iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.80232

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 IV Apr 2026- Available at www.ijraset.com

CredVerify: Implementation and Validation of an Academic Certificate Verification Framework Using Blockchain

Sarvesh Baban Pawar[1], Gaurav Narayan Shevkar[2], Dhanashri Ramesh Shinde[3], Gayatri Ashok Somase[4], Priti Shivaji Lahane[5]

[1, 2, 3, 4]*Student,* [5]*Associate Professor, MET's Institute of Engineering, MET Bhujbal Knowledge City, Adgaon, Nashik, Maharashtra, India*

Abstract: ***Academic certificate manipulation has proven to be a major obstacle in educational and corporate sectors, compromising trust and reliability in traditional document verification methods. CredVerify is proposed as a blockchain-based academic certificate verification system that provides transparency, originality, and protection from unauthorized manipulation. The system uses smart contracts to store cryptographic hash values and important certificate data on a decentralized storage ledger. Authorized bodies like colleges can safely issue academic documents, while companies and third parties like employers can verify them instantly without any lengthy processes. A prototype of CredVerify was implemented to check its practicality and real-world adaptability. It was tested under various conditions to assess its performance, validation speed, and efficiency. Experimental results show that CredVerify greatly lessens the time required for verification compared to existing traditional verification systems. It also enhances security as it prevents certificate tampering and unauthorized modifications. The blockchain-based design eliminates dependence on centralized storage systems and improves trust amongst all concerned parties. Overall, CredVerify provides a scalable, secure, fast, and efficient system for academic certificate verification.***

Keywords: CredVerify, Blockchain, Academic Certificate Verification, Smart Contract, Tamper-Proof System, Data Security, Fraud Detection, Transparency, Access Control, Cryptographic Hash

I. INTRODUCTION

Academic credential validation plays a very important role in ensuring reliability and authenticity in educational and corporate environments. But, the high number of manipulated certificates in recent times has caused significant problems for colleges, companies, and many authorities. Traditional validation methods are error-prone and time-consuming as they are dependent on centralized storage ledgers and manual efforts. Systems like these are prone to multiple types of breaches like unauthorized access, data breaches, and document manipulation. To solve these issues, blockchain technology provides a decentralized and secure system that allows fast verification and immutable storage, as shown in recent studies and researches [12]. Studies also prove that blockchain-based verification frameworks improve transparency and data integrity [16].

In this paper, we propose CredVerify, a blockchain-based academic certificate verification system that provides safe and secure issuance of documents and instant verification services. The system uses smart contracts to store certificate hash values and details, making sure that they cannot be changed once they are stored. It also provides privacy protection methods to enhance trust and reliability while keeping sensitive data protected [1]. A prototype was implemented and tested to understand how good the system is under various conditions on the parameters of efficiency, security, and reliability. Similar existing systems have proven that blockchain-based systems are efficient and easily scalable in real-world application [6] [14].

II. LITERATURE REVIEW

Multiple studies and researches have explored the idea of blockchain-based academic certificate verification systems because of the secure and transparent nature of blockchain systems. The research proves that blockchain helps increase transparency, reduce delays, and improve reliability and authenticity [12] [16].

Recent studies also emphasize using smart contracts for issuing, verifying, and cancelling academic certificates, making sure that the process is highly secure and efficient [6]. Privacy protection methods like zero-knowledge proof mechanisms are being proposed to protect sensitive data and certificates without compromising on efficiency [1].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

Some systems incorporate technologies like QR codes and distributed storage to prevent manipulation and help in real-time validation. Moreover, implemented prototype models showcase that blockchain can be used to ensure high efficiency, strong scalability, and consequently high adoption in colleges and companies [14]. Overall, existing studies highly advocate for the integration of blockchain in traditional certificate verification systems to improve performance.

III. OBJECTIVES

The following objectives define the main goals for CredVerify:

1) To develop a secure, web-based blockchain application that ensures authenticity and immutability of academic credentials.
2) To design an intuitive interface for uploading, viewing, and validating certificates using unique transaction IDs.
3) To integrate smart contracts for automated certificate validation and access control.
4) To ensure immutability and authenticity of issued records through cryptographic hashing techniques.
5) To establish a backend framework for data processing, blockchain transaction handling, and API communication.

