iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** V **Month of publication:** May 2026

DOI: https://doi.org/10.22214/ijraset.2026.81915

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue V May 2026- Available at www.ijraset.com

Blockchain-Powered Administrative Platform for End-to-End Student Certificate Management: From Enrollment to Alumni Credential Services

Mrs Umadevi V[1], Abinaya A[2], Harini N[3], Janani A[4], Laavanya A S[5]
[1]*Head of the Department,* [2, 3, 4, 5]*UGScholar, Department of Computer Science and Engineering, Arunai Engineering college, Tiruvannamalai*

Abstract: ***Academiccredentialfraudhas become a major concern in modern education systems. The presence of forged certificates, slow manual verification procedures, and weaknesses in centralized databases reduce the reliability of institutional records.***
This research proposes a blockchainbasedadministrativeplatform designed to manage student certificates throughouttheiracademiclifecycle,from enrollment to alumni credential services. The platform uses decentralized blockchain architecture along with SHA256 cryptographic hashing and QR-code verification to ensure secure and tamperproof certificate management.
Certificates are securely stored in cloud infrastructurewhiletheblockchainstores only the cryptographic proof of authenticity.Thisdesignprotectsprivacy whileensuringdataintegrity.Thesystem enables instant verification for students, institutions, employers, and government agencies. Experimental evaluation shows high reliability with fast verification latency and strong tamper detection capabilities.
Keywords: Blockchain, Academic Certificates, SHA-256, QR Code Verification, Decentralized Storage, RBAC, DigiLocker, Smart Contracts.

I. INTRODUCTION

Educational certificates play an essential role in establishing trustbetween students, institutions, and employers. However, the increasingnumberof**fakeormanipulated certificates** has created serious challenges in recruitment, admissions, and institutional verification. Traditional certificate management systems depend mainly on paper documents or centralized databases.Theseapproachesarevulnerable to document forgery, data loss, and unauthorized modification.

To address these issues, this research proposes ablockchain-enabled certificate management platform. Blockchain technology provides a decentralized and immutable ledger where certificate information can be securely recorded and verified. By integrating cryptographic hashingandQR-codeverification,every issuedcertificatebecomespermanently traceable and cannot be altered without detection.

The proposed system supports multiple stakeholders including administrators, students, employers, and verification authorities. Role-based access control ensures that each participant interacts with the system securely while maintaining privacy. The platform manages the entire certificate lifecycle, beginning with student enrollment and extending to alumni credential verification.

II. LITERATURE SURVEY

Recent studies show that blockchain technology can significantly improve the security and transparency of academic credential systems. Rashmi and Harish proposedablockchain-basedframeworkfor academic certificate management that prevents unauthorized modification of records. Similarly, Venkatesh and Ramesh developed a decentralized verification model that allows employers to validate certificates without contacting the issuing institution directly.

Research from related domains has also influenced this work. Digital security frameworks such as AI-driven monitoring systems demonstrate the effectiveness of continuousintegritycheckinginpreventing tampering. Additionally, real-time system architectures used in deep learning applications show that complex backend processes can be delivered efficiently through lightweight API services.

Despite these developments, many existing blockchain-based certificate systems still lack several important capabilities, including

QR-code based verification, integration with national digital repositories,detailedaccesscontrol mechanisms, and support for alumni credential services. The proposed platform aims to address these limitations.

III. PROBLEM STATEMENT

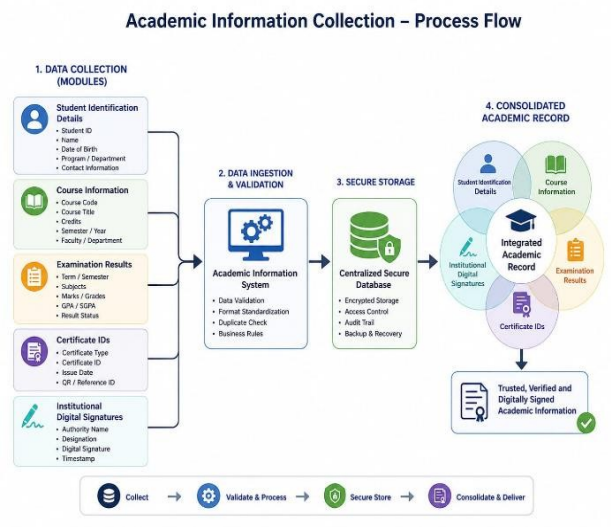
Educational institutions currently face multiple challenges related to certificate management and verification. These challenges include:

- Difficultyindetectingfakeor forged certificates
- Slowandinefficientmanual verification processes
- Securityrisksassociatedwith centralized storage systems
- Possibility of document alteration over time
- Lackofaunifiedandsecure platform for long-term academic record storage
- Limitedstudentcontrolover their own academic credentials

These issues reduce institutional credibility, increase administrative workload,andallowfraudulentactivitiesto occur.Therefore,a secure,decentralized, and easily verifiable certificate management system is required.

IV. PROPOSEDMETHODOLOGY

The proposed platform operates as a decentralized system that manages the complete lifecycle of student certificates through several integrated modules.



A. Data Input

The system collects structured academic informationincludingstudentidentification details, course information, examination results, certificate IDs, and institutional digital signatures.

B. CertificateHashing

EachcertificateisconvertedintoaSHA256 cryptographic hash that represents all certificate attributes. Since hashing produces a unique digital fingerprint, any modificationinthecertificatedataresultsin a completely different hash value. Blockchain Recording

Thegeneratedhashvaluesarestoredonthe blockchain using smart contracts. These smart contracts ensure that only authorized institutional administrators can issue certificates and that once recorded, the data cannot be modified.

C. CloudStorage

Actual certificate documents are stored securely in cloud storage systems. The blockchain maintains only the cryptographic proof of the document, ensuring both privacy and integrity. Role-Based Access Control

The system supports multiple user roles suchasadministrators,students,employers, and system administrators. Each role has controlled permissions for accessing and verifying certificate data.

D. Real-TimeVerification

A REST-based API allows instant certificate verification. When a QR code printed on the certificate is scanned, the systemretrievestheblockchainrecordand verifies its authenticity within milliseconds.

V. SYSTEM ARCHITECTURE

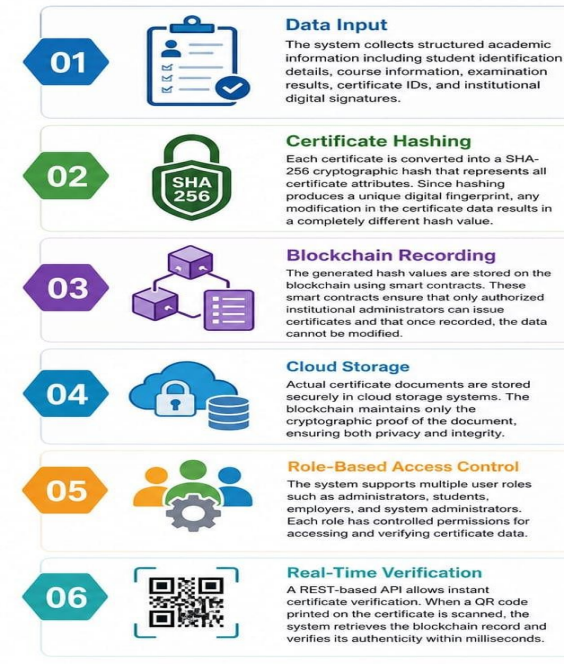
The architecture of the proposed platform is structured into **five functional layers**, each responsible for a specific stage in the certificate management process. These layers work together to enable secure certificate generation, storage, and verification.

1) Data Input Layer: Educational institutions upload certificate-related details through secure HTTPS communicationchannels.Atthisstage,the system validates the incoming data to ensure that the records meet predefined formatting and integrity requirements before further processing.

2) Processing and Hashing Layer: After successful validation, the data is cleaned andstandardizedforconsistency.A

3) SHA256 cryptographic hash is then generated for every certificate to create a unique digital fingerprint. In addition, a QR code containing the reference to the certificaterecordisproduced.TheLCAPI prepares the corresponding blockchain transaction to register the certificate information.

4) Blockchain Layer: The generated hash value is transmitted to the blockchain network where smart contracts verify the transaction and record it on the distributed ledger. Once stored, the certificate hash becomes permanent and tamperresistant, ensuring that any modification to the original data can be easily detected.



5) Storage Layer: While the blockchain maintains the hash reference, the actual certificate files are securely stored in cloud storage systems with strict access control policies. Integration with DigiLockerenablesstudentstosafelyretrieveandshare their official digital certificates when required.

Aspect	Paper1:AI-DrivenDigitalImmune System
Domain	Enterprise Cybersecurity
Core Technology	Forest, LSTM, XGBoost, Autoencoder
DataSource	Networklogs,endpointtelemetry,threat feeds
Detection	Anomaly detection + behaviora l analytics
Deployment	Visualizationdashboard+orchestration
Accuracy	93.8%threatdetection;MTTD−55%
Relevance Here	Pipeline +automated response → blockchainverification workflow

6) Verification and Output Layer: The platform provides a REST-based verification service that allows users to confirm certificate authenticity. When a QR code on a certificate is scanned, the system retrieves the corresponding blockchain record and verifies its validity. Institutions can also generate printed certificates embedded with secure QR codes for easy verification.

VI. EXPECTED OUTCOMES

1) Tamper-Resistant Credential Storage The proposed system creates a secure and immutable digital repository for storing academic certificates throughout a student's educational lifecycle.
2) Secure Cryptographic Verification The use of cryptographic hashing mechanisms helps prevent the creation and circulation of fake or manipulated academic documents by enabling reliable authenticity checks.
3) Improved Operational Efficiency Automation of the verification process significantlydecreasesthetimerequiredfor manual validation and reduces the administrative workload for educational institutions.
4) InstantCredentialVerificationThe platform enables rapid and dependable verification of certificates for employers, universities, and other authorized parties through real-time validation mechanisms.
5) Enhanced Security through Blockchain By integrating blockchain technology with SHA-256 hashing, the system ensures strong data integrity and prevents unauthorized modification of certificate records.
6) Student Ownership and Portability Through integration with DigiLocker, students gain easier access to their verified digital credentials and can securely share them when required.
7) End-to-End Credential Lifecycle Management Theplatformsupportsscalablemanagement of academic records even after graduation, allowing institutions to efficiently provide alumni credential services.

VII. ALGORITHMIC APPROACH

The proposed system operates based on **three key mechanisms** that ensure the security,integrity,andefficientverification of academic certificates.

1) Cryptographic Integrity (SHA-256):ThesystemappliestheSHA- 256 cryptographic hashing algorithmtogenerateauniquedigital fingerprintforeverycertificaterecord. Thishashvalue representsall certificateattributes, including student details, course information, institution data, and issuance timestamp. Any modificationtotheoriginalcertificate data produces a completely different hash value, allowing the system to immediatelydetecttampering whencomparedwiththeblockchain record.

2) Distributed Consensus through Smart Contracts: Certificate issuance and management are governedbyblockchainsmartcontracts, which enforce institutional authorization policies.Thesesmartcontractsvalidate certificate transactions before they are recorded on the blockchain. Since the blockchainoperatesunderadistributed consensus mechanism, no single administrator can modify or manipulate certificate records without network validation.

3) QR Code-Based Verification: Eachcertificateisembeddedwithaunique QR code that contains a reference to its correspondingblockchainrecord.Whenthe QRcodeisscanned,theverificationsystem retrieves the storedhash from the blockchain and compares it with the certificatedata.Thisprocessenablesfast, device-independent, and user-friendly credentialverificationwithoutrequiring manual data entry.

VIII. CONCLUSION

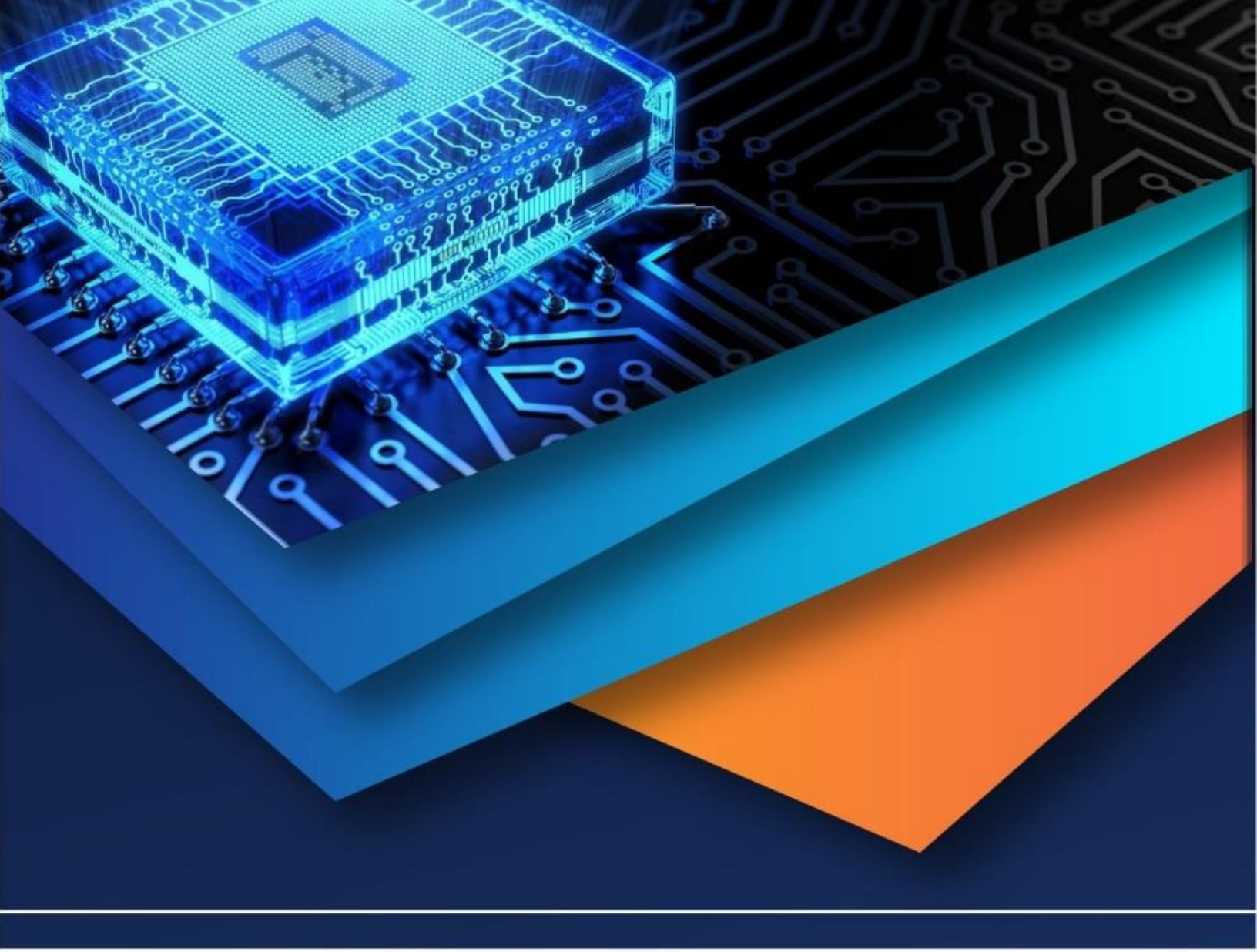
Thisstudyintroducesablockchain-based platform designed to securely manage studentcertificatesfrom enrollmentto alumni verification services. By combining blockchain immutability, SHA-256cryptographichashing,andQR-code verification, the system ensures that academic credentials remain tamper-proof and easily verifiable.

The decentralized architecture removes reliance on centralized storage systems and improvesinstitutionaltrust.Integrationwith national digital repositories further enhancescredentialportabilityforstudents. Experimental results demonstrate high reliability,fastverificationspeed,andstrong resistance to certificate tampering.

Theproposedplatformprovidesaneffective solution forpreventing academiccredential fraud while simplifying the verification process for institutions, employers, and government organizations.

REFERENCES

[1] R. H. C. Rashmi and S. Harish, “A Secure and Transparent Model for Academic Credential Management Using Blockchain Technology,” International Journal of Advanced Research in Computer Science, vol. 17, no. 2, pp. 112–120, 2026.
[2] N. Venkatesh and K. S. Ramesh, “Blockchain-Based Student Academic Certificate Verification System,” International Journal of Computer Applications,vol.185,no.12,pp.25–31, 2024.
[3] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.
[4] M.Crosby,P.Pattanayak,S.Verma,and Kalyanaraman, “Blockchain Technology: Beyond Bitcoin,” Applied Innovation Review, no. 2, pp. 6–19, 2016.
[5] MinistryofElectronicsandInformation Technology,“DigiLocker:Digital DocumentWalletFramework,” GovernmentofIndia,2023.
[6] A. Grech and A. F. Camilleri, BlockchaininEducation,Luxembourg: Publications Office of the European Union, 2017.
[7] M. Sharples and J. Domingue, “The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward,” Proceedings of the European Conference on Technology Enhanced Learning, vol. 9891, pp. 490–496, 2016.
[8] F. Turkanović, M. Hölbl, K. Košič, M. Heričko, andA. Kamišalić, “EduCTX: ABlockchain-Based Higher Education Credit Platform,” IEEE Access, vol. 6,
[9] pp.5112–5127,2018.
[10] H.Chen,M.Pendleton,L.Njilla,andS. Xu, “A Survey on Ethereum Systems Security: Vulnerabilities, Attacks, and Defenses,” ACM Computing Surveys, vol. 53, no. 3, pp. 1–43, 2020.
[11] J. Chen, X. Du, and K. Fan, “A Blockchain-Based Framework for Secure Sharing of Academic Certificates,” Future Generation Computer Systems, vol. 109, pp. 473–482, 2020.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY