A
REPORT
ON

# Designing a Blockchain-Driven eVault System for Legal Document Preservation

*Submitted by,*

**Ms. MADHUBALA S - 20211ISR0034**
**Ms. B KRIPASHINI - 20211ISR0045**

*Under the guidance of,*

**Dr. PRAVEENA K N**

*in partial fulfillment for the award of the degree of*

**BACHELOR OF TECHNOLOGY**

**IN**

**INFORMATION SCIENCE AND ENGINEERING**

**(ARTIFICIAL INTELLIGENCE AND ROBOTICS)**

**At**

GAIN MORE KNOWLEDGE
REACH GREATER HEIGHTS

**PRESIDENCY UNIVERSITY**

**BENGALURU**

**MAY 2025**

# PRESIDENCY UNIVERSITY

## PRESIDENCY SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

## CERTIFICATE

This is to certify that the Project report **"Designing a Blockchain-Driven eVault System for Legal Document Preservation"** being submitted by "MADHUBALA S, B KRIPASHINI" bearing roll number "20211ISR0034, 20211ISR0045" in partial fulfillment of the requirement for the award of the degree of Bachelor of Technology in Information Science Engineering is a Bonafide work carried out under my supervision.

Praveena K.N

**Dr. PRAVEENA K N**
Assistant Professor
Senior Scale
PSCS
Presidency University

**Dr. ZAFAR ALI KHAN**
Professor & HoD
PSCS
Presidency University

**Dr. MYDHILI NAIR**
Associate Dean
PSCS
Presidency University

**Dr. SAMEERUDDIN KHAN**
Pro-Vice Chancellor - Engineering
Dean –PSCS / PSIS
Presidency University

# PRESIDENCY UNIVERSITY

## PRESIDENCY SCHOOL OF COMPUTER SCIENCE AND ENGINEERING

## DECLARATION

I hereby declare that the work, which is being presented in the report entitled **“Designing a Blockchain-Driven eVault System for Legal Document Preservation”** in partial fulfillment for the award of Degree of **Bachelor of Technology** in **Information Science and Engineering(AI & ROBOTICS)**, is a record of my own investigations carried under the guidance of **DR. PRAVEENA K N, Assistant Professor-Senior scale, Presidency School of Computer Science and Engineering, Presidency University, Bengaluru.**

I have not submitted the matter presented in this report anywhere for the award of any other Degree.

| **Name** | **Roll No and** | **Signature of the Student** |
|---|---|---|
| **Madhubala S** | **20211ISR0034** | Madhubala |
| **B Kripashini** | **20211ISR0045** | B. Kripashi |

# ABSTRACT

Ensuring the safe and unalterable storage of legal documents is a significant challenge in today's digital environment. Traditional document management methods frequently encounter problems such as unauthorized access, data manipulation, and inefficiencies in retrieval processes. This report introduces a Blockchain-Based eVault for Legal Records, utilizing blockchain's decentralized nature to improve security, accessibility, and transparency. The suggested system incorporates cryptographic hashing and smart contracts to protect the integrity and confidentiality of documents while facilitating easy access for authorized users. By removing the requirement for intermediaries and creating a trustless setting, this approach reduces the risk of fraud, enhances operational efficiency, and ensures adherence to regulations.

This eVault, built on blockchain technology, aims to transform the management of legal records by providing a decentralized, secure, and verifiable storage solution. The incorporation of encryption and access controls guarantees that only authorized personnel can view sensitive documents, making it an ideal choice for legal practitioners, government agencies, and businesses. Furthermore, blockchain technology reduces the risks linked to data breaches and document tampering, ensuring the integrity and durability of legal records. This initiative showcases the revolutionary capabilities of blockchain in legal documentation, promoting a more efficient, transparent, and resistant method of record-keeping.

# ACKNOWLEDGEMENTS

First of all, we indebted to the **GOD ALMIGHTY** for giving me an opportunity to excel in our efforts to complete this project on time.

We express our sincere thanks to our respected dean **Dr. Md. Sameeruddin khan**, Pro-VC-Engineering and Dean, Presidency School of Computer Science and Engineering & Presidency School of Information Science, Presidency University for getting us permission to undergo the project.

We express our heartfelt gratitude to our beloved Associate Dean **Dr. Mydhili Nair,** Presidency School of Computer Science and Engineering, Presidency University, and **"Dr. Zafar Ali Khan"**, Head of the Department, Presidency School of Computer Science Engineering & Information Science, Presidency University, for rendering timely help in completing this project successfully.

We are greatly indebted to our guide **Dr. Praveena K N,** Assistant Professor-Senior Scale and Reviewer **Ms. Smitha S P**, Assistant Professor School of Computer Science Engineering & Information Science, Presidency University for his inspirational guidance, and valuable suggestions and for providing us a chance to express our technical capabilities in every respect for the completion of the internship work.

We would like to convey our gratitude and heartfelt thanks to the CSE7301 Internship/University Project Coordinator **Mr. Md Ziaur Rahman and Dr. Sampath A K,** department Project Coordinators **"Dr. Afroz Pasha"** and Git hub coordinator **Mr. Muthuraj.**

We thank our family and friends for the strong support and inspiration they have provided us in bringing out this project.

**MADHUBALA S**
**B KRIPASHINI**

# LIST OF TABLES

# LIST OF FIGURES

# TABLE OF CONTENTS

# CHAPTER-1

# INTRODUCTION

## 1.1 INTRODUCTION

Handling legal documents securely in today's digital landscape poses difficulties like data alteration and illicit access. Traditional storage solutions frequently prove to be inefficient and lack transparency, rendering them insufficient for contemporary legal standards. This initiative suggests a Blockchain-Based eVault, leveraging blockchain's decentralized and immutable technology to enhance the security, availability, and dependability of legal records.

Blockchain technology offers a reliable and decentralized approach to the storage and administration of legal records. By employing cryptographic methods and smart contracts, it ensures the integrity of data while limiting access to those who are authorized. This addresses the weaknesses commonly found in traditional centralized storage systems, such as data breaches and unauthorized alterations. Additionally, it improves transparency and operational efficiency by reducing the need for intermediaries.

Blockchain technology offers a reliable and decentralized approach to the storage and administration of legal records. By employing cryptographic methods and smart contracts, it ensures the integrity of data while limiting access to those who are authorized. This addresses the weaknesses commonly found in traditional centralized storage systems, such as data breaches and unauthorized alterations

## 1.2. Developing Blockchain-Based eVault for Legal Records: A Technological Solution

### 1.2.1 Overview of Blockchain-Based eVault for Legal Records

The Blockchain-Based eVault for Legal Records provides a safe and effective way to handle legal documents. Traditional methods of record-keeping frequently face challenges such as data breaches, unauthorized changes, and slow retrieval times. Leveraging the decentralized and tamper-resistant framework of blockchain, this system guarantees the authenticity and integrity of legal documents.

Smart contracts facilitate automated validation and access management, decreasing reliance on intermediaries and lowering the risk of human mistakes. This innovative method boosts data protection while enhancing the efficiency, transparency, and dependability of managing legal records.

The implementation of a Blockchain-Based eVault revolutionizes the management of legal records by providing a secure and transparent mechanism for document storage. In contrast to traditional centralized systems, blockchain spreads data across several nodes, which guarantees redundancy and removes the possibility of single points of failure. This strengthens both the security and availability of legal records, making them less vulnerable to cyber threats and unauthorized changes. Additionally, the cryptographic elements of blockchain protect sensitive information, ensuring that only permitted users can access particular documents. By utilizing this technology, legal organizations can enhance productivity, lower operating expenses, and create a more dependable digital record-keeping system.

A blockchain-based eVault improves both the security and efficiency of managing legal records by allowing immediate access and verification. Traditional paper-based and centralized digital systems often suffer from lengthy verification processes and are susceptible to document tampering. Through blockchain technology, every transaction and change is permanently documented on an unchangeable ledger, guaranteeing authenticity and transparency. Smart contracts facilitate tasks such as access management and document verification, reducing administrative workload. By adopting this decentralized approach, legal organizations can enhance their operations, foster trust, and ensure the secure long-term storage of data.

### 1.2.2 Objectives and Goals of the Project

**System Design and Technology Integration**

**Objective:** Create a blockchain-enabled eVault to provide secure, tamper-resistant, and efficient storage for legal documents, improving data integrity, accessibility, and minimizing dependence on intermediaries.

**System Architecture and Integration of Technology:**

**Design of Blockchain Framework :**

The eVault built on blockchain technology features a decentralized framework for the secure, transparent, and tamper-proof handling of legal documents. This system consists of several essential elements, such as a blockchain ledger, smart contracts, encryption protocols, and user authentication processes.

**Network Architecture Design:**

The design of the network architecture outlines the methods of communication and operation among blockchain nodes, thereby guaranteeing secure and effective data management. It may be a Public Blockchain (available to everyone), a Private Blockchain (limited to certain users), or a Consortium Blockchain (governed by several legal entities). This framework affects data security, scalability, and the governance of the system.

