e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 10, October 2024

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.521

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Developing a Blockchain Based eVault for Storing Legal Records

Srilakshmi CH[1], Rohit S.V[2], Sandeep Kaushik R[3], Sreejay V[4]

Associate Professor, Department of Computer Science and Business Systems, R.M.D. Engineering College, Chennai, India[1]

Student, Department of Computer Science and Business Systems, R.M.D. Engineering College, Chennai, India [2]

Student, Department of Computer Science and Business Systems, R.M.D. Engineering College, Chennai, India [3]

Student, Department of Computer Science and Business Systems, R.M.D. Engineering College, Chennai, India [4]

ABSTRACT: The eVault project introduces an innovative solution for the secure and efficient management of legal records through blockchain technology. In today's digital landscape, traditional legal document storage methods face numerous challenges, including vulnerability to tampering, limited transparency, and fragmented access. eVault addresses these issues by leveraging blockchain's decentralized architecture, which ensures immutability, transparency, and enhanced security for legal professionals and individuals. This tamper-proof platform enables the secure storage, management, and retrieval of diverse legal records, such as contracts, deeds, and court documents. All data stored within eVault is encrypted, preserving confidentiality while providing authorized users with easy access when needed. Our objective is to create a secure, transparent, and accessible ecosystem that caters to the needs of all stakeholders, including lawyers, judges, clients, and registrars.

KEYWORDS: eVault; Blockchain; Legal documents; Decentralized Architecture, Secure Storage;

I. INTRODUCTION

In the digital age, the management and storage of legal records have become crucial challenges that require innovative solutions. Traditional methods of storing legal documents, often reliant on physical archives or centralized digital systems, are prone to inefficiencies such as data tampering, limited accessibility, and fragmented information management. These challenges are compounded bythe increasing complexity of legal processes and the growing demand for secure, transparent, and easily accessible legal records. As a response to these pressing issues, blockchain technology emerges as a transformative solution, offering a decentralized, secure, and immutable platform for managing legal records.

Blockchain technology offers unique benefits that address the limitations of traditional legal record storage. Fundamentally, blockchain is a distributed ledger that records transactions or data in an immutable, transparent, and secure manner. Each block in the blockchain contains a cryptographic hash of the previous block, ensuring that records cannot be altered without detection. This structure creates a chain of records that are virtually tamper-proof, enhancing the security and trustworthiness of the stored data. In the context of legal records, this is particularly important, as it ensures that documents such as contracts, deeds, and court filings remain unaltered and verifiable.

A key feature of blockchain technology is its ability to support smart contracts—self-executing contracts with terms directly written into code. In the legal domain, smart contracts can automate and enforce legal agreements, streamlining processes such as property transactions, contract execution, and dispute resolution. This automation reduces the need for intermediaries, minimizes the risk of human error, and enhances the overall efficiency of legal processes. For instance, in real estate, smart contracts can automatically transfer ownership once payment is confirmed, ensuring that all parties adhere to the agreed terms without the need for manual intervention.

II. LITERATURE SURVEY

[1] 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..
It introduces a system utilizing blockchain for secure storage and management of criminal records, emphasizing authenticity, data integrity, and protection against tampering. By integrating criminal records into a blockchain and employing a peer-to-peer cloud network for decentralization, the system aims to prevent unauthorized alterations and enhance overall data security..

[2] 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..
This paper proposes a blockchain-based data storage and access framework for PingER, a global Internet performance measurement project. Utilizing a permissioned blockchain and Distributed Hash Tables (DHT), metadata is stored on the blockchain while actual files are stored off-chain via DHT in a decentralized manner.

[3] 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).
The paper proposes a solution by generating encryption keys consistently from data chunks, allowing deduplication while maintaining encryption. The paper outlines the security mechanisms and evaluates the system's effectiveness in achieving secure deduplication.

[4] 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.
It addresses the critical issue of offsite data recovery and security in the face of cyber-attacks and disasters. Cyber threats, especially related to data storage, have become highly sophisticated and challenging to defend against. Ransomware attacks targeting sensitive data have shown a significant rise, highlighting the need for secure offsite storage solutions

[5] Lemieux, V. L. (2021). Blockchain and Recordkeeping. Computers, 10(11), 135.
Paper describes about Blockchain, a distributed ledger technology, aims to create immutable records of transactions. It's rapidly transforming various sectors like healthcare, real estate, and finance, promising trustworthy and secure recordkeeping.

