International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 05 | May - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Tampering Detection in Judiciary Using Blockchain

Mahesh Mulay[1], Suvarna Potdukhe[2], Apeksha Deshmukh[3], Ekant Nakhate[4] ,Ashlesha Sitaphale

Department of Information Technology, RMD Sinhgad School Of Engineering, Pune, India

---

Abstract : Evidence tampering is a major issue in the Indian Judiciary. Digital evidence is tampered very often and tampering detection becomes a major trouble and takes a lot of time. In the current E-Judiciary system the documents are stored in centralized servers that are accessible to the public. Though the system is secure, being centralized makes it prone to cyber attacks. In this paper we are going to discuss a way of detecting the tampering of evidence by integrating the Blockchain technology and decentralized servers for early detection and elimination of this to an extent.

Key Words: *Blockchain, E-Judiciary, Decentralization, Interplanetary File System(IPFS), Solidity Contracts.*

1.INTRODUCTION

Maintaining the integrity of judicial records has become crucial in a time when legal documents are becoming more digital and centralized systems are susceptible to manipulation and illegal access. There has never been a greater need for an open and safe document verification system. By decentralizing the storage and verification of legal documents, a blockchain-based document tampering detection system offers a revolutionary solution to this problem.

The blockchain-based strategy gives people authority over document verification while using cryptographic techniques to protect sensitive data. The technology guarantees openness, builds trust, and offers a dependable remedy for the increasing threats of document fraud and tampering in the legal field by utilizing decentralized networks and smart contracts. The fundamental ideas and benefits of blockchain technology in document verification are described in this introduction, which also highlights how it has the potential to completely transform the effectiveness and security of legal institutions.

2. Body of Paper

I. Fundamentals of the Concept:

- Blockchain Technology: Blockchain is a decentralized, distributed ledger technology that records transactions securely and transparently. It operates on a peer-to-peer network, where every transaction is verified and stored in a block, which is then linked to the previous block using cryptographic hashing, forming an immutable chain. The key features of blockchain include decentralization, transparency, and security, making it highly suitable for judicial document verification. By leveraging blockchain, judicial records can be protected from unauthorized alterations, ensuring the integrity of legal evidence.
- E-Judiciary: E-Judiciary refers to the digital transformation of the judiciary system, where traditional paper-based legal processes are replaced with electronic case management, digital evidence handling, and virtual court proceedings. The goal of E-Judiciary is to enhance efficiency, accessibility, and transparency in legal systems. However, the increasing reliance on digital documents raises concerns regarding data security and authenticity. Blockchain technology, when integrated with E-Judiciary, provides a robust solution by ensuring that legal documents remain tamper-proof and easily verifiable.
- Decentralization: Decentralization is a key principle of blockchain technology, where data is stored across multiple nodes rather than a central authority. In traditional centralized systems, judicial records are stored in databases that can be vulnerable to cyberattacks and unauthorized modifications. Decentralization distributes control, reducing the risk of a single point of failure and making the system more resilient to tampering. This approach enhances transparency and allows legal professionals, courts, and concerned authorities to access and verify judicial records without dependency on a single entity.
- Interplanetary File System: IPFS is a peer-to-peer network protocol designed for decentralized file storage and sharing. Unlike traditional centralized storage systems, IPFS breaks files into smaller pieces, distributes them across the network, and assigns each file a unique cryptographic hash. When a file is retrieved, the system checks its hash to ensure data integrity. In the context of judicial document management, IPFS provides a secure method for storing evidence and legal documents, ensuring that files remain tamper-proof while being easily accessible to authorized users.
- Solidity Smart Contracts: Smart contracts are self-executing contracts written in Solidity, a programming language used for Ethereum-based blockchain applications. These contracts automatically enforce agreements and execute predefined conditions without requiring intermediaries. In judicial document verification, Solidity smart contracts can be used to authenticate legal records by ensuring that their cryptographic hashes match the stored hashes on the blockchain. If any discrepancies are found, the system can immediately flag potential tampering, enhancing security and trust in judicial proceedings.

II. Literature Review:

In the literature review, we have studied 5 research papers from renowned authors and the following is the summarization of our literature review.

1. Paper Title: A. Ranjan, A. N. Singh, A. Kumar, B. S. Prashanth and M. V. Manoj Kumar, "Transforming Judicial Systems with Blockchain: A Court Case Governance System for Tamper-Proof and Transparent Legal Processes," 2023 International Conference on Applied Intelligence and Sustainable Computing (ICAISC), Dharwad, India, 2023, pp. 1-7, doi: 10.1109/ICAISC58445.2023.10200234.
Summary: This paper explores the implementation of blockchain for enhancing judicial processes, focusing on ensuring tamper-proof governance and transparency. The study utilizes blockchain networks, peer-to-peer file sharing, and IPFS to improve the integrity of judicial records. However, it highlights that the proposed system is limited in its scope and does not fully cover the entire judiciary system. Furthermore, it is susceptible to biases due to the involvement of multiple stakeholders.

2. Paper Title: O. Salau and S. A. Adeshina, "Secure Document Verification System Using Blockchain," 2021 1st International Conference on Multidisciplinary Engineering and Applied Science (ICMEAS), Abuja, Nigeria, 2021, pp. 1-7, doi: 10.1109/ICMEAS52683.2021.9739812.
Summary: This research examines how blockchain can be leveraged to verify document authenticity. The study identifies key challenges in detecting forged documents, particularly when they are skillfully fabricated using advanced techniques. By integrating IPFS, hashing, and public key infrastructure (PKI), the system ensures tamper-proof document storage. However, the paper notes that the proposed system is contextually specific to Nigeria and lacks global applicability.

3. Paper Title: B. C. J, T. K. T, Y. Y and H. V, "Court Ledger-Decentralized and Tamper-Proof Solution for Storing Evidence," 2023 International Conference on Recent Advances in Electrical, Electronics, Ubiquitous Communication, and Computational Intelligence (RAEEUCCI), Chennai, India, 2023, pp. 1-8, doi: 10.1109/RAEEUCCI57140.2023.10134019.
Summary: This paper introduces a forensic blockchain application for securely storing legal evidence. The proposed system enhances transparency, security, and auditability through a private blockchain network and smart contract-based verification. However, the study acknowledges that its classification model could be further improved using AI and machine learning techniques to enhance accuracy and efficiency.

4. Paper Title: M. L. S. S, M. P. N and M. A. Shettar, "Block chain Based Framework for Document Verification," 2022 2nd International Conference on Artificial Intelligence and Signal Processing (AISP), Vijayawada, India, 2022, pp. 1-5, doi: 10.1109/AISP53593.2022.9760651.
Summary: The authors of this paper propose an Ethereum-based system for improving document immutability. Using Solidity smart contracts and SHA-256 hashing, the framework ensures that legal documents remain untampered. The study demonstrates increased security but notes that the proposed system is still not generalized for diversified use. Further enhancements in terms of scalability and additional features are suggested to make the system more robust.

5. Paper Title: M. Aldwairi, M. Badra and R. Borghol, "DocCert: Nostrification, Document Verification and Authenticity Blockchain Solution," 2023 Fifth International Conference on Blockchain Computing and Applications (BCCA), Kuwait, Kuwait, 2023, pp. 652-657, doi: 10.1109/BCCA58897.2023.10338908.
Summary: This study presents DocCert, a blockchain solution for nostrification and document authentication. The system assigns a digital certificate to documents and stores their signatures on the blockchain for verification. While the paper reports positive results in preventing unauthorized modifications, it acknowledges that the system has only been tested against common cyber threats and may still be vulnerable to targeted attacks.

Gaps in Existing Research

While these studies demonstrate promising applications, they each have limitations:

- Scalability Issues: Many proposed frameworks struggle to handle large volumes of legal documents efficiently.
- Contextual Limitations: Some models are tailored to specific jurisdictions, making them less applicable in a broader legal context.
- Security Concerns: Although blockchain is highly secure, vulnerabilities still exist, especially in smart contract execution and targeted attacks.
- Lack of Integration with Existing Systems: Many solutions do not provide seamless integration with traditional legal documentation processes.

This research seeks to integrate these methodologies to address existing gaps and develop a robust tampering detection system that is scalable, secure, and adaptable to various judicial frameworks.

III. Our Proposed Methodology:

Our proposed method involves utilizing blockchain technology to ensure the integrity and security of judicial documents. The process consists of the following steps:

- Document Hash Generation: When a judicial document is created, a cryptographic hash is generated using a secure hashing algorithm such as SHA-256. This hash acts as a unique digital fingerprint, ensuring that any modifications to the document will result in a completely different hash. This guarantees the authenticity of the document at the time of its creation.
- Blockchain Storage: Once the hash is generated, it is stored securely on a decentralized blockchain network. This ensures immutability, preventing unauthorized alterations. The decentralized nature of blockchain eliminates single points of failure, making it resistant to cyberattacks and fraudulent modifications. Each stored hash is time-stamped and linked to the previous block, forming a verifiable chain of evidence records.
- Document Verification: To verify a document, its cryptographic hash is recalculated and compared with the hash stored on the blockchain. If the newly computed hash matches the stored hash, it confirms that the document has remained unchanged since its original storage. This allows for easy and transparent verification of judicial documents without requiring access to the actual document itself.
- Tampering Detection: If a discrepancy is found between the newly computed hash and the stored hash, the system flags the document as potentially tampered. The framework provides real-time alerts, enabling judicial authorities to take immediate action against unauthorized modifications. By integrating blockchain with digital signatures and smart contracts, the system enhances security and automates the verification process.
- Integration into the Indian Judiciary: To effectively implement this framework in the Indian judiciary, integration with existing digital case management systems is essential. Legal documents can be hashed and stored on a public or permissioned blockchain network, allowing authorized personnel to verify their authenticity seamlessly. The use of IPFS for decentralized document storage can further enhance security and accessibility. Additionally, smart contracts can be utilized to automate evidence submission, verification, and retrieval processes, reducing manual intervention and minimizing the risk of errors or tampering.

IV. Future Scope:

The results affirm that blockchain has the potential to enhance document verification and security in judicial systems. The findings align with prior research, demonstrating that decentralization and cryptographic security significantly reduce tampering risks. However, the study also highlights implementation barriers, including technological limitations and institutional reluctance. Addressing these challenges requires strategic policy interventions, further research, and pilot projects to test real-world feasibility. Future studies should also explore AI integration to enhance the detection mechanisms in blockchain-based judiciary systems

3. CONCLUSION:

We observed that different methods of detection and elimination of document tampering have been made or proposed by different authors and programmers using Blockchain with different techniques. The methods have been tried and tested against different samples and the methods have proved themselves promising, but not totally effective. IPFS has been used in most of the cases and the results have been good but not totally effective. Every method has its own flaw. The authors are working in order to eliminate these flaws in the systems.Based on the survey we conclude that the integration of blockchain technology into the judicial system for document tampering detection offers a transformative approach to securing legal records. Traditional methods struggle with challenges in verifying the integrity and authenticity of legal documents thus by utilizing blockchain's immutable ledger and self-supervising capabilities, the system ensures traceability and real-time detection of unauthorized alterations in legal documents.In addition we are planning to work further on the studied methodologies by integrating them in order to eliminate each others' flaws and make a system that has most effective features to detect the document tampering using features like Blockchain, Ethereum Networks, Solidity Smart Contracts, IPFS and SHA-256 Algorithm. We look forward to executing and eliminating this tampering in the Judiciary with full effectiveness.

4.REFERENCES:

1. 1. A. Ranjan, A. N. Singh, A. Kumar, B. S. Prashanth and M. V. Manoj Kumar, "Transforming Judicial Systems with Blockchain: A Court Case Governance System for Tamper-Proof and Transparent Legal Processes," 2023 International Conference on Applied Intelligence and Sustainable Computing (ICAISC), Dharwad, India, 2023, pp. 1-7, doi: 10.1109/ICAISC58445.2023.10200234.
2. O. Salau and S. A. Adeshina, "Secure Document Verification System Using Blockchain," 2021 1st International Conference on Multidisciplinary Engineering and Applied Science (ICMEAS), Abuja, Nigeria, 2021, pp. 1-7, doi: 10.1109/ICMEAS52683.2021.9739812.
3. B. C. J, T. K. T, Y. Y and H. V, "Court Ledger-Decentralized and Tamper-Proof Solution for Storing Evidence," 2023 International Conference on Recent Advances in Electrical, Electronics, Ubiquitous Communication, and Computational Intelligence (RAEEUCCI), Chennai, India, 2023, pp. 1-8, doi: 10.1109/RAEEUCCI57140.2023.10134019.
4. M. L. S. S, M. P. N and M. A. Shettar, "Block chain Based Framework for Document Verification," 2022 2nd International Conference on Artificial Intelligence and Signal Processing (AISP), Vijayawada, India, 2022, pp. 1-5, doi: 10.1109/AISP53593.2022.9760651.
5. M. Aldwairi, M. Badra and R. Borghol, "DocCert: Nostrification, Document Verification and Authenticity Blockchain Solution," 2023 Fifth International Conference on Blockchain Computing and Applications (BCCA), Kuwait, Kuwait, 2023, pp. 652-657, doi: 10.1109/BCCA58897.2023.10338908.