IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

VOLUME : 10 ISSUE : 12 Print / Issue Publication Date: April 2026

ISSN : 2455-2143

DOI : 10.33564/IJEAST.2026.v10i12.012

Indexed In

Google SCHOLAR OPEN ACCESS doi Crossref

WWW.IJEAST.COM

editor@ijeast.com

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 10, Issue 12, ISSN No. 2455-2143, Pages 95-99
Published Online April 2026 in IJEAST (http://www.ijeast.com)

VERIFYCERTS: A SECURE BLOCKCHAIN-BASED SYSTEM FOR ACADEMIC CERTIFICATE VERIFICATION

Nadipena Mounika, Samireddi Jhansi, Patnaikuni Mahesh Babu, Kotyada Ramadevi, Dr.R. Rajender
Dept. of Computer Science and Systems Engineering
Lendi Institute of Engineering and Technology Vizianagaram, Andhra Pradesh, India

Abstract— **Fraudulent educational certificates have become a major issue today. Many students and job seekers use fake degree certificates, which can seriously affect employers and create problems for universities during admissions into higher studies. Existing systems that check certificates are often slow, costly, and not fully secure. To solve this, our project proposes a Blockchain-based Academic Certificate Verification System that provides a tamper-proof and low-cost solution for verifying academic records. In this system, every certificate is converted into a unique digital hash using the SHA-256 algorithm and stored securely on a blockchain network. This makes it impossible for anyone to change or forge the certificate details. The blockchain ensures that the certificate issuer, student, and verifier are all connected on a single transparent platform. The system allows institutions to issue certificates and verifiers to check them instantly using a QR code or transaction ID.**

Keywords— **Decentralized Ledger, Hashing Algorithms (SHA-256), Smart Contract Execution, Blockchain Technology, Certificate Verification, Technology Trustworthiness, Transparency.**

I. INTRODUCTION

With the rapid growth of digital education and online certification platforms, the need for secure, tamper-proof, and easily verifiable academic credentials has become critical. Traditional certificate management systems rely on centralized databases maintained by institutions or third-party authorities, making them vulnerable to data manipulation, forgery, single-point failures, loss of records, and unauthorized access. Moreover, certificate verification in such systems is often time-consuming, costly, and dependent on manual intervention from issuing authorities, resulting in inefficiency, delayed validation, and reduced trust among stakeholders.

To address these challenges, this paper proposes a blockchain-based certificate verification system that ensures the authenticity, integrity, and transparency of digital certificates. Blockchain technology offers key features such as decentralization, immutability, and cryptographic security, which collectively prevent unauthorized modifications and eliminate the possibility of certificate fraud. In the proposed system, certificates are digitally issued and their cryptographic hashes are securely recorded on the blockchain, ensuring that sensitive data is not exposed while maintaining verifiability.

Smart contracts automate the certificate issuance and verification processes, enabling instant and trustworthy validation without the need for intermediaries. Any stakeholder, such as employers or academic institutions, can verify a certificate in real time by comparing the certificate hash with the blockchain record, thereby significantly reducing verification latency and operational overhead.

The proposed approach enhances trust among institutions, employers, and certificate holders while ensuring ethical use and long-term integrity of academic credentials. By combining blockchain technology with secure access control mechanisms, the system provides a scalable, reliable, and future-ready solution for digital certificate management in modern educational and professional environments.

II. RELATED WORK

There have been various research works done on the use of digital technology in managing certificates. Initially, there were centralized database-based systems that made it easy for people to access their certificates but could not provide any level of assurance. In recent times, there has been increased interest in blockchain-based systems.

A. Existing System

These credentials are usually generated and stored physically or in centralized databases. Although digitization makes them more accessible, validation is still carried out manually and inefficiently. This process is also susceptible to tampering, hence posing risks such as forgeries, duplications, data theft, and even loss.

B. Proposed System

The proposed blockchain system for certificate verification is a decentralized approach that uses smart contracts on Ethereum. The certificates are encrypted and stored on the blockchain in a tamper-proof manner for easy verification. The proposed system will allow administrators, institutions, and verifiers role-based access. The verification of certificate

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 10, Issue 12, ISSN No. 2455-2143, Pages 95-99
Published Online April 2026 in IJEAST (http://www.ijeast.com)

authenticity will be automated and performed through smart contracts, eliminating any third-party entity to perform authentication. Verification will be performed by using the IDs of transactions stored on the blockchain.

III. METHODOLOGY

A. Certificate Generation

Institutions issue digital certificates, which contain student data like name, registration number, course, and date of issue. The Role-Based Access Control (RBAC) model ensures that only authorized institutions issue certificates.