III. PROPOSED SYSTEM

The Blockchain eVault System is designed to securely manage legal records through decentralized technology. By leveraging blockchain, the system offers tamper-proof documentation and transparent sharing between authorized entities like lawyers, judges, and other stakeholders.
The core architecture consists of three major layers:

- Frontend Layer: Built using React and ChakraUI, this layer provides an intuitive user interface (UI) for document management, access control, and secure sharing. It allows users to upload legal documents, view, share, and track document integrity.
- Backend Layer: The backend, developed with Node.js and Express, handles communication between the frontend and the blockchain network. It manages user authentication, uploads, and data retrieval. It also uses Ethers.js and Web3.js for smart contract interactions and document handling.
- Blockchain Layer: This layer consists of smart contracts written in Solidity. It enforces role-based access control (RBAC), allowing permissions to be granted only to authorized users based on their roles (e.g., judge, lawyer, third-party service). The blockchain stores document metadata, while the actual files are stored securely off-chain to optimize storage efficiency.

IV. METHODOLOGY OF APPROACH

System Specifications:

- Software: Anaconda, Python 3.7+, Notepad/MS Word, 64-bit OS, Windows 7+, Visual Studio Code.
- Hardware: Core i3 processor or higher, 4GB RAM, 80GB storage, Full HD webcam.

Architecture Diagram: The system consists of three layers:

- **Frontend**: React and ChakraUI are used to provide a user-friendly interface for uploading, viewing, and tracking documents.
- **Backend**: Node.js and Express handle user authentication, file management, and communication with the blockchain, using Ethers.js and Web3.js for smart contract interactions.
- **Blockchain**: Smart contracts written in Solidity ensure role-based access control (RBAC) for secure, tamper-proof storage of metadata. Actual documents are stored off-chain to optimize storage.

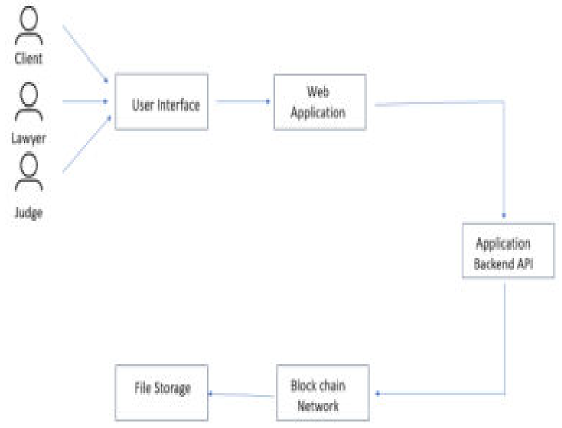


Figure 1 Architecture Diagram

User Authentication:

- Sign-Up/Log-In Process: When a user accesses the system for the first time, they go through a sign-up process where personal details like name, email, and password are provided. Returning users log in using their credentials.
- Backend Verification: The credentials are sent to the backend, where they are checked against a stored database of users. If valid, the user is authenticated.
- Authorization Token: Upon successful authentication, the backend generates a unique authorization token for the session. This token is critical for further API requests to ensure secure communication.
- Role Assignment: Based on the user’s profile (judge, lawyer, or other legal professionals), the system assigns different roles with specific access rights. For example, a judge may have higher-level access compared to a regular lawyer.

Document Upload:

- Upload Mechanism: After logging in, the user can upload legal documents using the frontend interface. The document is sent to the backend as a file along with metadata such as document type, owner, and user ID.
- Hashing Process: To ensure document integrity, the backend generates a cryptographic hash of the file. This hash is a unique fingerprint of the document, ensuring that even the slightest change will alter the hash.
- Off-Chain Storage: Since blockchain storage is expensive and limited, the actual document is stored off-chain in a secure external file storage system, such as IPFS or traditional cloud storage.
- Blockchain Recording: The generated hash, along with metadata like document owner and timestamp, is sent to the blockchain. The smart contract stores this data, ensuring transparency and immutability.

Document Sharing:

a. User Selection: When a user wants to share a document, they specify the recipient's address (another authorized user or entity). The recipient may be another lawyer, judge, or third-party involved in the legal process.

b. Permission Verification: The system interacts with a smart contract to check the roles and permissions of both the sender and recipient. If the sender is authorized to share the document and the recipient has the appropriate permissions, access is granted.

c. Blockchain Updates: Once access is granted, the blockchain is updated to reflect the sharing activity. This ensures that any future access to the document is transparent and traceable.

Role-Based Access Control:

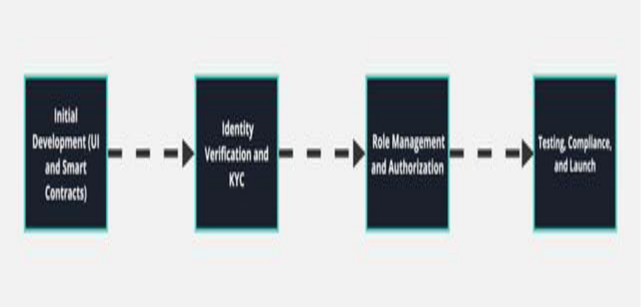
d. Smart Contract Role Management: Role-based access control is enforced via smart contracts. These contracts define who can upload, view, or share documents. For example, only judges might have the right to access all documents, while lawyers may only see the ones relevant to their case.

e. Permission Levels: There are different levels of permissions based on user roles. Judges might have full access (upload, download, share), lawyers might have limited access (download, share within a case), and third parties might only have read-only access.

f. Enforcement: Any action a user tries to perform, such as uploading, downloading, or sharing a document, is verified by the smart contract to ensure they have the required permissions. Unauthorized attempts are blocked.

Document Retrieval:

- Document Listing: Users can request to see all the documents they are authorized to access. The backend, after validating the user's authorization token, queries the blockchain for the list of document hashes and metadata.
- Frontend Display: The frontend receives this data and displays it to the user in a comprehensible format, allowing them to select and manage their documents.


Initial Development (UI and Smart Contracts)
Identity Verification and KYC
Role Management and Authorization
Testing, Compliance, and Launch

Court Proceedings:

a. Access for Legal Professionals: Judges, lawyers, and other authorized legal professionals can access documents relevant to their cases. They do so through the same frontend system that other users access, with their roles determining their access rights.

b. Blockchain Transparency: The blockchain logs all interactions with the documents, ensuring that every upload, download, and share is tracked. This helps provide transparency and accountability during court proceedings.

c. Efficient Case Management: The system allows for streamlined case management by providing fast and secure access to documents, reducing delays often associated with physical or insecure digital records.

Dispute Resolution

a. Document History: In case of a dispute over document ownership, authenticity, or access, the blockchain acts as an immutable record of all document-related transactions. This includes when the document was uploaded, who shared it, and who accessed it.

b. Verification of Ownership: Smart contracts manage ownership and permissions, which can be used to resolve any disputes regarding who originally uploaded the document or who was given access to it.

c. Transparent Audit Trail: Any actions involving a document (such as uploading, sharing, or downloading) are logged on the blockchain, allowing both parties and external auditors to review the transaction history and resolve conflicts.

Third-Party Integration:

a. API Integration: The system provides APIs for third-party services like legal databases, government entities, or external KYC providers. These external services can request access to specific documents, but only if they meet the system's security and role-based access criteria.
b. Smart Contract-Based Authorization: Smart contracts manage API permissions, ensuring that third-party services only gain access to documents after verifying the user's consent and role-based authorization
c. KYC as Service: Third-party KYC services are integrated to verify the identities of users without exposing sensitive data. This allows for seamless document verification and sharing, while maintaining user privacy and security.

V. RESULT AND DISCUSSION

The project introduces a robust and secure platform tailored for legal professionals, encompassing clients, lawyers, and judges, with a focus on streamlining interactions and managing legal processes. The innovative integration of blockchain technology for file storage elevates the system's capabilities by ensuring the integrity and immutability of critical legal documents and data. This blockchain-backed infrastructure safeguards against unauthorized alterations or tampering, offering a tamper-proof repository for legal records. The user-friendly web application enhances the overall user experience, promoting efficient communication and seamless information retrieval. Through a well-designed backend API, the system facilitates smooth interactions, realtime updates, and collaboration among legal professionals, enhancing the platform's scalability and adaptability. With an emphasis on data security, transparency, and reliability, this comprehensive solution stands as a promising advancement for the legal industry, facilitating the administration of legal cases and services while ensuring a trustworthy and efficient workflow for all stakeholders.

VI. CONCLUSION

Implementing an eVault for legal records using blockchain technology offers numerous advantages. Blockchain's decentralized and immutable ledger ensures the integrity of records, safeguarding them against tampering or unauthorized access. The cryptographic techniques employed by blockchain enhance security, maintaining the confidentiality of sensitive legal data. Transparency and traceability are inherent features, providing all stakeholders with the ability to verify the authenticity of records and track their history. By digitizing record-keeping processes and automating tasks through smart contracts, organizations can realize efficiency gains, reduce administrative overheads, and streamline operations. Furthermore, blockchain-based eVaults facilitate compliance with regulatory requirements by offering a secure and auditable solution for record management. The global accessibility of blockchain enables seamless access to legal records from anywhere, promoting collaboration and efficiency across geographically dispersed teams. While the benefits are promising, successful implementation necessitates careful consideration of factors such as regulatory compliance, data privacy, and interoperability. Nonetheless, the potential of blockchain based eVaults to revolutionize legal record management is significant, offering a robust and future-proof solution for organizations seeking to modernize their processes

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.

INTERNATIONAL JOURNAL OF
MULTIDISCIPLINARY RESEARCH
IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com