IV. SYSTEM ARCHITECTURE

CredVerify is built around four core components that issue, store, and validate academic certificates effectively. They are explained and illustrated below:

A. College (Issuer)

The college is the authority that handles the generation and issuance of the academic certificates. It creates the details and readies them for authentication. After the details are created, they are forwarded for signing and attestation. The college is the main source of academic certificate records. It is ensured that only authorized colleges can create and issue certificates. The college also keeps the records on their end for possible future uses.

B. Accreditation Authority (Attester)

The accreditation authority checks and verifies the originality of the issued document. It first checks whether the college is permissioned to issue certificates. Then, it checks all the data inside the certificate to make sure it is correct. Once everything has been verified, it attests the certificate and verifies its authenticity. The authority helps enhance trust in the issued documents. This prevents fake, makeshift colleges from using manipulated certificates. It also ensures legal compliance with all rules and regulations.

C. Blockchain (Storage and Validation Layer)

The blockchain is the primary storage unit for all the issued and attested certificates and documents. It helps keep the system decentralized and secure by storing all hash values and certificate data in an immutable and tamper-proof ledger. This means that the certificate data cannot be modified once it is stored. The blockchain also provides transparency and helps ensure integrity in the verification process. This facilitates secure and instant validation without the hassle of requiring any third party. It also provides auditability by constantly keeping and updating a permanent history.

D. Employer (Verifier)

The employer of a company uses the system to verify the certificates of students during the recruitment process. He/she checks the authenticity of the certificate using the blockchain methods of the system. They can easily and instantly check the originality of the certificate data, thus increasing efficiency and reducing unnecessary delays. This helps enhance trust and reliability between the company and the student. It also helps in reducing the delays that sometimes occur because of the employers having to contact the colleges manually.

The student is not just a component in the system as he/she acts as an important actor as well. This is because, in the end, the student is the rightful owner of the certificate and all the data therein. Once the certificate is issued by the college and attested by the concerned authority, it is sent to the student for their personal use. The student is solely responsible for the storage and sharing of the certificate. The student is the main initiator of the verification process because he/she is the one who provides the certificate and its data for verification. Therefore, he/she plays an important role in controlled sharing, smooth verification, and efficient portability.

