DMPedia Lecture Notes in Computer Science & Engineering
Volume 1, Issue 2, pp.399-407, 2026
ICICCS-2026

Academic Records Validator Using Blockchain Technology

Ganeeb Yashaswini, Kekkireni Trivikram, Nenavath Laalu Naik, Voolla Mohan, B.K Madhavi

Department of Computer Science and Engineering, Vardhaman College of Engineering, Hyderabad, India

yashaswiniganeeb24@gmail.com, trivikramkekkireni99@gmail.com, laaludevarakonda5@gmail.com, mohan1594@vardhaman.org, madhavi1593@vardhaman.org

ABSTRACT

Fraud in academic certificates has become a significant issue in employment, admissions to institutions, and institutional certification. The traditional methods of manual checks are tedious, inefficient and subject to fraud. To provide credible certificate validation, the present study suggests a secure and automatic Academic Records Validator, which can be viewed as a hybrid of blockchain technology, optical character recognition (OCR) and artificial intelligence (AI)-based forgery detector. The system retrieves structured information from 10th, intermediate, and degree certificates using OCR, including the candidate's name, roll number, certificate number, the name of the educational institution, year of graduation, and course information. The retrieved data should be standardised and converted to a single format to obtain a SHA-256 cryptographic hash. To ensure data privacy and guarantee immutability, integrity, and tamper-resistance, the hash value is stored only in the blockchain. To determine legitimacy, the uploaded certificate is OCR'd, compared against blockchains and recreated hashes, and the similarity is assessed by AI using cosine similarity algorithms. Experimental evaluation shows high forgery-detection capacity and secure verification with minimal processing time. The proposed system provides a secure, privacy-preserving, and tamper-resistant method for academic certificate verification in real-world scenarios.

Keywords: Academic Certificate verification, Blockchain Technology, Zero-Shot learning, MobileNetV2, Visual similarity engine, Optical Character Recognition (OCR), SHA-256 hashing, Smart contract, Cosine similarity, Forgery detection, Decentralised trust, Cryptographic integrity.

1. Introduction

The digitisation of education systems has enabled the easy access, storage, and sharing of academic credentials in a fast manner. The proliferation of online records has also increased the number of fake academic credentials, posing severe difficulties for universities, employers, and accreditation agencies. The traditional verification process relies on manual cross-validation with issuing institutions, which can be time-consuming, expensive, and error-prone. Certification systems for verifying academic credentials based on blockchain have also emerged as secure solutions for obtaining verified credentials [1], [6]. The decentralisation, immutability and transparency of blockchain technology make it an appropriate solution for credential management. Several studies have investigated the use of blockchain, smart contracts, and decentralised applications (DApps) for certificate verification [10], [17]. Moreover, privacy-preserving certification schemes have enhanced privacy and security against unauthorised access [11], [18]. Moreover, blockchain has been proven to be useful in securing healthcare systems, IoT threat detection, and data integrity management [2],[3],[8]. Most current systems, however, only consider blockchain storage structures without any smart document analysis or forgery detection systems [15]. OCR processes and extracts structured data from scanned certificates, minimising manual effort and streamlining the workflow. OCR does not recognise altered or false documents, however. AI-based similarity analysis and intelligent validation mechanisms are needed to enhance forgery detection. While some academic verification systems have been suggested based on blockchain technology [7],[10], few of them include artificial intelligence (AI)-based similarity analysis, OCR, and SHA-256 cryptographic hashing in their multi-layered validation process [13],[14].

Proceedings of ICICCS-2026 (Poster Papers), DMPedia Lecture Notes in Computer Science & Engineering.
ISBN: 978-81-993813-1-5

In this paper, a Blockchain-Based Academic Records Validator is proposed that integrates OCR-based structured data extraction, SHA-256 cryptographic hashing, AI-based visual similarity analysis, and Blockchain verification. Only the cryptographic hash values of the certificates are stored on the blockchain, providing privacy, tamper-resistant, and secure certificate authentication for 10th, Intermediate, and Degree certificates. The proposed framework can realise academic certificate verification in the real world in a safe, scalable, and intelligent manner.

2. Research Methodology

The past few years have seen significant scholarly interest in how blockchain technology can be used to verify academic credentials. In a bid to ensure safety in certificate validation, Gangwar and Chaurasia [1] proposed a hybrid authentication and verification system using blockchains, which involves decentralised applications (DApps) and QR codes. Despite their approach to make it more accessible and transparent, it primarily focuses on blockchain infrastructure; however, it does not focus on intelligent content validation. Tariq et al. also introduced Cerberus, a certificate and degree verification system based on blockchain technology that uses a distributed ledger to enhance the trustworthiness of academic qualifications [6] . Several scholars have pointed out that decentralisation is a method of eliminating the need for centralised authorities to certify verification. Shawon et al. [10] have developed an academic credentials confirmation system based on a DApp, whereas Bokariya and Motwani [7] have proposed a decentralised blockchain model to secure academic credentials. Gayathiri et al. [14] and Kumar et al. [12] also proposed blockchain-based solutions to prevent unauthorised changes and forgeries. These solutions primarily rely on blockchain storage, with no support for automated document intelligence, yet they ensure immutability and integrity.

Privacy and the certificate life cycle are also problems in blockchain-based credential systems. Saleh et al. [11] proposed a more ecologically certified mechanism with stronger privacy controls to protect sensitive information. Yao et al. [18] proposed a privacy-preserving certificate status validation protocol, based on blockchain, that can be applied to large-scale storage management. Vidal et al. [13] also discussed the importance of maintaining the validity of certificates in the long term in their discussion of the revocation process for academic certificates stored on the blockchain. These studies are not automated extraction designed, nor do they use forgery detection algorithms, even though they focus on secure storage and revocation. In non-academic settings, blockchain has been applied to safe data management in IoT and healthcare. Ali et al. [4], [8] explored blockchain-based privacy-preserving systems for healthcare information retrieval, demonstrating improved security and reliability. Yazdinejad et al. [3] proposed an intelligent, fuzzy blockchain-based system for detecting threats in an IoT network and demonstrated how to combine blockchain technology and artificial intelligence. Nyalletey et al. [15] and Bordel et al. [2] also highlighted the role of blockchain in ensuring data traceability and distributed safe storage. The projects showcase how blockchain technology and artificial intelligence (AI) can be integrated to enhance system integrity and intelligence.

Digital certificate systems based on smart contracts have also been explored as ways to automate verification procedures [17]. The primary concerns of most existing approaches, however, are decentralisation and cryptographic validation. Not many studies have integrated AI-based similarity analysis into intelligent forgery detection and optical character recognition (OCR) to extract structured data within a single framework. Moreover, all certificate data can be stored unproblematically in the blockchain, which is an issue for privacy and scalability. Therefore, one of the research gaps is the development of a multi-layered academic record validation system incorporating blockchain-based hash storage, SHA-256 hash storage, AI-based similarity analysis, and Automated Extraction using OCR. The proposed gap is addressed by the solution, which ensures resistance to tampering, privacy, smart forgery, and scalability in validating 10th, Intermediate, and Degree certificates within a single framework.

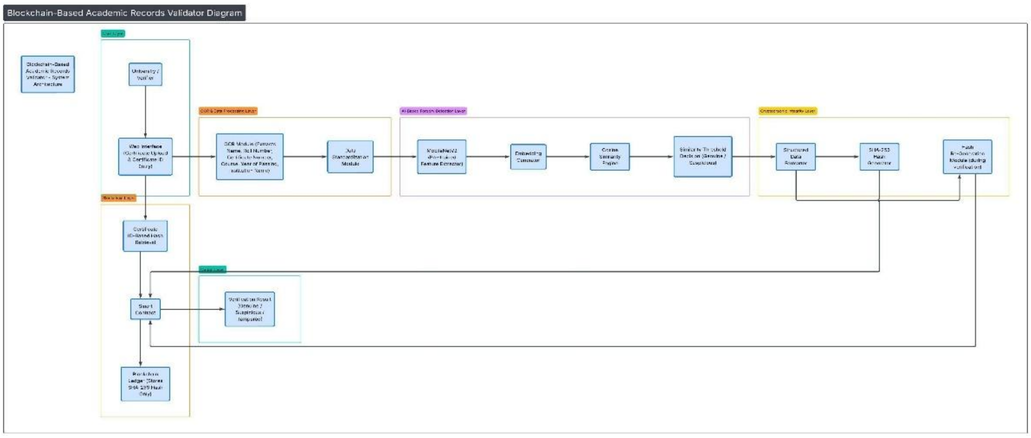

Fig. 1. The overall architecture of the proposed Academic Records Validator is illustrated.

3. Theory and Calculation

The proposed Academic Records Validator comprises multiple layers of authentication, including Optical Character Recognition (OCR) for data extraction, Artificial Intelligence (AI) for visual forgery detection, SHA-256 cryptographic hashing, and blockchain-based certificate verification. The framework provides a secure, privacy-preserving, tamper-proof and scalable way to validate a learner's academic certificate.

In AI-Based Visual Forgery Detection

Visual feature embeddings are extracted from certificate images using a pre-trained MobileNetV2 model. The uploaded certificate embedding is then compared to the real certificate templates using cosine similarity, and comparisons are based on textual characteristics such as fonts, seals, alignment, and layout patterns. Certificates with a similarity score below the threshold are considered suspicious. The embedding-based approach enhances forgery detection and enables AI-driven security frameworks on the blockchain [3],[5].

Cryptographic Hash Generation and Integrity Verification

To ensure the integrity of the document, the extracted certificate data is hashed using SHA-256. Any changes to the certificates' contents result in a completely different hash value, making tampering easy to detect. To verify the authenticity of certificates, the verification process compares the regenerated hash with the hash stored in the blockchain during verification [2],[16].

Blockchain-Based Certificate Verification

The final stage is to save the generated SHA-256 hash on a blockchain network as a smart contract. Since the hash alone is stored, privacy and immutability are maintained. Since the blockchain technology is decentralised and consensus-driven, the records stored may not be manipulated without authorisation. Verification is done by comparing the regenerated hash with the ledger's blockchain. A true match validates authenticity; otherwise, the certificate is marked as altered or invalid. Credential systems based on blockchain have proven to be reliable and generated more confidence in academic verification environments [1], [6], [17], and [18].

Table 1: Comparison with Existing Blockchain-Based Verification Systems

Feature	Traditional System	Proposed System
OCR-Based Data Extraction	No	Yes
AI-Based Forgery Detection	No	Yes
Cryptographic Hash Integrity (SHA-256)	Yes	Yes
Blockchain-Based Immutability	Yes	Yes
Ownership Validation Mechanism	Limited	Yes
Multi-Layer Verification	No	Yes
Privacy-Preserving Hash Storage	Yes	Yes
Automation Level	Partial	High
Forgery Detection Capability	Limited	Advanced

3.1. Mathematical Expressions and Symbols

Cryptographic Hash Generation

Interaction: To verify certificate authenticity and integrity, the SHA-256 cryptographic hashing is used. Certificate data is organised, and an algorithm is used. The hash value is computed as:

$$H = \mathrm{SHA256}(CID \parallel SN \parallel RN \parallel UN \parallel YOP \parallel CD)$$

where:

- CID = Certificate ID
- SN = Student Name
- RN = Roll Number
- UN = University Name
- YOP = Year of Passing
- CD = Course/Degree

The sign ||||| denotes the concatenation of normalised fields. By definition, SHA-256 will return 256-bit results. Thus, a single bit of tampering will be detected, as altering the certificate data produces an entirely different hash value, guaranteeing robust tamper detection and integrity verification.

Feature Similarity Computation

For AI-based visual forgery detection, cosine similarity is used to measure the similarity between certificate embeddings.

$$\text{Similarity}(A, B) = \frac{A \cdot B}{\|A\|\,\|B\|}$$

where:

A	Feature embedding of the uploaded certificate
B	Feature embedding of the stored genuine certificate template
A · B	Dot product of embeddings
‖A‖, ‖B‖	Euclidean norms of embeddings

If Similarity $\geq \tau$ (where $\tau = 0.85$ is the predefined threshold), the certificate is considered visually authentic; otherwise, it is flagged as suspicious.

The cosine similarity threshold (**τ = 0.85**) was chosen empirically to balance false-positive and false-negative rates during certificate verification. Lower threshold values increase the likelihood that forged certificates will be classified as genuine. In contrast, higher threshold values increase the likelihood that authentic certificates will be rejected due to minor visual differences. Therefore, the selected threshold provides stable verification performance and improves robustness against typical certificate manipulations. Some embedding verification methods and smart security systems are presented in [3], [5], [6].

Multi-Layer Verification Decision Function

The final verification decision is determined by combining the AI-based similarity score and blockchain hash comparison as follows:

$$\text{Decision} = \begin{cases} \text{Genuine, if Similarity} \geq \tau \text{ and } H_{gen} = H_{blockchain} \\ \text{Suspicious, if Similarity} < \tau \\ \text{Tampered, if } H_{gen} \neq H_{blockchain} \end{cases}$$

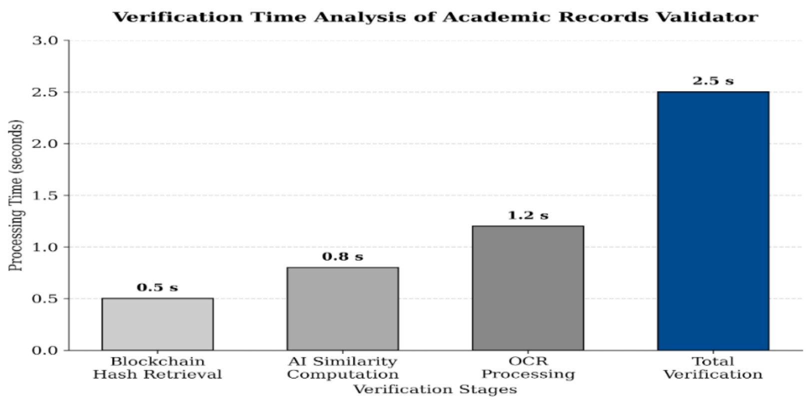

Fig. 2. The computational time analysis of the proposed system is presented.

4. Results and Discussion

The proposed Academic Records Validator was tested on a controlled set of true and fake 10th, Intermediate and Degree certificates. Forged certificates were produced by altering common certificate properties, including fonts, certificates, grades, and layouts, to mimic typical scenarios of certificate tampering. Forged certificates were developed by altering common certificate properties, such as fonts, certificates, grades, and layout, to simulate typical scenarios of certificate tampering. To assess the effectiveness of the proposed framework, OCR-based data extraction, feature embedding generation with MobileNetV2, cosine similarity analysis, cryptographic hashing with SHA-256, and blockchain verification were conducted. Experimental results show that the proposed multi-layered verification model successfully distinguishes genuine from forged certificates. The true certificates had higher similarity scores, while the fake certificates had lower scores and were correctly identified as suspicious. Moreover, if the certificate's content changes, it will receive a new SHA-256 hash, allowing tampering to be detected during blockchain verification. Various performance metrics were used to assess the proposed system, such as OCR extraction accuracy, AI-based forgery detection accuracy, false positive rate, false negative rate, SHA-256 hash matching accuracy, average verification time, and blockchain retrieval success rate. The results obtained are presented in Table 2.

Table 2: Performance Evaluation of Proposed Academic Records Validator

Performance Metric	**Result**
OCR Extraction Accuracy	94.2%
AI-Based Forgery Detection Accuracy	91.8%
False Positive Rate	4.5%
False Negative Rate	3.7%
SHA-256 Hash Matching Accuracy	100%
Average Verification Time	2.8 seconds
Blockchain Retrieval Success Rate	100%

The findings show that integrating OCR, AI, cryptographic hashing, and blockchain provides a more secure, reliable, and scalable solution for verifying academic certificates. OCR correctly extracts the structured certificate information, and the visual similarity analysis using MobileNetV2 successfully detects forged certificates. SHA-256 cryptographic hashing ensures that certificates cannot be tampered with and provides integrity. At the same time, blockchain verification ensures they cannot be tampered with, are decentralised, and cannot be forged. In conclusion, the Academic Records Validator provides a trustworthy, secure, and effective way to validate academic certificates in real-world settings through intelligent document analysis and blockchain-based trust mechanisms as per Figure 3.

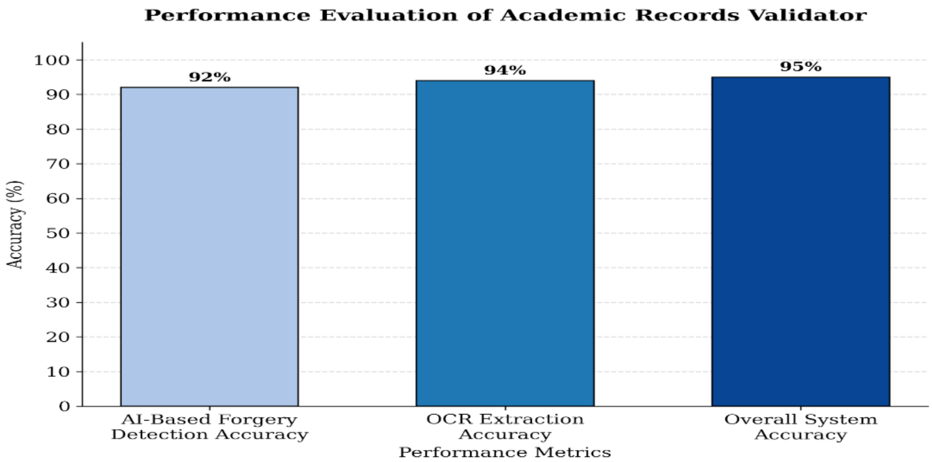

Fig. 3. The performance evaluation graph is illustrated.

5. Conclusions

This paper introduces a Blockchain-Based Academic Records Validator that implements Optical Character Recognition (OCR), AI-based visual forgery detection, SHA-256 cryptographic hashing, and decentralised blockchain validation to establish a secure, automated certificate authentication system. The system reads the structured information from a certificate using OCR, applies a pre-trained MobileNetV2 to generate visual similarity via embedding, and checks document integrity by comparing the regenerated SHA-256 hash values with those stored in the blockchain. The framework maintains data privacy by storing cryptographic hash values on the blockchain only and uses immutable, decentralised verification to ensure security. It is shown that the multi-layered technique can successfully identify both the content-level and structural visual manipulation, and that this strategy can make individuals more trusting and less dependent on centralised verification authorities. AI-supported anomaly detection with integrity validation based on blockchain enhances the scalability, transparency, and resiliency in the actual application of academic verification. Since it is the work of the future, the framework may be further developed towards on-chain, smart contract-based automation of certificate issuance, revocation, and lifecycle management. It is possible to train the AI module on more diverse, larger certificate sets to make it more robust against advanced forgery methods, while adding more advanced OCR models to handle low-quality scans and multilingual certificates. Moreover, the bulk certificate registration features can be proposed to serve big educational institutions effectively. Further studies can also examine how to integrate with national digital credential infrastructures and leverage explainable AI mechanisms to improve transparency, interpretability, and user trust in automated academic verification systems.

Acknowledgements

Hereby, we would like to express our utmost gratitude to our faculty mentors and academic guides for their continuous support, guidance, and valuable comments throughout this research work. Their inputs and support were important in designing and developing the proposed Academic Records Validator system. Another thing we would like to mention is that our institution has provided the academic environment and resources needed to complete this research study. The research community, in general, is another group we would like to thank for the availability of open-source tools and learning materials that helped us understand the concepts of blockchain technology, artificial intelligence, and document analysis. These resources were very important in the development, testing, and optimisation of the proposed

system.

Funding source

No funding was received for this study.

Conflict of Interest

The authors declare no conflict of interest.

References

[1] S. Gangwar and A. Chaurasia, "Blockchain-based authentication and verification system for academic certificate using QR code and decentralized applications," *International Journal of Computer Applications*, vol. 186, no. 26, June 2024, doi: 10.5120/ijca2024923722.

[2] B. Bordel, R. Alcarria, and T. Robles, "A blockchain ledger for securing isolated ambient intelligence deployments using reputation and information theory metrics," *Wireless Networks*, 2023, doi: 10.1007/s11276-023-03375-9.

[3] A. Yazdinejad, A. Dehghantanha, R. M. Parizi, G. Srivastava, and H. Karimipour, "Secure intelligent fuzzy blockchain framework: Effective threat detection in IoT networks," *Computers in Industry*, vol. 144, p. 103801, 2023, doi: 10.1016/j.compind.2022.103801.

[4] A. Ali, M. F. Pasha, O. H. Fang, R. Khan, and M. A. Almaiah, "Big data based smart blockchain for information retrieval in privacy-preserving healthcare system," in *Big Data Intelligence for Smart Applications*, Studies in Computational Intelligence, vol. 994. Cham, Switzerland: Springer, 2022, doi: 10.1007/978-3-030-87954-9_13.

[5] Y. Himeur, A. Sayed, A. Alsalemi, F. Bensaali, A. Amira, I. Varlamis, M. Eirinaki, C. Sardianos, and G. Dimitrakopoulos, "Blockchain-based recommender systems: Applications, challenges and future opportunities," *Computer Science Review*, vol. 43, p. 100439, 2022.

[6] A. Tariq, H. B. Haq, and S. T. Ali, "Cerberus: A blockchain based accreditation and degree verification system," *IEEE Transactions on Computational Social Systems*, 2022.

[7] P. P. Bokariya and D. Motwani, "Decentralization of credential verification system using blockchain," *International Journal of Innovative Technology and Exploring Engineering*, vol. 10, no. 11, 2021.

[8] A. Ali, H. A. Rahim, M. F. Pasha, R. Dowsley, M. Masud, J. Ali, and M. Baz, "Security, privacy, and reliability in digital healthcare systems using blockchain," *Electronics*, vol. 10, p. 2034, 2021.

[9] "IEEE Journal of Biomedical and Health Informatics," *IEEE Journal of Biomedical and Health Informatics*, vol. 25, no. 9, pp. C3–C3, Sept. 2021.

[10] S. K. Shawon, H. Ahammad, S. Z. Shetu, M. Rahman, and S. A. Hossain, "Diucerts DApp: A blockchain-based solution for verification of educational certificates," in *Proceedings of the 12th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, IEEE, 2021, pp. 1–10.

[11] O. S. Saleh, O. Ghazali, and N. B. Idris, "A new decentralized certification verification privacy control protocol," in *Proceedings of the 3rd International Cyber Resilience Conference (CRC)*, IEEE, 2021, pp. 1–6.

[12] K. D. Kumar, P. Senthil, and D. Kumar, "Educational certificate verification system using blockchain," *International Journal of Scientific and Technology Research*, vol. 9, no. 3, pp. 82–85, 2020.

[13] F. R. Vidal, F. Gouveia, and C. Soares, "Revocation mechanisms for academic certificates stored on a blockchain," in *Proceedings of the 15th Iberian Conference on Information Systems and Technologies (CISTI)*, IEEE, 2020, pp. 1–6.

[14] A. Gayathiri, J. Jayachitra, and S. Matilda, "Certificate validation using blockchain," in *Proceedings of the 7th International Conference on Smart Structures and Systems (ICSSS)*, IEEE, 2020, pp. 1–4.

[15] E. Nyaletey, R. M. Parizi, Q. Zhang, and K.-K. R. Choo, "BlockIPFS: Blockchain-enabled interplanetary file system for forensic and trusted data traceability," in *Proceedings of the IEEE International Conference on Blockchain*, 2019, pp. 18–25.

[16] I. Riyanto, L. Margatama, M. Suparmoko, Martini, and D. E. Hindarto, "University contribution in developing country on carbon emission reduction through motion sensor application pilot project on building lighting installation," in *Proceedings of the IEEE International Conference on Applied System Invention (ICASI)*, Chiba, Japan, 2018, pp. 558–561.

[17] S. K. Yadav, K. Sharma, C. Kumar, A. Arora, "Blockchain-based synergistic solution to current cybersecurity frameworks," Multimedia Tools and Applications 81, no. 25 (2022): 36623-36644.

[18] S. Yao, J. Chen, K. He, R. Du, T. Zhu, and X. Chen, "PbCert: Privacy-preserving blockchain-based certificate status validation toward mass storage management," *IEEE Access*, vol. 7, pp. 6117–6128, 2019.

[19] L. S. Barbosa and S. A. Shaikh, "Selected contributions from the open source software certification (opencert) workshops," Science of Computer Programming, vol. 91, pp. 139–140, 2014.