**Cryptographic Security Design:**

The Cryptographic Security Design protects the integrity and confidentiality of data by utilizing encryption and hashing methods. SHA-256 hashing guarantees the authenticity of documents, while AES and RSA encryption secure sensitive legal documents from unauthorized individuals. Furthermore, digital signatures verify ownership and deter data manipulation, thereby enhancing overall security.

**Anticipated Advantages:**

**Enhanced Security**: Guarantees the safeguarding of legal documents through blockchain encryption and its unchangeable nature.

**Improved Accessibility:** Enables permitted individuals to safely retrieve legal documents at any time and from any location.

**Operational Efficiency:** Streamlines the verification and management of documents, minimizing manual effort and processing duration.

**Challenges:**

Handling significant amounts of legal documentation while ensuring the efficiency of blockchain technology.

Guaranteeing compliance with legal and data privacy regulations in different regions.

Addressing pushback from conventional legal organizations and navigating technical intricacies.

**Upcoming enhancements:**

Utilizing AI to facilitate quicker and more precise access to legal documents.

Presenting biometric verification alongside multiple levels of access rights for enhanced security.

Introducing biometric identification with various tiers of access permissions to improve security.

### Blockchain Infrastructure:

Blockchain Solutions**:** Ethereum, Hyperledger Fabric, or Binance Smart Chain for reliable and decentralized record management**.**

Validation Method**:** PoW, PoS, or PBFT to authenticate and ensure the safety of transactions.

### Smart Contracts& Automation:

Smart contract creation: Employing Solidity(Ethereum) or Chain code (Hyperledger) to facilitate the automation of document verification and access management.

Access control mechanisms: Implementing role-based or attribute-based permissions to ensure secure management of documents.

### User Authentication & Identity Verification:

Multi-Factor Authentication (MFA): Enhancing security using one-time passwords (OTPs), biometric data, or authentication applications.

Decentralized Identity(DID): Adopting self-sovereign identity(SSI) solutions such as uPort or Sovrin for verifying user identities.

### Frontend & User Interface:

Web App: Developed using React, Angular, or Vue.js to ensure smooth user engagement

Mobile App: Optional application for Android/iOS to provide secure access to documents.

### Backend & API Integration:

Backend Development: Use Node.js or Python to manage requests and blockchain transactions.

RESTful or GraphQLAPIs**:** Facilitating interaction between the frontend and the blockchain network.

### Network & Infrastructure:

Decentralized Nodes: Operating blockchain nodes to ensure decentralization.

Cloud and On-Premise Servers: Facilitating blockchain nodes and providing off-chain storage options.

### Components Required for Blockchain-Based eVault for Legal Records

1. **Permissioned Blockchain Environment**: Allows only verified participants to access and manage sensitive records.
2. **Dedicated Node Infrastructure**: Runs blockchain nodes to securely validate and store transaction data.
3. **Activity Monitoring Module**: Logs system operations for detailed auditing and legal oversight.
4. **Instant Alert Mechanism**: Notifies users of access requests, modifications, or unauthorized attempts.
5. **Trusted Certificate Support**: Integrates with digital certificates for document origin verification.
6. **Regulatory Compliance Checker**: Automatically evaluates whether processes align with legal standards.
7. **Optimized File Handling**: Uses compression techniques to manage storage efficiently for large documents.
8. **Ledger Transparency Interface**: Provides authorized users with access to view blockchain transaction records.
9. **Secured User Session Handling**: Protects login sessions with encryption, tracking, and auto-expiry features.
10. **Disaster Recovery Setup**: Maintains data continuity through automated backup and failover systems.

**Secure Data Handling: Managing Storage and Access Control.**

### 1.3.1. Economic Benefits of Blockchain-Based eVault for Legal Records

1. **Unchangeable Document Storage:** Guarantees that legal records remain intact and immune to tampering.
2. **Permission Management Systems:** Establishes role-based access for secure handling of documents.
3. **Sophisticated Encryption Methods:** Utilizes AES-256 and RSA to safeguard data against unauthorized access.
4. **Automated Smart Contracts:** Enables secure and efficient verification of documents.
5. **Decentralized Storage Options:** Utilizes IPFS or cloud platforms for scalable and secure data preservation.
6. **Multi-Factor Authentication (MFA):** Improves login security throughthe use of OTPs, biometrics, or authentication applications.
7. **Cryptographic Digital Signatures:** Verifies documents and prevents forgery.
8. **Rapid and Secure Data Access:** Facilitates effective searching and retrieval of legal records.
9. **Thorough Audit Trails:** Monitors all document interactions for transparency and accountability.
10. **Compliance with Legal and Regulatory Standards:** Ensures conformity with data protection laws and industry regulations.
11. **Time-Based Logging:** Captures timestamps for every document action to ensure traceability.
12. **User Interaction Tracking:** Monitors all user activities for improved transparency and control.
13. **Instant Access Revocation:** Automatically removes access rights when user permissions change.
14. **Distributed Backup System:** Stores multiple record copies across the network for data protection.
15. **Encrypted Metadata Management:** Safeguards document details and access logs using encryption.
16. **Privacy-Preserving Proofs:** Confirms document ownership without revealing sensitive content.

17. **User-Controlled Encryption Keys:** Allows individuals to manage their own secure encryption keys.
18. **Document Version History:** Keeps track of all changes to prevent data loss or manipulation.
19. **Secured API Integration:** Ensures only authenticated applications and users can interact with the system.
20. **Automated Threat Response:** Detects and reacts to security breaches with real-time alerts and protocols.

### 1.3.2 Scalability and Adaptability of the System

**Scalability of Blockchain-Based eVault for legal Records:**

1. **Scalable Blockchain Network**: Supports the addition of more nodes to improve security and manage increasing volumes of legal records.

2. **Adaptive Storage Solutions:** Merges on-chain and off-chain storage methods for efficient processing of substantial document quantities.

3. **Smooth System Compatibility:** Guarantees integration with diverse legal systems and record management platforms.

4. **Versatile Modular Design:** Facilitates straightforward upgrades and the incorporation of new technologies for future growth.

**Adaptability of the Blockchain-Based eVault for Legal Records:**

1. **Dynamic Access Control:** Sets up role-based permissions to meet various legal and organizational standards.
2. **Effortless System Integration:** Connects smoothly with current legal databases and document management systems.
3. **Adherence to Changing Regulations:** Adjusts to new legal standards and data privacy policies.
4. **Cross-Blockchain Interoperability:** Functions across various blockchain networks for improved flexibility and compatibility.
5. **Expandable Architecture:** Increases storage and processing capabilities to accommodate growing amounts of legal documentation.
6. **Long-Term Design: Facilitates the seamless integration of AI, smart contracts, and enhanced security features for ongoing innovation.**

# CHAPTER-2
# LITERATURE SURVEY

## Figure 2.1

| No | Reference | Objective | Methodology | Findings/Contribution | Limitations |
|---|---|---|---|---|---|
| 1 | Zhanget al., 2018 | To build a secure digital notary using block chain. | Utilized blockchain for secure timestamps and document logging. | Enabled reliable and unchangeable proof of document existence. | Did not connect with real-world legal document systems. |
| 2 | Verma & Singh, 2019 | To automate legal record validation through smart contracts. | Designed Ethereum-based smart contracts for storing and validating documents. | Proved automated, trustless legal document validation. | Scalability issues due to high transaction costs. |
| 3 | Kumar & Reddy, 2020 | To safeguard government records with blockchain-based storage. | Applied Hyperledger Fabric for permissioned record storage. | Improved security and transparency of sensitive records. | Poor integration with traditional databases. |
| 4 | Patel & Thomas, 2021 | To securely distribute legal files using decentralized tech. | Combined Ethereum and IPFS for encrypted file sharing. | Ensured secure access and distributed legal data storage. | Lacked robust access control and identity management. |
| 5 | Sharma & Gupta, 2022 | To enhance evidence security in legal processes. | Implemented blockchain to track evidence chain-of-custody. | Strengthened legal evidence integrity and traceability. | Only focused on evidence, not full legal records. |

# CHAPTER-3

# RESEARCH GAPS OF EXISTING METHODS

## 3.1 Challenges in Existing Legal Record Management Systems

Conventional legal record management systems encounter various obstacles, including a lack of transparency, the potential for unauthorized access, and susceptibility to data manipulation. Manual procedures often result in delays, inefficiencies, and challenges in confirming the authenticity of legal documents.

### 3.1.1 Exorbitant Startup Expenses

**High Initial Investment in Blockchain Implementation**

Applying blockchain technology for managing legal records typically incurs significant upfront costs due to the requirement for specialized infrastructure, experienced developers, and secure data transfer. These costs pose a challenge for smaller legal organizations and governmental agencies to implement such systems. Current solutions also fail to offer cost-effective, scalable frameworks capable of maintaining secure and efficient long-term storage of legal documents.

### 3.1.2 Lack of Standardized Legal Frameworks

One significant barrier to the implementation of blockchain-based legal record systems is the lack of globally recognized legal and regulatory frameworks. Different regions have distinct regulations regarding digital signatures, data privacy, and the acceptance of blockchain in legal proceedings, which complicates international legal activities. Without a standard approach, ensuring compliance, interoperability, and confidence in blockchain-based legal documentation systems becomes challenging. This uncertainty hampers widespread adoption and restricts the legal validity and enforceability of the system.