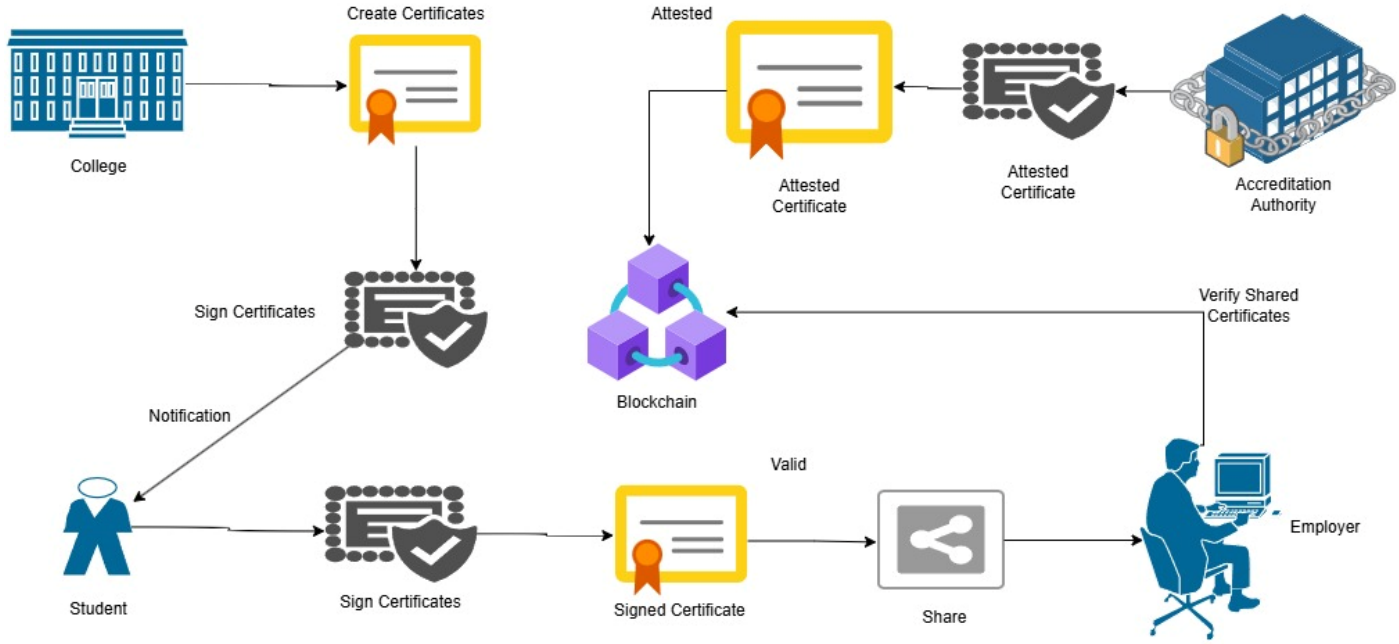


Fig. 1- Detailed CredVerify System Architecture

V. CORE ALGORITHMS AND IMPLEMENTATION

A. Certificate Hash Creation

The process of creating the hash value for a certificate involves converting all unique data in the certificate to a fixed-length special value. Even if a minute change is made in the certificate, the existing hash value will not be valid anymore. It acts like a digital fingerprint of the document. This makes sure the process remains authentic and tamper-proof. The hash is then stored on the blockchain for future use.

B. Digital Signature Verification

Digital signatures help ensure that the certificate is issued by an authorized college. The system validates this signature value using the issuer's public key value. If the data in the certificate has been manipulated, the validation does not pass. This ensures originality of the certificate data. It makes sure that the document has not been altered before being stored on the blockchain.

C. Smart Contract Execution

Smart contracts automate the processes of certificate issuance, storage, and verification. They implement existing rules without the need for human intervention. Once they are deployed, smart contracts function in an immutable and transparent ecosystem. They make sure that only authorized people can issue or cancel certificates. This drastically reduces the dependency on third parties and significantly improves trust between stakeholders.

D. Blockchain Consensus Mechanism

Consensus ensures that all the nodes in the blockchain agree on the validity of all transactions. It makes sure that malicious attackers cannot tamper with the system by causing selective nodes to crash. Only verified transactions are updated in the ledger. This maintains security and integrity. It also ensures a decentralized operation by avoiding single-point failure susceptibility.

E. Certificate Verification and Integrity Check

This process involves comparing the certificate hash with the existing hash on the blockchain. It is done by the employer during the verification process. If the hash values match, the document is considered original. If there is any difference, the document is shown as invalid and the process fails. This process helps maintain instant and secure verification without having to go to the concerned authority. It makes sure the verification is reliable and efficient.

VI. FLOWCHART-DRIVEN EXECUTION MODEL

CredVerify's design principle is that flowcharts should be treated as the main tool used when designing and developing a system (as opposed to only being used as a reference).

CredVerify follows a flowchart-driven execution model where all functions are performed in a sequential workflow. The workflow starts with the college issuing the student's certificate. Then, the certificate is verified and attested by the concerned authority. After it is approved, it is securely stored on the blockchain using smart contracts. This systematic process ensures that each and every certificate is checked to be valid, which is an important advantage of blockchain-based systems [12] [16].

The model ensures there is logical execution control by making sure that the transitions between the different stages like issuance, attestation, storage, and validation are clearly defined. Each stage provides its own independent output that acts as the input for the next stage. This helps reduce errors and skipping of steps. Structured frameworks like these are extensively discussed in modern literature about blockchain systems.

CredVerify also supports automated execution as smart contracts are used extensively throughout the system. Blockchain logic mandates access control to ensure that unidentified authorities cannot issue and/ or attest documents. If the certificate is not attested by the concerned authority for some reason like the one just mentioned, the process flow does not go to storage. This way, smart contract-enabled automation improves trust and accuracy.

During the certificate validation process, the company employer follows the workflow given in the flowchart and architecture to verify the academic certificates by submitting the required data. The system takes the certificate from the employer, creates a hash for it, and compares that hash with the already existing one. This blockchain-powered verification method helps makes the process faster and more efficient by eliminating human errors [5] [12].

