IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Tamper-Proof Certificate Authentication Using AI And Blockchain

[1]Amruth V, [2]Nikhil C K, [2]Ananya M Rao, [2]Kruthika, [2]Muizun Mujeeb

[1]Assistant Professor, Department of Information Science and Engineering, Maharaja Institute of Technology Mysore

[2]Student, Department of Information Science and Engineering, Maharaja Institute of Technology Mysore,

Abstract: This study has been undertaken to investigate the determinants of stock returns in Karachi Stock Exchange (KSE) using two assets pricing models the classical Capital Asset Pricing Model and Arbitrage Pricing Theory model. To test the CAPM market return is used and macroeconomic variables are used to test the APT. The macroeconomic variables include inflation, oil prices, interest rate and exchange rate. For the very purpose monthly time series data has been arranged from Jan 2010 to Dec 2014. The analytical framework contains**.**

Index Terms **-** Artificial Intelligence, Blockchain, Certificate Verification, OCR, Smart Contracts, IPFS, Document Forensics

I. INTRODUCTION

Traditional methods of validating academic and professional certificates usually involve inspecting physical documents or communicating directly with the issuing authority. While these methods are common, they take a lot of time, vary from one institution to another, and are easy to manipulate because digital editing tools are becoming more advanced. Current digital verification options offer small improvements but still rely on centralized databases or basic QR scans. These can fail if someone has tampered with the certificate itself. To address these issues, this work presents an integrated system using Artificial Intelligence and Blockchain that checks both the visual integrity of the certificate and its authenticity in a decentralized setting.

Current methods do not provide enough security and lack ways to detect tampering. Digital documents and scanned certificates can be easily altered with modern editing software. Most institutions verify only the visible text, so subtle but important changes—such as font mismatches, forged signatures, missing seals or watermarks, and layout problems often go unnoticed. Without AI-based forensic analysis, it is hard to spot sophisticated forgery. Furthermore, centralized verification databases are open to cyberattacks and unauthorized access. If a database is compromised, it allows for unnoticed changes to stored records, damaging trust in the verification process. In contrast, the proposed model uses Blockchain and IPFS to remove single points of failure, ensure transparency, and provide tamper-proof storage for certificate records. This greatly improves the reliability and trustworthiness of certificate verification.

II. OBJECTIVES

- **Understanding the Impact of Fake Certificates:** Analyzing how forged certificates affect organizations, recruitment processes, and overall trust in academic and professional records.
- **AI-Based Fake Certificate Detection:** Designing an AI model that detects manipulated certificates by examining text, fonts, signatures, layout, and other document features.

- **Blockchain-Driven Secure Storage**: Implementing a decentralized blockchain system to store certificate data in a tamper-proof and transparent manner.

- **User-Friendly Web Verification Platform:** Developing an interactive platform that enables students, employers, and institutions to upload, verify, and access certificates easily with real-time authentication results.

- **QR-Enabled Instant Verification:** Generating QR codes that allow users to instantly retrieve and verify certificate details stored on the blockchain.

III. Literature Review

Recent research shows a growing use of AI and blockchain technologies to improve certificate security. Afrianto and Heryanto [1] demonstrated that public blockchain infrastructure can store certificate details. This reduces reliance on centralized authorities. Priyadarshini et al. [2] proposed a blockchain verification model that can validate both certificates and issuing bodies. Other studies combined distributed storage with blockchain. Rajput et al. [3] introduced a blockchain and IPFS system for securely managing birth certificates using smart contracts. Luo et al. [4] highlighted challenges in validating digital credentials by examining PKI mechanisms used by browsers.

QR-based verification methods have also gained attention. Noorhizam et al. [5] created a hybrid blockchain and QR model for validating doctoral certificates without needing institutional communication. Tariq et al. [6] designed Cerberus, a permissioned blockchain system that supports revocation and multi-party validation. Rahaman et al. [7] proposed a blockchain system that can correct certificate errors, while Dewangan et al. [8] combined EdDSA signatures with IPFS for privacy-preserving storage. AI-driven forgery detection techniques have also evolved. Sun et al. [9] introduced a multi-level attention network for detecting synthetic certificates. Joren et al. [16] proposed OCR-graph features to assess document integrity. Their findings confirm that AI significantly improves the detection of subtle visual changes.