### 3.1.3 Limited Accessibility and User Awareness

Even with progress in digital technology, a significant number of legal professionals and users remain uninformed about blockchain-based options. A lack of technical expertise, particularly in legal institutions that are rural or underfunded, obstructs the **embrace of these** systems. Furthermore, obstacles to access, such as inadequate internet connectivity and the absence of user-friendly interfaces, further impede widespread adoption. This disparity diminishes the influence and accessibility of blockchain solutions in managing legal records, particularly in areas where they are most needed.

### 3.1.4 Inadequate Data Security in Centralized Systems

Centralized systems for managing legal records are significantly exposed to cyber attacks, unauthorized access, and data tampering. As all essential information is kept in one place, any security breach or system malfunction can lead to considerable data loss or compromise. Additionally, these systems frequently do not incorporate advanced encryption or real-time monitoring, rendering them less dependable for processing sensitive legal documents. This vulnerability highlights the necessity for decentralized and tamper-resistant solutions such as blockchain technology.

### 3.1.5 Poor Integration with Legacy Legal Systems

Many legal organizations continue to depend on legacy systems and manual processes, which complicates the adoption of contemporary blockchain solutions. Integration is stymied by compatibility challenges and a lack of standardized data formats. This interrupts the flow of data, leads to inefficiencies, and constrains the ability of blockchain to enhance legal operations and bolster record security.

### 3.1.6 Limited Scalability in Existing Blockchain Systems

Many current blockchain platforms encounter scalability challenges when handling a high volume of transactions or substantial data loads, as seen in legal document management. Increased network congestion, sluggish transaction processing, and restricted on-chain storage capabilities can lead to delays and diminish overall system efficiency. These constraints pose difficulties in utilizing blockchain technology effectively in settings that necessitate regular document uploads, verification, and retrieval, such as courts, law firms, and governmental registries.

### 3.1.7 Absence of User-Friendly Interfaces

Many blockchain-based systems are not designed with ease of use in mind, making them difficult for legal professionals to navigate. The presence of complex interfaces and technical processes can hinder non-technical users from efficiently managing or retrieving legal documents. Without a user-friendly and accessible design, adoption remains slow, particularly among legal institutions that are less familiar with emerging technologies.

### 3.1.8 Privacy Concerns in Public Blockchains

While blockchain provides transparency and immutability, the storage of sensitive legal documents on public blockchains presents considerable privacy issues. Legal records frequently include private personal and case-specific information that needs safeguarding from public view. In the absence of strong encryption and regulated access systems, there is a substantial risk of unauthorized disclosure. Such worries contribute to the reluctance of legal institutions to entirely embrace blockchain for the management of sensitive records.

### 3.1.9 Lack of Real-Time Document Verification

Numerous current legal record systems, including certain blockchain-based solutions, lack the capability for real-time document verification. This results in delays when verifying the authenticity and status of legal documents, particularly in urgent cases. In the absence of immediate validation features, legal processes become less efficient, and users may encounter outdated or unverified information, which undermines confidence in the system's dependability.

# CHAPTER-4

# PROPOSED MOTHODOLOGY

## 4.1 Proposed Methodology for Developing Block chain based evault for legal record

The proposed approach centers on establishing a secure, decentralized platform for the management of legal documents utilizing blockchain technology. It starts with gathering requirements from legal experts to ensure the system addresses practical needs. Smart contracts will facilitate the automation of procedures such as creating records, controlling access, and validating information. A permissioned blockchain, such as Hyperledger Fabric or a private Ethereum network, will be utilized to preserve confidentiality and integrity of the data. Security will be enhanced through the implementation of encryption methods and digital signatures. Lastly, a user-friendly interface will be crafted to allow legal professionals with limited technical skills to easily access and navigate the system.

## 4.2. System Architecture

Legal documents are extremely sensitive and necessitate secure, tamper-resistant storage and regulated access. Conventional record management systems encounter issues such as data breaches, loss, and difficulties in verification. This initiative suggests a blockchain-based eVault system that guarantees secure storage, convenient access, and data integrity through the use of encryption, smart contracts, and decentralized technologies.

**Technologies and Components Used in the System:**

**Encryption Methods:**

AES (Advanced Encryption Standard): Used for the symmetric encryption of legal documents. RSA (Rivest–Shamir–Adleman): Employed for key encryption and secure key distribution. SHA-256: Utilized for hashing and verifying file integrity via checksums.

**Access Control Mechanisms:**

Role-Based Access Control (RBAC): Allocates permissions according to user roles (e.g., judge, lawyer).

Attribute-Based Access Control (ABAC): Provides access based on user attributes (e.g., case type, department).

**Consensus and Data Verification:**

Proof-of-Work (PoW) / Proof-of-Stake (PoS): Employed for confirming blockchain transactions based on the specific platform.

**Merkle Trees:**

Utilized for rapid and secure verification of data.

**Data Compression (zlib):**

Decreases file size for effective storage.

File Storage Optimization:

**File Segmentation:**

Breaks files into smaller sections for improved storage and retrieval. Rabin Fingerprinting

**Technique:**

Identifies variable chunk borders for greater efficiency.

### 4.3. Workflow

The system operates in six phases:

**Phase 1**: User Registration & Authentication Individuals (judges, lawyers, clients) sign up and log in securely through credentials using MetaMask and private keys.

**Phase 2**: File Upload and Encryption Legal documents are secured with AES/RSA encryption prior to storage, and metadata is hashed using SHA-256 to ensure integrity.

**Phase3**: Blockchain Record Creation A smart contract is initiated to record file metadata and access logs on the blockchain ledger.

**Phase 4**: Decentralized Storage Encrypted documents are divided into chunks and uploaded to a decentralized storage solution (e.g., IPFS or Filecoin), guaranteeing tamper-proof preservation.

**Phase 5**: Access Control& Retrieval Access permissions are managed using RBAC/ABAC frameworks, permitting only authorized users to access and decrypt the records.

**Phase 6**: Verification and Audit Smart contracts keep a log of every access or modification attempt, facilitating traceable and auditable records.

### 4.4. Advantages of the Proposed System

1. Decentralized System: Eliminates dependence on a central authority for the validation or management of records.
2. Streamlined Workflow Automation: Smart contracts takeover repetitive legal responsibilities such as approvals and verifications.
3. Environmentally Friendly Approach: Encourages sustainable documentation practices by removing the necessity for physical records.
4. Accessible Across Multiple Platforms: Records can be securely retrieved from any device with the appropriate authentication.

# CHAPTER-5
# OBJECTIVES

The goal of this project is to create and deploy a blockchain-based eVault system designed for the secure and decentralized management of legal documents. Traditional methods of recordkeeping encounter numerous challenges, including data breaches, inefficiencies, and a lack of transparency. The proposed solution tackles these issues by incorporating blockchain technology, robust encryption, and automated smart contracts. To ensure document security, AES and RSA encryption is utilized, which guarantees confidentiality and secure data transmission. SHA-256 hashing protects data integrity by signaling any unauthorized changes. Files will be stored on decentralized networks such as IPFS or Filecoin, which decreases dependence on a central server and enhances availability. Smart contracts are employed to automate critical functions such as access verification, data logging, and record updates without the need for human involvement. Access control is managed through RBAC and ABAC models, delivering precise permissions at the user level. Each transaction is permanently recorded on the blockchain, ensuring total transparency and auditability.

## 5.1 Develop a Blockchain-Based eVault System for Legal Records

This stage involves developing a highly secure and decentralized eVault system utilizing blockchain technology to organize and store legal documents. The platform will act as a digital archive for essential legal records, including contracts, case files, and judgments, guaranteeing their storage in a tamper-proof and verifiable manner. Each document saved in the system will be permanently logged on the blockchain, enabling transparent monitoring of access and changes. In contrast to conventional centralized systems, this approach offers improved data integrity, accountability, and resistance to unauthorized alterations. Tailored for legal professionals, it ensures dependable and controlled access to records while upholding the utmost level of security.

## 5.2 Implement Secure Encryption Techniques for Data Protection

In this stage, strong encryption methods are implemented to guarantee the confidentiality and integrity of legal documents stored in the eVault. AES is used for encrypting file content, rendering the data unreadable to those without authorization. RSA is utilized for the secure exchange of keys, ensuring that encryption keys are transmitted safely between authorized individuals. To ensure data integrity, SHA-256 hashing is employed to create unique digital fingerprints for each file, enabling quick detection of any unauthorized modifications. Collectively, these techniques establish a multi-layered security framework that shields sensitive legal records from breaches, tampering, and unauthorized access.

### 5.3 Integrate Decentralized Storage using IPFS/Filecoin

At this phase, decentralized storage solutions like IPFS or Filecoin are employed to securely house encrypted legal documents across a distributed network. Rather than depending on a solitary centralized server, this method distributes data among numerous nodes, significantly diminishing the chances of system failures, data breaches, or unauthorized access. When a file is uploaded to the system, it is segmented into encrypted pieces and stored in different locations, each distinguished by a unique cryptographic hash. This guarantees the integrity of the data, facilitates straightforward retrieval, and improves fault tolerance. Decentralized storage not only enhances privacy and security but also offers a scalable approach for managing legal data over the long term.

### 5.4 Integrate Decentralized Storage using IPFS/Filecoin

This phase concentrates on establishing a secure access management system that governs user permissions based on their identity and roles. Role-Based Access Control (RBAC) restricts access according to set roles such as judge, lawyer, or client, ensuring that users can only view data pertinent to their duties. Attribute-Based Access Control (ABAC) enhances this by incorporating additional criteria like case assignments, user qualifications, and department ties to permit or deny access. By integrating RBAC and ABAC, we achieve a more flexible, secure, and accurate control over sensitive legal documents, safeguarding against unauthorized access and improving data confidentiality.

### 5.5 Automate Legal Record Verification using Smart Contracts

This phase focuses on utilizing smart contracts to enhance and secure the validation of legal documents within the blockchain-powered eVault. Smart contracts are automated programs that operate on the blockchain, executing specific tasks once certain conditions are fulfilled. In this framework, they manage responsibilities like verifying user access permissions, validating the authenticity of documents, and monitoring activities without the need for human intervention. For example, when a user tries to access a legal record, the smart contract automatically checks their credentials and allows access if they are authorized. This automation improves security, eliminates human errors, and guarantees transparent, traceable processes.

### 5.6 Ensure Tamper-Proof Audit Trails for All Transactions

The purpose of this step is to securely log every operation within the eVault, ensuring complete transparency. By leveraging the unchangeable characteristics of blockchain technology, every action— including file uploads, modifications, access events, or transfers— is permanently recorded and cannot be changed. These secure audit logs offer a dependable account of user activities, boosting trust and responsibility. This system is particularly beneficial for legal compliance and investigative purposes, providing a clear, verifiable record of all interactions with sensitive documents.

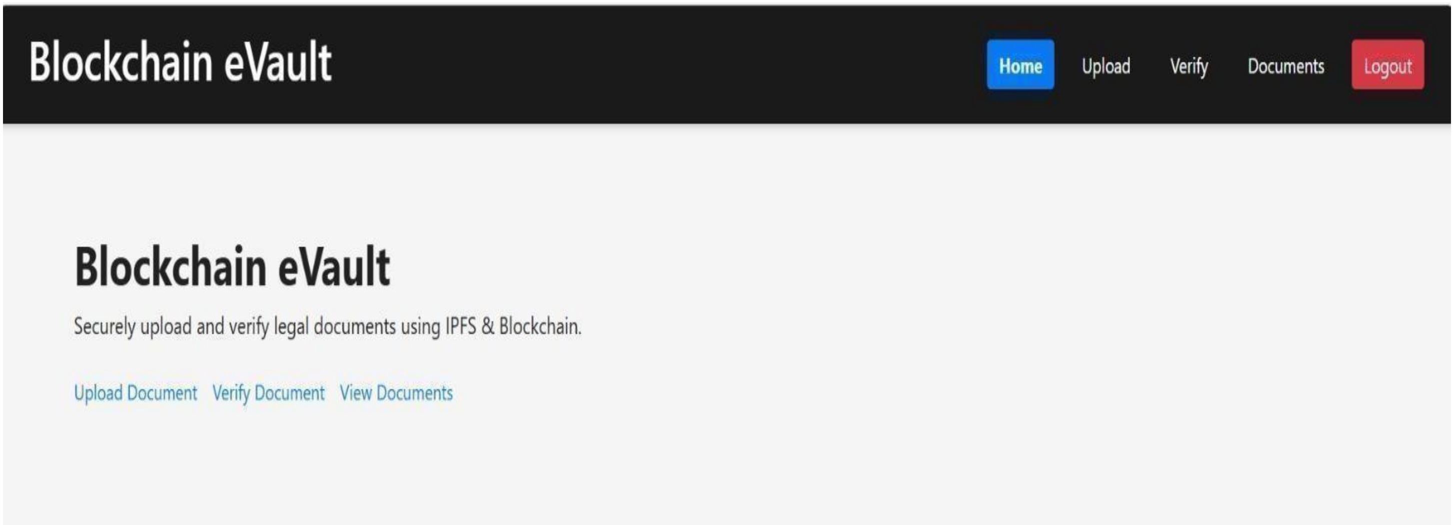
### 5.7 Enhance User Authentication with Multi-Factor Verification

This stage emphasizes enhancing the system’s security by adopting multi-factor authentication (MFA). Rather than relying solely on a password, users are required to confirm their identity through additional methods such as a one-time password, biometric scan, or a secure token. This multi-layered authentication approach guarantees that only authorized users can access the legal records, even if their main login details are compromised. By mandating several forms of verification, the system becomes significantly more secure and better equipped to withstand unauthorized access or cyber threats.

# CHAPTER-6

# SYSTEM DESIGN& IMPLEMENTATION

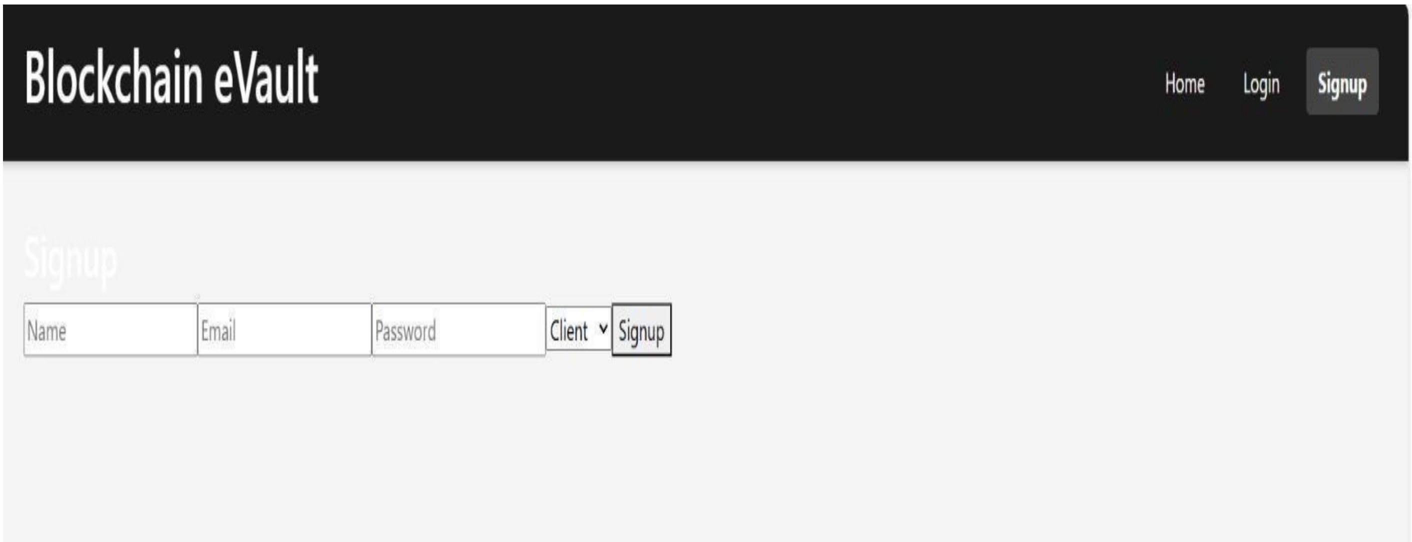
## SYSTEM DESIGN



Blockchain eVault

Securely upload and verify legal documents using IPFS & Blockchain.

**Chapter 6**
**Fig 6.1. Blockchain eVault Application Dashboard**



**Chapter 6**
**Fig 6.2. User Registration Screen Of The Blockchain eVault Application**

# Implementation

**Encryption and Access Control Mechanisms:**

Legal documents are safeguarded using AES for symmetric encryption alongside RSA for secure key distribution. To ensure file integrity, hashing with SHA-256 is employed. Access rights are governed through Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC), which establish user permissions based on their roles and identity characteristics, ensuring that access is restricted to authorized users only.

**Consensus and Blockchain Data Handling:**

The system operates with Proof-of-Work (PoW) or Proof-of-Stake (PoS) algorithms depending on the specific blockchain platform to achieve agreement within the network. Merkle Trees facilitate rapid and secure data validation, while compression utilities such as zlib assist in minimizing storage space requirements without compromising data quality.

**File Chunking Strategy:**

To enhance efficiency, files are segmented into smaller units utilizing Rabin's fingerprinting algorithm, which identifies optimal chunk boundaries. These smaller encrypted fragments improve storage distribution and expedite retrieval processes, making them more efficient.

**Decentralized Storage Systems:**

All encrypted file segments are stored throughout distributed storage networks such as IPFS or Filecoin, ensuring redundancy, data accessibility, and protection against centralized failures.

**Blockchain Infrastructure Setup:**

The eVault system is developed and tested using Ganache, while MetaMask is used to manage digital identities and access controls. Smart contracts are deployed to automate permission management, monitor system activities, and uphold a tamper-proof record of all transactions.

**Security and User-Friendly Features:**

Robust security measures, including private key authentication, multi-factor login, and activity logging, are incorporated. The system also features tools for metadata tagging, secure file uploads, and an intuitive interface designed for legal professionals.

**Process of Uploading Documents to a Blockchain Network**

**Document Selection:**

Users initiate the process by choosing the legal documents they intend to upload via a secure file input interface designated by the system.

**Metadata Collection:**

After a file is selected, the system automatically gathers essential metadata such as file type, size, creation date, and pertinent legal identifiers for efficient indexing and reference.

**Hashing and Preparation for Storage:**

Each document is processed with a cryptographic hash function (e.g., SHA-256), creating a unique digital fingerprint. This hash is subsequently recorded on the blockchain along with the metadata, facilitating future verification without the need to store the actual file on-chain.

**Digital Authentication:**

To confirm authenticity, users digitally sign the document using their private key. This signature validates the identity of the sender and ensures that the document remains unaltered, without revealing the actual content of the document.

**Audit Trail and Traceability:**

All transactions and interactions involving documents are permanently recorded on the blockchain. This audit trail offers transparency and traceability, aiding in the detection of unauthorized actions and guaranteeing legal compliance.

**Secure File Storage:**

The encrypted document is divided into chunks (using Rabin's fingerprinting) and stored in a decentralized network like IPFS or Filecoin. This approach safeguards against single-point failures and ensures redundancy.

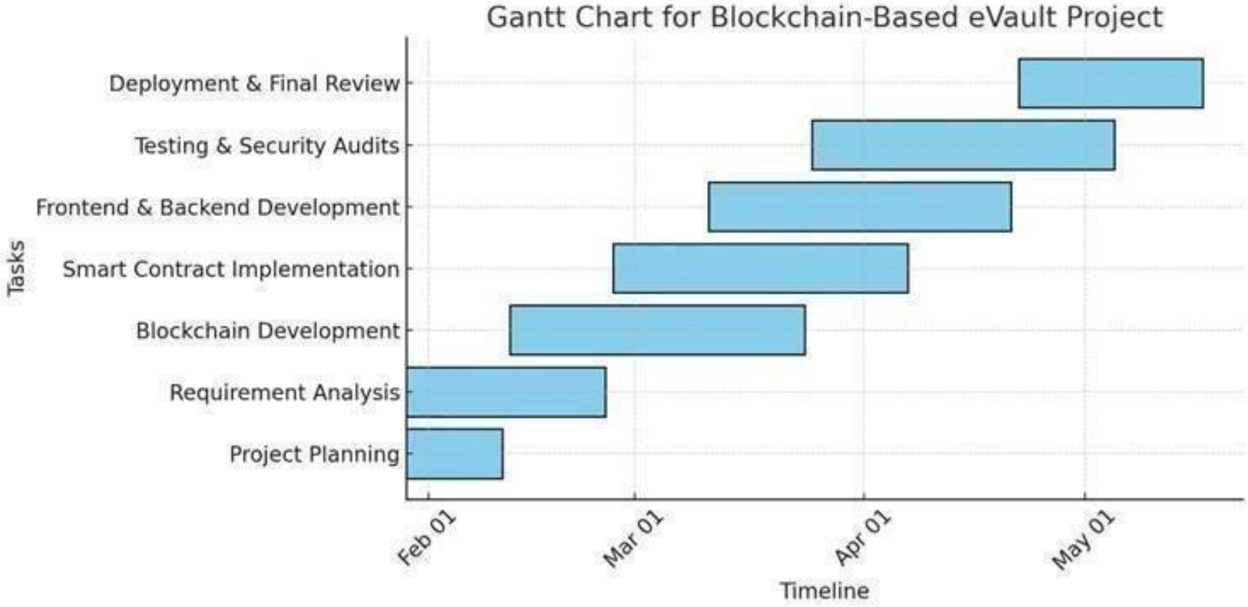
**Access Control:**

Role-Based Access Control and Attribute-Based Access Control policies are implemented to determine who has the authority to view, edit, or retrieve the document based on their specific roles.

# CHAPTER-7

## TIMELINE FOREXECUTION OF PROJECT

## (GANTT CHART)



# CHAPTER-8

# OUTCOMES

## 1. System Overview:

The suggested eVault system is a decentralized and highly secure platform designed for the storage and management of legal documents utilizing blockchain technology. It employs robust encryption techniques, distributed storage, and smart access control methods to safeguard the privacy and integrity of sensitive legal information. The system allows verified users—such as attorneys, clients, and judges—to upload, access, and verify documents without depending on a central authority.

## 2. Core Features:

➢ **Immutable Document Storage:**

The system utilizes the decentralized characteristics of blockchain technology to store hashes of documents, ensuring that once a file is added, it cannot be altered. This permanence protects legal records from being tampered with or edited without authorization.

➢ **Transparent Audit Trails:**

Every action—be it uploading, downloading, or viewing—is securely recorded on the blockchain. This immutable ledger provides a thorough account of every engagement with a document. It aids in detecting unauthorized access or errors via detailed audit trails.

➢ **Efficient Metadata Processing:**

Upon submitting a document, the system collects key metadata including name, size, format, and timestamp. This data facilitates the effective organization and retrieval of records as required. It preserves document privacy while providing robust search and filtering capabilities. Storing metadata on the blockchain enables transparent, traceable document histories. Users have the ability to track version history and connect related records effortlessly.

# CHAPTER-9

# RESULTS AND DISCUSSIONS

The eVault system, built on blockchain technology, was created to improve the storage, retrieval, and security of legal documents, and its effectiveness was assessed across various criteria. The use of AES for symmetric encryption and RSA for asymmetric encryption guaranteed that files remained confidential and securely protected throughout their entire lifecycle. The application of SHA-256 hashing further enhanced the system by ensuring the integrity of each stored document. During evaluations, any attempts at tampering or unauthorized alterations of data were promptly identified, showcasing the reliability of hash verification. Access control measures such as RBAC (Role-Based Access Control) and ABAC (Attribute-Based Access Control) were also effectively implemented, enabling flexible and secure management of permissions based on users' roles and attributes.

The architecture of the system demonstrated effectiveness in real-time operations. User-uploaded files were automatically processed to extract metadata and create unique cryptographic hashes. This data was securely stored on the blockchain to establish an unalterable record for each file. The file chunking algorithm improved storage efficiency by dividing large files into smaller segments prior to encryption and storage, significantly lowering latency during both upload and download activities. Rabin's fingerprinting algorithm ensured that the chunking process was dynamic and optimized. File retrieval was also straightforward, with the system quickly reassembling the chunks while preserving data accuracy. This method guaranteed that even high-volume data could be managed with minimal impact on system performance.

From a usability perspective, incorporating tools such as Ganache for local blockchain development and MetaMask for user authentication was very effective. Smart contracts were utilized to oversee document verification and access management, which operated seamlessly throughout various testing scenarios. The system allowed judges, lawyers, and clients to digitally sign documents using private keys, which improved authenticity and ensured non-repudiation. The audit logging feature monitored all activities on the platform, providing transparency and a comprehensive historical record for each document's lifecycle. These functionalities were evaluated across different user roles to guarantee that access rights and system responses matched each role, and the outcomes validated the system's reliability improving overall system reliability.

An assessment of scalability and future adaptability was conducted as well. Simulated environments with multiple users demonstrated that the system could efficiently manage several simultaneous uploads, downloads, and verifications without significant delays or system disruptions. Decentralized storage platforms such as IPFS and Filecoin were incorporated for secure off-chain storage, enabling the blockchain to manage metadata while preserving file confidentiality and enhancing storage efficiency. The implementation showed that the system has the capability to scale beyond small configurations and can be embraced by larger legal organizations. In summary, the proposed eVault system effectively resolved critical challenges in managing legal documents, encompassing data integrity, user verification, scalability, and resistance to tampering, thus establishing it as a dependable and future-ready solution for the legal field.

# CHAPTER-10

## CONCLUSION

The blockchain-based eVault provides a secure and trustworthy method for managing legal documents by employing cutting-edge technologies such as AES and RSA encryption, along with SHA-256 to ensure data integrity, and utilizing decentralized storage solutions like IPFS and Filecoin. These technologies collaborate to safeguard sensitive legal information, uphold its authenticity, and manage access efficiently. Incorporating smart contracts and digital signatures further enhances security and trust, optimizing legal processes and guaranteeing transparency.

In addition to bolstering security, the system is crafted to be scalable, user-friendly, and capable of producing real-time audit logs. These features assist in thwarting unauthorized access, document alterations, and data breaches. Built on a robust blockchain foundation, the eVault stands as an innovative answer for legal record management and presents the possibility for wider implementation in sectors that require secure and transparent document management.

Moreover, the eVault enhances the capabilities of legal professionals—including judges, attorneys, and clients—by offering a secure and intuitive platform for accessing and sharing documents. The implementation of role-based and attribute-based access control (RBAC & ABAC) ensures that only approved users can view sensitive information, fostering trust and accountability. By incorporating cutting-edge technologies into a cohesive solution, this initiative marks progress in the modernization of legal infrastructure.

# REFERENCES

[1] Verma, A., Bhattacharya, P., Saraswat, D., & Tanwar, S. (2021). NyaYa: Blockchain-based electronic law record management scheme for judicial investigations. Journal of Information Security and Applications, 63, 103025.

[2] Lemieux, V. L. (2021). Blockchain and Recordkeeping. Computers, 10(11), 135.

[3] Tasnim, M. A., Omar, A. A., Rahman, M. S., & Bhuiyan, M. Z. A. (2018). Crab: Blockchain based criminal record management system. In Security, Privacy, and Anonymity in Computation, Communication, and Storage: 11th International Conference and Satellite Workshops, SpaCCS 2018, Melbourne, NSW, Australia, December 11-13, 2018, Proceedings 11 (pp. 294-303). Springer International Publishing.

[4] Ali, S., Wang, G., White, B., & Cottrell, R. L. (2018, August). A blockchain-based decentralized data storage and access framework for pinger. In 2018 17th IEEE international conference on trust, security and privacy in computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE) (pp. 1303-1308). IEEE

[5] Malomo, O., Rawat, D., & Garuba, M. (2020). Security through block vault in a blockchain enabled federated cloud framework. Applied Network Science, 5(1), 1-18.

[6] Storer, M. W., Greenan, K., Long, D. D., & Miller, E. L. (2008, October). Secure data deduplication. In Proceedings of the 4th ACM international workshop on Storage security and survivability (pp. 1- 10).

[7] Batista, D., Mangeth, A. L., Frajhof, I., Alves, P. H., Nasser, R., Robichez, G., ... & Miranda, F. P. D. (2023). Exploring Blockchain Technology for Chain of Custody Control in Physical Evidence: A Systematic Literature Review. Journal of Risk and Financial Management, 16(8), 360

[8] Mohsin, K. (2021). Blockchain Law: A New Beginning

[9] Lemieux, V., Hofman, D., Batista, D., & Joo, A. (2019). Blockchain technology & recordkeeping. ARMA International Educational Foundation

[10] G. Li and H. Sato, “A privacy-preserving and fully decentralized storage and sharing system on the blockchain,” in Proceedings of the 2019 IEEE 43rd Annual Computer Software and Applications Conference, pp. 694–699, IEEE, Milwaukee, WI, USA, July 2019.

# APPENDIX-A

# PSUEDOCODE

```
import dotenv from"dotenv";
dotenv.config();

import express from "express";
import mongoose from"mongoose";
import cors from "cors";
import helmet from"helmet";
import compression from "compression";
import rateLimit from"express-rate-limit";

import documentRoutes from "./routes/documentRoutes.js";
import authRoutes from "./routes/authRoutes.js";
import videoRoutes from "./routes/videoRoutes.js";
import uploadRoutes from"./routes/uploadRoutes.js";
import errorHandler from
"./middlewares/errorMiddleware.js";

const app = express();

//Security& Performance
app.use(helmet());
app.use(compression());

app.use(cors({
   origin: "http://localhost:5173",
   credentials: true,
}));

const limiter = rateLimit({
```

```
windowMs: 15 * 60 * 1000,
   max: 100,
   message: { error: "Too manyrequests, tryagain later." },
});
app.use(limiter);


app.use(express.json({ limit: "50mb" }));
app.use(express.urlencoded({ extended: true }));


// MongoDB Connect
mongoose.connect(process.env.MONGODB_URI, {
   useNewUrlParser: true,
   useUnifiedTopology: true,
})
   .then(() => console.log("MongoDB connected
successfully!"))
   .catch(err => {
      console.error("MongoDB connection error:",
err.message);
      process.exit(1);
   });


mongoose.connection.on("disconnected", () => {
   console.warn("MongoDBdisconnected. Retrying...");
});


// Routes
app.use("/api/documents", documentRoutes); // this includes
/verify
app.use("/api/auth", authRoutes);
app.use("/api/videos", videoRoutes);
app.use("/api/upload", uploadRoutes);
```

```
// Health check
app.get("/", (req, res) => {
    res.status(200).json({ message: "eVault API is running!"
});
});


app.use(errorHandler);


const PORT = process.env.PORT || 5000;
app.listen(PORT, () => console.log(Server running on port
${PORT}));
```

server.js code

```
import React, { useState, useEffect } from"react";
import {
  BrowserRouter as Router,
  Routes,
  Route,
  NavLink,
  useNavigate,
} from "react-router-dom";


import Home from "./pages/Home.jsx";
import Upload from "./pages/Upload.jsx";
import Verify from "./pages/Verify.jsx";
import Documents from "./pages/Documents.jsx";
import Login from "./pages/Login.jsx";
import Signup from"./pages/Signup.jsx";
import JudgeDashboard from "./pages/JudgeDashboard.jsx";
import LawyerDashboard from
"./pages/LawyerDashboard.jsx";
import ClientDashboard from "./pages/ClientDashboard.jsx";
import "bootstrap/dist/css/bootstrap.min.css";
import "./App.css";
function MainApp() {
  const [user, setUser] = useState(null);
  const navigate = useNavigate();

  useEffect(() => {
    const storedUser = localStorage.getItem("user");
    if (storedUser) {
      try {
        setUser(JSON.parse(storedUser));
      } catch (error) {
        console.error("Invalid user data in localStorage:",
error);
        localStorage.removeItem("user"); // Clear broken data
      }
    }
  }, []);

  const handleLogout = () => {
    localStorage.removeItem("user");
    localStorage.removeItem("token");
    setUser(null);
    navigate("/login");
  };

  return (
    <div className="app-container">
      <nav className="navbar">
        <h1>Blockchain eVault</h1>
        <div className="nav-links">
```

```
<NavLink to="/" className={({ isActive }) =>
(isActive ? "active" : "")}>
            Home
          </NavLink>


          {user ? (
            <>
              {user.role === "judge" && (
                <NavLink to="/judge-
dashboard">Dashboard</NavLink>
              )}
              {user.role === "lawyer" && (
                <NavLink to="/lawyer-
dashboard">Dashboard</NavLink>
              )}
              {user.role === "client" && (
                <NavLink to="/client-
dashboard">Dashboard</NavLink>
              )}
              <NavLink to="/upload">Upload</NavLink>
              <NavLink to="/verify">Verify</NavLink>
              <NavLink
to="/documents">Documents</NavLink>
              <button className="logout-btn"
onClick={handleLogout}>
                Logout
              </button>
            </>
          ) : (
            <>
              <NavLink to="/login">Login</NavLink>
              <NavLink to="/signup">Signup</NavLink>
            </>
)}
    </div>
   </nav>

   <div className="content">
    <Routes>
     <Route path="/" element={<Home />} />
     <Route
      path="/upload"
      element={user ? <Upload /> : <Login
setUser={setUser} />}
     />
     <Route
      path="/verify"
      element={user ? <Verify/> : <Login
setUser={setUser} />}
     />
     <Route
      path="/documents"
      element={user ? <Documents /> : <Login
setUser={setUser} />}
     />
     <Route
      path="/judge-dashboard"
      element={
       user?.role === "judge" ? (
        <JudgeDashboard />
       ) : (
        <Login setUser={setUser} />
       )
      }
     />
```

```
<Route
      path="/lawyer-dashboard"
      element={
       user?.role === "lawyer" ? (
        <LawyerDashboard />
       ) : (
        <Login setUser={setUser} />
       )
      }
     />
     <Route
      path="/client-dashboard"
      element={
       user?.role === "client" ? (
        <ClientDashboard />
       ) : (
        <Login setUser={setUser} />
       )
      }
     />
     <Route path="/login" element={<Login
setUser={setUser} />} />
     <Route path="/signup" element={<Signup
setUser={setUser} />} />
    </Routes>
   </div>
  </div>
 );
}

function App() {
 return (
 <Router>
      <MainApp />
    </Router>
  );
}

export default App;
```

