*Journal of Harbin Engineering University*
*ISSN: 1006-7043*

Vol 46 No. 6
June 2025

# Developing A Blockchain-Based eVault For Legal Records

**Ms. Shalaka Bibikar[1], Dr. Aparna Hambarde[2]**

Research Scholar[1], Computer Department, K J College of Engineering and Management Research

Professor[2] Computer Department, K J College of Engineering and Management Research

**Abstract**

The research introduces a Blockchain-Based eVault for Legal Records (BEvLR), designed to address the shortcomings of traditional legal record management systems. The InterPlanetary File System (IPFS) and blockchain technology are integrated by the BEvLR to guarantee the secure, transparent, and immutable storage of legal documents. Documents are safeguarded from tampering, unauthorised access, and alterations by utilising the decentralised ledger of the blockchain. In order to guarantee that only authorised personnel, including lawyers, clients, and judges, have the ability to access or modify the documents, the system implements role-based access control (RBAC). Furthermore, the incorporation of an audit trail improves accountability and transparency by monitoring document interactions. The research demonstrates how this system improves the security, integrity, and scalability of legal document management, providing a foundation for future advancements like smart contract integration to automate legal processes.

***Keywords:*** Blockchain Technology, Legal Records, eVault, Data Security, InterPlanetary File System (IPFS).**I.**

**INTRODUCTION**

The management and storage of legal records are critical components of the legal system, as they maintain the integrity and authenticity of sensitive documents[1]. Traditional methods of storing these records, such as physical archives and centralized databases, often expose legal data to security risks, unauthorized access, and potential alterations[2]. A more sophisticated, tamper-proof solution is urgently required due to the growing demand for secure and efficient legal document management.[3].

The decentralised and immutable character of blockchain technology offers a transformative solution for the secure storage and management of documents [4]. It guarantees that a document cannot be altered or tampered with after it is published by utilising the cryptographic features of blockchain technology, thereby providing verifiable proof of authenticity [5]. The storage capabilities are improved by the incorporation of InterPlanetary File System (IPFS), which provides simple retrieval and decentralised and secure file storage[6].

This research suggests the creation of a Blockchain-Based eVault for Legal Records (BEvLR), a system that is designed to resolve the current deficiencies in legal document administration [7]. The system

employs role-based access control to guarantee that only authorised users, including attorneys, clients, and judges, have the ability to access or modify the records [8]. Additionally, all document interactions are tracked in a verifiable audit trail, enhancing transparency and accountability [9]. The system is designed to serve as a foundation for future advancements, including the integration of smart contracts to automate legal processes and improve scalability [10]. The BEvLR system will not only improve the security and integrity of legal records but also provide the necessary infrastructure for future advancements in legal technology, such as smart contracts for automating legal processes. Additionally, the research explores how the system's scalability could support the growing demands of the legal industry, ensuring that it can evolve with emerging needs [11].

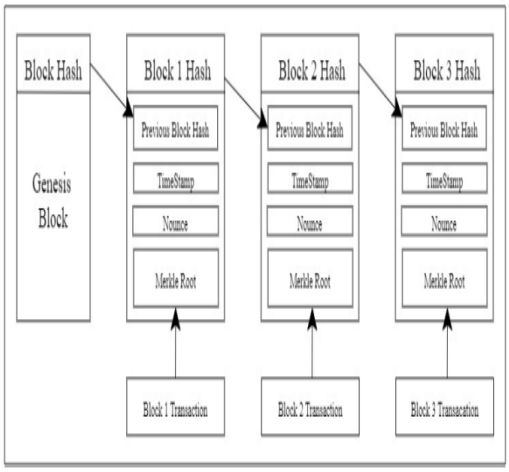


**Fig 1. Blockchain Proposal [12]**

The emergence of blockchain technology has created new opportunities for digital record-keeping and safe data management, particularly for sectors like the legal industry where data integrity and authenticity are critical [13]. Blockchain is a distributed and decentralized ledger system that stores data on many computers, guaranteeing that it is visible, safe, and unchangeable [14]. since of these characteristics, it is the perfect technology for handling private legal documents since it removes the possibility of illegal data changes and offers an auditable record for each transaction [15].

This paper aims to contribute to the ongoing exploration of blockchain applications in legal services, proposing a secure, efficient, and innovative solution for managing legal records [16]. The Blockchain-Based eVault for Legal Records (BEvLR) will address critical issues that traditional legal document management systems face, particularly concerning security, transparency, and data integrity. With blockchain's decentralized ledger technology, once a document is uploaded to the system, its data becomes immutable, ensuring that the document cannot be tampered with, altered, or deleted without leaving an indisputable trace. This guarantees that all legal records remain authentic and reliable.