Researchers have also looked into institution-based frameworks. Faaroek et al. [10] designed an academic portal with blockchain-enabled certificate storage. Lutfiani et al. [11] created a fraud prevention model using hashed records and digital signatures. Garba et al. [12], [19] proposed LightLedger, a decentralized authentication structure suitable for multiple domains. Other approaches, like AES-encrypted QR verification by Oyediran et al. [13] and neural-network-based fraud detection by Isizoh et al. [14], showcase the growing variety in this field. While existing solutions offer strong security, most only address one aspect, either forgery detection or blockchain integrity. This work aims to bridge that gap by providing a unified system that validates a document's authenticity using AI while ensuring its tamper-proof status through blockchain storage.

IV. System Design And Methodology

Hardware/Software Components

- **AI Forgery Detection Model:** Examines images for manipulation in structure, text, seals, watermarks, and signatures.

- **OCR Engine:** Extracts textual and layout information for accurate AI analysis.

- **Blockchain Network (Ethereum):** Stores certificate hashes for immutability.

- **Smart Contracts:** Govern certificate issuing, verification, and record retrieval.

- **IPFS Storage:** Preserves original certificates in a distributed environment.

- **QR Generator:** Creates scannable identifiers linking to blockchain or IPFS data.

- **Web Frontend:** Interface for certificate issuance, upload, and verification.
- **Backend Server:** Connects AI, IPFS, smart contracts, and QR modules.

Blockchain & Integrity Subsystem

- **Hash Generation:** Generates a unique SHA-256 hash for every issued certificate, ensuring that even a tiny modification in the document creates a completely different hash — making forgery instantly detectable.
- **Smart Contract Record:** Stores the generated hash, issuer information, certificate metadata, and timestamp securely on the blockchain, maintaining a permanent integrity record.
- **IPFS Integration:** Uploads and stores the original certificate file in IPFS and returns a CID, guaranteeing decentralized access and long-term preservation of the document.
- **QR Encoding:** Embeds either the blockchain transaction hash or the IPFS CID into a QR code printed on the certificate, enabling fast access to its validation source.
- **Decentralized Verification:** During verification, the verifier scans the QR code to compare on-chain certificate hash with the uploaded certificate. Any mismatch reveals manipulation or fraud immediately, ensuring fully transparent and trustworthy verification.

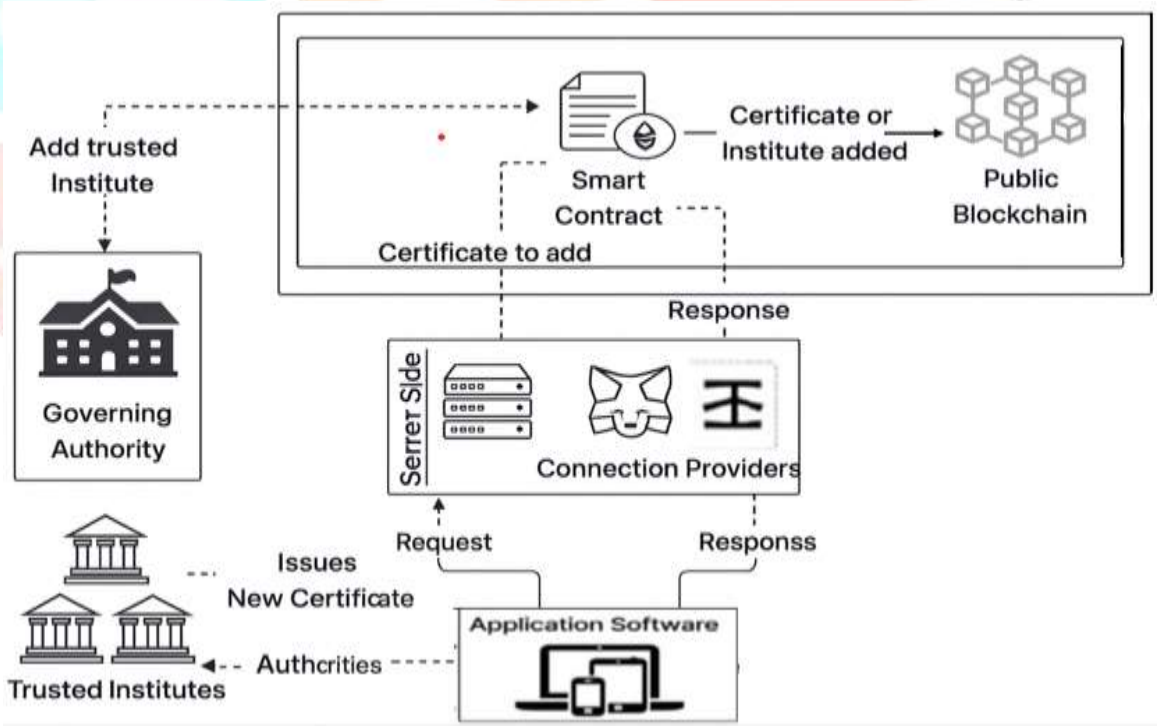

Fig. 1. Block Diagram of Certificate Issuer

AI Verification Subsystem

- **Preprocessing:** This step improves the quality of the uploaded certificate image by adjusting brightness, contrast, resolution, and orientation to ensure consistency. It removes noise and improves clarity, allowing for accurate further analysis.

- **OCR + Feature Extraction:** This process uses Optical Character Recognition and visual analysis techniques to extract text, layout structure, seals, logos, and formatting details from the certificate. The extracted features serve as key indicators to evaluate authenticity.

- **Forgery Detection:** A specialized machine learning model examines the extracted features to find signs of tampering. This includes pixel-level irregularities, modified text blocks, mismatched fonts, forged signatures, missing watermarks, and disrupted layout patterns**.**

- **Confidence Score:** This generates an authenticity or trust score based on how similar the uploaded certificate is to expected patterns of genuine documents. A higher score indicates legitimacy, while a lower score suggests potential manipulation.

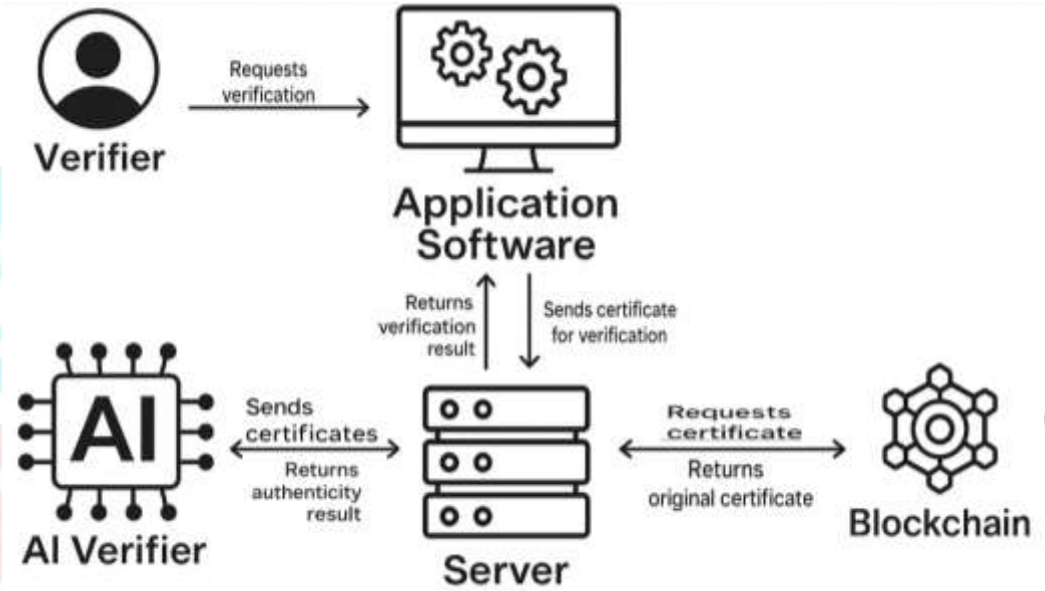

Fig. 2 Block Diagram of AI Certificate Verifier

V. WORKING PRINCIPLE

The system combines AI-based forgery detection with decentralized blockchain validation to ensure high accuracy and security.

1. QR-Based Instant Validation:

Every certificate contains a unique QR code that links directly to its blockchain record or IPFS-stored data. When someone scans the QR code, the system quickly retrieves the original certificate information without needing manual lookup. This makes authentication fast and convenient.

2. Blockchain Hash Verification:

During verification, the system creates a new hash from the uploaded certificate and checks it against the hash stored on the blockchain. If both hashes match, the system confirms the certificate has not been altered. A mismatch signals potential forgery or modification right away.

3. Certificate Upload & Preprocessing:

The verifier uploads the certificate to the system, which automatically removes noise, improves resolution, and adjusts orientation. The system then uses OCR to extract the text and structure needed for AI-based analysis.

4. AI Content Verification:

The AI Verifier examines various features of the certificate, such as layout structure, fonts, text spacing, signature patterns, seals, logos, and watermark textures, to find inconsistencies. It assigns a confidence score that suggests how likely it is that the certificate is genuine or has been tampered with.

5. Final Result Compilation:

The system combines outputs from both verification layers: blockchain hash matching and AI-based content analysis. It then generates a final authentication status.

Based on the findings, the system categorizes the certificate as:

- **Authentic**
- **Partially Mismatched**
- **Fake/Manipulated**

VI. Results And Discussion

All components of the proposed system were successfully implemented and evaluated. The AI module showed strong effectiveness in detecting forged certificates by identifying altered text areas, font inconsistencies, and tampered signatures with high precision. The blockchain subsystem stored certificate hashes reliably in a way that prevents unauthorized changes to issued records.

Verification requests were processed smoothly through the backend, which retrieved blockchain data and combined it with AI analysis to produce accurate and dependable results. The QR-based validation mechanism allowed instant access to certificate information, and the web interface offered a smooth user experience for students, issuing authorities, and verifiers. Overall, the system achieved higher detection accuracy, reduced human involvement, improved certificate security, and ensured quick and automated validation.

Additionally, the modular setup supports future improvements, including the integration of more advanced AI models, multi-chain compatibility, and expanded institutional onboarding. The evaluation confirms that the proposed framework is scalable, strong, and capable of real-world use across academic and professional environments.

VII. Conclusion And Future Work

The proposed system offers a smart and effective way to authenticate certificates securely by combining AI-based forgery detection with decentralized storage on blockchain. It checks both the visual details of the certificates and their cryptographic records. This approach prevents tampering, duplication, and unauthorized creation of certificates. QR-based instant validation and IPFS support make access simpler, increase transparency, and ensure that data cannot be changed. Test results show that the system is accurate, verifies quickly, and is more secure than traditional manual or centralized validation methods. These strengths highlight how practical and dependable this system is for real-world use in institutions.

While the system performs well, there are still areas for improvement. Future efforts could involve using better deep-learning models to spot more sophisticated and AI-generated forgeries. It could also include incorporating decentralized identity (DID) protocols for secure stakeholder authentication and enabling multi-chain interoperability to allow smooth cooperation between universities, government bodies, and businesses.

Additionally, creating web-based verification apps and streamlining certificate issuance processes on a large scale could make the system easier to use and encourage wider adoption. With these improvements, the framework could develop into a secure and globally usable digital credential system.

REFERENCES

[1] I. Afrianto and Y. Heryanto, "Design and Implementation of Work Training Certificate Verification Based on Public Blockchain Platform," vol. 10, 2025.