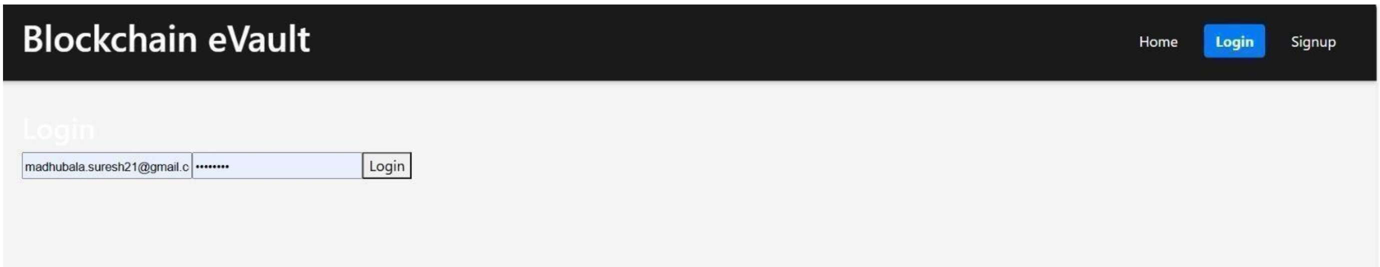
app.jsx

```
import axios from "axios";

const  API = axios.create({
  baseURL: "http://localhost:5000/api",
});

export default API;
```

api.js

# APPENDIX-B

## SCREENSHOT



madhubala.suresh21@gmail.c ••••••••

**Figure B.1. Login Interface Of Blockchain eVault System**

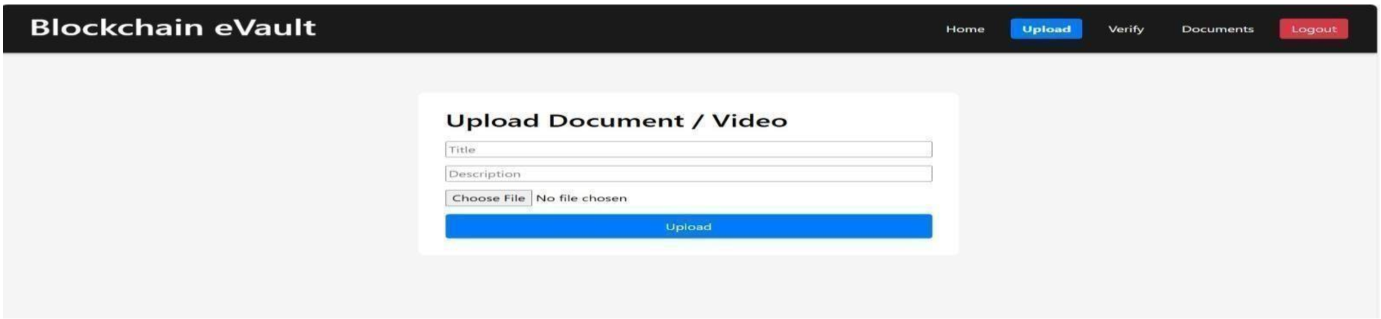
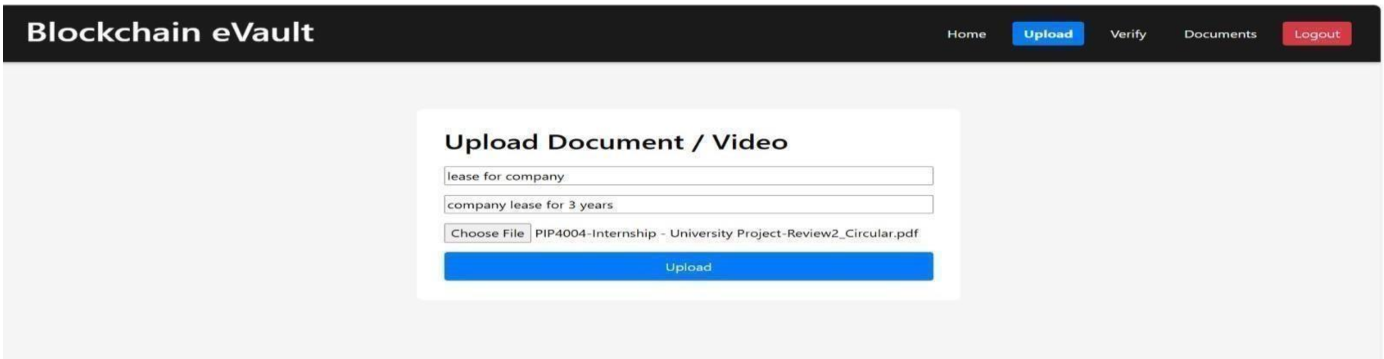


**Figure B.2. Document/Video Upload Interface Of Blockchain eVault**

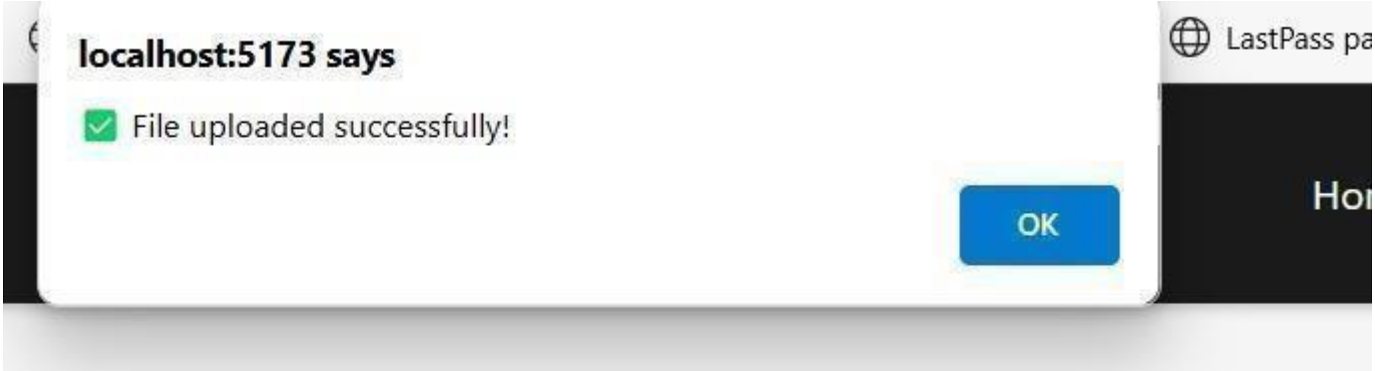


lease for company

company lease for 3 years

PIP4004-Internship - University Project-Review2_Circular.pdf

**Figure B.3. Document/Video Upload Interface With Metadata Input**



localhost:5173 says

✅ File uploaded successfully!

**FigureB.4. Confirmation Popup After Successful File Upload**

# APPENDIX-C

# ENCLOSURES

**1. Journal publication/Conference Paper Presented Certificates of all students.**

**2. Similarity Index / Plagiarism Checkreport clearly showing the Percentage (%). No need for a page-wise explanation.**

**3. Details of mapping the project with the Sustainable Development Goals (SDGs).**

# MADHUBALA S final report

ORIGINALITY REPORT

| 12% | 8% | 7% | 8% |
|---|---|---|---|
| SIMILARITY INDEX | INTERNET SOURCES | PUBLICATIONS | STUDENT PAPERS |

PRIMARY SOURCES

| | | |
|---|---|---|
| 1 | Submitted to Presidency University<br>Student Paper | 4% |
| 2 | Submitted to Northern Arizona University<br>Student Paper | 1% |
| 3 | Submitted to University College London<br>Student Paper | 1% |
| 4 | www.ijariit.com<br>Internet Source | 1% |
| 5 | Submitted to University of Greenwich<br>Student Paper | 1% |
| 6 | Submitted to Aston University<br>Student Paper | <1% |
| 7 | Naresh Kshetri, Purnendu Shekhar Pandey, Mohiuddin Ahmed. "Blockchain Technology for Cyber Defense, Cybersecurity, and Countermeasures - Techniques, Solutions, and Applications", CRC Press, 2025<br>Publication | <1% |
| 8 | www.freecodecamp.org<br>Internet Source | <1% |
| 9 | www.jetir.org<br>Internet Source | <1% |
| 10 | Arun Kumar Rana, Sumit Kumar Rana, Vishnu Sharma, Ritu Dewan. "Intelligent Data-Driven Techniques for Security of Digital Assets", CRC Press, 2025<br>Publication | <1% |

| | | |
|---|---|---|
| 11 | www.geeksforgeeks.org<br>Internet Source | <1% |
| 12 | Submitted to University of East London<br>Student Paper | <1% |
| 13 | kolvereid.reflection-network.eu<br>Internet Source | <1% |
| 14 | dev.to<br>Internet Source | <1% |
| 15 | fastercapital.com<br>Internet Source | <1% |
| 16 | John R. Vacca. "Cloud Computing Security - Foundations and Challenges", CRC Press, 2020<br>Publication | <1% |
| 17 | Laxmi Poonia, Seema Tinker. "Blockchain technology in addressing and mitigating the COVID-19 crisis: Empowering pandemic response", AIP Publishing, 2024<br>Publication | <1% |
| 18 | spectrum.library.concordia.ca<br>Internet Source | <1% |
| 19 | Submitted to ESoft Metro Campus, Sri Lanka<br>Student Paper | <1% |
| 20 | Submitted to Nanyang Technological University<br>Student Paper | <1% |
| 21 | api.w3programmer.net<br>Internet Source | <1% |
| 22 | Submitted to City University<br>Student Paper | <1% |
| 23 | Submitted to University Politehnica of Bucharest | <1% |

|  |  |  |
|---|---|---|
|  | Student Paper |  |
| 24 | rajivdewan.blogspot.com<br>Internet Source | <1% |
| 25 | Babeş-Bolyai University<br>Publication | <1% |
| 26 | Submitted to Kingston University<br>Student Paper | <1% |
| 27 | Matheen Fathima G, Shakkeera L. "Efficient task scheduling and computational offloading optimization with federated learning and blockchain in mobile cloud computing", Results in Control and Optimization, 2025<br>Publication | <1% |
| 28 | dspace.vut.cz<br>Internet Source | <1% |
| 29 | www.timreview.ca<br>Internet Source | <1% |
| 30 | "Blockchain and Applications, 6th International Congress", Springer Science and Business Media LLC, 2025<br>Publication | <1% |
| 31 | Yassine Maleh, Mohammad Shojafar, Mamoun Alazab, Imed Romdhani. "Blockchain for Cybersecurity and Privacy - Architectures, Challenges, and Applications", CRC Press, 2020<br>Publication | <1% |
| 32 | ebin.pub<br>Internet Source | <1% |
| 33 | ijmrset.com<br>Internet Source | <1% |
| 34 | jcsdf.nfsu.ac.in<br>Internet Source | <1% |

| | | |
|---|---|---|
| 35 | www.coursehero.com<br>Internet Source | <1% |

| | | | |
|---|---|---|---|
| Exclude quotes | Off | Exclude matches | Off |
| Exclude bibliography | On | | |