The integration of IPFS (InterPlanetary File System) further enhances the system's functionality by providing a decentralized, distributed storage system. This allows legal documents to be stored securely while ensuring that they can be retrieved efficiently. IPFS's decentralized nature ensures that files are not stored in a single, centralized server, reducing the risk of data loss or unauthorized access due to server failures or hacking attempts.

**II RELATED WORK**

**Pallavi R et al. (2023)** discussed the implementation of blockchain for legal record management, highlighting how blockchain's decentralized and immutable features can prevent tampering and ensure data integrity. They explain that traditional legal record systems are prone to inefficiencies and security issues, which blockchain addresses by offering secure and transparent transactions. Additionally, they emphasize the potential of smart contracts to automate legal processes, enhancing efficiency and accuracy in record management. The study demonstrates blockchain's ability to improve trust and transparency in legal systems, making it a promising solution for the future of legal record-keeping[17].

**Kakarlapudi, P.V., and Mahmoud, Q.H. (2021)** discussed the development of a blockchain-based system for private data management in their study. They highlight the importance of blockchain's decentralized and immutable nature in ensuring the privacy and security of user data, particularly in sectors like healthcare and data management. The authors present a proof-of-concept prototype developed using Hyperledger Fabric, a permissioned blockchain platform, to enhance data privacy and consent management. Their system ensures that sensitive data is protected from unauthorized access and exploitation while maintaining transparency to build user confidence[18].

**Swetha R et al. (2024)** discussed the development of a blockchain-based eVault for legal records, addressing challenges in legal document management. They highlight how blockchain technology's decentralized structure and immutable ledger ensure data integrity, authenticity, and accessibility, offering a secure solution for storing and managing legal documents. The authors emphasize the use of smart contracts and cryptographic techniques to automate verification, access control, and

auditing, enhancing security and streamlining operations. The system also ensures compliance with legal standards and provides a transparent, auditable record of all interactions, fostering trust and accountability among stakeholders[19].

**Yeshwantrao, S.A., Satpute et.al (2024)** proposed an innovative solution for managing legal records through blockchain technology in their work on eVault. The authors emphasize how blockchain's decentralized architecture and immutability overcome traditional challenges in legal record management, such as data tampering and fragmented access. The system they introduce ensures secure, tamper-proof storage for legal documents like contracts and court records, providing confidentiality through encryption. They argue that by combining blockchain's transparency with user-friendly interfaces, the eVault can greatly enhance the management and accessibility of legal records, fostering trust and security in legal processes[20]**.**

**Pratima Sharma et.al (2020)** proposed cloud technology gained popularity in recent years because of its efficiency and availability, which have shown promise in both academics and business. Despite being a widely used technology, the explosion of data sources has led to a rise in storage and use issues since traditional data management tools are unable to handle the rapidly expanding data. In the original cloud storage notion, The network may be the internet or an intranet, the front end platform can be a client or mobile device, and the back end platform can be a server or data storage[21].

**Naveen Kumar et.al (2020)** proposed the two main issues that users of e-health systems worry about are security and privacy of personal health information. Unauthorised users, including third-parties, should not be able to connect the owners of outsourced e-health records to them for privacy concerns. In order to achieve unobservable outsourced data access as well as data integrity, this paper suggests a symmetric, key-based strategy which uses multiple networks and blockchain. Blockchains enable forward secrecy, a crucial security need that prevents a medical health care professional from seeing any future health documents after her session ends[22].

**Mahalakshmi, B. et.al (2024)** proposed a blockchain-based eVault system for managing legal records in their study. They discuss how blockchain technology ensures the security, transparency, and immutability of legal documents by leveraging decentralization and cryptographic protocols. The system includes functionalities for user registration, document upload, and judge review, with all actions securely recorded on the blockchain. By integrating Interplanetary File System (IPFS) for document storage, the eVault ensures end-to-end encryption and tamper-proof data storage. Their work highlights the potential of blockchain to provide reliable, transparent, and efficient solutions for legal document management, while fostering trust in the legal system through immutable records of judgments and metadata[23].

**Jadhav, V., Jadhav et.al (2025),** presented SecureChain, a blockchain-based e-vault system for legal records. They propose a solution that addresses the limitations of traditional legal record-keeping systems, such as tampering, lack of transparency, and inefficient workflows. By using Ethereum smart contracts and IPFS, SecureChain ensures the tamper-proof storage and secure management of case records. The authors also discuss the integration of Aadhaar-based authentication and MetaMask for identity verification, along with role-based access control for lawyers, judges, and clients. Their system automates judge allocation through verifiable random functions (VRFs) and tracks case progress in real-time, providing transparent access to public case metadata[24].

**Dinde, S., and Shirgave, S. (2024**) discussed a decentralized legal document storage and access framework using blockchain technology in their paper. They emphasize the challenges faced by the legal sector due to traditional centralized systems that expose legal documents to risks like unauthorized access and tampering. Blockchain provides a solution through its decentralized ledger, ensuring data integrity and security. The authors propose using a permissioned blockchain to manage document metadata while storing actual documents off-chain for efficiency. They

also implement a Role-Based Access and Security model (RBAS) to ensure that only authorized personnel can access sensitive legal documents[25].

**III METHODOLOGY**

This study proposes a Blockchain-Based eVault for Legal Records (BEvLR) system to enhance the security and integrity of legal document management[26]. The methodology integrates blockchain technology and the InterPlanetary File System (IPFS) with role-based access control (RBAC) to ensure secure, transparent, and immutable storage of legal documents. The approach is validated through a systematic process that ensures robustness and efficiency.

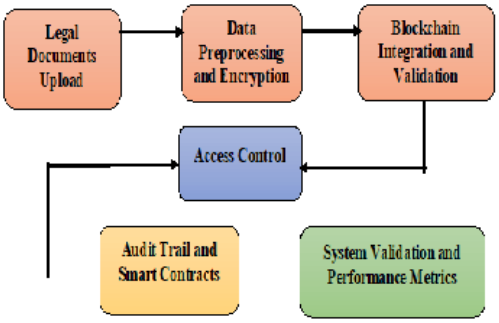


**Fig. 2. The Flow Diagram of the Proposed Work**

The process involves multiple stages:

***Legal Documents Upload:*** Legal documents are initially selected for upload into the BEvLR system. The documents are securely uploaded using IPFS to ensure decentralized storage.

***Data Preprocessing and Encryption:*** Preprocessing operations, such as data encryption and file verification, are carried out to guarantee that the documents are securely stored and ready for blockchain integration. This step ensures that no unauthorized access or modification is possible[27].

***Blockchain Integration and Validation:*** Once uploaded, documents are associated with a unique IPFS hash, and the transaction is recorded on the blockchain. This ensures that any interaction with the document, such as access or modifications, is transparent and traceable. Blockchain's decentralized ledger ensures that document integrity is maintained[28].

***Access Control:*** Role-based access control (RBAC) ensures that only authorized users (lawyers, clients, judges) can access or modify documents. The system verifies user credentials through secure authentication processes, providing differentiated access based on the role of the user[29].

***Audit Trail and Smart Contracts:*** An audit trail is automatically created for every interaction with the document, enhancing transparency and accountability. The system's potential integration with smart contracts is explored to automate document processing and legal workflows, improving operational efficiency[30].

***System Validation and Performance Metrics:*** The system is validated through simulated use cases and feedback from stakeholders. Metrics such as security, transparency, and data retrieval efficiency are measured to assess the system's effectiveness. The system's scalability is also tested to ensure it can handle increasing data volumes without compromising performance[31].

**Table 1. System Validation and Performance Metrics**

| Feature | Technique / Algorithm |
|---|---|
| File Deduplication | **SHA-256 hashing** |
| Decentralized File Storage | **IPFS via Pinata API** |
| Access Control | **Role-Based (RBAC)** |
| Session Persistence | **express-session** |
| IPFS Pinning + Content Hashing | **Pinata Content Hash Algorithm** |
| UI & Theme Styling | **CSS, Gradient, Flexbox Layout** |
| Upload Logic + Dynamic UI | **Vanilla JS + Fetch API** |
| Deduplication Record Store | **Local JSON file (hashes.json)** |

***Algorithm: Blockchain-Based eVault for Legal Records (BEvLR)***

***Start***

***Input:*** User selects a legal document to upload.

***Upload Document to IPFS:***

Upload the selected document to the InterPlanetary File System (IPFS).

Generate a unique IPFS hash for the document.

***Encrypt Document:***

Encrypt the document using AES encryption.

Hash the encrypted document using SHA-256.

***Store Metadata on Blockchain:***

Create metadata including the IPFS hash, timestamp, and user details.

Store this metadata on the blockchain to ensure immutability and traceability.

***Authenticate User:***

User logs in by providing credentials.

Validate credentials using JWT tokens and assign a role (lawyer, client, judge).

***Grant Access Based on Role:***

Based on the role (stored in JWT), grant access permissions (read, write, modify) to the document.

***Track Interactions (Audit Trail):***

Record all document interactions (view, modify, etc.) on the blockchain for accountability.

***Execute Smart Contracts (Optional):***

If needed, use smart contracts to automate document workflows (e.g., approval, review).

***End***

This algorithm encapsulates the core steps for securely managing legal documents, ensuring data integrity, and providing role-based access control.

**IV. RESULTS AND DISCUSSION**

This study explores the development and implementation of the Blockchain-Based eVault for Legal Records (BEvLR), a system designed to address the challenges faced by traditional legal record management methods. By integrating blockchain technology and the InterPlanetary File System (IPFS), this research investigates how these advanced technologies can enhance the security, integrity, and transparency of legal document storage and management. The study evaluates the effectiveness of the BEvLR system in safeguarding legal records and explores its potential for future advancements in the legal sector.

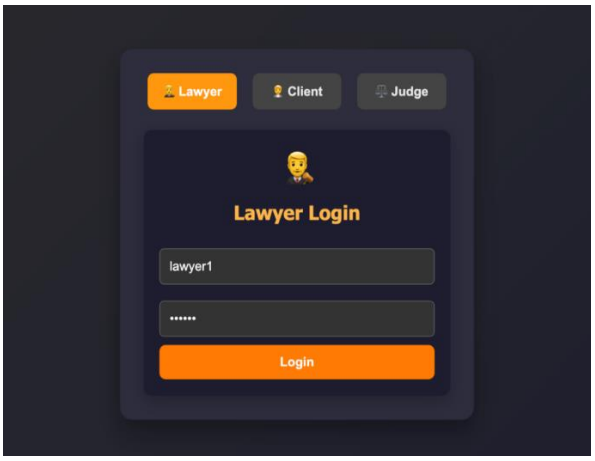


**Fig 3. Lawyer Login Interface**

The figure depicts the login screen of the Blockchain-Based eVault for Legal Records. It includes role-based logins for Lawyer, Client, and Judge users. The roles are icon-based, making it convenient for users to choose their role prior to login. The Lawyer Login area is live, in which the user (here "lawyer1") is invited to input the username and password. Once the credentials are input, the Login button can be pressed to gain entry into the system. The design is such that it is user-friendly, with a strong focus on role selection and safe authentication, so that each category of user enters only the applicable features of the legal document management system.

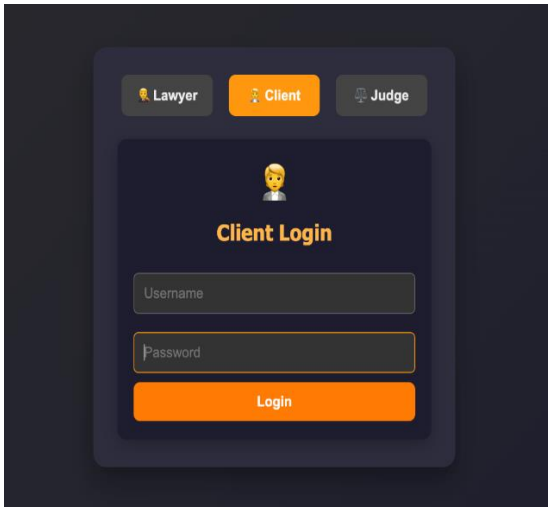


**Fig 4. Client Login Interface**

The figure shows the Client Login Interface for the Blockchain-Based eVault for Legal Records system. Similar to the lawyer login, the Client login section is highlighted, where users can log in by selecting the Client role. In the Client Login section, the user is prompted to enter their username and password. After entering the correct credentials, the Login button can be clicked to access the system. The interface is designed for easy navigation, ensuring that clients can securely access their relevant documents and features, while maintaining proper access control based on user roles.

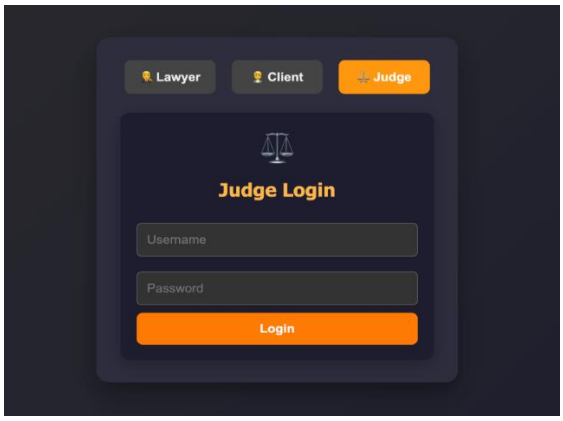


**Fig 5. Judge Login Interface**

The figure shows the Judge Login Interface for the Blockchain-Based eVault for Legal Records system. Similar to the Lawyer and Client login, the Judge Login section is highlighted, where users can log in by selecting the Judge role. In the Judge Login section, the user is prompted to enter their username and password. Once the correct credentials are provided, the Login button can be clicked to gain access to the system. This interface is designed for easy navigation and role-based access control, ensuring that judges can securely access the relevant legal documents and features within the system.

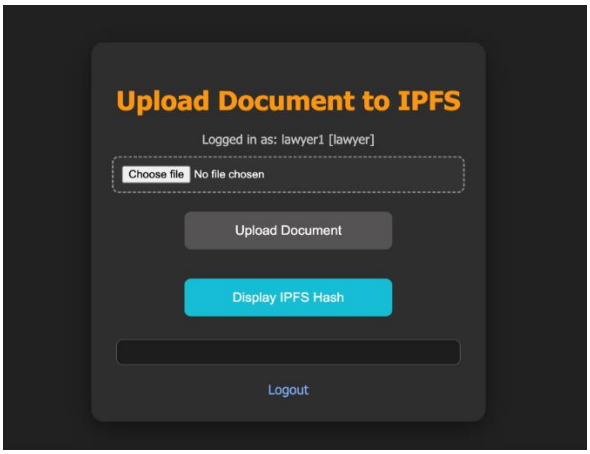


**Fig 6. Upload Document to IPFS Interface**

The figure shows the Upload Document to IPFS interface for the Blockchain-Based eVault for Legal Records system. This interface allows users to securely upload their legal documents to the IPFS network. To upload a document, users begin by clicking the "Choose File" button to select a file from their device. Once a document is selected, the user can click the Upload to IPFS button, which triggers the upload of the document to IPFS for secure storage. After the document is successfully uploaded, the user can click on the Display IPFS Hash button to view the unique IPFS hash that identifies the uploaded document on the decentralized network. Finally, there is a Logout button available, allowing users to safely exit the system after completing their task. This interface ensures a smooth and secure process for document storage and retrieval.

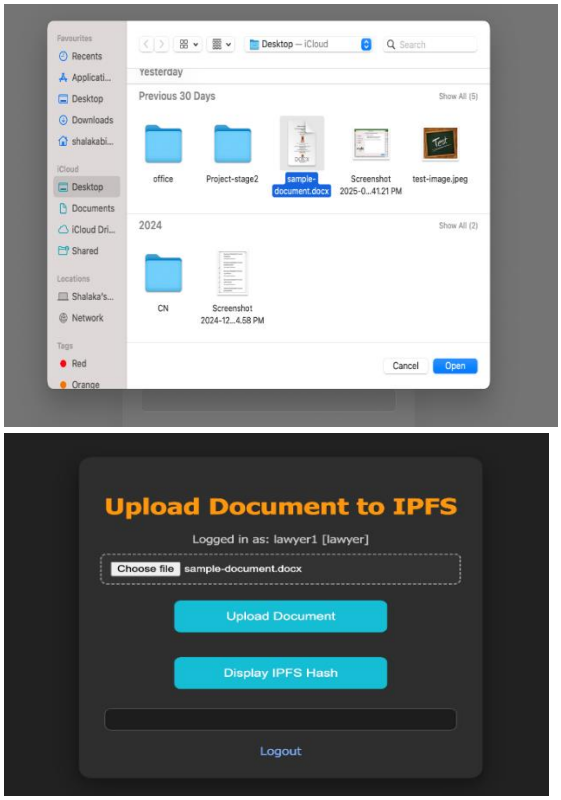


**Fig 7. Document Selection for Upload to IPFS**

This figure shows the document selection process in the Upload Document to IPFS interface of the Blockchain-Based eVault for Legal Records system. The user has clicked the "Choose File" button, and the file explorer window appears, allowing the user to browse their computer for the file they want to upload. In this case, the user has selected the "sample-document.docx" file for uploading. Once the file is selected, the user can proceed by clicking Open, which will upload the document to the IPFS network for secure storage. This step ensures that the correct document is chosen for upload and makes the file available for future retrieval using the IPFS hash.

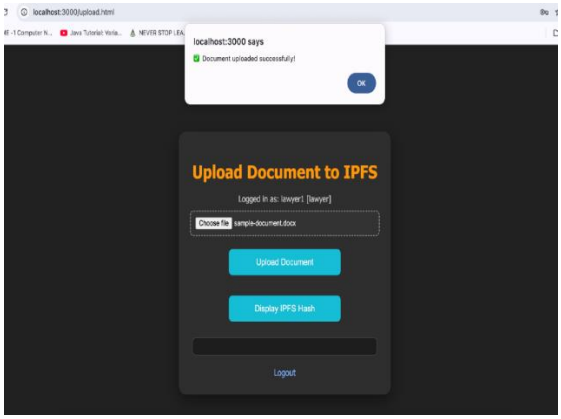


**Fig 8. Successful Document Upload to IPFS**

This figure represents the confirmation message displayed after a successful document upload to IPFS in the Blockchain-Based eVault for Legal Records system. The notification at the top of the screen shows the message "Document uploaded successfully!" confirming that the user's selected document, "sample-document.docx", has been successfully uploaded to IPFS. The user can now proceed to either Display IPFS Hash to view the unique identifier for the document or continue with other tasks. The interface also provides an option to Logout once the task is completed. This message assures the user that their document has been securely stored and can be retrieved later using its IPFS hash.

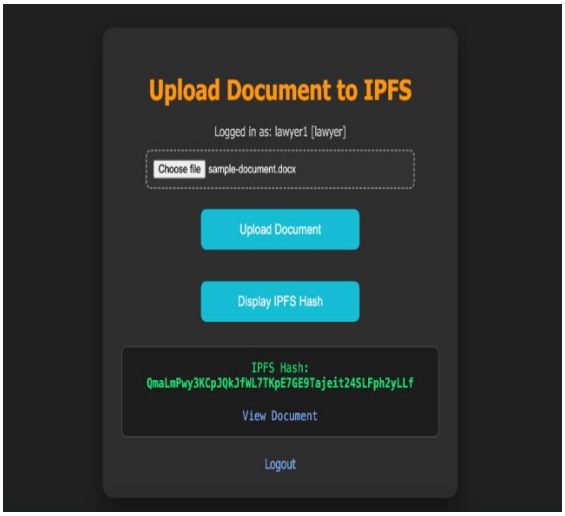


**Fig 9. Display IPFS Hash after Document Upload**

This figure shows the successful display of the IPFS hash after a document has been uploaded to the Blockchain-Based eVault for Legal Records system. After uploading the document, the system generates and displays the IPFS hash for the uploaded file, in this case, "QmaLmP..." which serves as a unique identifier for the document stored on IPFS. Additionally, the system provides a View Document option that allows the user to access the document using the generated IPFS link. This link ensures secure retrieval of the document in a decentralized manner. The Logout button is also available for the user to end their session once the task is complete. This interface ensures that the uploaded document can be easily accessed and tracked using its unique IPFS hash.

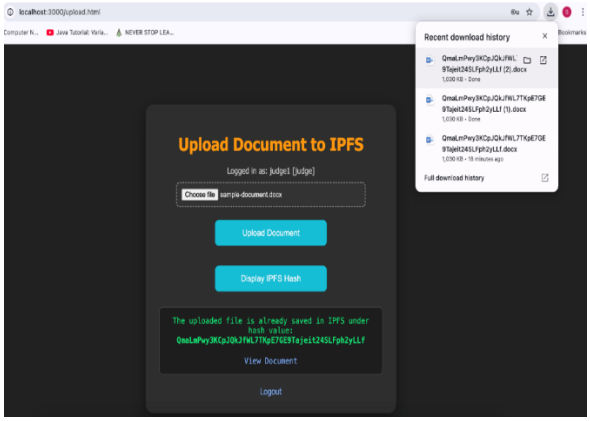


**Fig 10. Document Upload with IPFS Hash Display**

This figure illustrates the successful upload of a document to IPFS within the Blockchain-Based eVault for Legal Records system. After the user has selected and uploaded the document, the IPFS hash is displayed on the interface, confirming that the document has been stored securely. The IPFS hash in this case is: "QmaLmP...". This hash serves as a unique identifier for the uploaded document on the IPFS network. Additionally, the interface includes a View Document button that allows users to retrieve the uploaded document using its IPFS hash. The Logout option is also available for the user to end their session once they are finished.

## V. CONCLUSION

The Blockchain-Based eVault for Legal Records (BEvLR) offers a transformative solution for the secure and efficient management of legal documents. By combining blockchain technology with IPFS, the system ensures data immutability, transparency, and secure storage, addressing the vulnerabilities present in traditional legal record-keeping systems. Role-based access control and an audit trail enhance security and accountability, providing a clear and verifiable history of document interactions. The BEvLR system's scalability allows it to handle increasing volumes of data, making it a future-proof solution for the legal industry. This research shows that blockchain technology can effectively revolutionize legal document management, improving both security and operational efficiency, while setting the stage for future innovations like automated legal processes via smart contracts.

## REFERENCES

[1] 'Modernizing Contracts Across Idustries: A Review of Smart Contract Applications and the Evolving Legal Landscape', 2024.

[2] K. Pradeep Kumar, B. R. Prathap, M. M. Thiruthuvanathan, H. Murthy, and V. Jha Pillai, 'Secure approach to sharing digitized medical data in a cloud environment', *Data Science and Management*, vol. 7, no. 2, pp. 108–118, 2024, doi: 10.1016/j.dsm.2023.12.001.

[3] V. Potdar, 'Forensic Evidences made Tamper-Proof using Block Chain', *International Journal for Research in Applied Science and Engineering Technology*, vol. 11, no. 7, pp. 358–368, 2023, doi: 10.22214/ijraset.2023.54572.

[4] U. Ajuzieogu, 'Exploring Synergies and Transformative Potential of Blockchain at the Convergence of Emerging Technologies', no. December, 2024, doi: 10.13140/RG.2.2.21842.47044.

[5] M. K. Mohammed, A. A. Abdullah, and Z. A. Abod, 'Securing medical records based on inter-planetary file system and blockchain', *Periodicals of Engineering and Natural Sciences*, vol. 10, no. 2, pp. 346–357, 2022, doi: 10.21533/pen.v10i2.2855.

[6] M. Bin Saif, S. Migliorini, and F. Spoto, 'Efficient and Secure Distributed Data Storage and Retrieval Using Interplanetary File System and Blockchain', *Future Internet*, vol. 16, no. 3, 2024, doi: 10.3390/fi16030098.

[7] S. Anas, S. Anuragav, R. Abhishek, and K. Sachin, 'Evault for legal records', *arXiv (Cornell University)*, 2024.

[8] M. Uddin, S. Islam, and A. Al-Nemrat, 'A Dynamic Access Control Model Using Authorising Workflow and Task-Role-Based Access Control', *IEEE Access*, vol. 7, pp. 166676–166689, 2019, doi: 10.1109/ACCESS.2019.2947377.

[9] Thaier, 'Blockchain and Smart Contracts', *Transforming Climate FinanModernizing Contracts Across Industries: A Review of Smart Contract Applications and the Evolving Legal Landscapece and Green Investment with Blockchains*, no. April, pp. 303–317, 2023, doi: 10.1016/b978-0-12-814447-3.00022-7.

[10] Thaier, 'Modernizing Contracts Across Industries: A Review of Smart Contract Applications and the Evolving Legal Landscape', 2023.

[11] J. Goldenfein and A. Leiter, 'Legal Engineering on the Blockchain: "Smart Contracts" as Legal Conduct', *Law and Critique*, vol. 29, no. 2, pp. 141–149, 2018, doi: 10.1007/s10978-018-9224-0.

[12] 'Evault in blockchain to store and manage legal records', *IJPREMS*, Apr. 2024, doi: 10.58257/IJPREMS33256.

[13] R. Ghazali *et al.*, 'Blockchain for record-keeping and data verifying: proof of concept', *Multimedia Tools and Applications*, vol. 81, no. 25, pp. 36587–36605, 2022, doi: 10.1007/s11042-021-11336-7.

[14] K. L. Karst, 'The Freedom of Intimate Association', *The Yale Law Journal*, vol. 89, no. 4, p. 624, 1980, doi: 10.2307/795978.

[15] P. N. Bloom, G. R. Milne, and R. Adler, 'Avoiding Misuse of New Information Technologies: Legal and Societal Considerations', *Journal of Marketing*, vol. 58, no. 1, p. 98, 1994, doi: 10.2307/1252254.

[16] N. Upadhyay, 'Demystifying blockchain: A critical analysis of challenges, applications and opportunities', *International Journal of Information Management*, vol. 54, no. March 2019, p. 102120, 2020, doi: 10.1016/j.ijinfomgt.2020.102120.

[17] Deepak *et al.*, 'Exploring the Potential of Blockchain Technology in an IoT-Enabled Environment: A Review', *IEEE Access*, vol. 12, pp. 31197–31227, 2024, doi: 10.1109/ACCESS.2024.3366656.

[18] P. V. Kakarlapudi and Q. H. Mahmoud, 'Design and Development of a Blockchain-Based System for Private Data Management', *Electronics*, vol. 10, no. 24, p. 3131, Dec. 2021, doi: 10.3390/electronics10243131.

[19] M. V. Rajesh, V. Navya, R. Konjarla, and M. Birada, 'Blockchain-based e-vault for Legal Records', in *2024 3rd International Conference on Applied Artificial Intelligence and Computing (ICAAIC)*, Salem, India: IEEE, Jun. 2024, pp. 1389–1392. doi: 10.1109/ICAAIC60222.2024.10574924.

[20] S. S. Samant *et al.*, 'The Ocean's Treasure Trove: Bioactive Compounds from Sea Sponges', *Pharmacogn. Res.*, vol. 17, no. 2, pp. 452–461, Apr. 2025, doi: 10.5530/pres.20252085.

[21] P. Sharma, N. R. Moparthi, S. Namasudra, V. Shanmuganathan, and C. Hsu, 'Blockchain-based IoT architecture to secure healthcare system using identity-based encryption', *Expert Systems*, vol. 39, no. 10, p. e12915, Dec. 2022, doi: 10.1111/exsy.12915.

[22] Rituraj and N. Kumar, 'Cloud-based Secure Personal Health Record Management System using Mixnode and Blockchain', in *2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4)*, London, United Kingdom: IEEE, Jul. 2020, pp. 70–75. doi: 10.1109/WorldS450073.2020.9210317.

[23] Department of Paediatric Nursing, Nootan College of Nursing, Sankalchand Patel University, Visnagar, Gujarat - 384315, India and B. Mahalakshmi, 'Effect of aerobic exercise on anthropometric parameters among Indian primary school children', *Bioinformation*, vol. 20, no. 2, pp. 170–174, Feb. 2024, doi: 10.6026/973206300200170.

[24] N. Jadhav and D. J. Londhe, 'Policy support for the promotion of millets: Current status and its impact', *Journal of Drug Research in Ayurvedic Sciences*, vol. 8, no. Suppl 1, pp. S148–S151, Nov. 2023, doi: 10.4103/jdras.jdras_181_23.

[25] S. H. Dinde and S. K. Shirgave, 'Secure Authentication of IoT Devices Using Upgradable Smart Contract and Fog-Blockchain Technology', in *Data Management, Analytics and Innovation*, vol. 662, N. Sharma, A. Goje, A. Chakrabarti, and A. M. Bruckstein, Eds., in Lecture Notes in Networks and Systems, vol. 662. , Singapore: Springer Nature Singapore, 2023, pp. 863–878. doi: 10.1007/978-981-99-1414-2_60.

[26] J. N, A. S, A. S, A. R, and S. K, 'Evault for legal records', 2024, *arXiv*. doi: 10.48550/ARXIV.2403.01186.

[27] H. R. Penubadi *et al.*, 'Sustainable electronic document security: a comprehensive framework integrating encryption, digital signature and watermarking algorithms', *Heritage and Sustainable Development*, vol. 5, no. 2, pp. 391–404, Dec. 2023, doi: 10.37868/hsd.v5i2.359.

[28] N. Nizamuddin, K. Salah, M. Ajmal Azad, J. Arshad, and M. H. Rehman, 'Decentralized document version control using ethereum blockchain and IPFS', *Computers & Electrical Engineering*, vol. 76, pp. 183–197, Jun. 2019, doi: 10.1016/j.compeleceng.2019.03.014.

[29] K. Ren, W. Lou, K. Kim, and R. Deng, 'A Novel Privacy Preserving Authentication and Access Control Scheme for Pervasive Computing Environments', *IEEE Trans. Veh. Technol.*, vol. 55, no. 4, pp. 1373–1384, Jul. 2006, doi: 10.1109/TVT.2006.877704.

[30] X. Ye, N. Zeng, X. Tao, D. Han, and M. König, 'Smart Contract Generation and Visualization for Construction Business Process Collaboration and Automation: Upgraded Workflow Engine', *J. Comput. Civ. Eng.*, vol. 38, no. 6, p. 04024030, Nov. 2024, doi: 10.1061/JCCEE5.CPENG-5938.

[31] P. Jogalekar and M. Woodside, 'Evaluating the scalability of distributed systems', *IEEE Trans. Parallel Distrib. Syst.*, vol. 11, no. 6, pp. 589–603, Jun. 2000, doi: 10.1109/71.862209.