[2] R. Priyadarshini, R. Pandey, K. C. Ankit, D. Bhandari, B. Khadka, R. K. Barik, and M. J. Saikia, "A Faster, Integrated, and Trusted Certificate Authentication and Issuer Validation System Based on Blockchain," vol. 13, pp. 27037–27049, Feb. 2025.

[3] A. Rajput, K. Prajapati, J. J. Hathaliya, N. K. Jadav, S. Tanwar, and D. Garg, "Artificial Intelligence and Blockchain-enabled Secure Birth Certificate Management System," *IEEE ISCS Conference*, 2024.

[4] Z. Luo, J. Amann, and M. Vallentin, "On the Complexity of the Web's PKI: Evaluating Certificate Validation of Browsers," 2024.

[5] N. K. N. Noorhizam *et al.*, "Verification of Ph.D. Certificate Using QR Code on Blockchain Ethereum," 2023.

[6] A. Tariq, H. B. Haq, and S. T. Ali, "Cerberus: A Blockchain-Based Accreditation and Degree Verification System," vol. 10, no. 4, pp. 1503–1513, Aug. 2023.

[7] M. M. Rahaman, S. R. Shihab, M. K. Tonmoy, and R. Farhana, "Blockchain-based Certificates Authentication System with Enabling Correction," 2023.

[8] N. K. Dewangan, P. Chandrakar, S. Kumari, and J. J. P. C. Rodrigues, "Enhanced Privacy-Preserving in Student Certificate Management in Blockchain and Interplanetary File System," *Multimedia Tools and Applications*, vol. 82, pp. 12595–12614, Sep. 2022.

[9] Y. Sun, R. Ni, and Y. Zhao, "MFAN: Multi-Level Features Attention Network for Fake Certificate Image Detection," 2022.

[10] S. A. Faaroek, A. S. Panjaitan, Z. Fauziah, and N. Septiani, "Design and Build Academic Website with Digital Certificate Storage Using Blockchain Technology," 2022.

[11] N. Lutfiani, D. Apriani, E. A. Nabila, and H. L. Juniar, "Academic Certificate Fraud Detection System Framework Using Blockchain Technology," vol. 10, 2022.

[12] A. Garba, Z. Chen, Z. Guan, and G. Srivastava, "LightLedger: A Novel Blockchain-Based D omain Certificate Authentication and Validation Scheme," 2021.

[13] M. Oyediran, E. W. Adedayo, O. O. Olamide, J. A. Awokola, and Q. B. Sodipo, "Design and Implementation of a Certificate Verification System Using Quick Response (QR) Code," 2021.

[14] A. N. Isizoh *et al.*, "Certificate Fraud Detection Using Artificial Intelligence Technique," 2021

[15] J. G. Dongre, S. M. Tikam, K. T. Patil, and V. B. Gharat, "Education Degree Fraud Detection and Student Certificate Verification Using Blockchain," 2020.

[16] H. Joren, O. Gupta, and D. Raviv, "OCR Graph Features for Manipulation Detection in Documents," 2020.

[17] W. Ahmad, R. Laborde, D. W. Chadwick, R. Venant, A. Benzekri, E. Billoir, and O. Alfandi, "On the Validation of Web X.509 Certificates by TLS Interception Products," vol. 10, 2020.

[18] A. Rajput, K. Prajapati, J. J. Hathaliya, N. K. Jadav, S. Tanwar, and D. Garg, "Artificial Intelligence and Blockchain-enabled Secure Birth Certificate Management System," *IEEE ISCS Conference*, 2020.

[19] A. Garba, Z. Chen, Z. Guan, and G. Srivastava, "LightLedger: A Novel Blockchain-Based Domain Certificate Authentication and Validation Scheme," vol. 8, no. 2, pp. 1698–1710, Apr.–Jun. 2019.

[20] J. Feist, G. Grieco, and A. Groce, "Slither: A Static Analysis Framework for Smart Contracts," 2019.