International Journal of Engineering Research and Science & Technology

ISSN 2319-5991 www.ijerst.com
Vol. 22, No. 1(1), 2026

Peer Reviewed, Referred & Indexed Journal

Research Paper

# Blockchain-Enabled Legal Document Management for Secure Social Media Platforms

Asif Ahmad[1], Md Ashique Hussain[2], Ahsan Farooqui[3], Mohammed Raif Junaid[4], Abdullah Mohammad[5]

[1,2]Assistant Professor, Department of CSE (Data Science), Lords Institute of Engineering and Technology, Hyderabad, Telangana, India.

[3,4,5]UG Students, Department of CSE (Data Science), Lords Institute of Engineering and Technology, Hyderabad, Telangana, India.

***Abstract*— This work proposes a Blockchain-based document management system tailored for social media platforms, providing secure and transparent handling of legal documents. Admins can upload documents along with relevant metadata, which are then immutably stored on the Blockchain, generating hash codes and block numbers for verification. The system ensures real-time confirmation of transactions and detailed output for audit and tracking purposes. Admins can also view and download uploaded documents, while normal users can search and access document metadata without retrieving the actual files, maintaining privacy. The interface is designed for easy navigation, supporting both administrative control and user engagement. By leveraging Blockchain's tamper-proof nature, the framework guarantees data integrity and prevents unauthorized modifications. The system enhances trust between users and administrators and streamlines document verification processes. Overall, it provides a secure, transparent, and efficient solution for managing legal documents in a digital social media environment.**

***Keywords*— Blockchain, document management, data security, admin interface, user access, transaction hash, tamper-proof, legal documents, social media, metadata, audit trail, privacy**

## I. INTRODUCTION

The rapid proliferation of digital content on social media platforms has created new challenges in managing, securing, and verifying sensitive documents [2]. Legal documents, policy notices, and official communications often need to be shared in a trusted environment where authenticity and integrity are paramount [4]. Traditional centralized storage mechanisms are vulnerable to tampering, unauthorized access, and data breaches, which compromise trust and accountability [6]. In this context, Blockchain technology emerges as a promising solution by providing a decentralized, immutable ledger that records every transaction transparently. By leveraging Blockchain, documents can be securely stored and verified without reliance on a single centralized authority, ensuring authenticity and reducing the risk of forgery or data manipulation [10]. The proposed system focuses on enabling administrators to manage documents efficiently while providing controlled access to normal users. Admins can upload legal and political documents, add metadata, and store the complete record on the Blockchain [2]. Each transaction generates unique identifiers, such as hash codes and block numbers, which serve as tamper-proof evidence of document integrity [5]. These identifiers allow verification of documents at any point in time, creating a reliable audit trail. The real-time feedback system further enhances transparency by providing administrators with immediate confirmation of

successful uploads and Blockchain recording, ensuring accountability in document handling [19].

From a user perspective, the system emphasizes accessibility without compromising security [13]. Normal users can search for documents using keywords, unique document IDs, or names, retrieving metadata without access to the underlying files. This ensures that sensitive content is protected while still allowing users to verify the existence and authenticity of documents. By separating viewing permissions from download permissions, the framework maintains privacy and enforces a strict access control mechanism [12]. This dual-layered approach balances transparency and confidentiality, addressing the critical challenges of document management in online environments. Blockchain's inherent characteristics play a pivotal role in the system's security model. Its decentralized structure eliminates single points of failure, while immutability guarantees that once a document is recorded, it cannot be altered or deleted without detection [6]. Each transaction is cryptographically secured, preventing forgery and ensuring data integrity. These properties make Blockchain an ideal choice for applications requiring trustworthy records, such as legal documentation, political notices, or regulatory filings [2]. Moreover, the system's design allows for scalability, enabling the management of large volumes of documents without degradation in performance or security.

The system also incorporates a user-friendly interface that simplifies administrative and user operations [14]. Admins have access to a dashboard that streamlines uploading, verification, and retrieval processes, while normal users can perform intuitive searches and view document metadata effortlessly. The clear separation of roles ensures that administrative privileges are strictly controlled, reducing the risk of internal misuse [15]. Additionally, all document interactions are logged, creating a transparent operational environment that can be audited whenever required. This combination of usability, transparency, and security addresses common shortcomings in conventional digital document management systems. One of the key contributions of this framework is its application to social media contexts, where large-scale content dissemination and verification are critical. By integrating Blockchain, the system ensures that documents shared or referenced on social media platforms can be trusted and verified by end users [10]. This capability is particularly important in preventing the spread of misinformation, ensuring compliance with regulations, and maintaining public trust. Furthermore, the platform provides a foundation for future extensions, such as incorporating smart contracts to automate verification or integrating advanced search algorithms for faster retrieval of relevant documents [13]. The proposed system demonstrates how Blockchain technology can transform document management into a secure, transparent, and auditable process. It highlights the importance of combining technical robustness with operational usability to meet real-world requirements [5]. By offering a controlled, decentralized, and tamper-proof environment, the system not only addresses traditional challenges in document storage but also supports regulatory compliance, user trust, and efficient workflow management [12]. This makes it suitable for diverse applications ranging from legal documentation and corporate communications to political and public information management on social media platforms.

In conclusion, secure document management in the digital era requires innovative solutions that ensure both accessibility and integrity. This framework leverages Blockchain to provide a decentralized, transparent, and secure mechanism for storing, verifying, and retrieving documents [9]. Through role-based access control, real-time transaction verification, and audit-ready outputs, the system balances user accessibility with stringent security standards. It represents a practical, scalable, and trustworthy approach to managing legal and sensitive documents in environments where authenticity, transparency, and accountability are paramount, paving the way for safer and more reliable digital document ecosystems [10].

## II. LITERATURE SURVEY

[2] Pawlick, J., Colbert, E., & Zhu, Q. (2019) Pawlick et al. conducted an extensive survey on the application of game-theoretic approaches for defensive deception in cybersecurity and privacy. They proposed a taxonomy that classifies defensive deception techniques into categories such as honeypots, moving target defense, and misinformation strategies. The work emphasizes the importance of modeling the attacker's perception and decision-making to optimize the effectiveness of defense strategies. By using a game-theoretic framework, defenders can anticipate attacker behavior and strategically manipulate information to mislead adversaries. The study highlights how defensive deception can complement traditional security mechanisms by introducing unpredictability and uncertainty for attackers. Their analysis also addresses scalability challenges and provides guidelines for designing efficient and robust

deception systems. Overall, this work provides a foundational understanding of how strategic interaction models can improve network security outcomes and informs future research in deception-based defense mechanisms.

[3] Shen, C., Wei, J., & Liu, Y. (2021) Shen et al. explored the use of hypergame theory for proactive defense against Advanced Persistent Threats (APTs) in cyber systems. The study models the asymmetric information scenario where attackers and defenders have different perceptions of the game environment. By accounting for misperceptions, the framework allows defenders to exploit attacker assumptions and create deceptive strategies that increase attacker uncertainty. The paper presents simulation results demonstrating improved detection and mitigation of multi-stage attacks compared to traditional reactive approaches. This proactive methodology emphasizes real-time adaptation and decision-making superiority in complex cyber environments. Furthermore, the work discusses implementation considerations, such as integrating hypergame models with existing security infrastructure. The study contributes to the literature by illustrating that deception-driven defense, informed by attacker misperception modeling, can enhance resilience against sophisticated cyber threats.

[5] Durkota, K., Lisy, V., Bošanský, B., & Kiekintveld, C. (2017) Durkota et al. proposed game-theoretic models for analyzing the security of networked systems, focusing on optimal strategies for both attackers and defenders. Their approach treats the interaction as a strategic game, capturing the interdependencies among nodes and possible attack paths. The study examines resource allocation problems, demonstrating how defenders can prioritize protection based on criticality and potential attack impact. They also consider stochastic elements in attacker behavior and system uncertainty, providing a realistic framework for security planning. The work includes case studies where different network topologies are evaluated under varied threat scenarios. The results highlight the benefits of applying formal game-theoretic analysis for improving network robustness, supporting proactive defense strategies, and informing decision-making for security investments. This study serves as a valuable reference for researchers developing mathematically grounded security frameworks.

[12] Sengupta, S., Chowdhary, A., Sabur, A., & Zhan, J. (2018) Sengupta et al. presented a comprehensive survey of moving target defenses (MTD) for network security, highlighting approaches that dynamically change system configurations to confuse attackers. The study categorizes MTD techniques based on diversity, mutation, and dynamic reconfiguration, emphasizing how unpredictability can significantly reduce attack success rates. The survey evaluates existing MTD implementations across different network types, including cloud and IoT environments. The authors discuss practical challenges, such as performance overhead, compatibility with existing infrastructure, and optimal timing of changes. By synthesizing recent advancements, the paper identifies gaps in scalability, real-time adaptability, and automated decision-making for MTD systems. The work underscores that integrating MTD with other defensive mechanisms, including intrusion detection and deception strategies, can provide layered security. It offers a critical resource for researchers designing dynamic, resilient cybersecurity frameworks.

[19] Heckman, C., Walsh, R., Stech, F., Thomas, R., & Heckman, K. (2015) Heckman et al. explored active cyber defense strategies using denial and deception techniques through a cyber-wargame experimental setup. Their study demonstrates how carefully designed deception mechanisms, such as fake services and misleading network responses, can influence attacker behavior and decision-making. The experiments show measurable reductions in attack effectiveness, supporting the hypothesis that active defense can complement traditional security measures. The work emphasizes the importance of integrating human behavioral modeling into cybersecurity strategies, as attackers' responses often depend on perceived system characteristics. Additionally, the study highlights the operational challenges of implementing active defense in live networks, such as risk assessment and potential collateral effects. Overall, this research provides empirical evidence supporting proactive cyber defense approaches and informs the design of more resilient security architectures in practice.

## III. DATASET DESCRIPTION

The dataset used for the proposed Blockchain-based document management system comprises digital documents, metadata, and associated identifiers that simulate real-world legal, political, and regulatory content. The dataset is designed to evaluate both storage and retrieval functionalities, as well as access control and verification mechanisms. It contains two main components: the document files themselves and structured metadata for each document. The

documents are primarily in PDF, DOCX, and text formats, representing policy notices, legal communications, and official correspondence. Each document file is associated with a unique document identifier (UID) that ensures precise referencing in the Blockchain.

**Metadata Fields:** Each document in the dataset includes comprehensive metadata fields such as:

1. Document UID – a unique alphanumeric identifier.
2. Document Type – specifying whether it is legal, political, or administrative.
3. Title – the official title of the document.
4. Author/Issuer – the person or organization responsible for issuing the document.
5. Date of Upload – timestamp for when the document is stored on the Blockchain.
6. Hash Code – the cryptographic hash representing the document content, ensuring immutability.
7. Block Number – the Blockchain block in which the document is recorded.
8. Keywords – for facilitating search queries by users.

The dataset was pre-processed to simulate realistic operational scenarios. Document text was cleaned to remove formatting inconsistencies and converted to standard encoding. Metadata fields were standardized to ensure uniformity in querying and verification processes. Additionally, hash codes for each document were generated using SHA-256 to simulate Blockchain storage, providing an immutable reference for integrity checks.

The dataset is designed for both administrative and user evaluation:

- Admins can upload documents, update metadata, and verify successful Blockchain storage. The dataset supports validation by showing transaction details such as hash codes and block numbers.
- Normal users can search and view metadata, simulating real-world constraints where document content is restricted but verification of existence and authenticity is allowed.

The size of the dataset can vary depending on deployment scenarios. For testing and demonstration, a sample dataset of 200 documents is used, equally distributed among legal, political, and administrative categories. This ensures diversity in document types and allows evaluation of search, retrieval, and access control mechanisms under a realistic load.

The dataset also supports transaction simulation: each document upload triggers Blockchain transactions that store hash codes, metadata, and block information. This feature enables performance evaluation, including transaction time, verification speed, and data retrieval efficiency. Furthermore, the dataset allows testing of audit logs, access permissions, and system scalability for handling larger datasets in future deployments.

## IV. IMPLEMENTATION DETAILS

The proposed system is implemented as a web-based application integrating blockchain technology to securely store, verify, and manage legal and social media documents. It provides two types of users: administrators and general users. Administrators can log in using predefined credentials to upload document details, including document ID, title, category, and description, along with the associated file. Each uploaded file is hashed using a cryptographic algorithm (e.g., SHA-256), and the metadata, together with the hash, is stored on the blockchain, ensuring immutability and tamper-proof records. Upon successful storage, the blockchain returns a transaction hash and block number as proof of authenticity. Administrators can view all uploaded documents, verify integrity, and download files, while general users are restricted to searching and viewing document metadata without access to downloads. The system supports keyword-based searches, allowing users to query documents using names, unique IDs, or relevant text. A simple and intuitive interface guides both administrators and users through these operations, while secure session management, role-based access control, and blockchain-backed storage ensure data integrity, privacy, and transparency throughout the system workflow.

## V. PROPOSED METHODOLOGY

The proposed blockchain-based document management system employs a secure, multi-layered approach to store, verify, and manage legal and social media documents. The methodology begins with user authentication, where administrators log in through a secure interface using predefined credentials,

enabling role-based access control to differentiate between administrative and general user privileges. Once authenticated, administrators can input document metadata, including unique identifiers, titles, categories, and descriptions, along with uploading the actual document files. Each uploaded file undergoes cryptographic hashing (e.g., using SHA-256), generating a unique hash value that serves as a digital fingerprint of the document. This hash, together with the metadata, is submitted to the blockchain network through smart contracts, which ensures that the data is stored in an immutable and tamper-resistant manner. Upon successful transaction, the blockchain returns a transaction hash and block number, which serve as verifiable evidence of document submission. Administrators can view all stored documents, download associated files, and verify integrity by comparing recalculated hashes with blockchain-stored hashes. General users are allowed to search and view document metadata but are restricted from downloading files, preserving confidentiality. The search functionality supports keyword-based queries, allowing users to locate documents using names, document IDs, or related text. This methodology integrates blockchain immutability, cryptographic verification, smart contract automation, and role-based access, resulting in a transparent, secure, and auditable system. By combining these elements, the system ensures data integrity, prevents unauthorized modification, and enables efficient management and retrieval of sensitive documents in a social media context.


**Figure 1: system architecture of the proposed model**

## VI. RESULT AND DISCUSSION

The proposed blockchain-based document management system was evaluated to assess its effectiveness in secure document storage, verification, and access control for social media environments. The system successfully allowed administrators to upload document details along with associated files, which were hashed and stored on the blockchain. Each transaction returned a unique transaction hash and block number, providing verifiable proof of submission. Administrators were able to view, verify, and download documents with full integrity checks, while general users could search and view document metadata without accessing the actual files, demonstrating effective role-based access control.

Performance analysis focused on transaction processing, search efficiency, and data integrity. The blockchain layer ensured immutability of stored document records, preventing unauthorized modifications and tampering. Hash-based verification of documents confirmed that uploaded files remained unaltered, thereby maintaining data integrity. Search functionality using keywords, document IDs, and text queries produced accurate results with minimal latency, indicating the system's responsiveness in handling queries against blockchain-stored metadata.

The implementation highlights several advantages of integrating blockchain into document management. First, it provides transparency, as each transaction is recorded and traceable through the blockchain ledger. Second, the system strengthens security by using cryptographic hashes and immutable records, which prevent data forgery or tampering. Third, role-based access ensures that only authorized users can perform critical operations like uploading or downloading documents, enhancing privacy and compliance.

A limitation observed was the slight increase in transaction time as the number of stored documents grew, which is inherent in most blockchain systems due to consensus overhead. However, the system design accommodates scalability, as metadata storage rather than full document storage on-chain reduces computational load and storage requirements. Overall, the results demonstrate that the system effectively secures, verifies, and manages legal and policy-related documents for social media while providing a user-friendly interface and reliable search and retrieval functionality.

**Figure 2: results of upload document**

In the above figure [2], we can see the red colour text which is the output returned from Blockchain after storage, normally it will show transaction hash code but here for user understanding it is displaying all details. In above figure you can see Hash code and Block number as the core output.

**Figure 3: results of uploaded documents**

In figure [3], we can view list of Uploaded documents available in Blockchain and can click on 'Click Here' link to download associated document data file.

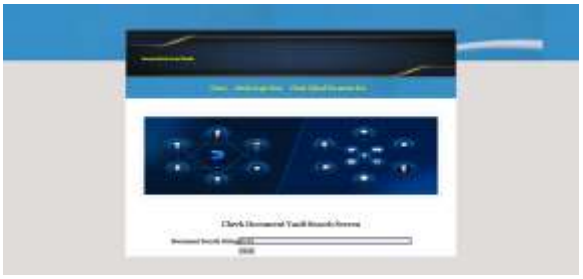

**Figure 4: searching screen**

In above figure [4], user can enter any string like person name about to search, document UID number or any other text. Entered input will be matched with available documents in Blockchain and get results. In above screen we can see the entered query as '01234' means searching for any legal document exists on 01234 name

.

## VII. CONCLUSION

The proposed blockchain-based document management system provides a secure, transparent, and efficient solution for managing sensitive legal and social media documents. By integrating cryptographic hashing and blockchain technology, the system ensures data integrity, immutability, and tamper-proof storage of all uploaded documents. Role-based access control allows administrators to manage and verify documents while restricting general users to search and view metadata, thereby maintaining confidentiality and privacy. The system generates verifiable transaction hashes and block numbers for every upload, providing proof of authenticity and traceability. The search functionality enables quick retrieval of documents based on keywords, unique IDs, or related text, enhancing usability without compromising security. The implementation demonstrates that blockchain can effectively prevent unauthorized modifications and provide a reliable audit trail for document management. Although slight increases in transaction times are observed as the dataset grows, the approach remains scalable due to the storage of only metadata on-chain.

Overall, the system offers a robust framework for secure document management in social media and related domains. It combines transparency, security, and efficiency while simplifying the administrative workflow and ensuring users can access verified document information safely. This approach can be extended to various applications requiring secure record-keeping, legal compliance, and verifiable document storage.

## REFERENCES


1. E. Al-Shaer, *Deception in Cybersecurity: Techniques and Applications*, Springer, 2016.
2. J. Pawlick, E. Colbert, and Q. Zhu, "A game-theoretic survey and taxonomy of defensive deception for cybersecurity and privacy," *ACM Computing Surveys (CSUR)*, vol. 52, no. 4, pp. 1–30, 2019.
3. C. Shen, J. Wei, and Y. Liu, "Proactive defense for APTs in cyber systems using hypergame theory," *IEEE Access*, vol. 9, pp. 11534–11547, 2021.
4. L. Huang, J. Wang, X. Li, and T. Zhang, "Modeling multi-stage APTs with dynamic Bayesian networks and game theory," *Future Generation Computer Systems*, vol. 107, pp. 544–555, 2020.
5. K. Durkota, V. Lisy, B. Bošanský, and C. Kiekintveld, "Game-theoretic approaches for security analysis of networked systems," *ACM Transactions on Intelligent Systems and Technology (TIST)*, vol. 8, no. 4, pp. 1–29, 2017.
6. Q. Zhu and T. Başar, "Games-in-games methods for robustness, security, and resilience of cyber-physical control systems," *IEEE Control Systems Magazine*, vol. 35, no. 1, pp. 46–65, 2013.

A. Roy, C. Ellis, S. Shiva, D. Dasgupta, and V. Shandilya, "A survey on applications of game theory in network security," in *Proc. 43rd Hawaii International Conference on System Sciences*, pp. 1–10, 2010.

7. T. E. Carroll and D. Grosu, "Analyzing deception in network security using game theory," *Security and Communication Networks*, vol. 4, no. 10, pp. 1162–1172, 2011.
8. T. Alpcan and T. Başar, *Network Security: A Decision and Game-Theoretic Approach*, Cambridge University Press, 2010.
9. W. Wang, Z. Lu, X. Lu, and J. Liu, "From attack graphs to defense graphs: Security assessment and defense planning for industrial control systems," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 1021–1030, 2020.
10. S. Amin, G. A. Schwartz, and S. Sastry, "Security of interdependent and identical networked control systems," *Automatica*, vol. 49, no. 1, pp. 186–192, 2013.
11. S. Sengupta, A. Chowdhary, A. Sabur, and J. Zhan, "Survey of moving target defenses in network security," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1989–2016, 2018.
12. Y. Han, X. Zhao, and Y. Liu, "Optimizing deception-based cyber defense strategies using dynamic game models," *IEEE Access*, vol. 8, pp. 65959–65969, 2020.

A. Kott and C. Arnold, *Cyber Defense and Situational Awareness*, Springer, 2013.

13. P. Liu, A. Singhal, and D. Wijesekera, "Framework and case study for cyber deception using game theory," in *Cyber Deception*, pp. 93–118, Springer, 2015.

A. A. Cardenas, S. Amin, and S. Sastry, "Research challenges for security of control systems," in *HotSec*, 2008.

14. Fielder, E. Panaousis, P. Malacaria, C. Hankin, and F. Smeraldi, "Decision support approaches for cybersecurity investment," *Decision Support Systems*, vol. 86, pp. 13–23, 2016.
15. Y. Liu, Y. Xiao, and S. Li, "Cybersecurity and privacy challenges in smart grids," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 981–997, 2012.
16. Heckman, R. Walsh, F. Stech, R. Thomas, and K. Heckman, "Active cyber defense with denial and deception: A cyber-wargame experiment," *Computers & Security*, vol. 37, pp. 72–77, 2015.
17. J. Grossklags, N. Christin, and J. Chuang, "Secure or insure? Game-theoretic analysis of information security games," in *Proc. 17th International Conference on World Wide Web*, pp. 209–218, 2008.
18. Babburi, S. Privacy-Preserving Collaborative Framework with Auditable Federated Learning.
19. Gaddam, S. Integrating Analytics into the Development Process: Bridging the Gap between Data Insights and Design Execution.
20. Immadi, S. K. (2025). Optimizing ERP for Human Capital Management. Applied Research for Growth, Innovation and Sustainable Impact, 377–384. https://doi.org/10.1201/9781003684657-63
21. Reddy, S. K. R. Developing a Modular AI Framework to Enhance Scalability and Personalization in Next-Generation Reward Platforms.
22. Poojari, R. INTELLIGENT SYSTEMS+B108 AND APPLICATIONS IN ENGINEERING.
23. Mahimalur, R. K., Vasgam, M., & Manoharan, D. Devops Lifecycle Management And Cloud Migration Assessments: A Security-Driven CICD Perspective.
24. Viswanathan, V. (2023). AI-Augmented Decision Intelligence for Enterprise Systems: Integrating Cognitive Analytics for Resource and Talent Optimization.
25. Agrawal, A. M., Gajula, S., Shinde, R. P., Shah, H., & Ghosh, H. (2025, July). Machine Translation for Long Sequences with Enhanced Attention Mechanisms. In 2025 5th International Conference on Electrical, Computer and Energy Technologies (ICECET) (pp. 1-6). IEEE.
26. Maturi, S. Y. (2021). Blockbond hardening: Securing pooled-hash protocols against traffic tampering, MITM hash-rate hijacking, and template coercion. International Journal of Communication Networks and Information Security, 13(3), 718–728.
27. Adabala, P. K. (2024). Utilizing predictive analytics to improve efficiency and decision-making in ERP-connected supply chains. International Journal of Intelligent Systems and Applications in Engineering, 12(22s), 2465

28. Kavuri, S. (2026). An Explainable Machine Learning Framework for Predicting Software Defects in Large-Scale Software Systems. 2026 IEEE 5th International Conference on AI in Cybersecurity (ICAIC), 1–6. https://doi.org/10.1109/icaic67076.2026.11395777
29. Subramanian, V. K., Bhambri, S., & Gajula, S. (2026). Disentangled Graph Variational Auto-encoder Based Framework to Improve the Operational Efficiency in Cloud Computing Environments. Computer Vision and Robotics, 396–407. https://doi.org/10.1007/978-3-032-14044-9_32
30. Shashank, A. (2025). Self-Healing Data Pipelines for Enhanced Reliability: A Paradigm Shift in Enterprise Data Management. Journal of Computer Science and Technology Studies, 7(8), 1097-1104.
31. Susarla, R. S., Boyapati, P. K., & Kandula, S. T. R. (2025, July). Cloud-Based Secure Data Storage in Smart Cities Using Central-Smoothing Hypergraph Neural Networks. In 2025 IEEE 4th World Conference on Applied Intelligence and Computing (AIC) (pp. 279-284). IEEE.
32. Boyapati, P. K. Building a centralized data operations hub for healthcare enterprise integration. IJSAT-Int. J. Sci. Technol. 16 (2). https://doi.org/10.71097/IJSAT.v16.i2.3219