B. Hash Generation Using SHA-256

The hash for each certificate is generated by a SHA-256 algorithm, resulting in a unique hash value of a fixed size.
Mathematical Representation:
$H=SHA256(C)$ (1)
Where: H = Generated hash value, C = Certificate data
The hash function ensures the integrity of the data, as even a small change in the certificate's data results in a completely different hash.

C. Blockchain Storage via Smart Contract

The hash value H is stored on the blockchain by the deployed smart contract on the Ethereum blockchain. The smart contract stores the following:
Certificate ID
Institution ID
Hash value
Timestamp

D. Verification Algorithm

During verification:
The uploaded certificate is hashed again:
$H'=SHA\ 256(C')$ (2)
The system retrieves stored hash H from blockchain.
If $H=H'$, certificate is valid. (3)
If $H\neq H'$, certificate is tampered. (4)

E. Security and Integrity Model

The security of the system is achieved through:

- Cryptographic hashing
- Blockchain immutability
- Smart contract automation
- Role-based access control
- Decentralized validation

This methodology eliminates the need for any central authority to perform the validation process while ensuring the security of the process.

IV. WORKFLOW OF THE SYSTEM

The workflow of the " VerifyCerts A Secure Blockchain-Based System for Academic Certificate Verification " shows the way in which the certificates are issued, stored, shared, and verified in an efficient way. It has three primary stakeholders in the system: Issuing Institution, Student, and Verifier (Employer/University).

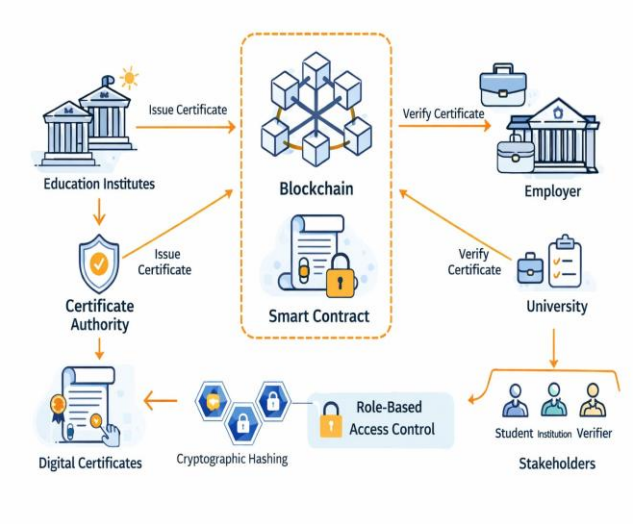

Fig. 1: Workflow of VerifyCerts Diagram

Step 1: Institution Registration and Authentication
To start off, the educational institutions that are authorized are required to register on the VerifyCerts platform. These institutions are then authenticated, as well as issued access credentials to the system. This helps to ensure that only authorized bodies are allowed to generate certificates on the platform, thereby ensuring that fake certificates are not created.

Step 2: Certificate Creation
With successful verification, a digital certificate is created by the institution in the name of the student. It contains important data like the name of the student, registration number, name of the course, name of the institution, date of issuance, and a unique ID of the certificate. This information forms the content of the certificate.

Step 3: Hash Generation Using SHA-256
Once the certificate is generated, the system uses the SHA-256 hashing algorithm to hash the certificate details. This hash is essentially a unique digital fingerprint of the certificate. If any information in the certificate changes even in a small way, the resulting hash will be completely different.

Step 4: Blockchain Storage via Smart Contract
The generated hash is sent on to the blockchain network along with metadata like certificate ID and issuing institution ID. This hash gets recorded on the decentralized ledger through a smart contract. Since blockchain data is immutable, this stored hash cannot be changed or deleted, thus ensuring the authenticity forever.

Step 5: Digital Certificate Issuance to Student
The digital certificate, post successful blockchain storage, is issued to the student via the platform. The student can download, store, and distribute the certificate whenever necessary. The actual certificate file would remain off-chain, whereas its hash on blockchain does the job of assuring authenticity.

Step 6: Certificate Sharing by Student
It is shared with the verifier by the student when they apply either for a job or higher education. This may involve uploading the certificate file in question or sharing the verification link in the secure form that the system has generated.

Step 7: Certificate Submission by Verifier
The verifier at the employer's or university's organization uploads the received certificate into the VerifyCerts verification portal. Verification doesn't have to involve contacting the issuing institution, thus avoiding all that could have caused delays and manual communication.

Step 8: Re-Hashing and Comparison
The system recalculates the SHA-256 hash of the uploaded certificate and compares it with the hash stored on the blockchain. If both hashes match, the certificate is confirmed to be original. If not, the certificate is marked as tampered or false.

Step 9: Verification Result Generation
On the basis of the result of the comparative verification, the certificate's valid or invalid status is instantly indicated as Valid or Invalid. In some cases, the name of the issuing body and the issue date may also be displayed to the verifier.

Step 10: Audit Logging and Transparency
Every verification request is securely logged for auditing purposes. This assists institutions and organizations in recording verification efforts, promoting transparency and accountability.

V. EXPERIMENTAL SETUP AND EVALUATION

Experimental Environment:

- Operating System: Windows/Linux
- Blockchain Platform: Ethereum Test Network
- Smart Contract
- Hashing Algorithm: SHA-256

To evaluate the overall performance of the VerifyCerts system, a controlled experimental environment was set up. Sample academic certificates issued by certified institutions to different student accounts were designed, created, and then verified by different verifier accounts under different conditions.
Performance Metrics:
Certificate Verification Time, Hash Generation Time, Smart Contract Transaction Time, Accuracy of Tamper Detection, System Response under Multiple Requests.

A. Certificate Verification Time

Moreover, the verification time of the certificate was calculated based on the time taken to receive the hash of the certificate through the blockchain system. The results show that the verification process takes a short time due to the interaction with the smart contract.

B. Accuracy of Verification Results

All valid certificates were correctly validated, while the tampered ones were correctly marked as invalid.
Accuracy of Tamper Detection:
Tampered certificates were intentionally modified and re-uploaded for verification. In all cases, the system successfully detected hash mismatches and marked the certificates as invalid. (Accuracy of tamper detection: 100%)

C. Resistance to Certificate Tampering

These tampered certificates led to a mismatch of the hashes during the process of verification. As the hash value of the certificates on the blockchain cannot be altered, the moment the certificates were altered, the change was noticed.

D. System Response under Multiple Verification Requests

The system demonstrated consistent performance in processing simultaneous verification requests. The response behavior of the blockchain verification remained consistent without compromising verification accuracy.

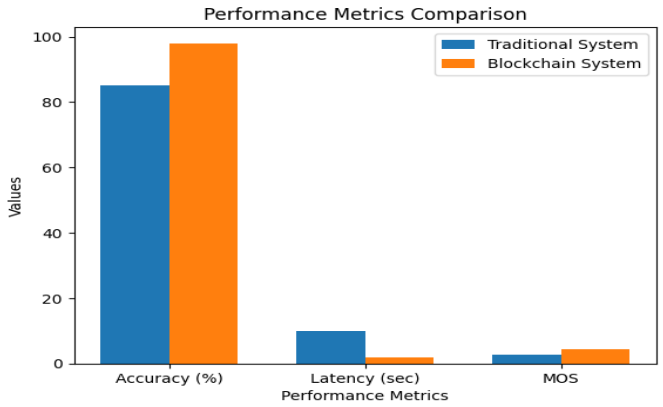

Fig. 2: Performance metrics Comparison Graph

VI. RESULTS AND DISCUSSION

The experimental results show that the VerifyCerts system has significant efficiency and reliability improvements when compared to traditional certificate verification techniques. Within seconds, the smart contract executes the verification procedure, as opposed to the days or weeks it takes with

International Journal of Engineering Applied Sciences and Technology, 2026
Vol. 10, Issue 12, ISSN No. 2455-2143, Pages 95-99
Published Online April 2026 in IJEAST (http://www.ijeast.com)

traditional methods. This is because of the human processes involved. There is the guarantee of the prevention of forgery due to the immutability characteristics of the blockchain. If the certificates have any changes, the hash values will always mismatch.

A. Cloud-Based Deployment

Furthermore, the system may function as a cloud-based application, allowing for universal access to the system and the ability to remotely verify the integrity and validity of the certificate.

B. Adoption by Educational Institutions

The idea of the system can be effectively used in the contexts of the university, college, and training institutions for issuing and managing digital certificates.

C. Use in Recruitment and Employment Verification

The employer/agency can verify the qualification/degrees without contacting the awarding institution, thus enhancing the speed of the employment/selection process and establishing trust in qualifications awarded.

D. Support for Large-Scale Verification

The system can handle the high volume of verification processes due to its decentralized blockchain-based processing. This makes it scalable to be implemented across a country or institutions.

E. Reduction in Administrative Overhead and Cost

The use of this system eliminates the need for manual validation and third parties, resulting in decreased costs and labor. All in all, the blockchain technology-driven system guarantees increased security, transparency, and scalability for "VerifyCerts."

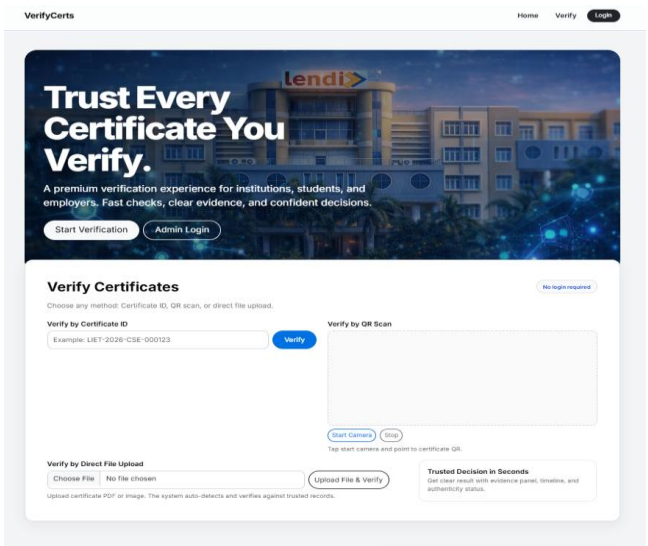

Fig. 3: User Interface

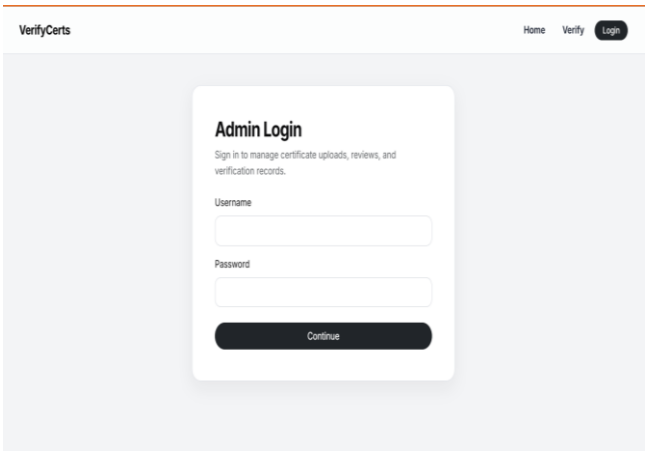

Fig. 4: Admin Login Page

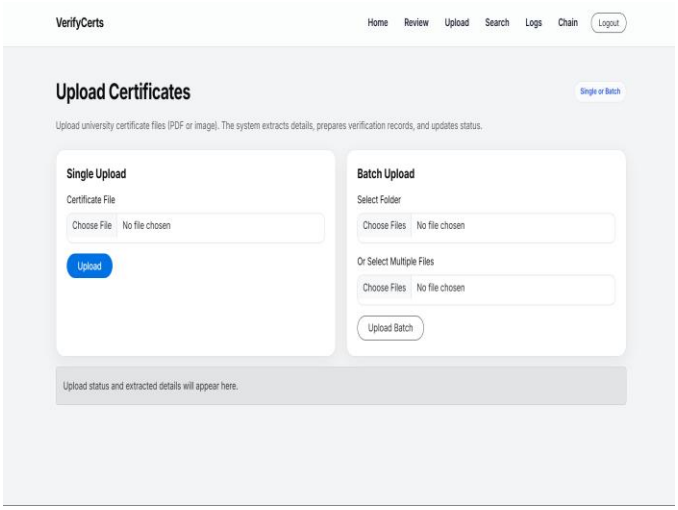

Fig. 5: Certificate Upload page

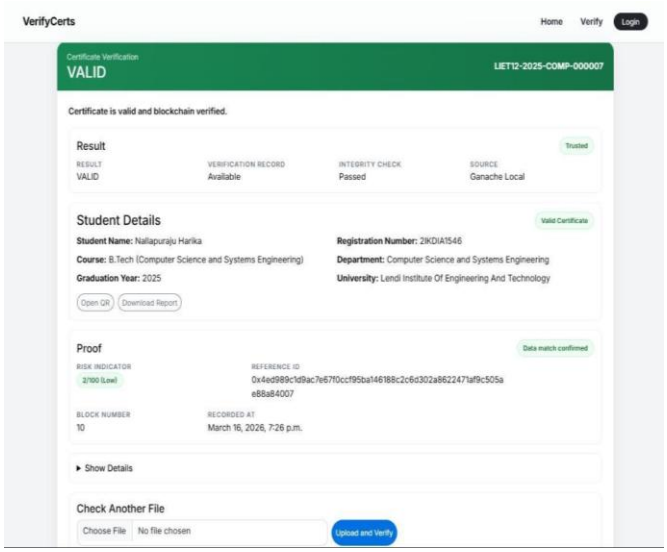

Fig. 6: Valid Result

VII. CONCLUSION

The VerifyCerts project has demonstrated the feasibility of the blockchain-integrated verification framework as it offers an effective platform for decentralized certificate verification. The project leverages the properties of blockchain to overcome the three major challenges of certificate forgery, verification delays, and dependency.

The proposed system promotes trust, transparency, and efficiency in the validation of credentials. Moreover, experimental results proved that the proposed VerifyCerts method is trustworthy and scalable, offering a strong alternative to conventional methods for verifying certificates.

VIII. REFERENCES

[1]. Sharples, M. and Domingue, J. (2016). The Blockchain and Kudos: A Distributed System for Educational Record, European Conference on Technology Enhanced Learning.

[2]. Grech, A. and Camilleri, A. (2017). Blockchain in Education, Publications Office of the European Union.

[3]. Nakamoto, S. and Chaum, D. (2008). Academic Credential Verification Using Cryptographic Hashing, Journal of Cryptographic Engineering.

[4]. Allen, C. and Dunphy, P. (2015). Decentralized Identity & Certificate Management System, Internet Identity Workshop Conference.

[5]. Christidis, K. and Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things, IEEE Access, Vol. 4.

[6]. Xu, L. and Chen, Y. (2018). QR Code Enabled Blockchain Certificate Verification, International Journal of Computer Applications.

[7]. Edge, J. and Singh, K. (2019). Blockchain for Education: Lifelong Learning Passport, ERCIM Blockchain Workshop.

[8]. Kumar, R. and Tripathi, S. (2019). Blockchain-Based Digital Certificate Authentication System, International Journal of Engineering Research & Technology.

[9]. Zhang, H. and Li, X. (2018). Secure Academic Records Sharing Using Blockchain Technology, IEEE International Conference on Data Science.

[10]. Sharma, P. and Gupta, R. (2020). Blockchain-Based E-Certificate System with Multi-Level Authentication, International Journal of Advanced Computer Science.

[11]. Nguyen, T. and Tran, M. (2020). Decentralized Academic Certificate Verification Using IPFS and Blockchain, International Conference on Emerging Technologies.

[12]. Patel, A. and Shah, D. (2019). Blockchain-Based Credential Verification with Digital Signatures, International Journal of Computer Science and Information Security.

[13]. Brown, M. and Davis, L. (2017). Tamper-Proof Certificate Verification Using Distributed Ledger Technology, International Conference on Blockchain Systems.

[14]. Wilson, E. and Moore, S. (2018). Blockchain-Based Academic Transcript Verification System, IEEE Conference on Information Systems.

[15]. Hernandez, G. and Lopez, F. (2020). Smart Contract Enabled Certificate Issuance and Verification System, International Journal of Blockchain Applications.

[16]. Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System, Cryptography Mailing List.

[17]. Crosby, M., Pattanayak, P., Verma, S. and Kalyanaraman, V. (2016). Blockchain Technology: Beyond Bitcoin, Applied Innovation Review, No. 2.

[18]. Turkanović, M., Hölbl, M., Košič, K., Heričko, M. and Kamišalić, A. (2018). EduCTX: A Blockchain-Based Higher Education Credit Platform, IEEE Access, Vol. 6.

[19]. Alammary, A., Alhazmi, S., Almasri, M. and Gillani, S. (2019). Blockchain-Based Applications in Education: A Systematic Review, Applied Sciences, Vol. 9, No. 12.

[20]. Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends, IEEE International Congress on Big Data.

IJEAST

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

ABOUT IJEAST

International Journal of Engineering Applied Science and Technology (IJEAST) is a peer-reviewed, open access journal that publishes high-quality research papers in the field of Engineering, Applied Science and Technology.

IJEAST aims to provide a platform for researchers, academicians, and professionals to share their innovative ideas, research findings, and practical experiences with the global scientific community.

FOCUS AREAS

- Engineering
- Applied Science
- Technology
- Innovation & Development
- Interdisciplinary Studies

PEER REVIEWED
All submissions are rigorously peer reviewed to ensure quality.

OPEN ACCESS
Free and unrestricted access to research for all.

GLOBAL REACH
Connecting researchers and professionals worldwide.

TIMELY PUBLICATION
We ensure a swift and efficient publication process.

For more information, visit our website
www.ijeast.com

INTERNATIONAL JOURNAL
OF ENGINEERING APPLIED SCIENCE
AND TECHNOLOGY

editor@ijeast.com
www.ijeast.com
India

2455-2143