IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Document Verification Using Blockchain AND AI

Mrs. Sindhu K, Karthik Naik K, Veda N, Sanjay Akash P, Mahalakshmi A

Assistant Professor, Student, Student, Student, Student
Department Of Artificial Intelligence and Machine Learning
Vijaya Vittala Institute of Technology, Bengaluru, India

Abstract: This project introduces a secure academic document verification system that leverages artificial intelligence and blockchain technology to ensure authenticity and integrity. Authorized administrators upload documents, which are verified using an AI-based method and then hashed using SHA-256. The resulting document hash is stored on the Ethereum blockchain via smart contract interactions, facilitated through MetaMask wallet integration for secure and user-friendly transaction signing. Students can verify documents by entering the hash ID, which is matched against the blockchain without needing access to the original file. This system ensures transparency, tamper resistance, and decentralized trust in academic credentials.

Keywords— IPFS, Blockchain, Verification, Smart Contract

I. INTRODUCTION

In today's digital age, the authenticity of academic and official documents is of paramount importance, yet remains vulnerable to forgery and unauthorized alterations. To address this challenge, our project introduces a secure and efficient document verification system that leverages the combined power of artificial intelligence and blockchain technology. Instead of relying on static or pre-trained models, the system dynamically verifies documents using AI techniques and stores verified information on the Ethereum blockchain via MetaMask integration. By generating a unique hash for each document and linking it to a smart contract, we ensure transparency, immutability, and accessibility. This approach not only empowers institutions with a tamper-proof method for registering documents but also allows students and third parties to verify document legitimacy using just a Doc ID — without the need for re-uploading files.

II. OBJECTIVE

The objective of this project is to develop a secure and transparent document verification system that uses artificial intelligence for document classification and blockchain for tamper-proof record storage. The system aims to enable authorized administrators to upload and verify academic or official documents, while allowing students and third parties to authenticate these documents using a unique hash ID. By integrating AI-based verification and blockchain smart contracts with MetaMask support, the solution ensures authenticity, eliminates the risk of forgery, and promotes trust in digital document handling.

III.LITERATURE SURVEY

The verification of academic and official documents has long relied on manual and centralized methods, which are often slow, error-prone, and vulnerable to tampering. With the emergence of digital technologies, researchers have explored the use of Artificial Intelligence (AI) for document classification and Blockchain for secure data storage. AI models, particularly those based on deep learning, have demonstrated effective performance in image classification tasks, including fake document detection
[1]. Blockchain, on the other hand, offers immutability, decentralization, and transparency, making it ideal for verifying the authenticity of records
[2].In recent years, institutions such as MIT have implemented blockchain-based diploma verification systems to combat credential fraud
[3]. Similarly, the use of smart contracts on Ethereum enables automated and verifiable record-keeping [4]. However, many existing solutions focus solely on storage or analysis. Our proposed system bridges this gap by integrating AI-powered classification with blockchain-based document verification. It also incorporates MetaMask wallet integration for secure, user-driven transactions on the Ethereum network, ensuring both intelligence and integrity in the verification pipeline.

IV. PROPOSED SYSTEM

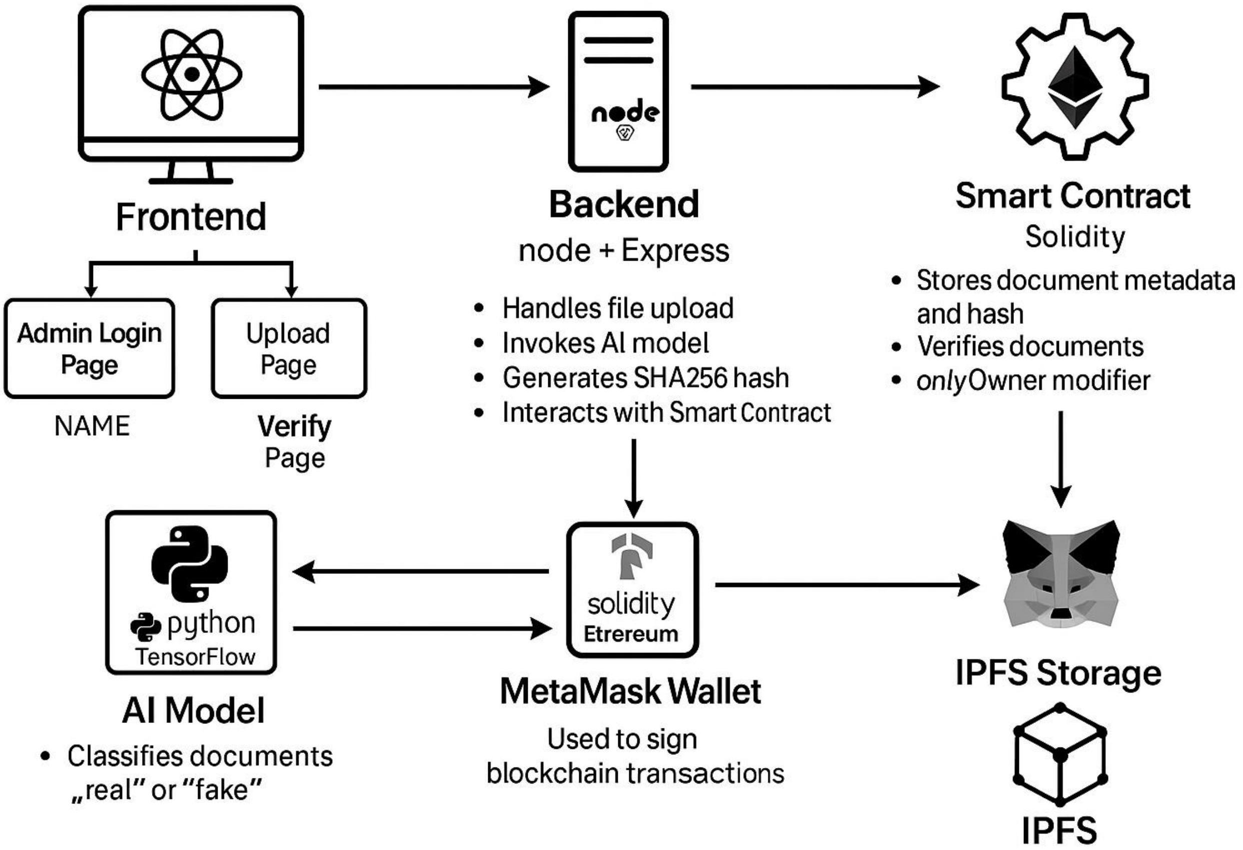


Fig. 1. Proposed System

A system architecture for document verification that combines a React-based frontend with pages for admin login, upload, and verification, a Node.js and Express backend that manages file uploads, invokes a Python TensorFlow AI model for classifying documents as real or fake, generates SHA256 hashes, and interacts with a Solidity smart contract on Ethereum. The smart contract securely stores document metadata and hashes, verifies documents, and restricts certain actions to the owner. MetaMask is used to sign blockchain transactions, while IPFS provides decentralized storage for the documents, ensuring security, authenticity, and tamper-resistance throughout the process

A. Admin login

The process begins with the administrator logging into the system through a secure web portal. This login page is part of the frontend built using React. Administrators are required to enter valid credentials, which are authenticated via a backend API. The backend, powered by Express.js, checks the credentials against stored admin records in a database. If the credentials are valid, a session or token is generated to maintain secure access during the session. Only after successful login can the admin access privileged features like document uploads and verification control.

B. Uploading The Document

After logging in, the administrator gains access to a dashboard interface where documents can be uploaded for verification. This dashboard provides a user-friendly form to submit documents—such as certificates or IDs. The uploaded file is sent to the backend using a secure API. The backend uses middleware (like Multer) to handle file uploads and temporarily stores them on the server. Once stored, the backend initiates the document verification process.

C. AI-Based Document Analysis

Once the document is received, it is passed to the AI model for analysis. This model is developed using Python and TensorFlow/Keras, and is trained to detect features typical of forged or manipulated documents. The backend triggers a Python script (predict.py) which loads the model and processes the uploaded file. The model returns:

A label (real or fake) indicating whether the document appears authentic,

A confidence score that quantifies how certain the model is about its prediction.

This AI-powered step helps automate the document vetting process and reduce the risk of approving forged records.

D. Storage on IPFS (If Verified)

If the document is classified as real, the next step is to securely store it on IPFS (Inter Planetary File System). IPFS is a decentralized storage protocol that ensures the file cannot be modified or tampered with. The backend reads the document and uploads it to IPFS using a service like Infura. Upon successful upload, IPFS returns a CID (Content Identifier), which uniquely represents the file

E. Recording Metadata on the Blockchain

After the document is stored on IPFS, the system records its metadata—including the document ID, IPFS CID, verification result, and confidence score—onto the Ethereum blockchain. This is done through a smart contract written in Solidity. The backend interacts with this contract using Ethers.js, sending a transaction that writes the metadata into a blockchain ledger. This process ensures that the document's verification record is immutable and cannot be altered by any party, making the verification highly trustworthy.

F. Generating a Document ID

Once the blockchain entry is complete, the system generates a unique Document ID. This ID is a reference number tied to the on-chain metadata and is used by students or verifiers to check the document's authenticity. This ID is displayed to the admin and may also be shared with the student.

G. Student Document Verification

On the user side, students or third-party verifiers visit the verification page. This interface allows them to enter the unique Document ID they've received. Upon submission, the frontend makes a request to the backend, which then fetches the document metadata directly from the blockchain via the smart contract. The result displayed includes:

- ➢ Whether the document is real or fake,
- ➢ The confidence score from the AI model,
- ➢ A link to the original document on IPFS.

This empowers students to prove the authenticity of their documents instantly, and verifiers to independently validate documents without needing direct confirmation from the issuing authority.

V. SOFTWARE REQUIREMENTS AND USED TECHNOLOGIES

A. Frontend Development Our frontend is developed using advanced frameworks such as React.js, complemented by HTML, CSS, and JavaScript.

B. Backend Development Backend development is primarily done in Java using Spring Boot. We have also used Python and the Flask framework. The backend services are communicated with via Axios.

C. Blockchain Integration

- Web3.js It is a decentralized web, where users interact with each other and applications without the need for intermediaries.
- Solidity Use Web3.js or equivalent libraries to interact with the blockchain from your web application.
- Smart Contracts A decentralized computer program running on blockchain network that automatically and deterministically executes agreements based on predefined conditions.

D. Databases

- MySQL Popular open-source relational database management system using for storage of the various records .
- Pinata IPFS cloud Pinata is a cloud service for keeping your NFT. This plugin makes NFT file storage easy for everyone.

E. Development Tools Integrated Development Environment (IDE), PyCharm, Vs Code. Package Managers npm (Node Package Manager) for managing frontend dependencies. Postman API development and testing tool for backend APIs. All these technologies have been used in the development of the system.

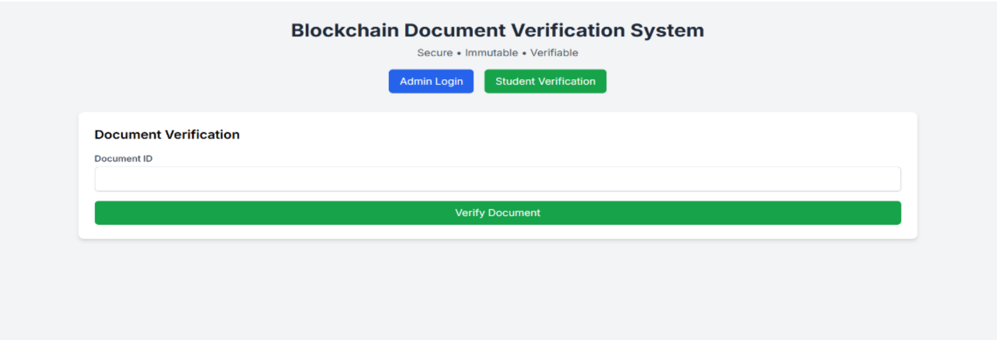
VI. FLOW OF SYSTEM

The system operates through the following flow:

- Admin Login: An administrator securely logs into the system.
- Document Upload: The administrator uploads a document (JPEG, JPG, PNG, or PDF).
- AI Verification: The uploaded document is sent to a mock AI model to check its authenticity.
- Blockchain Integration: If the AI model verifies the document, it is added to a mock blockchain, creating a secure, immutable record.
- Document Verification: A student or other party accesses the verification page and enters the document ID.
- Document Display: The system retrieves the document's information from the blockchain and displays it, along with its blockchain address and verification status.

VII.RESULTS

1) Main Dashboard
The main dashboard of the "Blockchain Document Verification System." At the top, there are buttons for "Admin Login" and "Student Verification", indicating the two primary access points. The system is branded as "Secure - Immutable - Verifiable," highlighting its key features.



Blockchain Document Verification System

Secure • Immutable • Verifiable

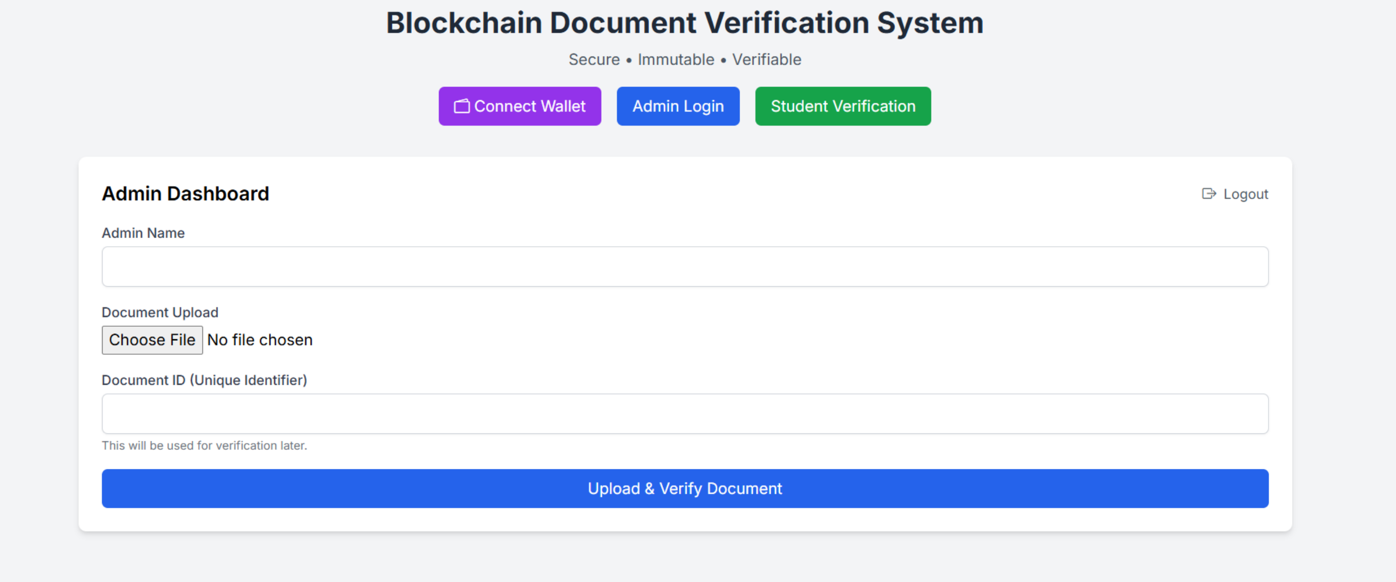
Document Verification

Document ID

Fig. 2. Main Dashboard

2) Dashboard of Administrator

Admin Dashboard includes options to "Connect Wallet," "Admin Login," and "Student Verification." The dashboard displays an "Admin Name" field and a "Logout" link. A "Document Upload" section is visible, allowing the admin to choose a file, and a "Document ID (Unique Identifier)" field is also present. The dashboard concludes with an "Upload & Verify Document" button.



Blockchain Document Verification System

Secure • Immutable • Verifiable

Admin Dashboard

Admin Name

Document Upload

No file chosen

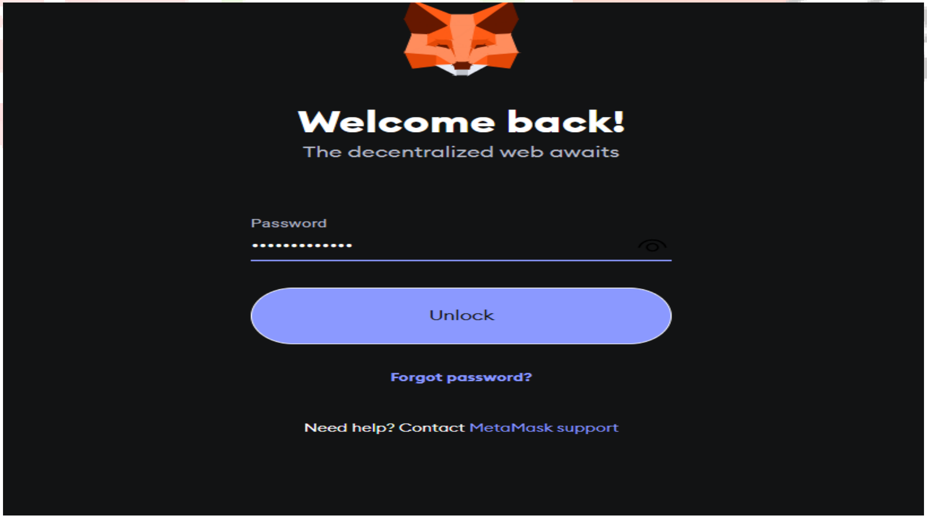
Document ID (Unique Identifier)

This will be used for verification later.

Fig. 3. Dashboard of Administrator

3) Connecting Wallet

The system prompts the administrator to establish a secure link between their MetaMask wallet and the document verification application. The MetaMask interface is presented, showcasing the available accounts within the wallet. The administrator selects the appropriate account, identified by its address (e.g., 0x94E66...6dBCB), to enable secure transaction signing and blockchain interactions within the document verification system. By confirming this connection, the application gains the necessary permissions to conduct operations on the blockchain using the administrator's designated account.



Welcome back!

The decentralized web awaits

Password

••••••••••••••

Need help? Contact MetaMask support

Fig.4.Login in to MetaMask.

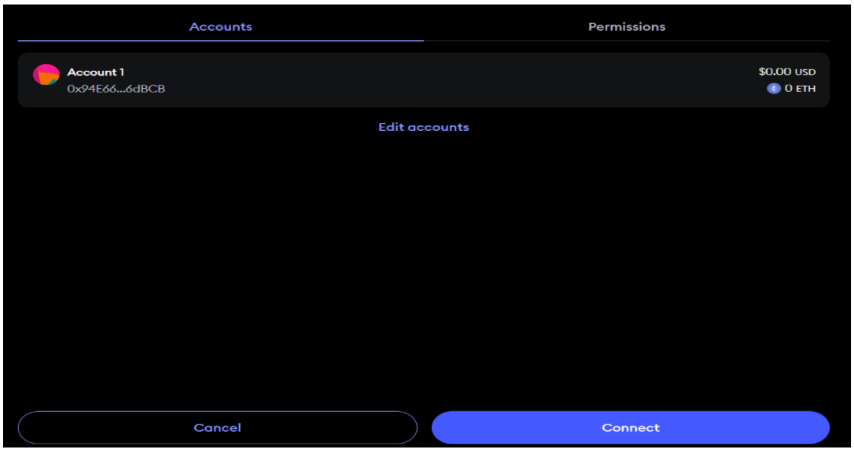
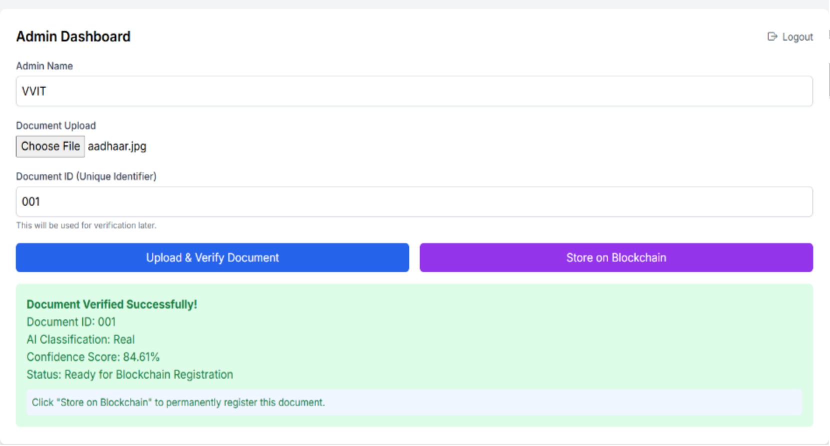


Fig. 5. Connection to wallet

4) Document Verification and Storing in Blockchain.

First, the administrator logs into the system and accesses the document upload feature. The admin uploads a document and assigns it a unique identifier. Once uploaded, the system employs an AI model to automatically assess the authenticity of the document. Upon successful AI verification, the status is updated, indicating the document is ready for blockchain registration. The administrator then initiates the storage of the document on the blockchain by clicking the appropriate button. A confirmation message indicates that the transaction was successful and the document has been permanently registered on the blockchain. Key details like the transaction hash and IPFS hash are then displayed. The system confirms that the document has been permanently registered on the blockchain and can now be verified by anyone using the IPFS URL. This entire process leverages blockchain technology to ensure the document's immutability and verifiable authenticity, enhancing trust and security.



Admin Name: VVIT

Document Upload: aadhaar.jpg

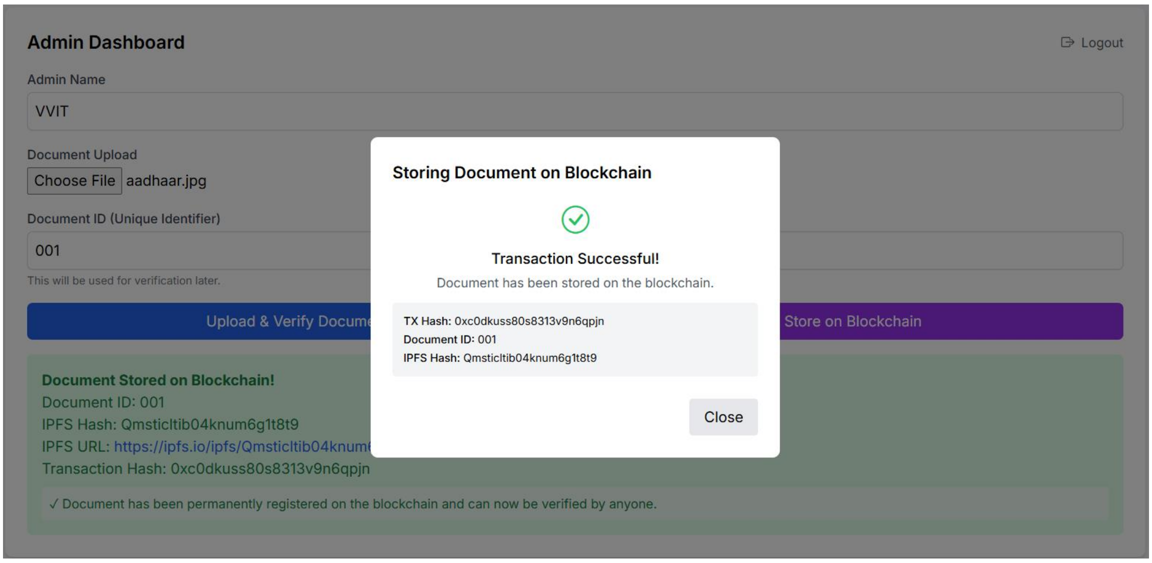
Document ID (Unique Identifier): 001

This will be used for verification later.

Document Verified Successfully!
Document ID: 001
AI Classification: Real
Confidence Score: 84.61%
Status: Ready for Blockchain Registration

Click "Store on Blockchain" to permanently register this document.

Fig.6. Document Upload and Verification



Admin Dashboard

Admin Name: VVIT

Document Upload: aadhaar.jpg

Document ID (Unique Identifier): 001

This will be used for verification later.

Storing Document on Blockchain

Transaction Successful!

Document has been stored on the blockchain.

TX Hash: 0xc0dkuss80s8313v9n6qpjn
Document ID: 001
IPFS Hash: Qmsticltib04knum6g1t8t9

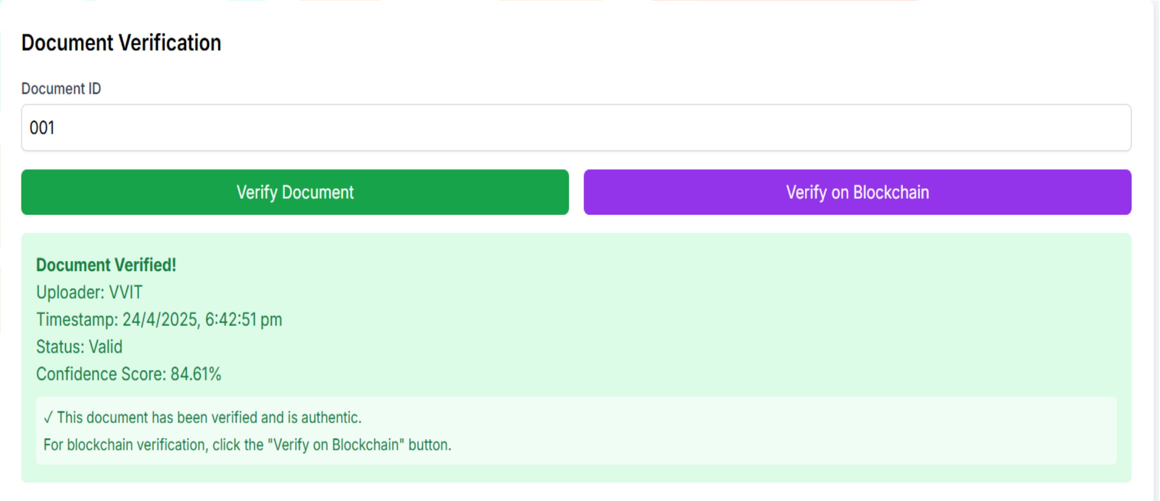
Document Stored on Blockchain!
Document ID: 001
IPFS Hash: Qmsticltib04knum6g1t8t9
IPFS URL: https://ipfs.io/ipfs/Qmsticltib04knum
Transaction Hash: 0xc0dkuss80s8313v9n6qpjn

✓ Document has been permanently registered on the blockchain and can now be verified by anyone.

Fig.7.Storing Document on Blockchain

5) Student Verification

The student can verify the document uploaded by the admin, knowing who uploaded the document and which document is uploaded, weather it is real or fake as of predicted by the model(ai).The student can also verify that is it stored on Blockchain or not by clicking the verify on blockchain button.



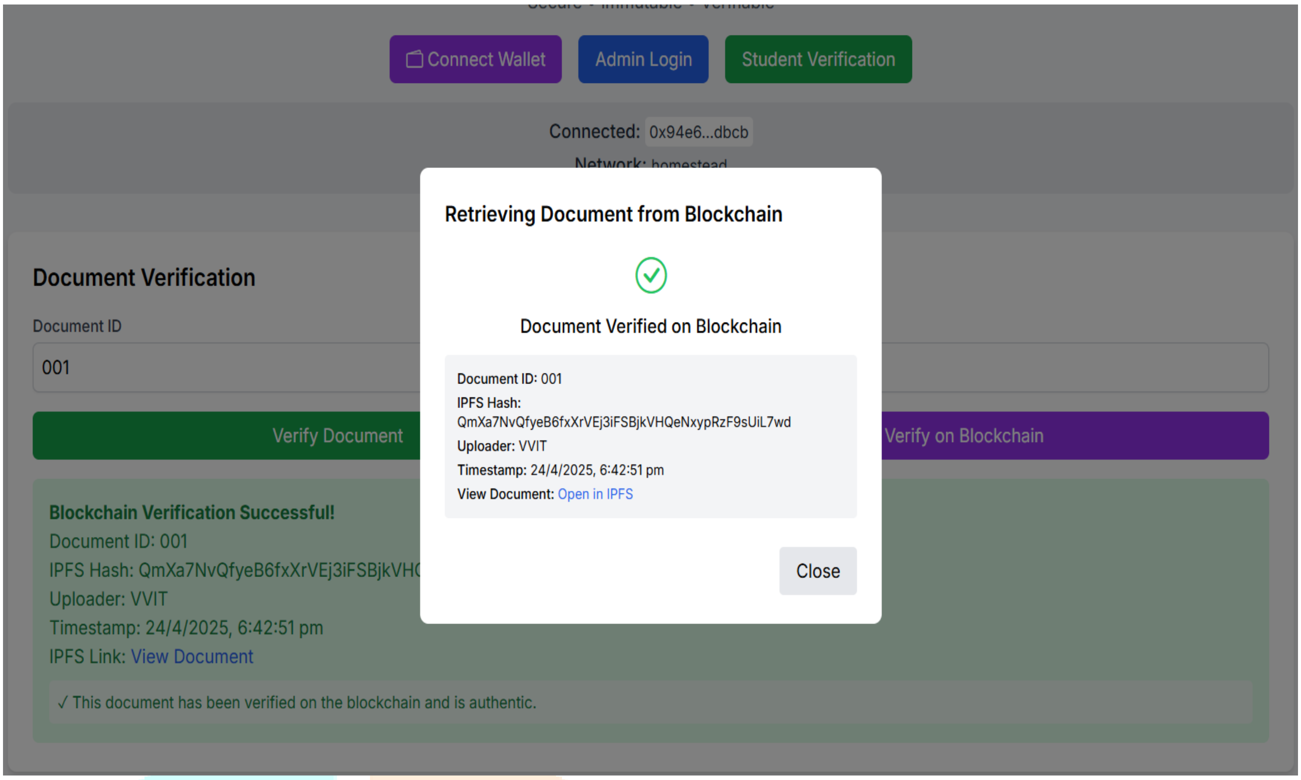
Document Verification

Document ID: 001

Document Verified!
Uploader: VVIT
Timestamp: 24/4/2025, 6:42:51 pm
Status: Valid
Confidence Score: 84.61%

✓ This document has been verified and is authentic.
For blockchain verification, click the "Verify on Blockchain" button.

Fig.8.Document Verification by Student



Connected: 0x94e6...dbcb
Network: homestead

Document Verification

Document ID
001

Blockchain Verification Successful!
Document ID: 001
IPFS Hash: QmXa7NvQfyeB6fxXrVEj3iFSBjkVH
Uploader: VVIT
Timestamp: 24/4/2025, 6:42:51 pm
IPFS Link: View Document

✓ This document has been verified on the blockchain and is authentic.

Retrieving Document from Blockchain

Document Verified on Blockchain

Document ID: 001
IPFS Hash: QmXa7NvQfyeB6fxXrVEj3iFSBjkVHQeNxypRzF9sUiL7wd
Uploader: VVIT
Timestamp: 24/4/2025, 6:42:51 pm
View Document: Open in IPFS

Fig.9.Document Verification on Blockchain

VIII. CONCLUSION AND FUTURE SCOPE

The developed system effectively combines AI-based classification with blockchain-enabled verification to offer a robust solution for academic document authentication. By eliminating manual intervention and leveraging secure technologies like smart contracts and cryptographic hashing, it ensures document integrity and builds trust among institutions and stakeholders. The system is designed with a student-verifier model where only authenticated administrators can upload and register documents, while students can independently verify them using a document hash, ensuring both access control and user empowerment.

Looking ahead, the platform holds strong potential for scalability and wider adoption. Integration with decentralized storage services like IPFS could further reduce reliance on centralized servers while preserving privacy. Advanced features such as institution dashboards, automated credential issuance, and blockchain interoperability could transform this into a standard framework for global educational verification. Future improvements may also include multi-chain support, mobile-friendly access, and enhanced analytics for institutions to track document requests and trends securely.

IX. REFERENCES

[1] S. Kadwe D. Dharmaraj, and D. Kharat, “EduDocs: Document Verification using Blockchain,” Proc. IEEE Int. Conf. Blockchain and Distributed Systems Security (ICBDS), 2024.

[2] H. Gaikwad, N. D’Souza, R. Gupta, and A. K. Tripathy, “A Blockchain-Based Verification System for Academic Certificates,” Int. Conf. Smart Computing and Communication (ICSCAN), Puducherry, India, 2021.

[3] A. Chowdhary, S. Agrawal, and B. Rudra, “Blockchain based Framework for Student Identity and Educational Certificate Verification,” Int. Conf. Electronics, Systems and Communication (ICESC), Coimbatore, 2021.

[4] A. Singh, S. Chauhan, and A. K. Goel, “Blockchain Based Verification of Educational and Professional Certificates,” Int. Conf. Communication Systems and Computing (ICCSC), Thiruvananthapuram, 2023.

[5] “University of Nicosia Issues Block-Chain Verified Certificates,” CoinDesk. [Online]. Available: https://www.coindesk.com/markets/2014/09/16/university-ofnicosia-issues-block-chain-verified-certificates/

[6] R. Arenas and P. Fernandez, “CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials,” Proc. IEEE ICE/ITMC, 2018.

[7] T. Kanan, A. T. Obaidat, and M. Al-Lahham, “SmartCertBlockChain for Educational Certificates,” Proc. IEEE JEEIT, 2019.

[8] M. U. Abdullahi, R. H. Umar, and A. M. Usman, “Certificate Generation and Verification System Using Blockchain Technology and QR Code,” IOSR J. Computer. Eng., vol. 24, no. 3, pp. 1-10, 2022.

[9] S. Kalaivanan, “Quality of Service and Priority Aware Models for Mobile Ad Hoc Networks,” New Horizon College of Engineering, 2021.

[10] K. V. Divya, S. Krithika, and A. Ramya, “A Meta-Analysis on Blockchain Technology and Bitcoins,” Int. J. Recent Advances in Science, Engineering and Technology (IJRASET), vol. 7, issue 5, May 2019.