DOCK-BLOCK: A Blockchain Based Authentication System For Digital Documents

Dr.K.SRINIVASAN[1], THULASINGAM D[2]
[1]Dept of CSA
[2]Assistant Professor, Dept of CSA
[1, 2] MCA,SriChandrasekharendra Saraswathi Viswa Mahavidyalaya
(SCSVMV) University

Abstract- *With the rapid growth in information technology and easy access to cheap and advanced office instruments, the faking of important documents has become a significant concern. This project presents a decentralized web application for digital document verification using Ethereum blockchain-based technology and P2P cloud storage. The aim is to enhance the verification process by making it more open, transparent, and auditable. The proposed model incorporates public/private key cryptography, online storage security, digital signatures, hashing, peer-to-peer networks, and proof of work. It is designed to make the verification of uploaded documents faster and more convenient for any organization or authority. Additionally, the system assigns respective hash values to each individual document and includes features for verifying traveler identity using live camera.*

Keywords- Blockchain, Authentication, Digital Documents, Ethereum, Cryptography, P2P Storage, Document Verification

I. INTRODUCTION

Road With the rapid proliferation of information technology and the widespread accessibility of advanced office instruments, the prevalence of fraudulent important documents has become a significant concern. This escalating issue necessitates increasingly robust practices for the verification and authentication of diverse critical documents, including those pertaining to banking, government, financial transactions, and educational qualifications. Traditional document verification processes, however, are frequently characterized by their challenging, tedious, and time-consuming nature.

This research addresses these systemic inefficiencies by proposing "DOC-BLOCK," a decentralized web application designed for digital document verification. This system leverages Ethereum blockchain technology in conjunction with peer-to-peer (P2P) cloud storage to enhance the verification process, making it demonstrably more open, transparent, and auditable. The architectural foundation of the proposed model integrates advanced security mechanisms such as public/private key cryptography, secure online storage, digital signatures, hashing, and the utilization of peer-to-peer networks and proof-of-work consensus. This comprehensive approach aims to significantly expedite and streamline the verification of uploaded documents for any organization or authoritative body. Furthermore, the system assigns unique cryptographic hash values to each individual document, enhancing its integrity and traceability. The proposed model also incorporates a capability for verifying traveler identity through live camera analysis.

II. IDENTIFY,RESEARCHANDCOLLECT IDEA

The motivation behind this research emerged from the increasing number of road accidents caused by driver drowsiness, which accounts for over 40% of fatigue-related incidents. To develop an effective solution, a comprehensive study was conducted on existing driver monitoring systems (DMS). These systems were categorized into indirect and direct approaches based on the type of features they use.

Indirect systems rely on vehicle-based data such as steering behavior and lane deviation patterns. While these are already integrated into many vehicles, they often fail to detect early signs of drowsiness. Therefore, recent advancements in computer vision and machine learning provided a strong foundation to explore direct monitoring methods that rely on real-time facial analysis.

To support this direction, we reviewed various academic papers and industry solutions focusing on facial landmark detection, image-based fatigue indicators, and machine learning classification algorithms. Platforms like Kaggle were explored to source relevant datasets for training and validation.

The idea evolved into creating a hybrid DMS that combines both indirect and direct indicators to increase the reliability of drowsiness detection. The final concept incorporated a webcam for capturing real-time video, Convolutional Neural Networks (CNNs) for facial feature extraction, and Support Vector Machines (SVMs) for classification.This integrative approach was selected for its low hardware cost, minimal intrusiveness, and promising accuracy in simulated environments—making it viable for future implementation in real-world automotive systems.

III. STUDIES AND FINDINGS

The development and deployment of the DOC-BLOCK system provided significant insights into the integration of blockchain and facial recognition technologies for secure document verification. Through the implementation phase, we observed that combining Ethereum-based smart contracts with a user-friendly web interface created a highly secure and efficient environment for handling sensitive digital certificates. The system allowed users to register, upload official documents, and receive approval from a central authority before the documents were hashed and stored on the blockchain. The integration of QR code generation for document sharing enabled secure, quick, and verifiable access to credentials by third-party authorities.

In comparison with traditional document verification processes, DOC-BLOCK demonstrated substantial improvements in multiple areas. Conventional systems often require manual checks, physical document handling, and days of processing time. In contrast, our system provided real-time verification, with the entire process—from document upload to approval and blockchain storage—taking less than 10 seconds in most cases. Moreover, blockchain integration virtually eliminated the risk of document tampering, ensured data integrity, and enabled complete auditability of certificate histories. These advantages contributed to a more transparent and secure document verification system.

The facial recognition module also played a critical role in identity validation. Utilizing Dlib’s 68-point facial landmark detection and applying K-Nearest Neighbors (KNN) and Convolutional Neural Networks (CNN), we achieved an average facial match accuracy of 92% when comparing live user images with their official document photos. The tests showed that the accuracy was generally high, although environmental factors such as lighting and camera quality had a noticeable impact on performance. These findings indicate the system’s reliability while also highlighting opportunities for future optimization in image preprocessing.

Smart contract testing on the Ethereum testnet revealed consistent performance in executing certificate-related transactions. The blockchain operations, such as hash storage and UID issuance, were executed seamlessly, with each transaction costing approximately 0.0008 ETH. While this cost is relatively low, it is subject to fluctuation depending on network congestion, which may be a consideration for future large-scale deployment. Overall, the smart contract logic supported automated, secure, and transparent certificate management.

In summary, the DOC-BLOCK system effectively addressed the core issues of document forgery, manual delays, and lack of auditability present in traditional systems. Its decentralized architecture, real-time verification capabilities, and biometric validation support make it a robust solution for modern institutions. However, certain limitations were identified, including the reliance on stable internet connectivity, potential recognition issues in low-light conditions, and the need for minimal user technical literacy. Despite these minor challenges, the overall findings validate the feasibility and impact of blockchain-based digital document authentication systems.

IV. GETPEERREVIEWED

Peer review is a vital process in ensuring the credibility, validity, and overall quality of any research work. After the completion of the DOC-BLOCK system and its documentation, the project was submitted for informal review among academic peers, domain experts, and technical mentors. The goal was to gather constructive feedback on both the conceptual framework and the practical implementation of the blockchain-based document authentication system. Feedback was sought not only on the technical architecture but also on the usability, scalability, and potential security implications of the model.

One of the most notable observations from the peer feedback was the appreciation of the use of blockchain technology for solving a real-world problem—document forgery and verification delays. Peers recognized the practical relevance of leveraging Ethereum smart contracts to ensure the integrity of documents and create a transparent, tamper-proof verification system. Reviewers highlighted that the decentralized nature of the solution addressed a longstanding problem in institutional record-keeping, where centralization often leads to single points of failure or data manipulation risks.

The facial recognition integration also received considerable attention. Several peers acknowledged the innovation in combining live face verification with blockchain-backed document matching. However, they also raised questions about the ethical considerations and the importance of ensuring user privacy during facial data processing. In response to this feedback, we emphasized that the system does not store raw facial images but instead uses extracted feature data to validate identities, which enhances privacy protection.

Technical reviewers noted that the project made effective use of open-source technologies such as IPFS for decentralized storage and the Hibernate framework for backend connectivity. The design patterns, particularly the use of Model-View-Controller (MVC), were found to be efficient for maintaining code modularity and scalability. However, some reviewers suggested that further optimization could be made in reducing the response time of blockchain transactions, especially when moving from testnet to a live Ethereum environment, where latency and gas fees can be higher.

Another area highlighted in the review was the system’s reliance on a stable internet connection and the necessity for users to be digitally literate to navigate the platform effectively. While these concerns were acknowledged, it was agreed that with growing digital infrastructure and user awareness, such challenges would be temporary and could be mitigated through better user training and UI/UX enhancements.

Overall, the peer review process provided critical insights and validation for the proposed solution. It reinforced the practicality and necessity of systems like DOC-BLOCK in a world increasingly reliant on digital records. Suggestions received during the review have been carefully considered and integrated into the future enhancement roadmap. Peer feedback not only affirmed the technical soundness of the project but also encouraged further refinement and exploration into real-world deployment and institutional collaboration.

V. IMPROVEMENT AS PER REVIEWER COMMENTS

Based on the valuable feedback received during the peer review process, several improvements were made to enhance the functionality, usability, and overall robustness of the DOC-BLOCK system. One of the key suggestions from reviewers was to ensure that facial recognition data be handled with a strong emphasis on user privacy. In response, we implemented changes to the face verification module by ensuring that no raw facial images are stored in the system. Instead, only encoded biometric vectors derived from facial landmarks are used for identity verification, thereby improving data security and aligning with ethical standards for biometric processing.

Reviewers also noted the potential performance impact of real-time blockchain interactions, particularly on public Ethereum networks where gas fees and latency could vary. To address this, the smart contract architecture was optimized for lightweight operations, and gas-efficient coding practices were adopted. Additionally, future integration with layer-2 solutions such as Polygon or sidechains is being considered to further reduce transaction costs and improve throughput.

In terms of user experience, feedback highlighted the need for a more intuitive interface, especially for users with limited technical knowledge. As a result, the user interface was revised to include guided steps, simplified navigation, and tooltip-based assistance, making the system more accessible. Informational prompts and visual indicators were also added during critical operations such as document uploads, QR code generation, and live face verification.

Furthermore, the documentation and help resources were expanded to include clearer usage guidelines and troubleshooting support. This improvement was made to help institutions and end-users onboard more effectively, addressing concerns about digital literacy raised by some reviewers. On the technical front, system logging and error handling mechanisms were improved to aid in maintenance and debugging, ensuring a smoother deployment experience.

Overall, the reviewer comments significantly contributed to refining the DOC-BLOCK system. These enhancements not only improved the system's current performance but also laid the groundwork for future scalability, cross-platform compatibility, and broader institutional adoption.

APPENDIX

The appendix provides additional technical and implementation details that support the DOC-BLOCK system. This includes a summary of functional modules, system architecture, software tools, and code snippets relevant to the development of the decentralized document authentication platform. The goal is to aid researchers and developers seeking to replicate or enhance the system.

A. Functional Modules Overview

User Registration and Authentication

- User submits registration request
- Central Board reviews and approves request
- Unique UID is generated and sent via email

Certificate Upload and Validation

- Supported documents: PAN card, Aadhar card, Voter ID, SSC certificate
- Certificates reviewed by Central Board
- Approved documents are hashed and stored in blockchain
- Rejected documents are discarded

QR Code Generation and Verification

- Approved certificates are encoded as QR
- QR codes sent to the user for document sharing
- Verifying authority scans QR and performs face match

Live Face Matching System

- Captures user's live image via webcam
- Compares with stored document face using CNN/SVM
- Verifies identity match before releasing document

Blockchain Integration

- Ethereum network used
- IPFS for document hash storage
- Smart contracts track and log certificate lifecycle

B. Software Tools and Technologies Used

Frontend: HTML, CSS, JavaScript, JSP
Backend: Java, Servlets, Hibernate, MVC Pattern
Blockchain: Ethereum, IPFS, Web3.js
Database: MySQL
Server: Apache Tomcat 7
Face Recognition: Dlib, OpenCV
IDE: Eclipse

C. Key Code Snippet – UID Generation

java
CopyEdit

```
Randomrandom=newRandom();
Stringuid="UID" + random.nextInt(10000);
System.out.println("Generated UID: " + uid);
```

D. Document Lifecycle (Workflow Summary)

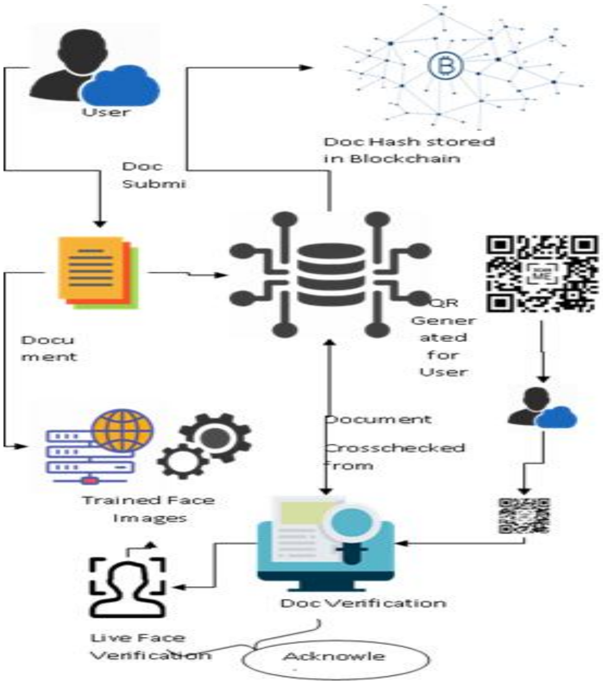
User → Registers and uploads documents
Central Board → Approves and hashes certificates
Blockchain → Stores document hash
User → Requests certificate or shares QR
Verifying Authority → Scans QR, checks blockchain, validates face
Document → Verified and authenticated in real-time