Overall, flowchart-driven execution gives CredVerify a clear structure that enhances the scalability and usability of the system. It helps in reducing delays and making sure that all concerned parties can co-ordinate smoothly. The fixed workflow path ensures that all certificates follow the same pipeline. Similar real-world systems have proven that such architectures enhance reliability and performance.

VII. CONCLUSION

CredVerify successfully shows how blockchain can be used for creating safer and more efficient academic certificate verification frameworks. The system implementation makes sure that all certificate records remain immutable and transparent using smart contracts. It also significantly reduces the chances of fraud and tampering by using a decentralized blockchain framework instead of a traditional centralized one. The results of the experimental prototype prove that CredVerify has better and faster verification performance compared to traditional frameworks. Overall, the model proposes a faster, better, and more scalable solution to the problem of academic certificate verification.

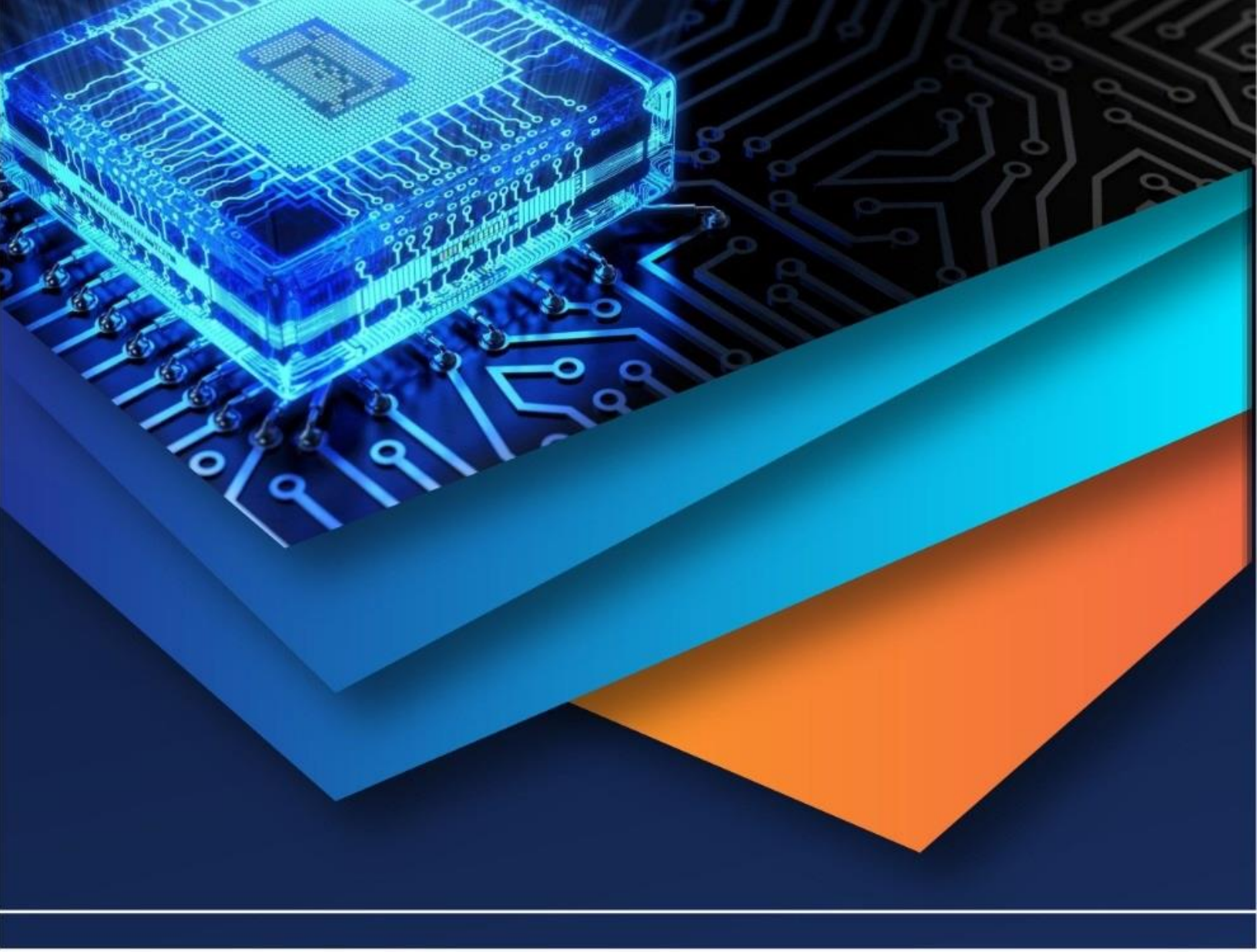
VIII. ACKNOWLEDGEMENT

We express sincere gratitude to Dr. Priti Lahane and Prof. Kunal Ahire for their invaluable guidance and support. We also thank the Department of Information Technology at MET's Institute of Engineering, Nashik, for providing resources and infrastructure for this research.

REFERENCES

[1] M. S. Rahman, M. S. Islam, and M. M. Hasan, "ZKBAR-V: Zero-Knowledge Proof-Enabled Blockchain-Based Academic Record Verification System," IEEE Access, vol. 12, pp. 1–15, 2024.
[2] J. A. Ojo and O. O. Adeyemi, "Development of Blockchain-Based Academic Credential Verification System," Open Journal of Applied Sciences, vol. 14, no. 2, pp. 1–12, 2024.
[3] A. O. Adebayo, S. O. Akinyemi, and A. A. Lawal, "Design and Implementation of a Blockchain-Based Certificate Verification System," UI Journal of Science, Logic, ICT and Robotics, vol. 7, no. 1, pp. 25–33, 2023.
[4] S. P. Patil and R. S. Patil, "Blockchain Based Academic Credential Verification System," International Journal of Engineering Research & Technology (IJERT), vol. 10, no. 6, pp. 410–415, 2021.
[5] M. A. Al-Khouri, "Blockchain Framework for Academic Certificates Verification," International Journal of Advanced Computer Science and Applications (IJACSA), vol. 15, no. 7, pp. 350–358, 2024.
[6] A. K. B. Sahoo, P. K. Das, and S. K. Panda, "BCVS: Blockchain-Based Digital Educational Certificate Verification System," Journal of Engineering, Technology and Industrial Applications (JETIA), vol. 10, no. 3, pp. 88–96, 2024.
[7] A. M. Alsharif and M. A. Alqahtani, "Privacy-Enabled Academic Certificate Authentication and Verification Using Blockchain," Journal of Systems Architecture, vol. 156, pp. 1–12, 2025.
[8] S. O. Bamidele and T. A. Ogunleye, "Study on Blockchain-Based Certificate Verification and Validation," PhilArchive Preprint, vol. 1, no. 1, pp. 1–9, 2023.

[9] R. S. Mehta and A. Sharma, "Academic Credential Verification System Using Blockchain," International Journal of Innovative Science and Research Technology (IJISRT), vol. 8, no. 4, pp. 1120–1126, 2023.
[10] K. Jadhav and P. Deshmukh, "Blockchain-Based Verification System for Academic Certificates," International Journal of Research Publication and Reviews (IJRPR), vol. 6, no. 5, pp. 120–126, 2025.
[11] A. N. Ibrahim and H. A. Yusuf, "Secure Digital Academic Certificate Verification System Using Blockchain," International Journal of Information and Computer Security (IJICS), vol. 22, no. 3, pp. 275–289, 2024.
[12] S. H. Almutairi and R. S. Alharbi, "Blockchain Technology for Enhanced Security of Academic Records," Journal of Information Systems Engineering and Management, vol. 9, no. 2, pp. 1–10, 2024.
[13] A. A. Khan, M. Rahman, and S. Ahmed, "A Decentralized Academic Certificate Issuance System Using Smart Contracts on the TRON Network," arXiv preprint arXiv:2601.08513, vol. 1, pp. 1–14, 2026.
[14] M. H. Rahman, S. Das, and M. A. Hossain, "ShikkhaChain: A Blockchain-Powered Academic Credential Verification System," arXiv preprint arXiv:2508.05334, vol. 1, pp. 1–16, 2025.
[15] D. R. Coleman and J. K. Patel, "Decentralized Credential Status Management: A Paradigm Shift in Digital Trust," arXiv preprint arXiv:2406.11511, vol. 1, pp. 1–18, 2024.
[16] 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, pp. 1–11.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY