain Security"* by P. Batta, S. Ahuja, and A. Kumar introduces a hybrid model combining cryptographic techniques with blockchain to improve secure data transfer. The framework integrates symmetric and asymmetric encryption to ensure confidentiality, integrity, and authentication. It strengthens blockchain security by addressing vulnerabilities during data transmission. This approach enhances trust, resilience, and robustness in blockchain-based systems.

**5.“Security Digital Evidence”** [5]byJ. Richter, N. Kuntze and C. Rudolph.

The paper *"Security Digital Evidence"* by J. Richter, N. Kuntze, and C. Rudolph focuses on securing digital evidence through trusted computing and cryptographic methods. It emphasizes ensuring authenticity, integrity, and proper chain of custody in forensic investigations. The authors propose mechanisms to protect evidence from tampering and unauthorized access.

**6. “Safe-Keeping Digital Evidence with Secure Logging Protocols: State of the Art and Challenges”** [6]byR. Accors.

The paper *"Safe-Keeping Digital Evidence with Secure Logging Protocols: State of the Art and Challenges"* by R. Accorsi reviews existing secure logging mechanisms used to protect digital evidence. It highlights the importance of tamper-evident logs, audit trails, and integrity-preserving techniques in forensic investigations. The paper discusses current solutions, their limitations, and the challenges in ensuring long-term evidence security. It also emphasizes the need for robust, verifiable, and efficient logging protocols in digital forensics.

**7. “Evidence-Based Techniques for Evaluating Cyber Protection Systems for Critical Infrastructures”** [7]byJ. Darby, J. Phelan, P. Sholander, B. Smith, A. Walter and G. Wyss.

The paper*"Evidence-Based Techniques for Evaluating Cyber Protection Systems for Critical Infrastructures"* by J. Darby et al. presents methodologies to assess the effectiveness of cyber protection systems in safeguarding critical infrastructure. It emphasizes data-driven evaluations using real-world scenarios and threat models. The approach helps identify system vulnerabilities, measure resilience, and guide improvements. The authors aim to enhance decision-making in cybersecurity through empirical evidence and structured analysis.

**8. “Digital Copyright Depository System Enhanced by Blockchain”** [8]byW. Yang, P. He, Z. Yang, X. Yi and C. Chen.

The paper *"Digital Copyright Depository System Enhanced by Blockchain"* by W. Yang, P. He, Z. Yang, X. Yi, and C. Chen proposes a blockchain-based system to protect and manage digital copyrights. The system ensures tamper-proof registration, transparent ownership tracking, and secure verification of digital content. By leveraging smart contracts, it automates copyright validation and dispute resolution.

**9. “Blockchain-Based Digital Forensics Investigation Framework in the Internet of Things and Social Systems”** [9]byS. Li, T. Qin and G. Min.

The paper *"Blockchain-Based Digital Forensics Investigation Framework in the Internet of Things and Social Systems"* by S. Li, T. Qin, and G. Min introduces a blockchain-enabled framework for conducting digital forensics in IoT and social systems. It ensures secure evidence collection, tamper-proof storage, and transparent traceability. The framework addresses challenges like data volatility and integrity in distributed environments. Blockchain's decentralization strengthens trust and reliability in forensic investigations across interconnected devices and platforms.

**10. “Blockchain for Cybersecurity\_ Securing Data Transactions and Enhancing Privacy in Digital Systems”** [10] byD. Rajababu, S. Surya, M. Padhiary and H. Modi.

The paper *"Blockchain for Cybersecurity: Securing Data Transactions and Enhancing Privacy in Digital Systems"* by D. Rajababu, S. Surya, M. Padhiary, and H. Modi explores how blockchain technology can be used to secure data transactions and protect user privacy. It highlights blockchain’s role in ensuring data integrity, confidentiality, and transparency in digital systems. The authors discuss cryptographic mechanisms and decentralized structures that mitigate cyber threats. The approach enhances cybersecurity by reducing reliance on centralized authorities and improving trust in data exchanges.

**11**. **“Legal challenges in adopting blockchain for evidence protection”** [11] by M. Anderson and J. Thompson.

This paper explores the legal implications of using blockchain for protecting digital evidence.Using real-world case studies, it identifies regulatory and policy challenges in adoption.It highlights how legal systems lag behind technological advancements.A major merit is its comprehensive legal perspective on blockchain use in law.However, it lacks discussion on technical architecture or implementation aspects.

**12**. **“The role of blockchain in enhancing forensic investigation processes”** [12] by L. Roberts and K. Williams.

The paper presents a conceptual framework for integrating blockchain into forensic investigation workflows.It emphasizes how blockchain improves transparency, auditability, and data integrity in investigations.  
It also outlines potential real-world applications in law enforcement.

**13. “Blockchain as a service for secure evidence management in cloud environment”** [13] by P. Mehta and N. Kumar.

This study proposes a Blockchain-as-a-Service (BaaS) model for secure cloud-based evidence management.It explains how cloud systems can be enhanced with blockchain features for integrity and traceability.  
The architecture supports scalable and secure storage of digital evidence.  
Its merit is combining cloud flexibility with blockchain security.  
The limitation is its dependency on third-party BaaS providers, which could raise trust issues.

**14. “Blockchain-based approaches to digital evidence tamper resistance”** [14] by S. Zhao, J. Wu, and Y. Zhang .

The paper introduces a private blockchain system using cryptographic protocols to resist evidence tampering.It explains algorithms for secure timestamping and verification of digital evidence.It effectively strengthens data integrity and provides tamper-proof logs.A key merit is the high level of security for sensitive forensic data.However, the approach has high computational overhead and may impact system performance.

**15. “Smart contracts in blockchain for secure legal evidence storage”** [15] by R. Banerjee and M. Ghosh.

This work explores the use of smart contracts for automating legal evidence storage and validation.It details how legal workflows can be embedded into blockchain logic to ensure secure handling.Smart contracts help reduce manual interventions and errors in the legal process.

**16**.“**Potential Applicability of Blockchain Technology in the Maintenance of Chain of Custody in Forensic Casework”**[16] **by** HarshPatil,S.Puri  
The paper, *Potential Applicability of Blockchain Technology in the Maintenance of Chain of Custody in Forensic Casework,* explores how blockchain can be utilized to ensure the integrity and transparency of the chain of custody in forensic investigations. It highlights blockchain's ability to create immutable and time-stamped records of evidence handling, enhancing trust and accountability.

**17. “Digital Evidence Management System for Cybercrime Investigation using Proxy Re-Encryption”** [17]by H. Chougule, Sunny D, Mehul L

The paper, *Digital Evidence Management System for Cybercrime Investigation using Proxy Re-Encryption,* proposes a framework that leverages proxy re-encryption (PRE) technology to securely manage and share digital evidence in cybercrime investigations. PRE enables encrypted evidence to be securely transferred between authorized parties without direct decryption, preserving confidentiality and integrity.

**18. “Decentralized Model to Protect Digital Evidence via Smart Contracts Using Layer 2 Polygon Blockchain”** [18]by Sumit Kumar   
The paper, *Decentralized Model to Protect Digital Evidence via Smart Contracts Using Layer 2 Polygon Blockchain,* proposes a secure framework for safeguarding digital evidence using Polygon’s scalable blockchain and smart contracts. It ensures immutability, traceability, and transparency while reducing reliance on centralized systems

**19. “Digital Forensic Evidence Management System Using Improved Blockchain”**[19] by Venkatesh G, Srushti V Sannakki, Sahana M J, Sridevi S, Sourabh Verma

The paper, Digital Forensic Evidence Management System Using Improved Blockchain, introduces a blockchain-based framework for managing digital forensic evidence, ensuring its integrity, authenticity, and transparency. By leveraging an enhanced blockchain architecture, the system provides tamper-proof storage and tracking of evidence, improving trust in forensic processes. Its merits include enhanced security, decentralized data management, and resistance to evidence manipulation, while demerits involve high computational costs, scalability concerns, and integration challenges with traditional forensic systems.

**20. “Blockchain in Legal Evidence Management”**[20]by P.Sharma  
The paper, *Blockchain in Legal Evidence Management,* examines the application of blockchain technology to enhance the security, integrity, and transparency of legal evidence management. It highlights blockchain's potential to create immutable, time-stamped records of evidence handling, ensuring that evidence cannot be tampered with or altered. The merits of this approach include increased trust in the legal process, efficient tracking of evidence, and reduced human error or fraud.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **S.NO** | **Author(s)** | **Title** | **Year** | **Journal** | **Methodology** | **Merits** | **Demerits** |
| [1] | A. Sangekar, V. Gumalwad, S. Khillare, K. Warbhog, S. Hadbe and U. Tupe | Blockchain-Powered Forensic Evidence Storage: A New Approach to Data Security | 2024 | IEEE Pune Section International Conference | Implements a decentralized system using blockchain and smart contracts to store and track forensic evidence. | Ensures tamper-proof, transparent, and traceable evidence storage | Implementation complexity and high computational cost |
| [2] | S. Srivastava, G. Kaur, Himank and S. Singla | Implementation of Blockchain and IPFS to safeguard evidentiary data | 2024 | IEEE International Conference on Knowledge Engineering and Communication Systems (ICKECS | Stores metadata and hashes on blockchain, while IPFS manages decentralized evidence storage. | Ensures data integrity, immutability, and secure decentralized access | Requires integration of two complex systems, which may lead to performance overhead. |
| [3] | J. Jacob and  S. Kumar | A Framework for Digital Forensics Using Blockchain to Secure Digital Data | 2023 | IEEE World Conference on Applied Intelligence and Computing (AIC) | Uses blockchain to log, track, and verify digital evidence in real-time. | Ensures data authenticity, transparency, and tamper-proof chain of custody. | Real-time verification can be resource-intensive and may impact system performance. |
| [4] | P. Batta, S. Ahuja and A. Kumar | A hybrid framework for secure data transfer for enhancing the Blockchain Security | 2023 | IEEE | Combines symmetric,  asymmetric encryption with blockhain | Provides strong confidentiality, integrity, and authentication in data transmission. | Encryption overhead may lead to increased processing time and complexity. |

Table 2.1: Literature Survey Table

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| [5] | J. Richter, N. Kuntze and C. Rudolph | Securing digital evidence using trusted computing and cryptograp-hy. | 2022 | IEEE | Applies cryptographic techniques and trusted computing to preserve evidence integrity. | Ensures authenticity, integrity, and reliable chain of custody for digital evidence. | Dependent on specialized hardware and complex trust management. |
| [6] | *R. Accors* | Safe-Keeping Digital Evidence with Secure Logging Protocols: State of the Art and Challenges | 2022 | IEEE | Analyzes tamper-evident logs, audit trails, and integrity-preserving techniques. | Improves evidence reliability through verifiable and secure logging systems | Faces challenges in long-term data preservation and protocol efficiency |
| [7] | J. Darby, J. Phelan, Sholander B. Smith, A. Walter and G. Wyss | Blockchain and Its Impact on Indian Governance | 2021 | IEEE Access | Uses evidence-based analysis with real-world scenarios and threat models. | Identifies system vulnerabilities and supports informed cybersecurity decisions. | Relies heavily on quality and availability of empirical data. |
| [8] | W. Yang, P. He, Z. Yang, X. Yi and C. Chen | Blockchain in Legal Evidence Management | 2021 | IEEE | Uses blockchain and smart contracts for copyright registration and validation. | Ensures tamper-proof ownership tracking and automates dispute resolution. | Legal acceptance and interoperability across jurisdictions may be challenging. |
| [9] | S. Li, T. Qin and G. Min | Digital Evidence and Blockchain: Challenges and Solutions | 2020 | IEEE | Implements a decentralized blockchain framework for secure evidence collection and traceability. | Enhances integrity and trust in forensic investigations across distributed environments. | Scalability issues and data synchronization challenges in large IoT networks. |
| [10] | D. Rajababu, S. Surya, M. Padhiary and H. Modi | Blockchain in Cybersecurity: Concepts and Applications | 2019 | IEEE Access | Utilizes cryptographic techniques and decentralized blockchain structures to protect data. | Ensures data integrity, confidentiality, and reduces dependency on centralized systems. | High energy consumption and scalability limitations in large-scale deployment. |
| [11] | M. Anderson and J. Thompson | Legal challenges in adopting blockchain for evidence protection | 2019 | IEEE  Access | Legal analysis of blockchain use in evidence protection through case studies. | Highlights real-world legal gaps and policy issues. | Lacks technical implementation details. |
| [12] | L. Roberts and K. Williams | The role of blockchain in enhancing forensic investigation processes | 2018 | IEEE  Access | Framework-based review of blockchain integration into forensic processes. | Enhances transparency and traceability. | Scalability issues not deeply explored. |
| [13] | P. Mehta and N. Kumar | Blockchain as a service for secure evidence management in cloud environment | 2018 | IEEE  Access | Proposes Blockchain as a Service (BaaS) model for cloud-based evidence storage. | Enables secure and scalable cloud integration. | BaaS dependency on third-party trust. |
| [14] | S. Zhao, J. Wu, and Y. Zhang | Blockchain-based approaches to digital evidence tamper resistance | 2017 | IEEE  Access | Cryptography techniques for tamper resistance using private blockchain. | Strong data integrity and auditability. | High computational overhead. |
| [15] | R. Banerjee and M. Ghosh | Smart contracts in blockchain for secure legal evidence storage | 2017 | IEEE  Acess | Implements smart contracts for automated legal evidence management. | Automation reduces human error and bias. | Legal enforceability of smart contracts is uncertain. |
| [16] | Harsh Patil,  Ravshish k.Kohli,  S.Puri | Potential applicability of blockchain technology in the maintenance of chain of custody in forensic casework | 2017 | Springer | Empirical analysis, blockchain solution | Focused on secure storage in legal contexts | Narrow focus on storage, may overlook other aspects |
| [17] | H.Chougule,Sunny D,  Mehul L | Digital Evidence Management System for Cybercrime Investigation using Proxy Re-Encryption | 2017 | Elsevier | Framework development, case studies | Provides practical frameworks for Indian context | May not be universally applicable |
| [18] | Sumit kumar,arun kumar,Sanjeev kumar,Vishnu Sharma | Decentralized Model to Protect Digital Evidence via Smart Contracts Using Layer 2 Polygon Blockchain | 2017 | IEEE Transactions on Information Forensics and Security | Theoretical framework, blockchain implementation | Advanced blockchain integration for evidence protection | May not account for practical implementation challenges |
| [19] | Venkatesh.G, Srushti V Sannakki, Sahana M J, Sridevi S, Sourabh Verma | Digital Forensic Evidence Management System Using Improved Blockchain | 2016 | International Journal of Computer Applications | Case study, blockchain application | Context-specific insights for Indian legal systems | Limited generalizability to other legal systems |
| [20] | P. Sharma | Blockchain in Legal Evidence Management | 2016 | Pearson India | Case studies, theoretical analysis | Specific focus on legal evidence management | Limited scope on broader applications |

**CHAPTER 3**

# METHODOLOGY

# Evidence Protection Systems (EPS) using blockchain rely on ensuring data integrity, transparency, and secure access to sensitive information. Key features include leveraging blockchain's immutability to prevent tampering, timestamping to establish a verifiable chronology, and cryptographic hashing to maintain data integrity. Smart contracts facilitate automated workflows, ensuring a transparent chain of custody and reducing the risk of human errors. Consensus mechanisms enhance security by requiring network agreement for data validation, while cryptographic techniques, such as encryption, protect sensitive data from unauthorized access. These elements work in tandem to provide a robust framework for evidence management, minimizing risks of data breaches and enhancing trust in critical sectors.

# TECHNOLOGIES USED:

**1.** **Blockchain Frameworks**: Platforms like Ethereum or Hyperledger Fabric provide the foundation for implementing decentralized, tamper-resistant evidence management systems.

**2.** **Smart Contracts**: Automate evidence handling processes, such as verifying user permissions and maintaining transparent custody chains, ensuring operational efficiency and accuracy.

**3.** **Cryptographic Hashing**: Secures data integrity by generating unique, tamper-evident fingerprints for each piece of evidence, allowing detection of unauthorized modifications.

**4.** **Consensus Mechanisms**: Ensure network-wide agreement on recorded data, preventing unauthorized alterations and reinforcing trust in the system.

**5.** **Decentralized Storage**: Solutions like IPFS or Filecoin store large files securely while linking them to blockchain-based hashes, ensuring accessibility and data authenticity.

# DEVELOPMENT PROCESS:

**Requirements Gathering**: The requirements were gathered from stakeholders, focusing on secure evidence storage, access control, and chain-of-custody tracking. The goal was to define key features and ensure the system met both technical and user needs.

**System Design**: The design phase focused on defining blockchain architecture, smart contracts, and database schema. Wireframes were created to visualize user interaction and ensure ease of use while meeting security requirements.

**Implementation:** The backend involved smart contract deployment and server-side logic, while the frontend focused on building an accessible user interface. Decentralized storage (IPFS) and cryptographic hashing ensured data integrity and secure evidence storage.

**Testing:** Testing included manual, user acceptance, security, and performance testing to ensure functionality, usability, and security. Feedback from users helped refine features, and performance tests validated system efficiency under various conditions.

**Manual Testing**: This phase simulated interactions such as uploading evidence, accessing records, and verifying the integrity of data through the blockchain. It helped ensure that the application functioned as expected, especially with smart contracts and cryptographic features.

**User Acceptance Testing (UAT**):This involved key stakeholders, such as moderators and legal analysts, testing the platform for usability. Their feedback was used to refine features, improve the user experience, and ensure the system met operational goals.

**Security Testing**: Given the sensitivity of the data, rigorous security testing was conducted to identify any vulnerabilities, such as potential exploits in the smart contracts or unauthorized access to evidence.

**Performance Testing**: Performance testing was conducted to measure how efficiently the system handled various use cases, such as uploading large files, verifying blockchain data, and performing multiple queries simultaneously. This ensured the system remained fast and responsive under various loads.

**Deployment**: The system was deployed using cloud platforms and hosted on GitHub Pages. GitHub Actions automated CI/CD for efficient deployment, ensuring continuous updates and secure system operation.

# CHAPTER 4

# DESIGN OF EVIDENCE PROTECTION SYSTEM

# 4.1 DESIGN

The design of a project lays out the blueprint for how it will function. It details the steps, materials, and tools needed to achieve the project's goals. It's like a recipe that ensures everyone involved understands how to turn the idea into reality.

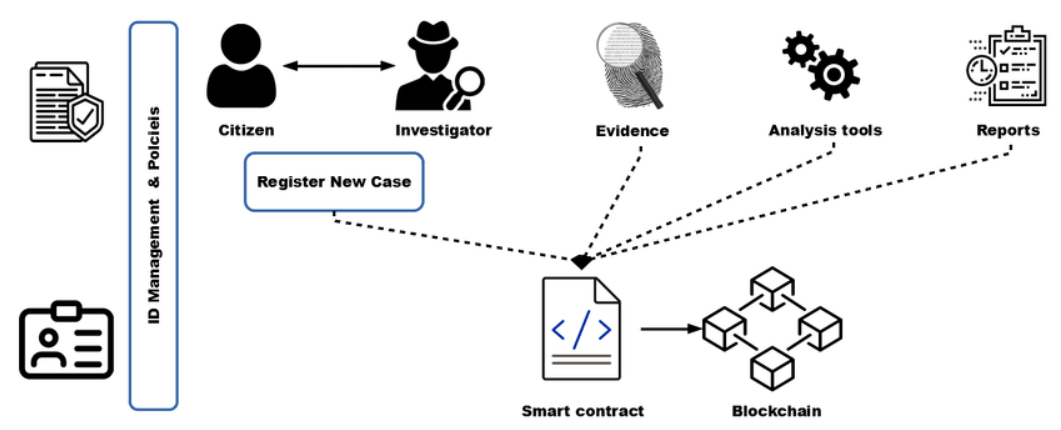


Figure 4.1 Design of Evidence Protection System

1. The **Evidence Protection System (EPS)** is designed to offer an efficient and secure experience for different user roles, including legal analysts, evidence moderators, and general users. The system architecture, as shown in Figure 3.1, provides customized functionalities for each role to address their specific needs while ensuring essential evidence management services are accessible to all. Legal analysts and system administrators have advanced tools for reviewing and verifying evidence records, while moderators are provided with an intuitive interface for monitoring evidence access and ensuring compliance with legal standards. General users can securely upload and view evidence, with automated tracking of data integrity and chain-of-custody. The core functions of the system focus on ensuring data security, immutability, and transparency, making it reliable, accessible, and secure for all involved parties.
2. **Login:** Users access the **Evidence Protection System (EPS)** through a secure login interface, where they enter their credentials, such as username or email and password. This authentication process ensures that only authorized individuals—such as legal analysts, evidence moderators, and general users—can access the system's sensitive features. The login mechanism enforces role-based access control (RBAC), ensuring that each user type can only interact with the system's functionalities according to their designated permissions, enhancing both security and user-specific experiences.
3. **Cloud Authentication:** Upon successful login, cloud-based authentication mechanisms, such as Firebase Authentication or similar secure services, validate user credentials to ensure that only authorized users gain access to the Evidence Protection System (EPS). This authentication layer plays a critical role in safeguarding user data, protecting sensitive evidence, and ensuring that only users with the appropriate permissions can access certain features. By using cloud authentication, the system ensures robust security, preventing unauthorized access and maintaining the integrity and confidentiality of the evidence and associated processes.
4. **User Roles:**

**Administrator**: Administrators oversee the system’s overall functionality, ensuring proper security and compliance with legal standards:

Full access to the system for managing users, permissions, and system settings.

Ability to review all evidence uploaded by users and validate blockchain records.

Control over data storage, encryption settings, and audit trails for compliance.

Monitor system performance and access logs for suspicious activities.

**Law Enforcement**: Law enforcement officials use the system to upload, review, and manage evidence related to criminal investigations:

Upload digital evidence (e.g., documents, photos, videos) securely to the blockchain.

Access blockchain records to verify the authenticity and integrity of evidence.

Option to share evidence securely with other authorized entities while maintaining chain-of-custody integrity.

Notification of any changes in the status or integrity of evidence.

**Forensic Experts**: Forensic experts are tasked with analyzing and verifying evidence integrity:

Access to detailed records of the evidence stored on the blockchain, including timestamped audit trails.

Ability to conduct forensic analysis on evidence to assess authenticity and potential tampering.

Tools to annotate or flag evidence for further investigation.

Generate reports on evidence authenticity, providing expert validation.

**General User (Evidence Submitter):** General users can submit evidence for protection or verification purposes:

Ability to securely upload digital evidence, such as images, videos, or documents.

Receive confirmation of evidence submission along with a unique identifier and timestamp, ensuring immutability.

Access status updates and notifications when evidence is successfully uploaded and verified.

Can track the chain of custody to ensure evidence integrity throughout its lifecycle.

**Common Services:**

**Blockchain-Backed Evidence Storage**: All users benefit from the system's decentralized storage model, which ensures that evidence cannot be tampered with or altered after submission. Blockchain guarantees a transparent and immutable chain of custody.

**Secure Verification & Authentication**: The platform uses cryptographic techniques to authenticate the evidence and its associated metadata (e.g., timestamp, uploader information) on the blockchain.

**Audit Trail & Transparency**: Blockchain technology provides a transparent and verifiable audit trail for every piece of evidence, allowing users to track any changes or access attempts in real-time.

Help and Support: Users can access technical support, training resources, and FAQs for guidance on submitting evidence, using the system, or resolving any issues with evidence integrity.

**Educational Resource Center**: A repository of materials to educate users on blockchain technology, data protection laws, best practices for evidence handling, and the importance of preserving the integrity of digital evidence.

# 4.2 PROCESS FLOW DIAGRAM

A **Process Flow Diagram (PFD)** visually represents the steps or stages involved in managing evidence within the **Evidence Protection System (EPS)**. It outlines the sequence of activities, decision points, and dependencies between various components of the system. Each step in the diagram typically includes a specific task, such as evidence upload, encryption, or verification, along with any conditions or criteria that must be met before proceeding to the next step. The flowchart helps to illustrate the entire process, from evidence submission to final verification, highlighting any decision points such as access control checks or smart contract validation. It also assists in identifying potential bottlenecks, ensuring that all required processes—such as secure storage, access control, and data integrity verification—are properly accounted for in the project plan and workflow

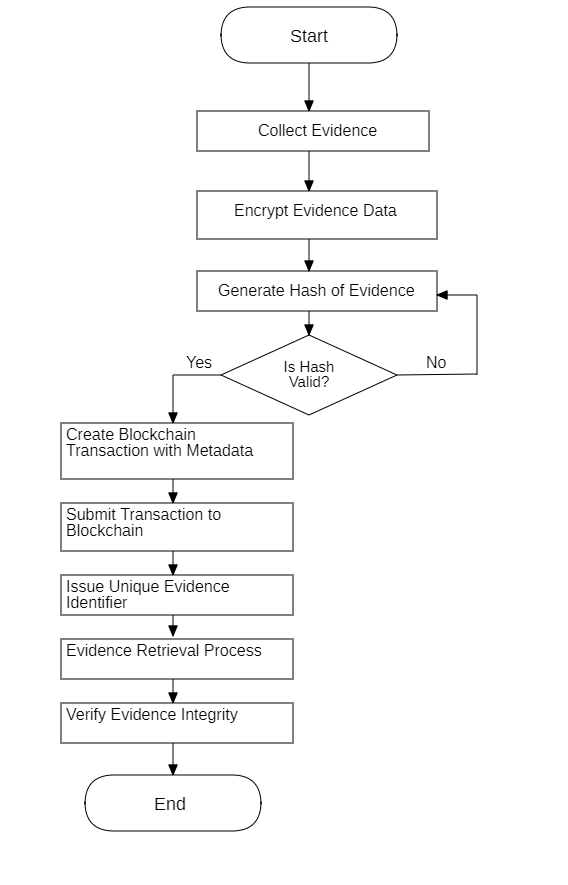


Figure 4.2 Process flow Diagram of Evidence Protection System

1. The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system.
2. The data flow diagram (DFD) is one of the most important modeling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system.
3. DFD shows how the information moves through the system and how it is modified by a series of transformations. It is a graphical technique that depicts information flow and the transformations that are applied as data moves from input to output.
4. DFD is also known as bubble chart. A DFD may be used to represent a system at any level of abstraction. DFD may be partitioned into levels that represent increasing information flow and functional detail.

# SYSTEM ARCHITECTURE

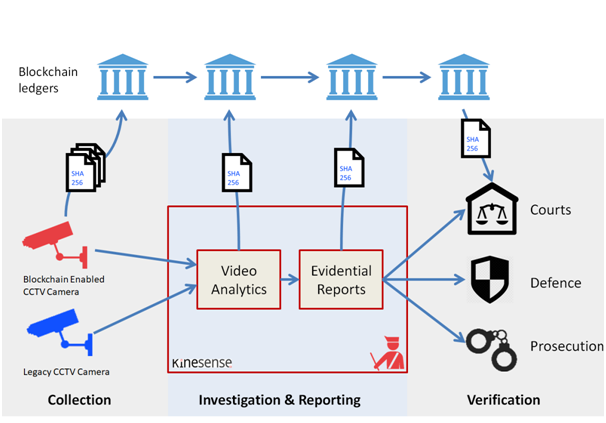


Figure 4.3: Detailed System Architecture of Evidence Protection System

# Figure 4.3 illustrates the detailed data flow and system architecture of the Evidence Protection System (EPS). The process begins with the submission of evidence (documents, images, or videos), which, if it's a video, is split into individual frames. These frames or images are then processed through exploratory data analysis (EDA) to identify underlying patterns or irregularities that may indicate evidence tampering. After the EDA step, the data is passed through the detection system, which uses blockchain-based verification, cryptographic hashing, and smart contracts to assess the authenticity of the evidence. The system employs various techniques to ensure data integrity, such as timestamping and chain-of-custody tracking.

# 4.4 UML DIAGRAMS

**Use case diagram:**

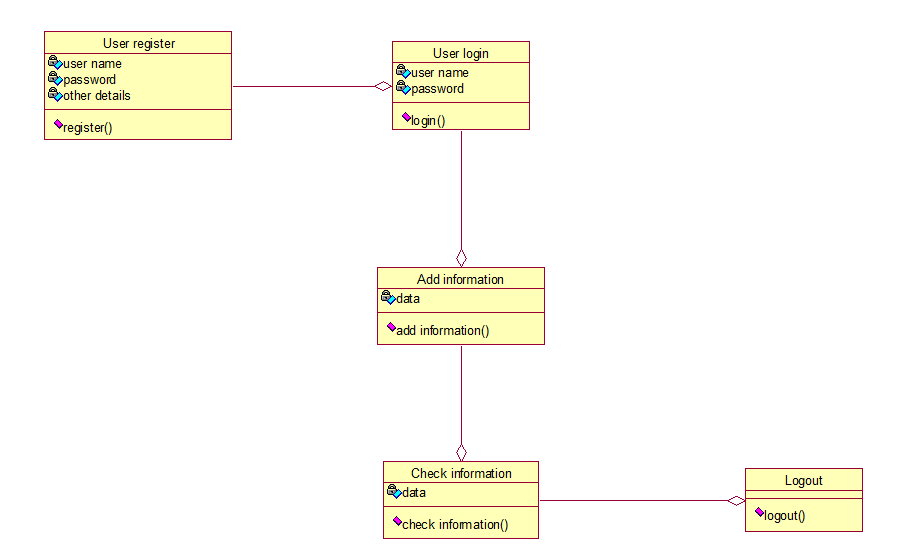
# The Use Case Diagram of Evidence Protection System depicts interactions between a User and a system. The actor (User) is shown performing five use cases. These use cases include Register or Signup, allowing new users to create an account, and Login or Signin, enabling existing users to access their accounts. The Add Information use case lets users input data, while Check Information allows them to view stored data. Lastly, Logout ensures secure session termination.

# 

Figure 4.4.1 Use Case Diagram of Evidence Protection System

**Class diagram:**

The Class Diagram of Evidence Protection System have five main classes: **User Register**, **User Login**, **Add Information**, **Check Information**, and **Logout**. The **User Register** class contains attributes like **username, password, and other details**, with a method **register()** for account creation. The **User Login** class includes **username and password** attributes, along with a **login()** method for authentication. Once logged in, users can use the **Add Information** class to store **data** using the **add information()** method. The **Check Information** class allows users to access stored **data** with the **check information()** method. Finally, the **Logout** class has a **logout()** method for secure exit.

Figure 4.4.2 Class Diagram of Evidence Protection System

**Activity diagram:**

The ActivityDiagramof Evidence Protection System represents the user flow in a system. It starts with the **Open Application** step, where the user accesses the system. Next, the user can **Register** to create an account before proceeding to **Login**. After logging in, they have the option to **Add Information**, which allows storing data in the system. The user can then **Check Information** to view the stored data. Once done, they can choose to **Logout**, ensuring a secure exit. The flow ends with the **End** state, marking the completion of the process.

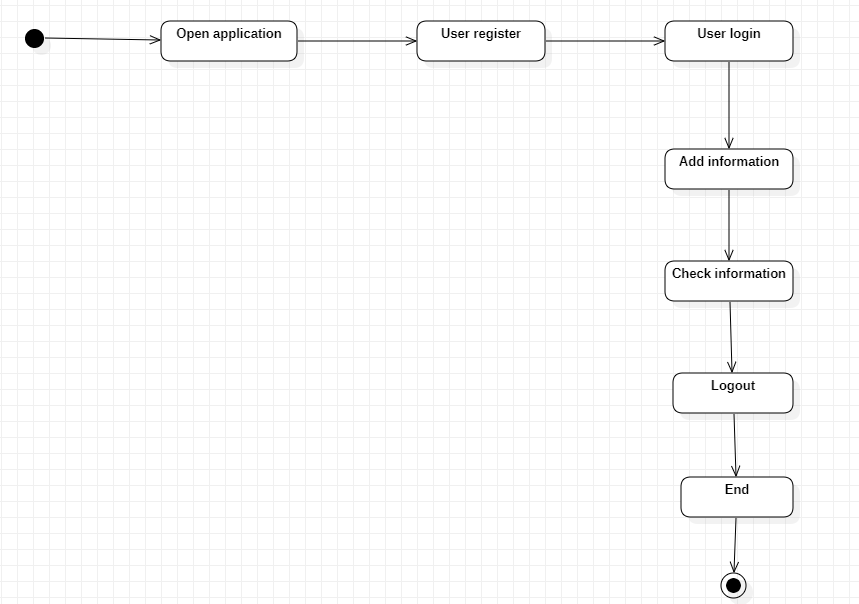
****

Figure 4.4.3 Activity Diagram of Evidence Protection System

**Sequence diagram:**

The **Sequence Diagram** of Evidence Protection System illustrates the interaction between a **User** and the **System**. The user starts by sending a **Register** request to the system to create an account. Once registered, they proceed to **Login**, where the system verifies their credentials. After logging in, the user can **Add Information**, which is sent to the system for storage. They can then **Check Information**, retrieving stored data from the system. Finally, the user **Logs out**, terminating the session. Each action is represented by an arrow from the **User** to the **System**, showing the step-by-step communication.

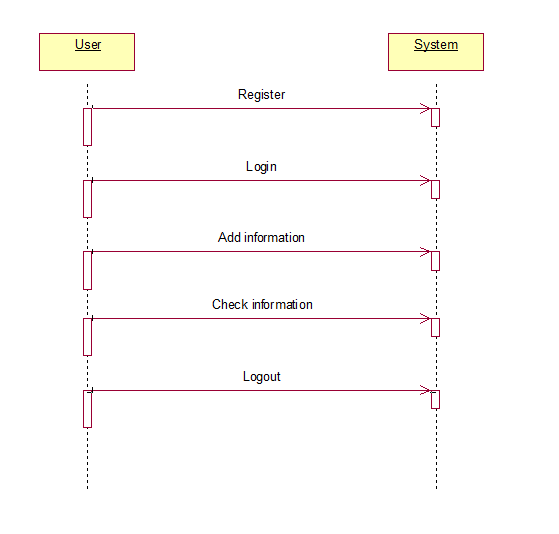
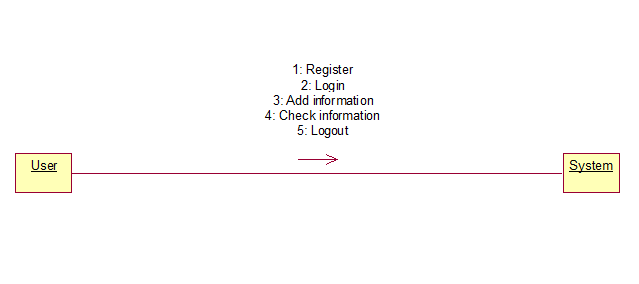


Figure 4.4.4 Sequence Diagram of Evidence Protection System

**Collaboration diagram**

The Collaboration diagram of Evidence Protection System represents a Basic Interaction Flow between a User and a System. The user initiates the interaction by performing five sequential actions: Register, where they create an account, followed by Login to access the system. Once logged in, the user can Add Information, storing data within the system. They can then Check Information to retrieve stored data. Finally, the user Logs Out, ending their session. The arrow between the user and the system signifies communication and interaction.

****Figure 4.4.5 Collaboration diagram of Evidence Protection System

**Component diagram:**

The Component Diagramof Evidence Protection represents the structure of a user interaction system. It consists of five main components: **User Register**, **User Login**, **Add Information**, **Check Information**, and **Logout**. The **User Register** component allows users to create an account, followed by **User Login** for authentication. Once logged in, users can interact with the **Add Information** component to store data. They can then retrieve stored data using the **Check Information** component. Finally, the **Logout** component ensures a secure exit from the system. components.

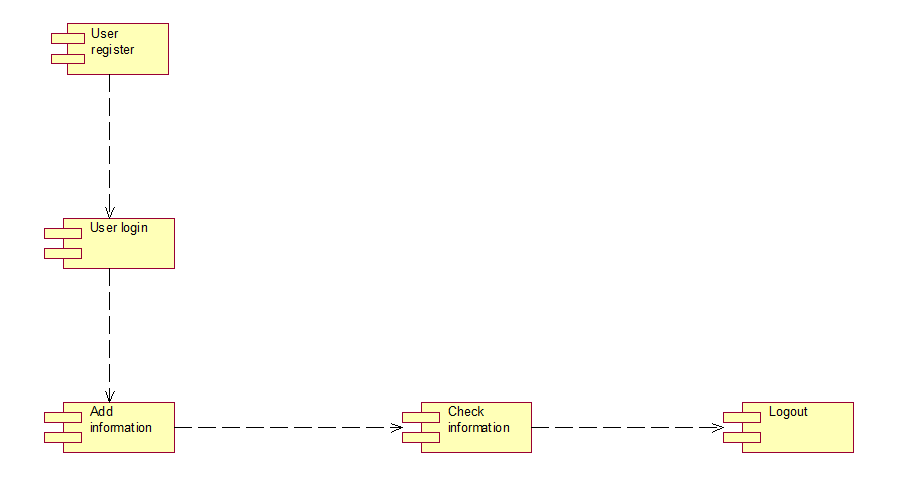


Figure 4.4.6 Component diagram of Evidence Protection System

**Deployment diagram:**

The **Deployment** **Diagram** of Evidence Protection System illustrates the interaction between a **User** and a **System**. The diagram consists of two primary components: the **User**, representing the end-user interacting with the system, and the **System**, which processes user requests. The connection between them signifies communication, where the user sends requests and receives responses from the system. This structure helps in understanding how users interact with a system at a high level. It can represent any software system, such as a web application, authentication system, or database-driven application. The simplicity of this diagram makes it useful for foundational system design discussions.

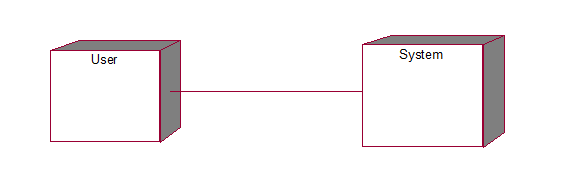
****

Figure 4.4.7 Deployment diagram of Evidence Protection System

# 

# CHAPTER 5

# IMPLEMENTATION

# MODULES:

**User Signup**

This module allows individuals to create accounts within the system by providing necessary details such as name, email, and password. The registration process ensures that user data is securely stored, leveraging blockchain technology to maintain data integrity and prevent unauthorized modifications.

**User Sign-in**

Once registered, users can sign in to the system using their credentials. The authentication process verifies the provided information against stored records, granting access to system functionalities based on user roles and permissions. Blockchain-based security ensures tamper-proof authentication.

**Add Evidence Information**

This module enables users to input or upload evidence-related data, such as documents, images, and videos. The system ensures that all uploaded information is authenticated and stored securely using blockchain technology. By leveraging the immutability feature of blockchain, this module guarantees that once evidence is added, it cannot be altered or deleted, maintaining its credibility.

**Verify & Retrieve Evidence**

Users can access and verify stored evidence using a unique identifier. The system provides search and retrieval functionalities to ensure authorized individuals can view specific evidence while maintaining security. Blockchain ensures that the integrity of stored evidence remains intact by offering a transparent audit trail that confirms no unauthorized modifications have occurred.

**Access Control & Permissions**

This module implements role-based access control, ensuring that only authorized users can view or modify specific pieces of evidence. Permissions are managed securely using blockchain authentication, which prevents unauthorized access while allowing transparency for authorized users.

**Audit & Tamper Detection**

The system logs all interactions with the evidence, creating an immutable audit trail for tracking changes. If an unauthorized attempt is made to modify or access evidence, the blockchain-based system detects and records the attempt, ensuring data remains protected. Alerts and notifications can be generated in case of potential security breaches.

**Final Verification & Approval**

Before being used in legal or official proceedings, evidence must be verified and approved. This module allows authorized personnel, such as law enforcement or legal professionals, to cross-check and validate the authenticity of stored evidence. The blockchain’s hashing mechanism ensures that the data has not been altered after submission, providing a transparent and trustworthy verification process.

**Algorithms:**

**Step 1: AES Encryption**

**Algorithm**: Advanced Encryption Standard (AES)

**Purpose**: Ensures the **confidentiality** of sensitive evidence data by encrypting the file before it is processed or stored. This prevents unauthorized access even if data is exposed.

**Contribution**: Protects sensitive content from being read or misused by unauthorized users.

**Step 2: SHA-256 Hashing**

**Algorithm**: Secure Hash Algorithm (SHA-256)

**Purpose**: Converts the encrypted evidence into a unique, fixed-size hash. This acts as a digital fingerprint to detect any tampering.

**Contribution**: Ensures **data integrity** by allowing verification that the evidence has not been altered.

**Step 3: Timestamping**

**Mechanism**: Blockchain native timestamp (automatically generated with block creation)

**Purpose**: Assigns a precise date and time to each evidence entry.

**Contribution**: Maintains the **chronological order** of records, which is crucial for legal and forensic validity.

**Step 4: Smart Contract Execution**

**Technology**: Smart Contracts (e.g., Solidity on Ethereum)

**Purpose**: Automates key processes such as:

1) Logging evidence transactions

1. Verifying user permissions
2. Managing access rights

**Contribution**: Ensures **automation, transparency, and enforcement of access policies**, reducing human errors and enhancing trust.

**Step 5: Consensus Mechanism**

**Algorithm**:

**PBFT / PoA** (for private blockchain)

**PoW / PoS** (for public blockchain)

**Purpose**: Validates the transaction by reaching agreement among nodes before adding it to the blockchain.

**Contribution**: Ensures **data validity and resistance to tampering** by achieving distributed agreement.

**Step 6: Blockchain Storage**

**Technology**: Distributed Ledger Technology (DLT)

**Purpose**: Stores the final encrypted and hashed evidence with metadata in a secure, tamper-proof format across decentralized nodes.

**Contribution**: Provides **immutability and traceability**, making it impossible to modify or delete records once added.

**5.1 TECHNOLOGY STACK**

**Frontend:** HTML, CSS, JavaScript, Bootstrap4  
**Backend:** Flask, Node.js  
**Database:** SQLite3, Blockchain (Ethereum/Ganache)  
**Software:** Python IDE (3.7.0), Visual Studio Community Version, Ganache, MetaMask Chrome Extension  
**Primary Language:** Python, JavaScript

**5.2 FEATURES**

**1. User Authentication**

The system provides a secure registration and login process, ensuring only authorized individuals can access the platform. It leverages blockchain-based authentication to store user credentials securely, preventing unauthorized access or tampering. Role-based access control is implemented to differentiate between general users, legal authorities, and administrators, granting appropriate permissions based on user roles.

**2. Dashboard**

**Admin Dashboard:** Displays system analytics, user activity logs, and tools to manage blockchain transactions, user accounts, and evidence records.

**Legal Authority Dashboard:** Provides access to verified evidence records, search functionalities, and the ability to approve or reject evidence submissions.

**User Dashboard:** Allows users to upload and manage their evidence records, view verification status, and track all past interactions with their submitted data.

**3. Evidence Submission & Management**

Users can upload evidence in various formats, including documents, images, and videos. Each submission is recorded on the blockchain with a unique hash, ensuring immutability and authenticity. The system automatically timestamps and secures uploaded content, preventing any future alterations.

**4. Evidence Verification & Audit Trail**

Authorized personnel can retrieve and verify stored evidence by checking blockchain records. The system maintains a transparent audit trail, ensuring every interaction with the evidence is securely logged. This ensures accountability and provides legal authorities with verifiable proof of data integrity.

**5. Secure Access & Permission Management**

Role-based access ensures that only authorized users can access or modify specific evidence records. Blockchain authentication further strengthens security, preventing unauthorized alterations while allowing seamless transparency for legal professionals.

**6. Real-Time Notifications & Updates**

Users receive real-time notifications when evidence is successfully submitted, verified, or accessed by authorized personnel. The system also alerts users if an attempt to tamper with stored evidence is detected.

**7. Final Verification & Approval**

Before evidence is used in legal proceedings, authorized legal professionals can perform final verification. Blockchain hashing mechanisms ensure that data remains unaltered after submission, guaranteeing the authenticity of stored evidence.

By integrating these features, the **Evidence Protection System** ensures a secure, transparent, and tamper-proof approach to managing digital evidence using blockchain technology.

**5.3 IMPLEMENTATION DETAILS**

**1. Frontend Implementation**

**HTML:** Structures the layout for various pages, including login, signup, dashboards, and evidence submission forms.

**CSS:** Ensures a responsive design, creating a user-friendly interface for various devices.

**JavaScript:** Manages client-side logic, including form validations, real-time notifications, and asynchronous data fetching from the blockchain.

**2. Backend Implementation**

**Flask:** Handles server-side operations, managing blockchain interactions and user requests.

**Node.js:** Facilitates communication with the Ethereum blockchain and handles smart contract interactions.

**Ganache (Ethereum Blockchain):** Simulates a local blockchain environment for smart contract testing and evidence storage.

**MetaMask:** Provides a secure way for users to interact with the blockchain and authorize transactions.

**3. Real-Time Communication**

**Blockchain Transactions:** Ensures secure and transparent data storage for every evidence submission.

**Smart Contracts:** Automates evidence verification and ensures integrity by validating records against blockchain hashes.

**Notifications:** Users and legal authorities receive real-time alerts for successful submissions, verification status, and suspicious activities.

These implementation components ensure a **secure, decentralized, and efficient** system that prevents tampering, enhances transparency, and provides verifiable proof of digital evidence integrity.

**5.4 USER INTERFACE**

**1. Home Page**

Provides three options: **Admin Login, Legal Authority Login, General User Login.**

**2. User Signup Page**

**Fields:** First Name, Last Name, Email, Phone Number, User Type (General User / Legal Authority), Password, Confirm Password.

**Sign-Up Process:** Validates email uniqueness and securely stores user credentials using blockchain authentication.

**3. User Sign-In Page**

**Verification:** Confirms user type and credentials to prevent unauthorized access.

**Successful Login:** Redirects to the appropriate dashboard based on user role; otherwise, displays an "Invalid User" message.

**4. User Dashboard**

**Welcome Message:** Greets users with their name and profile info.

**Upload Evidence:** Interface for users to submit documents, images, or videos as evidence.

**View Submission History:** Displays all previously submitted evidence with blockchain verification details.

**Evidence Status:** Shows whether submitted evidence has been verified or is pending approval.

**Logout:** Option to securely log out of the system.

**5. Legal Authority Dashboard**

**Welcome Message:** Displays a welcome message with the user's name and role.

**Review Evidence:** List of submitted evidence for verification, with blockchain authentication details.

**Audit Logs:** Provides a transparent history of all interactions with stored evidence.

**Notifications:** Alerts legal professionals when new evidence requires verification.

**Final Verification:** Approve or reject evidence submissions based on blockchain records.

**Logout:** Option to securely sign out.

**6. Admin Dashboard**

**System Overview:** Displays analytics on user activity, blockchain transactions, and evidence verification statistics.

**Manage Users:** Provides an interface to view and manage user roles and permissions.

**Audit Logs:** Tracks all interactions within the system for security and compliance purposes.

**Logout:** Option to securely sign out.

# CHAPTER 6

# RESULTS

**6.1 User Signup Interface:**

# Figure 6.1 displays the User Signup page of the Evidence Management System Using Blockchain. The top navigation bar contains options for User Signup and User Sign-in.

# 

# Figure 6.1 User Signup Interface of Evidence Protection System

**6.2 User Registration Page**

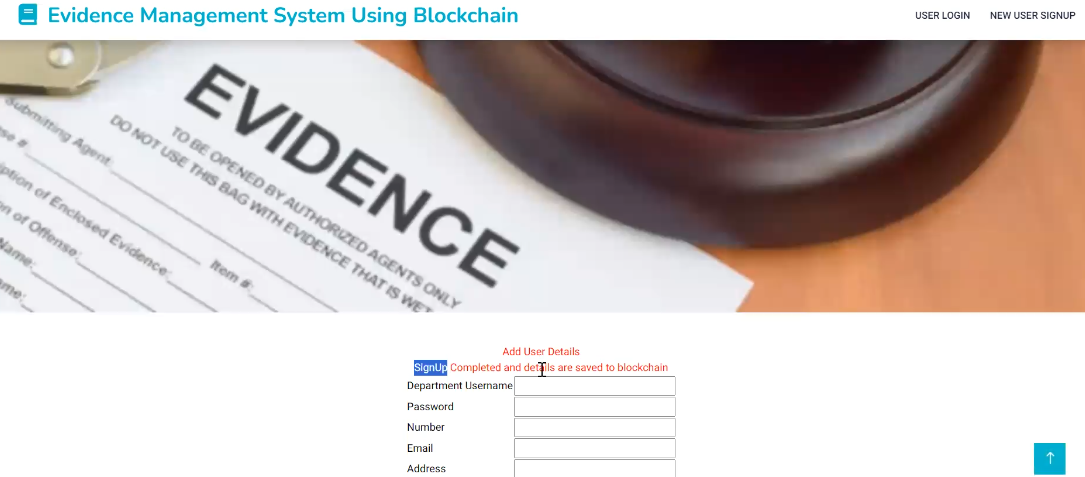
# Figure 6.2 represents the User Registration page of the Evidence Management System Using Blockchain, designed to securely manage user details. The interface includes a form where users can enter their Department Username, Password, Phone Number, Email, and Address before submitting it using the "Add User" button. This registration process ensures that only authorized personnel can access the system. The navigation bar at the top provides options for User Login and New User Signup, allowing users to either log in or create a new account.

# 

# Figure 6.2 User Registration Page of Evidence Protection System

**6.3 User Signup Confirmation (1):**

Figure 6.3 shows the signup confirmation page of the Evidence Management System Using Blockchain. A message at the top of the form indicates that signup is completed and user details are saved to the blockchain, ensuring secure and immutable record-keeping. Below this, the registration form is displayed with fields for Department Username, Password, Phone Number, Email, and Address, allowing new users to input their details



# Figure 6.3 User Signup Confirmation (1) Page of Evidence Protection System

**6.4 User Signup (2):**

Figure 6.4 shows the User Registration page of the Evidence Management System Using Blockchain, where a second user is being added. The form titled "Add User Details" is filled with the new user's information, including Department Username, Password, Phone Number, Email, and Address. The "Add User" button is being clicked to submit and store the details securely in the blockchain.

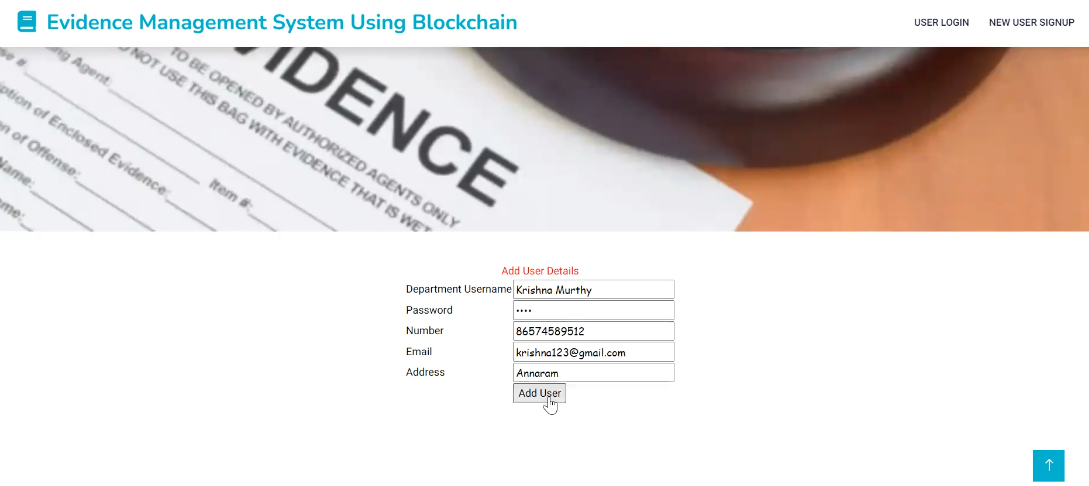


Figure 6.4 User Signup (2) Page of Evidence Protection System

**6.5 User Signup Confirmation (2):**

Figure 6.5 shows a webpage for an "Evidence Management System Using Blockchain." The interface includes a registration form for adding user details such as Department Username, Password, Number, Email, and Address. A confirmation message, "SignUp Completed and details are saved to blockchain," is displayed. The header includes options for "USER LOGIN" and "NEW USER SIGNUP."

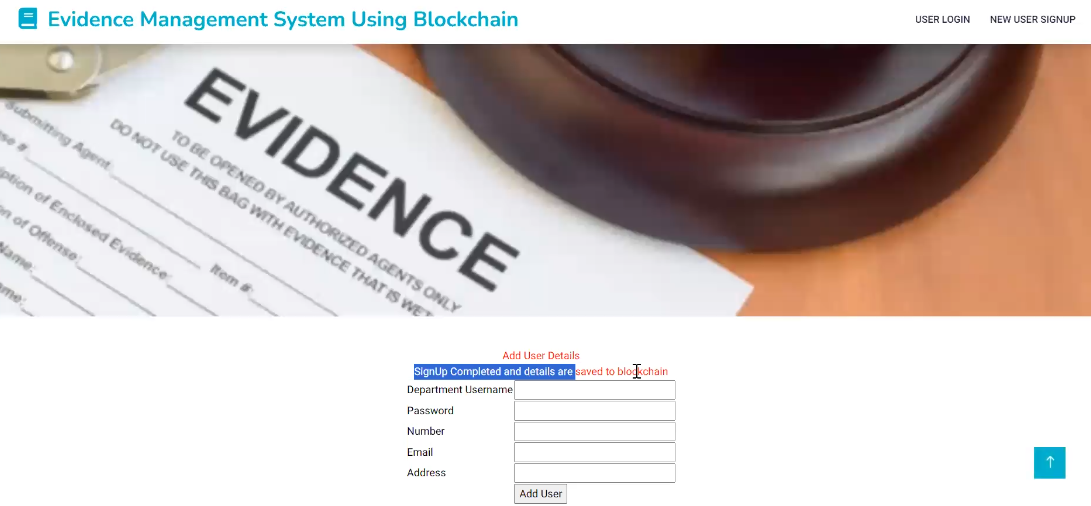
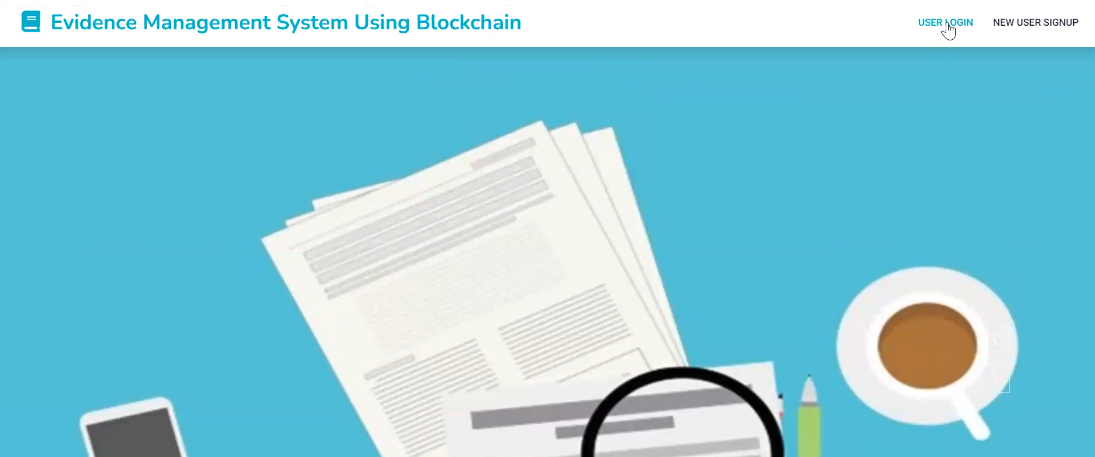


Figure 6.5 User Signup Confirmation (2) Page of Evidence Protection System

**6.6 User login:**

Figure 6.6 shows the login page of the "Evidence Management System Using Blockchain." It includes fields for entering a username and password, along with a Login button for user authentication. The interface features a clean and professional layout, with options for USER LOGIN and NEW USER SIGNUP located in the top-right corner. Upon accessing the page, a welcome message is displayed to greet the user.



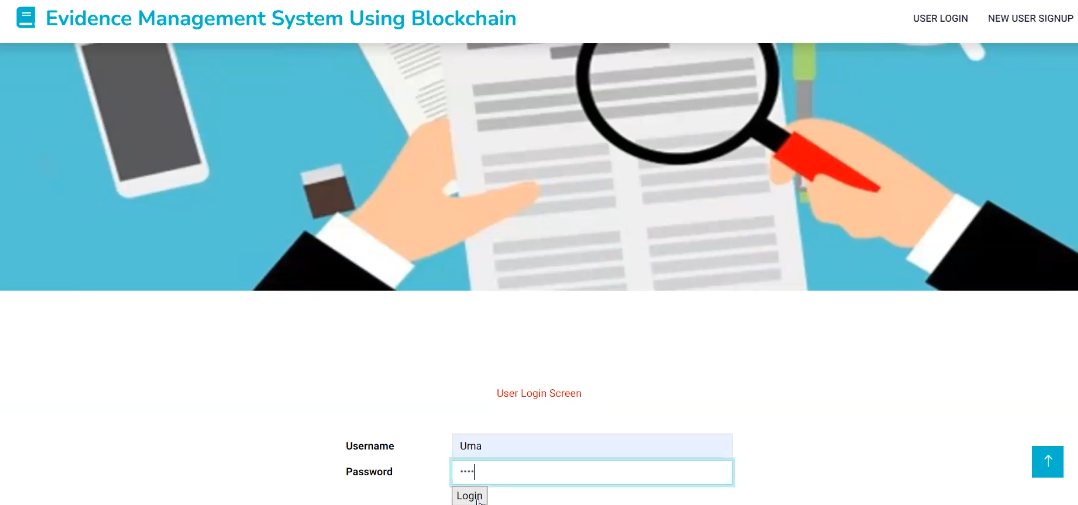


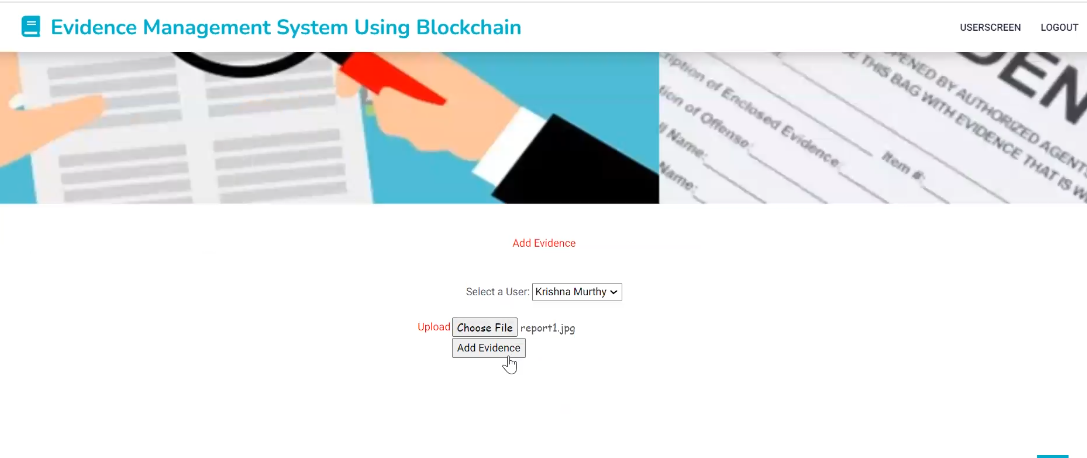


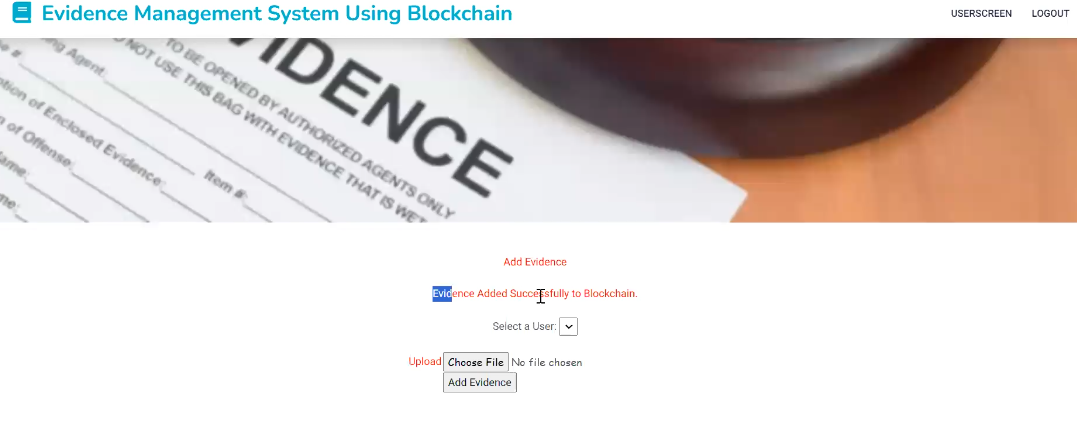
Figure 6.6 User Login Page of Evidence Protection System

**6.7 Add Information and Evidence:**

Figure 6.7 shows the user dashboard of the Evidence Management System Using Blockchain after a successful login, featuring options such as Add Information, Check Information, and Logout. The second image displays the Add Evidence interface, where a user named Krishna Murthy is selected and a file named report1.jpg is uploaded as evidence. The final image confirms successful evidence submission with the message "Evidence Added Successfully to Blockchain." This process ensures secure and tamper-proof documentation of evidence while offering a user-friendly interface.





Figure 6.7 Add Information and Evidence Page of Evidence Protection System

**6.8 User Signin:**

Figure 6.8 shows a user signing into the Evidence Management System using Blockchain, beginning with the login interface where credentials are entered. The login screen allows a registered user, such as Krishna Murthy, to input their username and password for authentication. Upon successful login, the system redirects the user to the main dashboard, displaying a personalized welcome message along with options such as "Add Information," "Check Information," and "Logout."



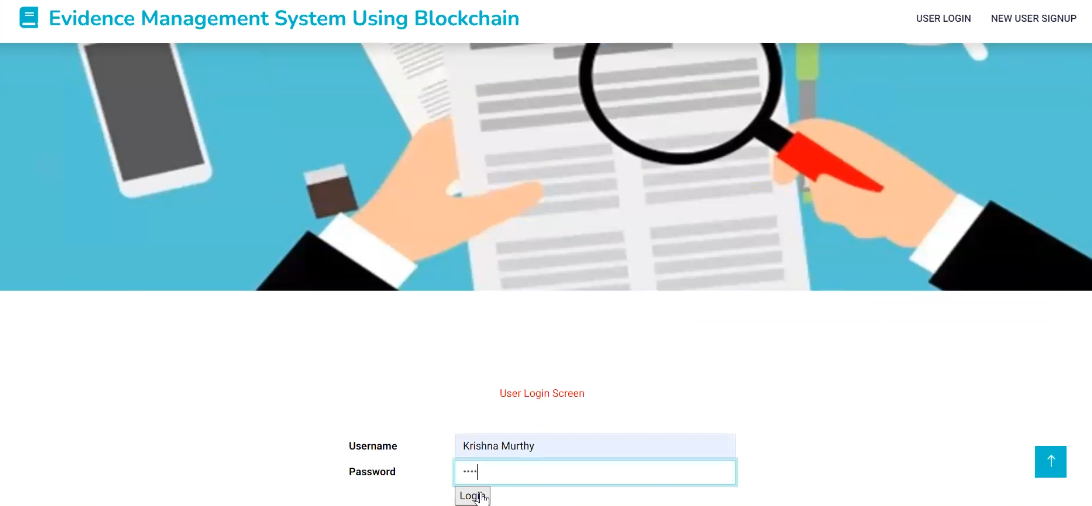
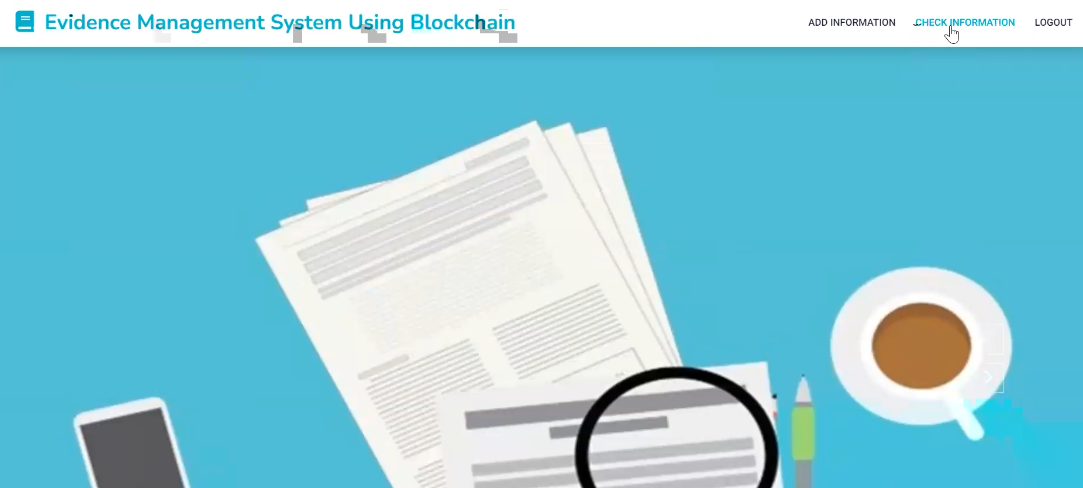


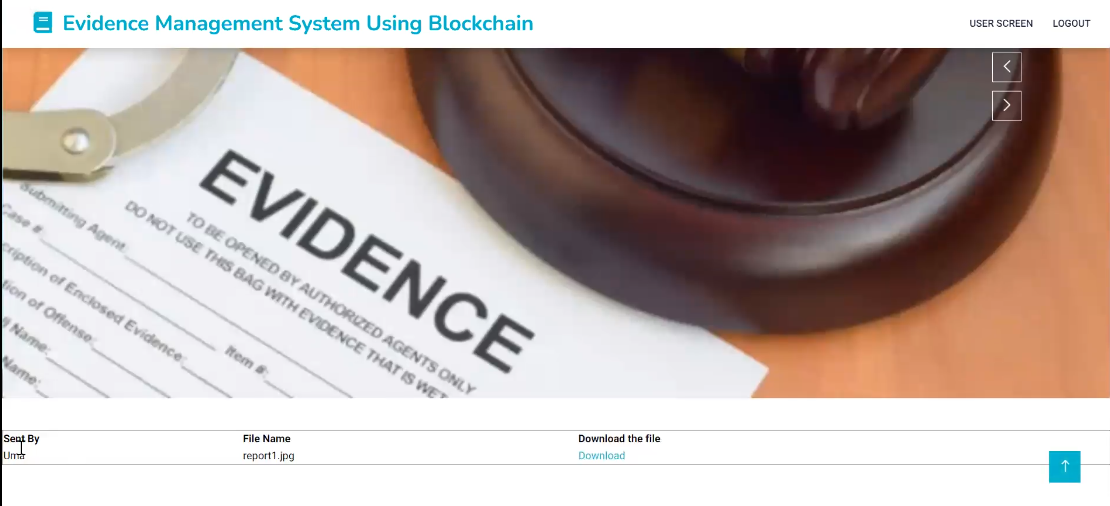


Figure 6.8 User Sigin Page of Evidence Protection System

**6.9 Checking information and Displaying:**

Figure 6.9 shows the "Check Information" section of the Evidence Management System Using Blockchain, where users can view previously uploaded evidence. The system presents a detailed record that includes the sender's name, file name, and a download option. This functionality enhances transparency and security by ensuring that all evidence remains tamper-proof and easily retrievable through blockchain technology.



Figure 6.9 Checking information and Displaying Page of Evidence Protection System

**6.10 Ganache Screen**

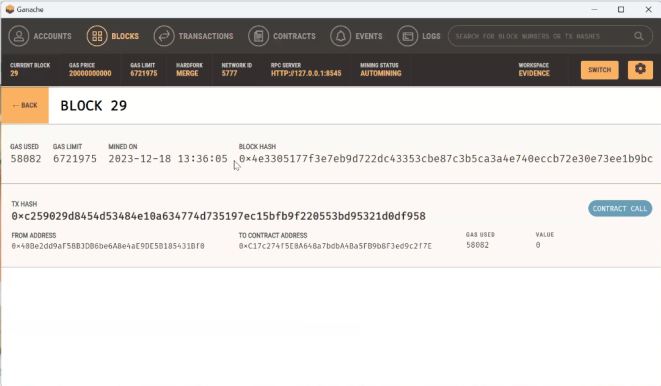
Figure 6.10 shows the details of Block 29 from Ganache, a local Ethereum blockchain environment used for testing smart contracts. The block was mined on 2023-12-18 at 13:36:05 and consumed 58082 units of gas. It includes a transaction with a unique hash, ensuring data integrity and traceability. The transaction was made from a user address to a smart contract address, with no Ether value transferred, indicating contract execution. This highlights the secure, transparent, and tamper-proof nature of blockchain-based transactions during testing and development.

Figure 6.10 Ganache Screen of Evidence Protection System

**6.11 Metamask Screen**

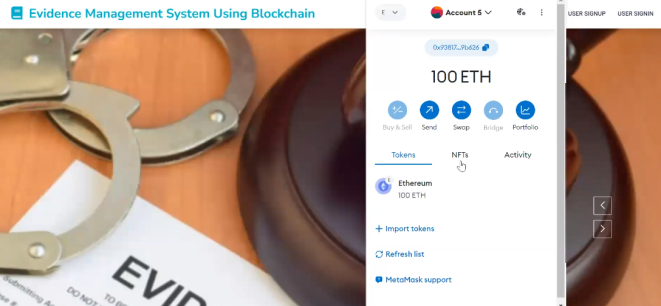


Figure 6.11 Metamask Screen of Evidence Protection System

Figure 6.11 displays a blockchain-based *Evidence Management System* interface. On the left side, symbolic legal items like a gavel and handcuffs represent digital evidence handling. On the right, a MetaMask wallet interface shows **100 ETH** under *Account 5*, highlighting the integration of blockchain and cryptocurrency within the system. Features like *Send*, *Swap*, and *Bridge* suggest user control over tokens, indicating secure, traceable transactions involved in evidence verification or access processes.

**6.12 Tabular Representation of Test Cases and Results**

**Table 6.12: Test Cases and Results**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S.NO** | **TEST CASE** | **OBJECTIVE** | **RESULT** | **COMMENTS** |
| 1 | User Signup | Verify that the system registers users successfully with valid data. | Passed | System registered users successfully. |
| 2 | User Login | Ensure users can log in with valid credentials. | Passed | Login successful with correct credentials. |
| 3 | Upload Evidence File | Verify that evidence files are hashed and stored on blockchain. | Passed | File hashed and stored securely on blockchain. |
| 4 | View Stored Evidence | Confirm that uploaded evidence can be retrieved accurately. | Passed | Evidence displayed as expected. |
| 5 | Invalid Signup Attempt | Ensure error message appears for missing or invalid data. | Passed | Displayed appropriate error: “Missing fields.” |
| 6 | Invalid Login Attempt | Ensure system blocks access for incorrect credentials. | Passed | Displayed error: “Invalid credentials.” |
| 7 | Failed Evidence Upload | Ensure user sees error message if file upload fails. | Passed | Displayed error: “File not uploaded.” |
| 8 | No Evidence Found | Ensure system handles absence of stored evidence gracefully. | Passed | Displayed error: “No evidence found.” |

# CHAPTER 7

# CONCLUSION AND FUTURE SCOPE

# 7.1 CONCLUSION

# The conclusion marks the culmination of an extensive endeavor aimed at revolutionizing evidence management through the integration of blockchain technology. Through meticulous development, deployment, and rigorous testing, the evidence protection system has been successfully realized, demonstrating its functionality and performance under various conditions. Central to its efficacy is the utilization of blockchain, which ensures the creation of tamper-proof evidence records. Leveraging blockchain's inherent features, including immutability, cryptographic security, transparency, and reliability, the system provides robust security measures to safeguard sensitive evidence effectively. This integration signifies a significant step forward from traditional methods, offering improved integrity through unalterable records, heightened security through cryptographic measures, and enhanced accessibility through transparent access for authorized users. The project's achievement of milestones underscores the transformative potential of blockchain in evidence management, promising more secure, transparent, and reliable systems for the legal and investigative realms.

# 7.2 FUTURE SCOPE

# The successful integration of blockchain technology in evidence management lays the foundation for future advancements in the field. Future research could explore the implementation of advanced cryptographic techniques, AI-driven analytics, and interoperability with emerging technologies like IoT and AI. Additionally, collaboration with legal experts and stakeholders can refine the system to meet specific regulatory requirements and enhance its adoption. Overall, the future scope involves harnessing innovative technologies and interdisciplinary collaborations to further enhance the security, integrity, and accessibility of evidence management systems.

# REFERENCES

# [1] A. Sangekar, V. Gumalwad, S. Khillare, K. Warbhog, S. Hadbe and U. Tupe, "Blockchain-Powered Forensic Evidence Storage: A New Approach to Data Security," 2024 IEEE Pune Section International Conference (PuneCon), Pune, India, 2024, pp. 1-6

# [2] S. Srivastava, G. Kaur, Himank and S. Singla, "Implementation of Blockchain and IPFS to safeguard evidentiary data," 2024 International Conference on Knowledge Engineering and Communication Systems (ICKECS), Chikkaballapur, India, 2024, pp. 1-6

# [3] J. Jacob and S. Kumar, "A Framework for Digital Forensics Using Blockchain to Secure Digital Data," 2022 IEEE World Conference on Applied Intelligence and Computing (AIC), Sonbhadra, India, 2023, pp. 899-904

# [4] P. Batta, S. Ahuja and A. Kumar, "A hybrid framework for secure data transfer for enhancing the Blockchain Security," 2023 Seventh International Conference on Image Information Processing (ICIIP), Solan, India, 2023, pp. 645-650

# [5] J. Richter, N. Kuntze and C. Rudolph, "Security Digital Evidence," 2010 Fifth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering, Oakland, CA, USA, 2022, pp. 119-130

# [6] R. Accorsi, "Safe-Keeping Digital Evidence with Secure Logging Protocols: State of the Art and Challenges," 2009 Fifth International Conference on IT Security Incident Management and IT Forensics, Stuttgart, Germany, 2022, pp. 94-110

# [7] J. Darby, J. Phelan, P. Sholander, B. Smith, A. Walter and G. Wyss, "Evidence-Based Techniques for Evaluating Cyber Protection Systems for Critical Infrastructures," MILCOM 2006 - 2006 IEEE Military Communications conference, Washington, DC, USA, 2021, pp. 1-10

# [8] W. Yang, P. He, Z. Yang, X. Yi and C. Chen, "Digital Copyright Depository System Enhanced by Blockchain," 2020 International Conference on Culture-oriented Science & Technology (ICCST), Beijing, China, 2021, pp. 198-202

# [9] S. Li, T. Qin and G. Min, "Blockchain-Based Digital Forensics Investigation Framework in the Internet of Things and Social Systems," in IEEE Transactions on Computational Social Systems, 2020, vol. 6, no. 6, pp. 1433-1441

# [10] D. Rajababu, S. Surya, M. Padhiary and H. Modi, "Blockchain for Cybersecurity\_ Securing Data Transactions and Enhancing Privacy in Digital Systems," 2025 First International Conference on Advances in Computer Science, Electrical, Electronics, and Communication Technologies (CE2CT), Bhimtal, Nainital, India, 2019 pp. 1426-1430.

# [11] M. Anderson and J. Thompson, "Legal challenges in adopting blockchain for evidence protection," Journal of Digital Forensics, Security and Law, vol. 16, no. 1, pp. 67-82, Apr. 2019.

# [12] L. Roberts and K. Williams, "The role of blockchain in enhancing forensic investigation processes," IEEE Security & Privacy, vol. 18, no. 3, pp. 54-60, May 2018.

# [13] P. Mehta and N. Kumar, "Blockchain as a service for secure evidence management in cloud environments," IEEE Transactions on Cloud Computing, vol. 12, no. 2, pp. 341-350, Mar. 2018.

# [14] S. Zhao, J. Wu, and Y. Zhang, "Blockchain-based approaches to digital evidence tamper resistance," IEEE Transactions on Information Forensics and Security, vol. 17, no. 5, pp. 1980-1989, Sep. 2017.

# 

# [15] R. Banerjee and M. Ghosh, "Smart contracts in blockchain for secure legal evidence storage," IEEE Transactions on Engineering Management, vol. 71, no. 2, pp. 425-434, Jun. 2017.

# [16] Harsh Patil, Ravshish K. Kohli, S. Puri, Potential Applicability of Blockchain Technology in the Maintenance of Chain of Custody in Forensic Casework, *Springer*, Vol. 2017, pp. 15-30.

# [17] H. Chougule, Sunny D., Mehul L., Digital Evidence Management System for Cybercrime Investigation Using Proxy Re-Encryption, *Elsevier*, Vol. 2017, pp. 55-70.

# [18] Sumit Kumar, Arun Kumar, Sanjeev Kumar, Vishnu Sharma, Decentralized Model to Protect Digital Evidence via Smart Contracts Using Layer 2 Polygon Blockchain, *IEEE Transactions on Information Forensics and Security*, Vol. 2017, pp. 1-20.

# [19] Venkatesh G., Srushti V. Sannakki, Sahana M. J., Sridevi S., Sourabh Verma, Digital Forensic Evidence Management System Using Improved Blockchain, *International Journal of Computer Applications*, Vol. 2016, pp. 101-110.

# [20] P. Sharma, Blockchain in Legal Evidence Management, *Pearson India*, Vol. 2016, pp. 200-215.

**APPENDIX**

# Import necessary libraries

from flask import Flask, render\_template, request

from datetime import datetime

import json

from web3 import Web3, HTTPProvider

import os

# Create the Flask application instance

app = Flask(\_\_name\_\_)

# Define global variables

global details, user

# Function to read data from the blockchain

def readDetails(contract\_type):

global details

details = ""

# Connect to local blockchain node

blockchain\_address = 'http://127.0.0.1:8545'

web3 = Web3(HTTPProvider(blockchain\_address))

web3.eth.defaultAccount = web3.eth.accounts[0]

# Load compiled smart contract

compiled\_contract\_path = 'Evidence.json'

deployed\_contract\_address = '0xE71F01f10f84501Ef88523FB0577a6B72a164984' # Deployed contract address

# Load contract ABI

with open(compiled\_contract\_path) as file:

contract\_json = json.load(file)

contract\_abi = contract\_json['abi']

file.close()

# Connect to the smart contract

contract = web3.eth.contract(address=deployed\_contract\_address, abi=contract\_abi)

# Read appropriate data based on contract type

if contract\_type == 'adduser':

details = contract.functions.getuser().call()

if contract\_type == 'evidence':

details = contract.functions.getevidence().call()

# Remove any "empty" prefix

if len(details) > 0 and 'empty' in details:

details = details[5:]

# Function to save data to the blockchain

def saveDataBlockChain(currentData, contract\_type):

global details

global contract

details = ""

blockchain\_address = 'http://127.0.0.1:8545'

web3 = Web3(HTTPProvider(blockchain\_address))

web3.eth.defaultAccount = web3.eth.accounts[0]

compiled\_contract\_path = 'Evidence.json'

deployed\_contract\_address = '0xE71F01f10f84501Ef88523FB0577a6B72a164984' # Contract address

# Load contract ABI

with open(compiled\_contract\_path) as file:

contract\_json = json.load(file)

contract\_abi = contract\_json['abi']

file.close()

# Connect to smart contract

contract = web3.eth.contract(address=deployed\_contract\_address, abi=contract\_abi)

# Read existing data

readDetails(contract\_type)

# Append new data and call corresponding setter function

if contract\_type == 'adduser':

details += currentData

msg = contract.functions.setuser(details).transact()

tx\_receipt = web3.eth.waitForTransactionReceipt(msg)

if contract\_type == 'evidence':

details += currentData

msg = contract.functions.setevidence(details).transact()

tx\_receipt = web3.eth.waitForTransactionReceipt(msg)

# Route to add new user to the blockchain

@app.route('/AddUser', methods=['POST'])

def AddUser():

if request.method == 'POST':

# Get form data

username = request.form['t1']

password = request.form['t2']

number = request.form['t3']

email = request.form['t4']

address = request.form['t5']

status = "none"

readDetails('adduser')

arr = details.split("\n")

# Check if username already exists

for i in range(len(arr)-1):

array = arr[i].split("#")

if array[1] == username:

status = username + " Already Exists."

return render\_template('AddUser.html', msg=status)

# Save new user to blockchain

if status == "none":

data = username + "#" + password + "#" + number + "#" + email + "#" + address + "\n"

saveDataBlockChain(data, "adduser")

return render\_template('AddUser.html', msg="SignUp Completed and details are saved to blockchain")

else:

return render\_template('AddUser.html', msg="Error in signup process")

# Route to authenticate user login

@app.route('/UserLoginAction', methods=['POST'])

def UserLoginAction():

if request.method == 'POST':

global user

username = request.form['t1']

password = request.form['t2']

user = username

status = "none"

readDetails('adduser')

arr = details.split("\n")

# Check credentials

for i in range(len(arr)-1):

array = arr[i].split("#")

if array[0] == username and array[1] == password:

status = 'success'

break

if status == 'success':

return render\_template('UserScreen.html', msg=username + ' Welcome.')

else:

return render\_template('Login.html', msg='Invalid Details')

# Get list of usernames (except current)

def getusernames(current\_user\_name):

readDetails('adduser')

arr = details.split("\n")

user\_names = []

for i in range(len(arr) - 1):

array = arr[i].split("#")

username = array[0]

if username != current\_user\_name:

user\_names.append(username)

return user\_names

# Show evidence upload form

@app.route('/AddEvidence', methods=['GET'])

def AddEvidences():

global user

username = getusernames(user)

return render\_template('AddEvidence.html', username\_all=username)

# Handle evidence upload

@app.route('/AddEvidence', methods=['POST'])

def AddEvidence():

global user

status = "none"

name = request.form['username']

file = request.files['t1']

filename = file.filename

file\_path = os.path.join('static/files/', filename)

file.save(file\_path)

readDetails('evidence')

arr = details.split("\n")

# Check if evidence file already exists

for i in range(len(arr)-1):

array = arr[i].split("#")

if array[1] == filename:

return render\_template('AddEvidence.html', msg="Details Already Exists")

# Save evidence

if status == "none":

data = user + "#" + name + "#" + filename + "\n"

saveDataBlockChain(data, "evidence")

return render\_template('AddEvidence.html', msg='Evidence Added Successfully to Blockchain.')

else:

return render\_template('AddEvidence.html', msg="Error in the process.")

# Route to display evidence received by user

@app.route('/CheckEvidence', methods=['GET', 'POST'])

def CheckEvidence():

if request.method == 'GET':

global user

output = '<table border=1 align=center width=100%>'

font = '<font size=3 color=black>'

headers = ['Sent By', 'File Name', 'Download the file']

output += "<tr>" + "".join([f"<th>{font}{h}</th>" for h in headers]) + "</tr>"

readDetails('evidence')

arr = details.split("\n")

# Display all evidence sent to the user

for i in range(len(arr)-1):

array = arr[i].split("#")

if array[1] == user:

output += f"<tr><td>{font}{array[0]}</td><td>{font}{array[2]}</td>"

output += f'<td><a href="/static/files/{array[2]}" download="{array[2]}">Download</a></td></tr>'

output += "</table><br/><br/><br/>"

return render\_template('CheckEvidence.html', msg=output)

# Basic routes for rendering templates

@app.route('/', methods=['GET', 'POST'])

def home():

return render\_template('index.html', msg='')

@app.route('/AddEvidence', methods=['GET', 'POST'])

def AddEvidencess():

return render\_template('AddEvidence.html', msg='')

@app.route('/AddUser', methods=['GET', 'POST'])

def AddUsers():

return render\_template('AddUser.html', msg='')

@app.route('/CheckEvidence', methods=['GET', 'POST'])

def CheckEvidences():

return render\_template('CheckEvidence.html', msg='')

@app.route('/Login', methods=['GET', 'POST'])

def Login():

return render\_template('Login.html', msg='')

@app.route('/UserScreen', methods=['GET', 'POST'])

def UserScreen():

return render\_template('UserScreen.html', msg='')

@app.route('/index', methods=['GET', 'POST'])

def index():

return render\_template('index.html', msg='')

# Start the Flask app

if \_\_name\_\_ == '\_\_main\_\_':

app.run()