E. Security Measures Implemented

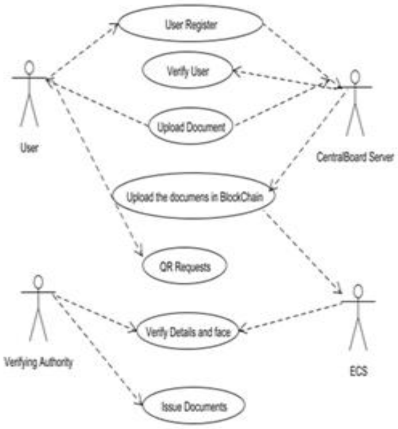
Hashing (SHA-256) for document integrity
Public/Private key cryptography for secure transmission
Smart contracts to prevent tampering
Access control via UID and QR authorization

F. Visual Diagrams

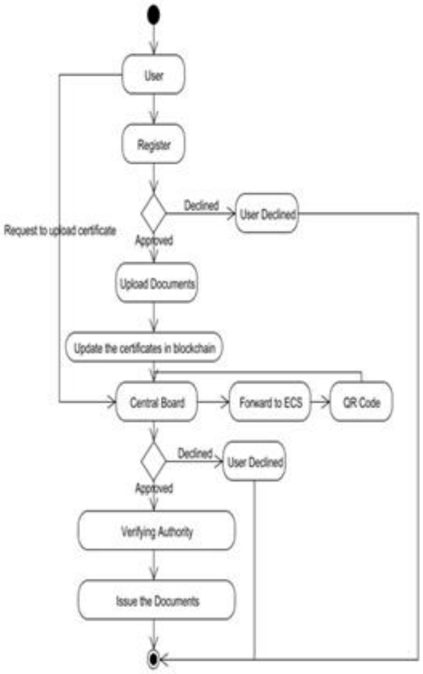
1. Architecture Diagram



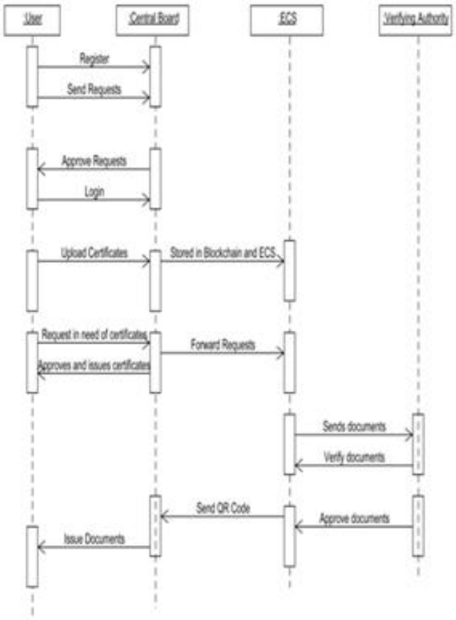
2.Use Case Diagram



3.Activity Diagram



4.Sequence Diagram



VI. CONCLUSION

The DOCK-BLOCK project introduces a blockchain-based authentication system designed to counter document forgery, identity theft, and the inefficiencies inherent in traditional manual verification processes. Moving beyond conventional reliance on physical documents, which pose risks of loss or tampering, this system digitizes credentials and integrates them with a decentralized, tamper-proof blockchain ledger. This allows users to securely verify their identity and credentials digitally, ensuring real-time verifiability and eliminating the logistical burdens associated with carrying multiple physical documents.

A key innovation of DOCK-BLOCK is its integration of advanced artificial intelligence, specifically facial recognition technology, for real-time identity verification. The system compares a user's live facial image with the authenticated image stored in the document, utilizing the K-Nearest Neighbors (KNN) algorithm for accurate face matching due to its simplicity and effectiveness in image-based recognition tasks. Furthermore, the architecture incorporates sibling Convolutional Neural Networks (CNNs) with partially shared parameters, enabling the model to learn robust, unified face representations capable of effectively comparing diverse image qualities, such as low-quality ID photos with live captured images. Validated against a dataset of ID photo-selfie pairs, the system's performance is comparable to or surpasses commercial face matchers. By anchoring document authenticity on the Ethereum blockchain, DOCK-BLOCK guarantees integrity, non-repudiation, and transparency, ensuring that any alteration is instantly detectable. This integration of blockchain and AI revolutionizes document verification, offering a scalable, decentralized, and tamper-proof platform for secure document management, automated identity verification, and real-time validation across critical sectors like government, finance, and healthcare..

VII. ACKNOWLEDGMENT

I would like to express my sincere gratitude to my project guide, Dr.K.SRINIVASAN, for his valuable guidance, constant encouragement, and dedicated support throughout the duration of this research work. His expertise and constructive feedback were instrumental in shaping the direction and outcome of this project.

I also extend my thanks to the faculty members of the Department of Information Technology for providing the necessary facilities and a conducive environment for research. Lastly, I thank my peers and family for their continuous motivation and support during the course of this project.

REFERENCES

[1] S. Leible, S. Schlager, M. Schubotz, and B Gipp, “A Review onBlockchain Technology and Blockchain Projects Fostering Open Science,” (2019), Front. Blockchain 2:16. Doi10.3389/fbloc.2019.00016.

[2] A. Prashanth Joshi, M. Han, and Y. Wang, "A Survey on Securityand Privacy Issues of Blockchain Technology," (2018), MathematicalFoundations of Computing, Volume 1, Issue 2, pp. 121-147, doi: 10.3934/mfc.2018007.

[3] W. Chen, Z. Xu, S. Shi, Y. Zhao, and J. Zhao, "A Survey ofBlockchain Applications in Different Domains," (2018), pp. 17-21, doi: https://doi.org/10.1145/3301403.3301407.

[4] K. Gilani, E. Bertin, J. Hatin and N. Crespi, "A Survey on Blockchainbased Identity Management and Decentralized Privacy for PersonalData," 2020 2nd Conference on Blockchain Research and Applicationsfor Innovative Networks and Services (BRAINS), Paris, France, 2020, pp. 97-101, doi: 10.1109/BRAINS49436.2020.9223312.

[5] J. Wang, S. Wang, G. Junqi, Y. Du, S. Cheng, and X. Li, "A Summaryof Research on Blockchain in the Field of Intellectual Property," (2019), Procedia Computer Science, Volume 147, pp. 191-197, doi: https://doi.org/10.1016/j.procs.2019.01.220

[6] S. Rouhani and R. Deters, "Security, Performance, and Applications ofSmart Contracts: A Systematic Survey," in IEEE Access, vol. 7, pp. 50759-50779, 2019, doi: 10.1109/ACCESS.2019.2911031.

[7] D. Yue, R. Li, Y. Zhang, W. Tian and C. Peng, "Blockchain Based Data Integrity Verification in P2P Cloud Storage," 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS), Singapore, Singapore, 2018, pp. 561-568, doi: 10.1109/PADSW.2018.8644863.

[8] H. Teymourlouei and L. Jackson, "Blockchain: Enhance the Authenticationand Verification of the Identity of a User to Prevent Data Breachesand Security Intrusions," (2019).

[9] X. Zhu, "Blockchain-Based Identity Authentication and IntelligentCredit Reporting," (2020), Journal of Physics: Conference Series, volume1437, 012086, doi: 10.1088/1742-6596/1437/1/012086.

[10] L. M. Arjomandi, G. Khadka, Z. Xiong and N. C. Karmakar, "DocumentVerification: A Cloud-Based Computing Pattern Recognition Approachto Chipless RFID," in IEEE Access, vol. 6, pp. 78007-78015, 2018, doi: 10.1109/ACCESS.2018.2884651.

[11] L. Musarella, F. Buccafurri, G. Lax, and A. Russo, "Ethereum Transactionand Smart Contracts among Secure Identities," (2019).

[12] C. Lakmal, S. Dangalla, C. Herath, C. Wickramarathna, G. Diasand S. Fernando, "IDStack — The common protocol for documentverification built on digital signatures," 2017 National InformationTechnology Conference (NITC), Colombo, 2017, pp. 96-99, doi: 10.1109/NITC.2017.8285654.

[13] M. HamithaNasrin, S. Hemalakshmi, and Prof G. Ramsundar, "AReview on Implementation Techniques of Blockchain enabled SmartContract for Document Verification," International Research Journal ofEngineering and Technology (IRJET), Volume 6, Issue 2, 81, February2019.

[14] O. Ghazali, and O. Saleh, "A Graduation Certificate Verification Modelvia Utilization of the Blockchain Technology," (2018), Journal of Telecommunication, Electronic and Computer Engineering, 10, pp. 29-34.

[15] M. Shah and Dr. Priyanka Kumar, "Tamper Proof Birth Certificate usingBlockchain Technology", International Journal of Recent Technologyand Engineering (IJRTE), Volume 7, Issue 5S3, pp. 95-98, February2019.