# *Designing a Blockchain-Driven eVault System for Legal Document Preservation*

Dr. Praveena K N
*Dept of Computer Science and Engineering*
*Presidency University*
Bangalore, India
Praveenakn@presidencyuniversity.in

Madhubala S
*Dept of Information Science and Engineering*
*presidency university*
Bangalore, India
madhubala.suresh21@gmail.com

B Kripashini
*Dept of Information Science and Engineering*
*Presidency University*
*Bangalore, India*
*kripashinik@gmail.com*

***Abstract*— This research focuses on building a blockchain-integrated eVault designed to securely store and manage legal documentation. In response to the increasing need for dependable digital record systems, the proposed solution employs blockchain to uphold data accuracy, traceability, and ease of access. Through the integration of smart contracts and encryption protocols, the system streamlines key processes such as validation, permission control, and audit tracking, thereby boosting both security and operational effectiveness. The decentralized architecture and unchangeable ledger offer a strong foundation for handling legal records, while also aligning with regulatory compliance requirements. Furthermore, blockchain's inherent ability to log all interactions fosters transparency and enforces accountability in record-keeping.**

***Keywords—Blockchain,eVault,LegalRecordsManagement***

## I. INTRODUCTION

The legal industry is experiencing a considerable digital shift as automation and electronic documents improve access and workflow. Protecting digital records of legal documents, however, is still problematic in terms of guaranteeing reliability, security, and uninterrupted access. A lack of adequate protection to prevent illegitimate access, information leaks, and tampering are common issues faced by conventional systems..

To solve these problems, "eVault for Legal Records using Blockchain" is the project suggested which intends to utilize the power of blockchain technology. Sensitive legal documents can be managed more effectively with blockchain technology due to its unresolved single point of failure, immutability, decentralized structure, and cryptographic fortification. Blockchains make all records fully transparent and verifiable while ensuring resistance to alteration.

This project is centered on creating a secure eVault for legal documentation, utilizing blockchain as its core technology. enhancing security, transparency, and operational efficiency.. The system seeks to provide a guarded interaction environment to legal practitioners, clients, and governing custodians through compliance with set legal and regulatory guidelines ensuring protection of sensitive documents.

Through this progress the project envisions a future in which judicial procedures become more efficient, self-consistent and not susceptible to fraud, therefore contributing to a stronger and more technologically sophisticated legal infrastructure.

## II. RELATED WORKS

Incorporating blockchain into legal record-keeping systems has become a major focus in recent research, prompting the development of novel approaches that strengthen transparency, security, and the reliability of stored data. Verma and Ashwin, for instance, proposed NyaYa, an Electronic Law (EL) management framework built on blockchain, which addresses these critical areas.encompassing Phases like stakeholder registration, case monitoring across organizations, and settlement through smartmonitoring across organizations, and settlement through smart contracts were incorporated. Simulations indicated that NyaYa surpassed conventional electronic legal (EL) storage systems in terms of mining costs, response times for queries, and trust reliability, ultimately improving the efficiency and security of managing digital evidence.

Lemieux examined the broader applications of blockchain as a distributed ledger technology across sectors like finance, healthcare, and real estate. The study emphasized blockchain's capacity to provide secure and transparent recordkeeping through cryptographically linked transaction blocks, highlighting benefits such as improved change detection and enhanced privacy via public-private key encryption, while also acknowledging challenges related to scalability and legal implications.

Tasnim et al. developed a blockchain-based system focused on securely managing and storing criminal records. By embedding these records within the blockchain and leveraging decentralized peer-to-peer cloud networks, their method aimed to eliminate the risk of data tampering while enhancing overall security. allowed law enforcement and other authorized

# MADHUBALA S madhu_finalref

ORIGINALITY REPORT

| 6% | 5% | 3% | 1% |
|---|---|---|---|
| SIMILARITY INDEX | INTERNET SOURCES | PUBLICATIONS | STUDENT PAPERS |

PRIMARY SOURCES

| | | |
|---|---|---|
| 1 | www.jetir.org<br>Internet Source | 2% |
| 2 | fastercapital.com<br>Internet Source | 1% |
| 3 | ijmrset.com<br>Internet Source | 1% |
| 4 | Submitted to Sheffield Hallam University<br>Student Paper | <1% |
| 5 | Tarik CHAFIQ, Rida AZMI, Abdelhamid FADIL, Ouadoud Mohammed. "Investigating the Potential of Blockchain Technology for Geospatial Data Sharing: Opportunities, Challenges, and Solutions", Geomatica, 2024<br>Publication | <1% |
| 6 | nextbillion.ai<br>Internet Source | <1% |
| 7 | Demir, Ahmet Serhat. "A Fully Decentralized Framework for Securely Sharing Digital Content.", Middle East Technical University (Turkey), 2024<br>Publication | <1% |
| 8 | mafiadoc.com<br>Internet Source | <1% |
| 9 | pure.tue.nl<br>Internet Source | <1% |
| 10 | "Advances in Computer Science and Ubiquitous Computing", Springer Nature, 2018<br>Publication | <1% |

|  |  |  |
|---|---|---|
| 11 | "Blockchain and Applications, 6th International Congress", Springer Science and Business Media LLC, 2025<br>Publication | <1% |
| 12 | Debasis Chaudhuri, Jan Harm C Pretorius, Debashis Das, Sauvik Bal. "International Conference on Security, Surveillance and Artificial Intelligence (ICSSAI-2023) - Proceedings of the International Conference on Security, Surveillance and Artificial Intelligence (ICSSAI-2023), Dec 1–2, 2023, Kolkata, India", CRC Press, 2024<br>Publication | <1% |
| 13 | ijrpr.com<br>Internet Source | <1% |
| 14 | www.ijprems.com<br>Internet Source | <1% |
| 15 | Shangping Wang, Yinglong Zhang, Yaling Zhang. "A Blockchain-Based Framework for Data Sharing with Fine-grained Access Control in Decentralized Storage Systems", IEEE Access, 2018<br>Publication | <1% |
| 16 | Yassine Maleh, Mohammad Shojafar, Mamoun Alazab, Imed Romdhani. "Blockchain for Cybersecurity and Privacy - Architectures, Challenges, and Applications", CRC Press, 2020<br>Publication | <1% |

|  |  |  |  |
|---|---|---|---|
| Exclude quotes | Off | Exclude matches | Off |
| Exclude bibliography | On |  |  |

# SUSTAINABLE DEVELOPMENT GOALS

SUSTAINABLE DEVELOPMENT GOALS
1 NO POVERTY
2 ZERO HUNGER
3 GOOD HEALTH AND WELL-BEING
4 QUALITY EDUCATION
5 GENDER EQUALITY
6 CLEAN WATER AND SANITATION
7 AFFORDABLE AND CLEAN ENERGY
8 DECENT WORK AND ECONOMIC GROWTH
9 INDUSTRY, INNOVATION AND INFRASTRUCTURE
10 REDUCED INEQUALITIES
11 SUSTAINABLE CITIES AND COMMUNITIES
12 RESPONSIBLE CONSUMPTION AND PRODUCTION
13 CLIMATE ACTION
14 LIFE BELOW WATER
15 LIFE ON LAND
16 PEACE, JUSTICE AND STRONG INSTITUTIONS
17 PARTNERSHIPS FOR THE GOALS

- SDG 16 – Peace, Justice, and Strong Institutions This initiative improves transparency, accountability, and safety in legal processes by utilizing a blockchain system for the management of legal records. It promotes equitable access to justice and reinforces trust in institutions.
- SDG 9 – Industry, Innovation, and Infrastructure Through the adoption of advanced blockchain technology, the project encourages innovation in digital infrastructure. It provides a secure, scalable solution for legal documentation.
- SDG 11 – Sustainable Cities and Communities Dependable legal documentation is essential for ensuring property rights, legal identity, and access to civic services. The eVault system contributes to inclusive and sustainable urban development.
- SDG 17 – Partnerships for the Goals The effectiveness of the eVault system relies on collaboration among legal authorities, governmental organizations, and technology providers. This fosters strong partnerships aimed at establishing a transparent legal framework.