iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** V **Month of publication:** May 2025

DOI: https://doi.org/10.22214/ijraset.2025.70255

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

Blockchain Solution for Document Integrity and Forgery Mitigation

Sania Begum[1], Madhu Priya[2], Gillella Swapnil[3], G. Swapna Rani[4]
[1, 2, 3]*CSE, GCET, Hyderabad, India*
[4]*Assistant Professor, GCET, Hyderabad, India*

Abstract: ***Ensuring document authenticity and security is a critical challenge in the digital era. Traditional document verification methods are often susceptible to forgery, unauthorized modifications, and inefficiencies. This paper presents a Blockchain-Based Digital Notary System, leveraging blockchain's decentralized and immutable nature to provide a tamper-proof and transparent document verification solution. The system integrates IPFS-based secure storage, SHA-256 hashing, and smart contracts to store document metadata while ensuring privacy and integrity. Users can upload, verify, and authenticate documents through a seamless interface, while verifiers and issuers have dedicated functionalities for approval and digital signing. The architecture is built on Node.js, Express.js, MongoDB, Solidity, Ganache, and Truffle, ensuring efficient backend processing and smart contract execution. By eliminating third-party dependencies and enabling real-time validation, this system enhances trust, security, and efficiency across various industries, including legal, educational, and financial sectors. Future improvements focus on scalability, interoperability, and regulatory compliance to broaden adoption in institutional frameworks.***

General Terms: Blockchain, Digital Fingerprint (Hash), Decentralized Storage, Smart Contracts ,Verification System, Tamper-proof, Authentication

Keywords: Forgery Prevention, Document Verification, User Authentication, Decentralized Network ,Data Integrity ,Secure File Storage,Transparency and Trust, Real-time Validation , Cryptographic Hashing.

I. INTRODUCTION

In today's digital age, document authenticity and security have become crucial concerns for organizations and individuals across various sectors. Traditional document verification methods rely on centralized authorities such as notaries, government agencies, and third-party verification services. These centralized systems introduce several limitations, including vulnerability to fraud, high operational costs, inefficiencies in processing, and reliance on intermediaries. Documents stored in conventional databases can be tampered with, altered, or even forged, leading to significant risks in legal, financial, educational, and healthcare domains. Given these challenges, there is a growing need for a secure, automated, and decentralized solution that ensures the integrity, authenticity, and accessibility of digital documents. Blockchain technology offers a revolutionary approach to document verification by leveraging its decentralized, immutable, and transparent nature. Unlike traditional systems, blockchain does not rely on a single authority for verification. Instead, it distributes data across a secure and tamper-proof ledger, ensuring that once a document's details are recorded, they cannot be modified or deleted. In the proposed Blockchain-Based Digital Notary System, documents are hashed using cryptographic algorithms, and the resulting hash is stored on the blockchain. This hash acts as a unique digital fingerprint for the document, allowing anyone to verify its authenticity without exposing its contents. The actual document is securely stored using Inter Planetary File System (IPFS), a decentralized storage network that prevents unauthorized access while ensuring efficient retrieval. The system is designed to provide a user-friendly and efficient document verification process. Users can upload documents, which are then hashed and stored on the blockchain. Verifiers, such as government officials or academic institutions, can access the stored document hashes and confirm their authenticity in real time. Additionally, issuers such as universities, banks, and legal authorities can digitally sign and approve documents through smart contracts, ensuring they remain legally valid and verifiable at any time. This eliminates the need for intermediaries, reducing verification time and costs while enhancing security and trust.

A. Objectives

1) Secure & Tamper-Proof Storage– Utilizes SHA-256 hashing and smart contracts to prevent document alteration or duplication.
2) Decentralized & Transparent Verification – Ensures real-time validation and fraud prevention without relying on central authorities.
3) Industry Applications – Ideal for secure documentation in education, finance, healthcare, and government sectors.
4) Future Enhancements – Focus on scalability, legal compliance, and interoperability for widespread adoption.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue V May 2025- Available at www.ijraset.com

II. LITERATURE OVERVIEW

Ensuring document authenticity and preventing forgery remain critical challenges across various industries. Researchers have explored blockchain technology as a transformative solution for secure document verification. Traditional document authentication methods often suffer from inefficiencies, dependency on centralized authorities, and vulnerability to tampering. In response, blockchain offers a decentralized, immutable, and transparent approach to document verification. By leveraging cryptographic hashing and smart contracts, blockchain-based systems ensure real-time validation, fraud prevention, and secure record-keeping. However, challenges such as scalability, legal compliance, and integration with existing systems remain key concerns. Various frameworks, including Ethereum, Hyperledger Fabric, and IPFS, are commonly used for such applications.

A. Motivation for the Proposed Framework

This paper provides an analytical perspective on the role of blockchain in document verification. Its relevance to our project includes:

Analytical Insights- It highlights how blockchain ensures document integrity, eliminating forgery risks and enhancing trust in authentication systems.

Evaluating Implementation- The study offers insights into smart contract functionality, cryptographic hashing, and decentralized verification methods, ensuring alignment with best practices.

Comparative Analysis- A comparison between blockchain and traditional document verification systems helps benchmark efficiency and security improvements.

III. SYSTEM ANALYSIS

A. Existing System

The current document verification systems rely on centralized authorities such as government institutions, educational organizations, and notary offices. These systems present several limitations:

- Centralized Control: Verification depends on third-party entities, increasing the risk of fraud, data manipulation, and unauthorized alterations.
- High Verification Costs & Delays: Manual verification requires significant time and resources, leading to inefficiencies and delays in document authentication.
- Security Vulnerabilities: Documents stored in centralized databases or physical records are susceptible to forgery, tampering, and unauthorized access.
- Limited Accessibility: Users often face bureaucratic hurdles in retrieving verified documents, making the process slow and inconvenient.

B. Proposed System

The proposed Blockchain-Based Digital Notary System leverages blockchain technology to provide a secure, transparent, and decentralized approach to document verification.

- Decentralized & Tamper-Proof Storage: Using SHA-256 cryptographic hashing, document fingerprints are securely stored on the blockchain, ensuring integrity and preventing unauthorized alterations.
- Real-Time Verification: Documents can be authenticated instantly by comparing their hash with the one recorded on the blockchain, eliminating delays associated with manual verification.
- Smart Contracts for Automation: Digital signatures and smart contracts enable automated validation processes, ensuring that documents are verified and authorized without human intervention.
- Enhanced Security & Fraud Prevention: The system eliminates the risk of document duplication and forgery by maintaining immutable records on the blockchain.
- Scalability & Interoperability: Designed to integrate with existing enterprise systems, government databases, and educational institutions while ensuring compliance with legal and regulatory frameworks.

IV. METHODOLOGY

A. System Configuration

1) Hardware: For running this web application we must require the processor with minimum configuration of 32-bit and intel processor of i3 or more is acceptable. Stable internet connection for blockchain interactions and IPFS access.

2) *Software:* The system must be well equipped with latest version any browser available to run the web application and Google OTP Authentication (User Login & Registration) Ganache Local Blockchain for Testing Smart Contracts and an IPFS server for storing the data in a distributed database and Node.js application with Nod.js for backend. Web3.js / Ethers.js for Connecting the React frontend with blockchain. Solidity & Truffle for Smart contract development, deployment, and testing.Express.js for Backend API for handling document verification requests. VS Code & Windows PowerShell for writing and running frontend, backend, and smart contract code. The configuration will support both the technical requirements and the user-friendly operation of the system across a variety of devices and infrastructures

B. System Architecture

1) *Module Description The Blockchain-Based Digital Notary System consists of four primary modules:* User Authentication Module, Document Upload Module, Verification Module, and Document Issuance & Security Module. *Each module is designed to facilitate secure, tamper-proof, and real-time document verification, eliminating forgery risks and third-party dependencies.*

- User Authentication Module
  Users log in using Google OTP authentication. This ensures that only authorized users can upload and verify documents.

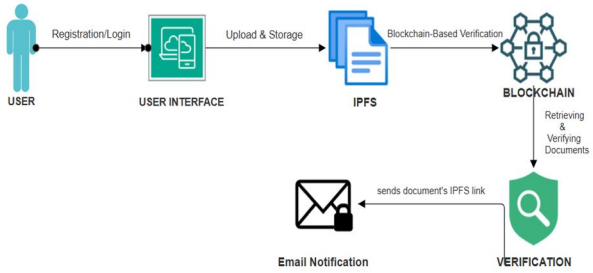


Fig. 1. System Architecture

- Document Upload Module
  Users select a file (PDF, PNG, JPG) and upload it. The file is stored on IPFS (Inter Planetary File System), which generates a unique CID (Content Identifier). A hash of the file is created and stored on the blockchain along with metadata. All the members are notified about the upload. If a duplicate document is uploaded (even from a different account), the system detects forgery and prevents storage.
- Verification Module
  Users can check whether a document already exists on the blockchain by uploading it for verification. If the document is found, the system shows its IPFS link and confirms its authenticity. If not found, it means the document has not been uploaded before.
- Document issuance & Security Module
  After uploading, users can send the document link via email to another person. The email contains a direct download link to the document stored on IPFS. The system resets the input fields after sending the email for convenience. Since blockchain data cannot be modified or deleted, it ensures that the document history remains tamper-proof. Even if someone uploads the same file with a different name, the system detects duplication and prevents forgery.

2) *Modular Workflow*

- User Authentication- Users log in using Google OTP, ensuring secure access.
- Document Upload- The document is uploaded to IPFS, generating a unique CID.
- Blockchain Hashing- The document hash is stored on the blockchain for verification.
- Verification Process-Users can check document authenticity by comparing hashes.
- Email Notifications- Approved documents are sent to users via EmailJS with IPFS links.155

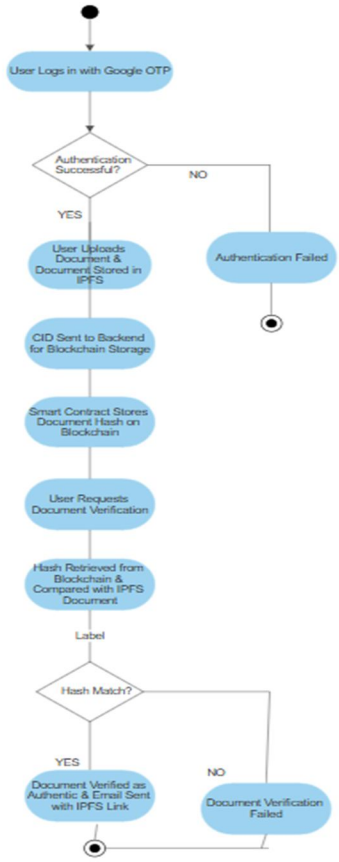


Fig. 2. Activity Diagram

3) *Activity and Sequence Diagrams:* The activity diagram depicts how the processes in the system flow. The way various system items interact with one another is depicted in a sequence diagram. A sequence diagram's time-ordering is one of its key features. This indicates that a step-bystep representation of the precise order in which the items interacted is provided. In the sequence diagram, several objects communicate with one another by sending "messages". The activity diagram depicts how the processes in the system flow. An activity diagram includes activities, actions, transitions, beginning and final states, and guard conditions, just like a state diagram.

A sequence diagram represents the interaction between different objects in the system shown in fig.3. The important aspect of a sequence diagram is that it is time-ordered. This

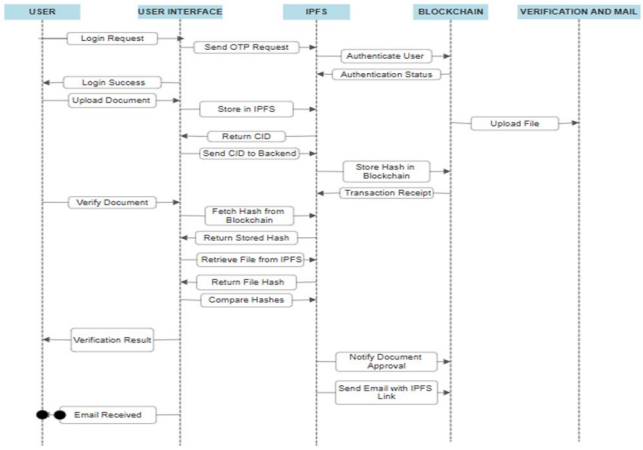


Fig. 3. Sequence Diagram

V. IMPLEMENTATION

To implement the system shown in the sequence diagram, we can break it down into the following components and technologies:

A. Front-End Implementation

The front-end of the system is developed using modern web technologies like React.js. The user interface provides an intuitive and seamless experience for users to interact with the platform. It includes forms for making document uploads, tracking verification status, and managing authentication. The system incorporates Google OTP Authentication for user login and verification. Users must enter an OTP sent to their registered email or phone to securely access document upload and verification functionalities. Web3.js is used to facilitate interaction between the front-end and the Ethereum blockchain, enabling the system to read from and write to smart contracts securely.

B. Back-End Implementation

The back-end is built using Node.js, which manages API endpoints and handles requests between the front-end and the blockchain. The back-end communicates with smart contracts deployed on the Ethereum blockchain using Ganache, a development environment that simplifies testing, deploying, and debugging smart contracts. Smart contracts, written in Solidity, govern the document verification process by managing hash storage, verifying transactions, and ensuring that all predefined conditions are met. The system also leverages IPFS (Inter Planetary File System) to securely store documents, while transaction logs and verification details are immutably recorded on the blockchain.

1) Google OTP Authentication-The system integrates Google OTP authentication to ensure only authorized users can access the platform. When users attempt to log in, an OTP is sent to their registered email or phone number. The backend verifies the OTP before granting access to document upload, verification, and retrieval services. This enhances security by preventing unauthorized access and ensuring user identity verification.

2) Ganache-Ganache is used in the blockchain-based document verification system to compile, deploy, and test Solidity smart contracts efficiently. It provides a local Ethereum blockchain for testing, allowing developers to simulate transactions without incurring gas fees. Ganache automates the deployment process, ensures contract functionality through rigorous testing, and simplifies script management for seamless interaction with the Ethereum blockchain, enhancing the system's security and reliability.

3) IPFS (Inter Planetary File System)-IPFS is used to store document-related data, such as uploaded files, verification receipts, and metadata, in a decentralized manner. Instead of storing large files directly on the blockchain, which is inefficient, IPFS generates a unique hash for each file and stores this hash on the Ethereum blockchain. The back-end uploads the documents to IPFS and records the hash in the smart contract, ensuring that the data is immutable and easily traceable. When a document needs to be retrieved, the system uses the hash to fetch the file securely from IPFS.

4) Blockchain Integration-Users interact with the blockchain through smart contracts deployed on Ethereum. When users submit documents or check their authenticity, the front-end prompts the user to authenticate via OTP. The signed transaction is then sent to the blockchain, where the smart contract verifies and processes it.

5) Ethereum Smart Contracts-Smart contracts manage the document verification process, ensure integrity, and automate validation. They prevent unauthorized modifications or misuse. All key actions, such as uploading documents, storing hashes, and verifying authenticity, are governed by smart contracts, ensuring security, transparency, and accountability.

VI. RESULTS

The implemented system demonstrates significant improvements in transparency, security, and efficiency in the management of document verification. By utilizing blockchain technology, all document verification transactions are recorded immutably, allowing users to verify document authenticity in real time and ensuring that records remain tamper-proof.

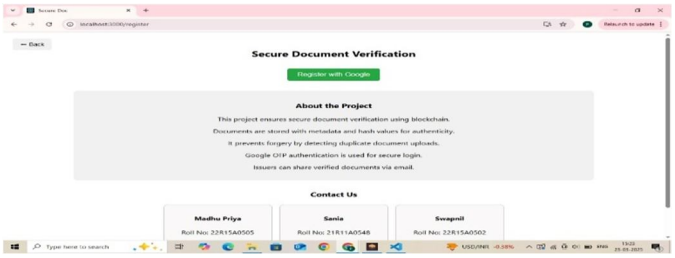


Fig. 5. Output Screen 1

Smart contracts automate the entire verification process, eliminating the need for intermediaries and minimizing administrative overhead while guaranteeing that document authenticity checks are conducted securely. The integration of IPFS ensures secure and decentralized storage of documents, enhancing data integrity and traceability.

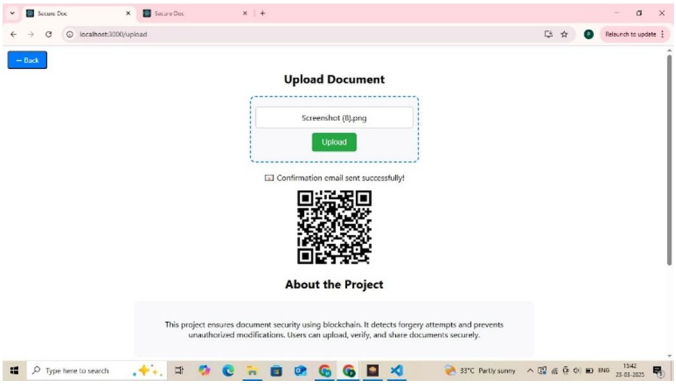


Fig. 6. Output Screen 2

The system's decentralized architecture prevents any single entity from manipulating verification records, thereby reducing the risk of fraud. Additionally, the integration of Google OTP authentication ensures that only authorized users can upload and verify documents, adding an extra layer of security. The user-friendly interface enhances accessibility, allowing seamless participation by individuals and organizations requiring document verification services.

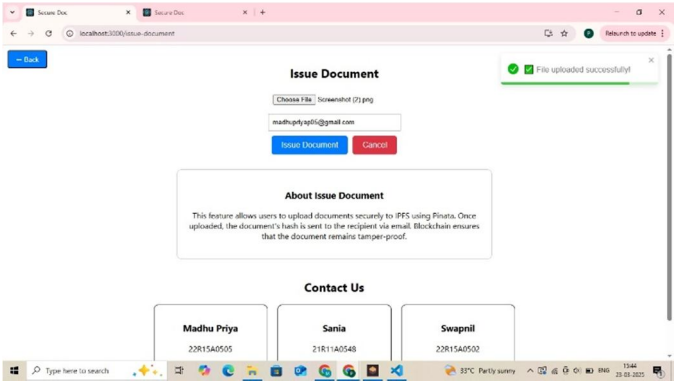


Fig. 7. Output Screen 3

Through these enhancements, the system promotes trust, ensures secure digital notarization, and prevents document forgery, making it an effective solution for reliable document integrity verification.

VII. CONCLUSION

The blockchain-based document verification system successfully enhances document integrity, security, and transparency by leveraging blockchain immutability, decentralized IPFS storage, and smart contracts. The implementation of Google OTP authentication ensures that only authorized users access and interact with the platform, adding an additional layer of security. By eliminating intermediaries and automating verification through smart contracts, the system significantly reduces the risks of document forgery, unauthorized modifications, and data manipulation. The integration of IPFS for decentralized storage further enhances traceability and ensures tamper-proof document storage. With a user-friendly interface and seamless authentication, the system fosters trust among users, enabling real-time verification while maintaining efficiency and reliability. This solution stands as a robust framework for secure document verification in various domains, including legal, healthcare, and educational sectors.

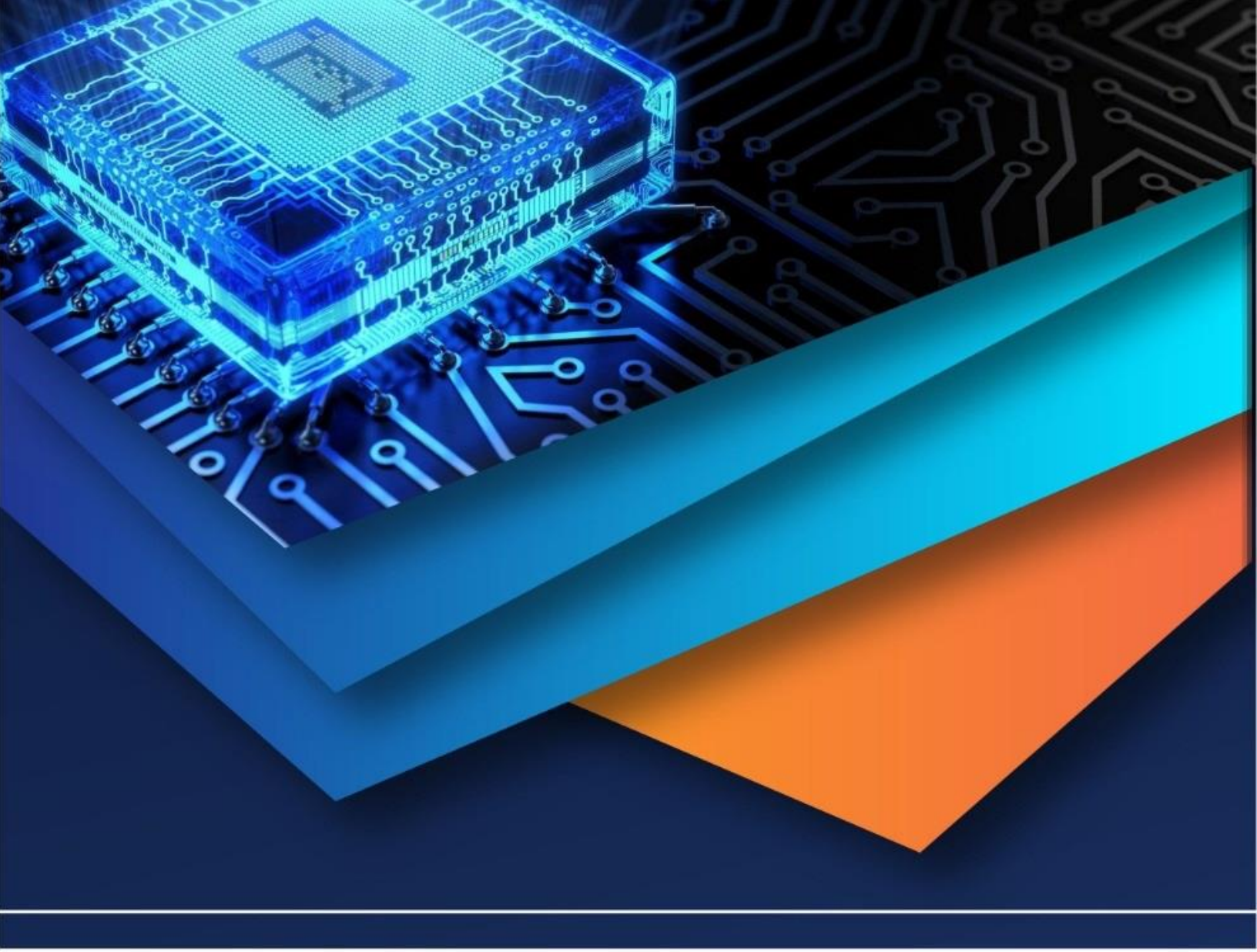
VIII. FURTHER ENHANCEMENTS

The blockchain-based document verification system can be further improved with several enhancements to increase its efficiency, scalability, and usability. Multi-Blockchain Support can be integrated, allowing compatibility with multiple blockchain networks such as Polygon, Solana, or Hyperledger to optimize cost and performance.

AI-Based Document Verification can be introduced to automatically analyse and validate document authenticity before storing hashes on the blockchain. Enhanced User Authentication methods, such as biometric authentication (fingerprint or facial recognition), can replace or complement OTP-based verification for added security. These enhancements will further strengthen security, improve performance, and expand the system's usability across diverse sectors.

REFERENCES

[1] Monther, Aldwairi., Mohamad, Badra., Rouba, Borgh (2023), "DocCert: Nostrification, Document Verification and Authenticity Blockchain Solution"
[2] Rafah, Amer, Jaafar., Saad, Najim, Alsaad (2023), "Enhancing Educational Certificate Verification With Blockchain and IPFS: A Decentralized Approach Using Hyperledger Fabric",TEM Journal
[3] Rahman, Md. Mijanur et al (2023). "Blockchain-based certificate authentication system with enabling correction."
[4] Jerinas, Gresch., Bruno, Rodrigues., Eder, J., Scheid., Salil, S., Kanhere., Burkhard, Stiller (2020), "The Proposal of a Blockchain-Based Architecture for Transparent Certificate Handling"
[5] Olaiya Samuel Oluwaseyi, R.O. Akinyede (2024). "Utilizing Blockchain Technology for University Certificate Verification System. "International Journal of Applied Information Systems.
[6] Hitesh (2023). "Digital Document Verification System Using Blockchain." International Journal of Creative Research Thoughts.
[7] Venkata Marella, Anoop Vijayan (2020). "Document Verification Using Blockchain for Trusted CV Information." Aalto University Publication.
[8] Roshni Bhave, Sudhir Agarmore (2024). "Novel Approach for Fake Detection Document Using Blockchain." AIP Conference Proceedings.
[9] Kenji Saito, Satoki Watanabe (2021). "Lightweight Selective Disclosure for Verifiable Documents on Blockchain."arXiv preprint arXiv:2103.07655.
[10] M. M. Rahman, M. T. K. Tonmoy, S. Shihab (2022). "A Blockchain-Based Online Document Verification System." International Journal of Computer Applications.
[11] V. Badhe, P. Nhavale, S. Todkar, P. Shinde, K. Kolhar (2020). "Digital Certificate System for Verification of Educational Certificates Using Blockchain." International Journal of Scientific Research in Science and Technology.
[12] T. S. Charitha, K. A. Baba (2022). "A System for Academic Certificates Verification Using Blockchain." International Journal of Research in Applied Science and Engineering Technology.
[13] M. H. Eldefrawy, K. Alghathbar, M. K. Khan (2011). "Formal Verification of a Modified Authenticated Multiple Key Agreement Protocol." International Journal of Network Security.
[14] Chen, L., Xu, L., Shah, N., Gao, Z., & Lu, Y. (2023). "Blockchain-Based Document Authentication System". Published in Journal of Blockchain Research.
[15] Wang, H., Li, Y., & Zhang, J. (2024). "Decentralized Document Verification Using Ethereum Smart Contracts". Published in International Journal of Distributed Ledger Technology.
[16] Singh, R., Patel, S., & Kumar, A. (2022). "Secure Academic Certificate Verification with Blockchain Technology". Published in IEEE Transactions on Education.
[17] Ghosh, A., Bose, R., & Banerjee, S. (2021). "A Survey on Blockchain Applications in Digital Identity Verification". Published in ACM Computing Surveys.
[18] Park, J., Kim, H., & Lee, D. (2023). "Blockchain for Healthcare Records: A Decentralized and Secure Solution". Published in Journal of Medical Systems.
[19] Brown, T., White, P., & Green, K. (2022). "Implementing Blockchain for Legal Document Management". Published in Harvard Journal of Law & Technology.
[20] Nguyen, M., Tran, B., & Hoang, V. (2023). "Blockchain-Based Land Registry System: A Transparent and Immutable Approach". Published in International Journal of Property Law.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY