A SYSTEM TO COMBAT FAKE CERTIFICATES IN EDUCATION SECTOR

Project Reference No.: *49S_BE_4641*

College : REVA University, Bengaluru
Branch : Department of Electronics and Communication Engineering
Guide : Prof. Md Tauseef
Student(s) : Ms. Saba Mulla
Ms. Shreya A
Mr. Sujal Naik
Ms. A V Sanjana

Keywords:

Optical Character Recognition (OCR), Blockchain, Certificate Verification, AI-based Validation, Academic Integrity, Gemini API, Smart Contracts, Image Processing, Authentication, Digital Records.

Introduction:

1. With the rapid digitalization of academic records, educational institutions increasingly rely on electronic documents for storing and sharing certificates. While this transition has improved accessibility and efficiency, it has also led to a significant rise in fake and tampered academic credentials. Employers, universities, and government agencies often face challenges in verifying the authenticity of submitted certificates due to the lack of a standardized and automated verification system.
2. Traditional verification methods, such as manual checks, email confirmations, and phone verification, are time-consuming, inconsistent, and prone to human error. These methods are not scalable, especially when handling large volumes of applications. Moreover, the absence of a unified system leads to delays and unreliable decision-making in recruitment and admissions processes.
3. To address these challenges, this project proposes an **A SYSTEM TO COMBAT FAKE CERTIFICATES IN EDUCATION SECTOR**, a web-based platform that automates certificate verification using advanced technologies. The system integrates Optical Character Recognition (OCR) to extract data from certificates and utilizes Gemini API-based AI validation to analyse and verify authenticity. Additionally, blockchain and QR-based verification mechanisms can be used for digital certificates to ensure tamper-proof validation.
4. The proposed solution enhances transparency, reduces manual effort, and provides a fast, reliable, and scalable approach to certificate verification. It aims to improve trust and integrity in academic and professional ecosystems.

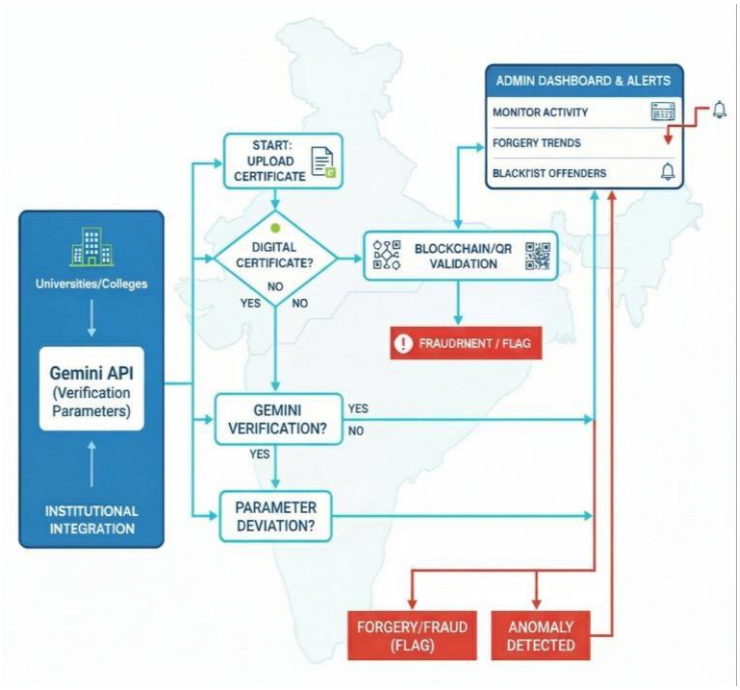

Figure 1: AI & Blockchain Fraud Detection Process

Objectives:

1. To develop a secure platform for academic certificate verification
2. To automate data extraction using OCR
3. To detect forged certificates using AI techniques
4. To ensure tamper-proof validation using Blockchain

Methodology:

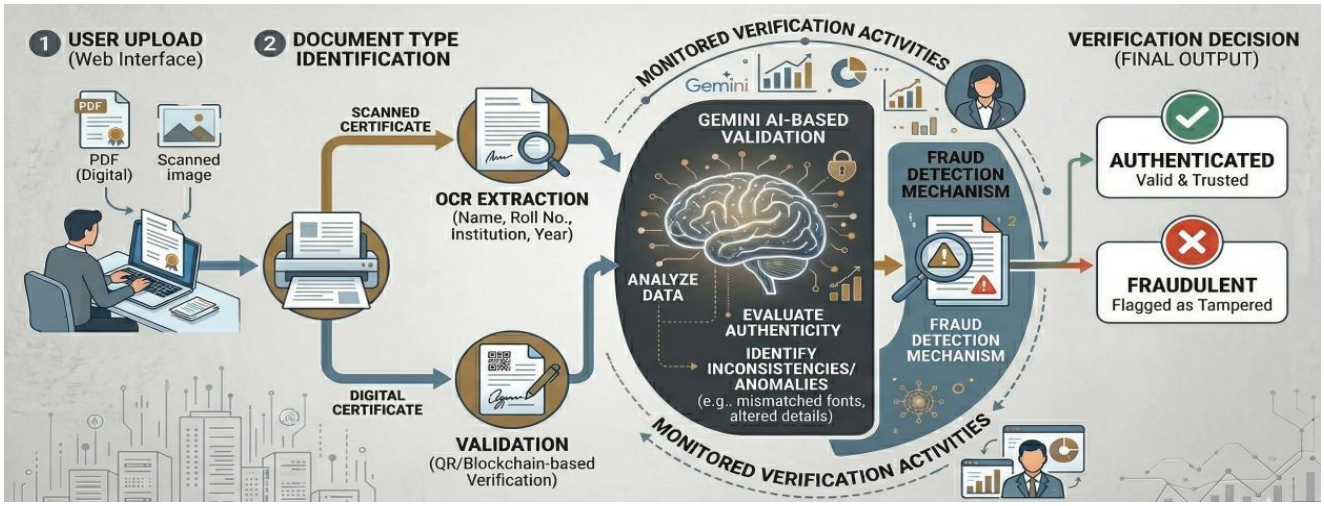

Figure 2: End-to-End Academic Certificate Authentication Process

1. The proposed system follows a structured and systematic approach for verifying academic certificates. The process begins with the user uploading a certificate through a web-based interface. The uploaded file can be either a digital certificate (PDF) or a scanned image.

2. Once the certificate is uploaded, the system identifies whether it is a digital or scanned document. For scanned certificates, OCR technology is used to extract key details such as student name, roll number, institution name, and year of passing. This extracted information is then processed and structured for further validation.
3. Instead of relying on traditional database matching, the system uses Gemini API-based AI validation to analyse the extracted data. The AI evaluates the authenticity of the certificate by identifying inconsistencies, irregular patterns, or anomalies that may indicate tampering or forgery.
4. For digital certificates, QR code or blockchain-based verification mechanisms can be used to validate authenticity. These techniques ensure that the certificate has not been altered and maintain data integrity.
5. The system also includes a fraud detection mechanism that flags suspicious certificates. All verification activities are monitored through the system, and a final decision is generated. The output classifies the certificate as **Authenticated**, **Fraudulent**, or **Needs Review**.
6. This methodology ensures a fast, automated, and reliable verification process while minimizing human intervention.

Result and Conclusion:

1. The developed system demonstrates an effective solution for automating academic certificate verification. The integration of OCR and AI-based validation enables accurate extraction and analysis of certificate data. The system successfully processes both digital and scanned certificates and provides quick verification results.
2. Testing was conducted using a combination of genuine and forged certificates to evaluate system performance. The OCR module achieved high accuracy in extracting relevant details, while the AI-based validation effectively identified inconsistencies in fake certificates. The system demonstrated the ability to detect tampered or manipulated documents with reliable accuracy.
3. The use of advanced technologies reduces dependency on manual verification methods and significantly improves processing speed. The system also provides consistent and unbiased verification results.
4. In conclusion, the project successfully addresses the problem of fake academic certificates by providing a secure, automated, and scalable solution. It enhances trust, transparency, and efficiency in academic verification processes.

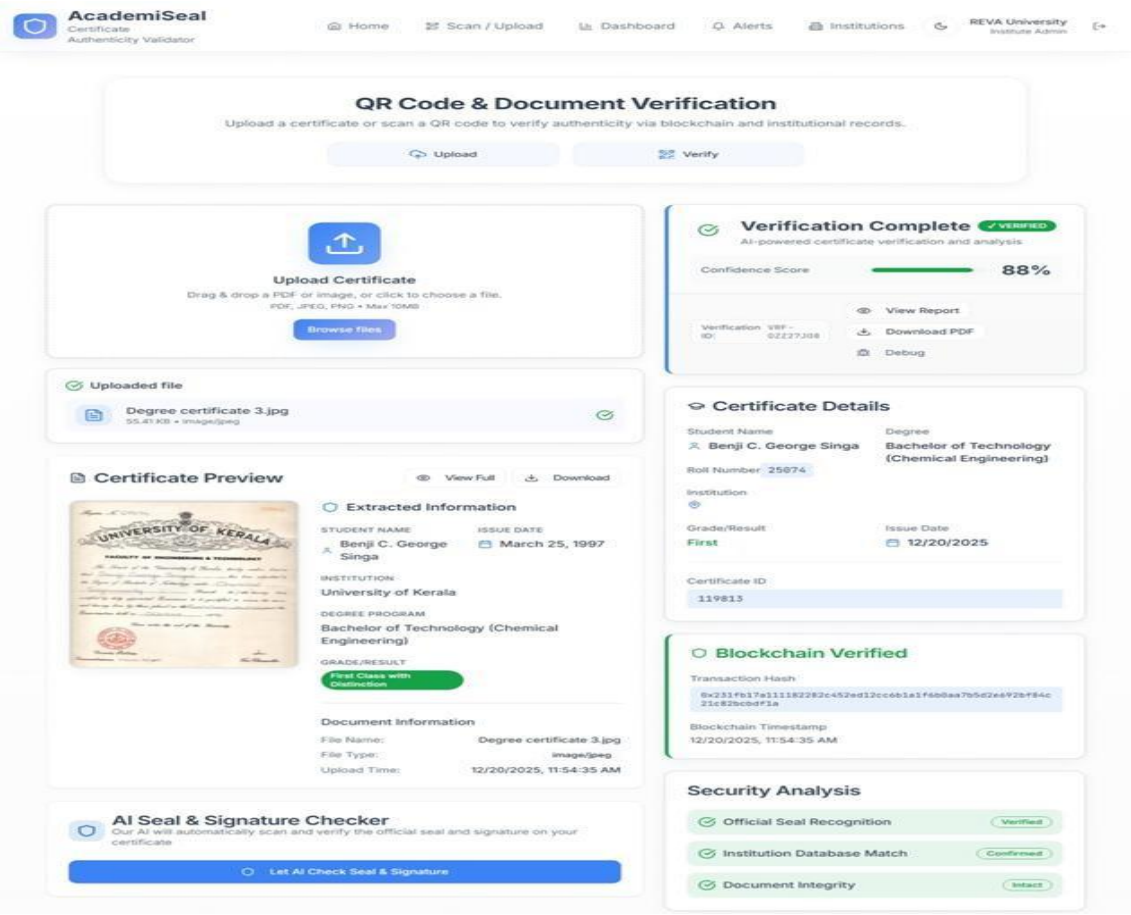

Figure 3: Result and Analysis

References:

[1] G. Eason, B. Noble, and I. N. Sneddon, “On certain integrals of Lipschitz-Hankel type involving products of Bessel functions,” Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955.

[2] J. Clerk Maxwell, A Treatise on Electricity and Magnetism, 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68–73.

[3] I. S. Jacobs and C. P. Bean, “Fine particles, thin films and exchange anisotropy,” in Magnetism, vol. III, G. T. Rado and H. Suhl, Eds. New York: Academic, 1963, pp. 271–350.

[4] S. Nakamoto, ”Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[5] V. Buterin, ”A Next-Generation Smart Contract and Decentralized Application Platform,” Ethereum White Paper, 2014.

[6] R. Smith, ”The Cost of Credential Fraud,” Journal of Higher Education Management, vol. 12, no. 4, pp. 45-50, 2019.

[7] A. Grech and A. Camilleri, ”Blockchain in Education,” JRC Science for Policy Report, European Commission, 2017.

[8] Tesseract OCR, ”Tesseract Open Source OCR Engine,” [Online]. Avail- able: https://github.com/tesseract-ocr/tesseract.

[9] Gemini Team, Google, ”Gemini: A Family of Highly Capable Multi- modal Models,” 2023.

Future Scope:

The future scope of this project includes:

1. Integration with national academic repositories such as DigiLocker and NAD for wider accessibility and validation.
2. Development of a mobile application to enable real-time certificate verification on portable devices.
3. Implementation of advanced AI models for improved accuracy in detecting forged or low-quality certificates.
4. Support for bulk verification to handle large-scale recruitment and institutional requirements.
5. Development of analytics dashboards to monitor verification trends and detect fraud patterns.