Soham Baban Kale, 2026, 14:3
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

TrustEdu: A Blockchain-Based Framework for Secure Educational Document Verification

Soham Baban Kale[1], Nikhil Anil Khose[2], Vaibhav Uttam Kolekar[3], Vedant Vaibhav Kondejkar[4], Prof. Amol Jagtap[5]

Department of Computer Engineering, AISSMS College of Engineering Pune, India

Abstract- Document verification has always been a manual, time-consuming task for institutions and companies alike. According to data released by India's Ministry of Education, close to one million students graduate every year and move on to either higher studies or employment. Each of them carries a set of academic records — mark sheets, certificates, diplomas — that need to be verified by receiving institutions or employers. The problem is that current verification systems are centralized, which opens them up to tampering, SQL injection, collusion attacks, and straightforward document forgery. There is no reliable mechanism in place that gives a third party instant confidence in a document's authenticity. This paper presents TrustEdu, a web-based digital document locker built on top of a custom blockchain. The system lets students upload their academic documents, get them verified by their institution, and then share a QR code or unique instrument ID with any third party — eliminating the need to carry physical documents altogether. Once a document clears institutional verification, its hash is stored on the blockchain, making any subsequent tampering immediately detectable. Smart contracts automate the verification logic, and the QR code serves as a tamper-evident link between the paper record and its blockchain entry. Results show that the system significantly reduces verification time while improving the integrity and trustworthiness of shared academic credentials.

Keywords: Blockchain, Document Verification, Smart Contracts, QR Code, AES Encryption, Digital Locker, Academic Credentials.

I. INTRODUCTION

Verifying someone's academic background is a problem that sounds simple but turns out to be surprisingly hard to solve well. A university wants to confirm a candidate's degree — the traditional route is a phone call, a physical letter, or an email that goes unanswered for days. Companies running large hiring drives repeat this process hundreds of times a month. On the other side, students have to physically carry original documents to every interview, every admission office, every government window — losing them can set back years of academic effort.

The real danger, though, is fraud. Centralized document databases are a single point of failure. Once breached, they can be altered silently. Degree mills produce fake certificates that look authentic enough to pass casual inspection. The Indian education system, with its sheer volume of graduates, is particularly exposed to this problem. Background verification firms estimate that a meaningful percentage of credentials submitted during hiring contain some form of misrepresentation.

Blockchain technology offers a fundamentally different approach. Because a blockchain is distributed and each block is cryptographically linked to the one before it, modifying a stored record without detection is computationally infeasible. This property — immutability — is exactly what document verification needs. The idea is straightforward: store not the document itself, but its cryptographic hash on-chain. If the hash of the document someone submits later matches what is stored on the blockchain, the document is genuine. If it does not match, tampering has occurred.

TrustEdu applies this principle to build a practical, working system. It combines a Java-based web portal, a custom blockchain, AES encryption for document storage, Bcrypt for password hashing, and a QR code layer that ties everything together. Students, institutional administrators, and third-party organizations each interact with the system through role-specific interfaces. This paper describes the architecture, methodology, and results of that system.

II. LITERATURE SURVEY

Several researchers have explored the intersection of blockchain technology and academic credential management over the past few years. The following works

informed the design decisions behind TrustEdu.

Garima Sethia et al. [1] used Hyperledger Fabric to build a tamper-proof ledger of university-issued certificates. Their system records certificate issuance as a Fabric transaction, which other network participants can query to verify authenticity. End-to-end encryption was used for all certificate-sharing operations. The limitation of this approach is its dependence on a permissioned enterprise blockchain, which is harder for smaller institutions to deploy and maintain.

A. Gayathiri et al. [2] took a simpler route by converting SSLC, HSC, and undergraduate certificates into digital form, generating a hash for each, and storing it on-chain. The focus was on reducing friction for students during the verification process. Their work demonstrated that even a basic hash-based approach provides a meaningful improvement over manual verification.

Pavitra Haveri et al. [3] built on Ethereum and introduced off-chain storage via IPFS to keep large document files out of the chain itself. They evaluated their system under different network conditions and difficulty levels, showing that performance degrades predictably as the network scales. Their use of a multi-node private chain is relevant to our approach of building a custom blockchain.

Padmavati E. et al. [4] focused specifically on certificate counterfeiting in the employment context. Their decentralized system stores certificates as blocks and generates a unique hash per student. They noted that the real value of the system is in raising the cost of forgery to a level where it is no longer practical.

Avni Rustemi et al. [5] conducted a systematic review of 34 blockchain-in-education studies published between 2018 and 2022. They identified six main research themes and highlighted that academic adoption of blockchain-based credential verification is still in early stages. Their analysis of research gaps — particularly around scalability and cross-institutional interoperability — shaped our decision to keep TrustEdu's scope focused on institutional-level deployment first.

Devdoot Maji et al. [6] described a system where a certificate issuer creates a credential, an internal review panel validates it, and the final verified record is assigned a unique hash key. Any organization can then query this key through a web portal. This multi-party validation model closely resembles the admin-student-company three-role structure in TrustEdu.

Yogita Dharmik et al. [7] addressed forgery at the point of document creation rather than storage. They deployed blockchain at generation time and assigned each document a QR code. Even if the QR code is physically compromised, server-side hash comparison detects any alteration. This QR-plus-hash approach is directly implemented in TrustEdu.

Latha S. S. et al. [8] used the Ropsten Ethereum testnet to build a document verification platform covering birth certificates, attendance records, and academic credentials. Their work showed that a single blockchain platform can handle multiple document types — which TrustEdu supports with its flexible upload module.

Jashuva Peyyala [9] combined blockchain with IPFS in a system called Secure Doc Verifier, emphasizing that users should maintain ownership and control over their data. The emphasis on user data ownership influenced our decision to require explicit user consent before a third party can access documents.

P. Visalakshi [10] addressed the KYC problem in the Indian banking context. Customers in India undergo the same document verification process repeatedly for different institutions. A blockchain-based one-time verification, as they proposed, would remove this redundancy — the same principle applies directly to academic credential verification across multiple employers or universities.

III. METHODOLOGY

System Modules

The TrustEdu system is divided into three primary actor-based modules, each with a dedicated interface and access level.

1. Administration Module (Educational Institution)

This module is operated by college staff or a designated verification authority. Administrators log in to view pending verification requests submitted by students. For each request, they can open the uploaded documents, cross-check them against institutional records, and either accept or reject the submission. When a document is accepted, the system triggers the blockchain write — the

document hash is stored on-chain and marked as institution-verified. Administrators can also upload fresh institutional documents directly into the system, for example, new mark sheets issued by the university after results are declared.

2. Student Module

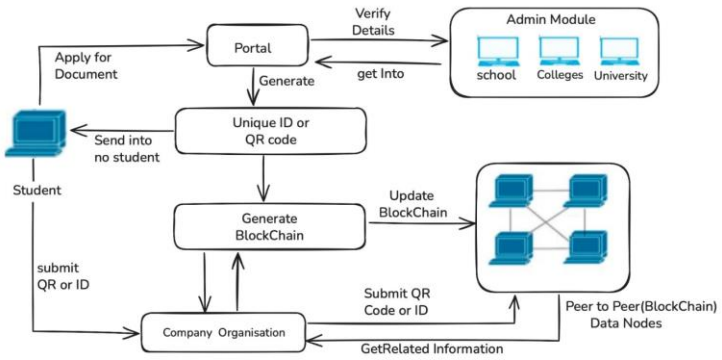
Students register on the portal with their institutional email ID and create a profile. From the dashboard, they can upload their academic documents — 10th mark sheet, 12th or diploma mark sheet, and BE/degree mark sheet — along with metadata like percentage scored, seat number, and passing year. Once uploaded, a verification request is automatically routed to the admin module. After verification is complete, the student receives a unique QR code and instrument ID tied to their verified records. They can then select which organization they wish to share records with and download the QR code in place of carrying physical documents.

3. Organization Module (Third-Party / Company)

This module serves employers, admission offices, or any third party needing to validate a candidate's academic background. Organizations log in to the portal and can either scan a QR code or enter an instrument ID to retrieve a student's verified profile. The system displays marks, seat numbers, and passing years — all drawn from blockchain-verified records. A transaction log provides an audit trail showing when the document was verified and by which institution.

Overall System Flow

The web gateway acts as a trusted neutral third party between students and institutions. It is responsible for routing verification requests, writing confirmed hashes to the blockchain, and generating the QR artifacts. Once institutional verification is complete, data is distributed across multiple blockchain data nodes. Smart contracts govern access rules — who can read, who can update, and under what conditions.



ARCHITECTURE DIAGRAM

IV. PROPOSED SYSTEM

Creating a Custom Blockchain

Rather than relying on an existing public blockchain or a permissioned enterprise network, TrustEdu implements a custom blockchain in a Java-based open-source environment. This gives the team full control over the mining strategy, block structure, and smart contract logic without the overhead of a third-party network.

Each block contains the document hash, student ID, timestamp, hash of the preceding block, and a nonce. The mining algorithm uses a chaotic code function in place of SHA-1, chosen for its stronger resistance to collision attacks — particularly relevant when the same document type is uploaded repeatedly by different students. When a document is submitted for revalidation, the same initial conditions produce the same hash, making the comparison deterministic and reliable.

QR Code and Instrument ID Generation

Once a block is mined and added to the chain, the system generates two output artifacts: a QR code and an alphanumeric instrument ID. Both encode a pointer to the student's blockchain record. The QR code is downloadable and printable. The instrument ID can be typed manually into the organization portal, covering scenarios where a camera scan is not possible.

Blockchain-Based Certificate Validation

When an organization submits a QR code or instrument ID, the system decodes the pointer, retrieves the corresponding block, recomputes the document hash

from the stored record, and compares it against the block's stored hash. A match confirms authenticity; a mismatch signals tampering. This comparison runs entirely server-side — neither the QR code nor the instrument ID alone can reconstruct or modify the underlying document.

Security Architecture
Document files are encrypted using AES before being written to the MySQL database. Passwords are hashed with Bcrypt before storage. Student, administrator, and organization credentials are held in separate database tables with no cross-access between roles. The decrypted document exists only in server memory during hash computation and is never written to disk in plaintext.

V. RESULTS

The following figures demonstrate the key workflows in the TrustEdu system.
Figure 1: Home Page The TrustEdu landing page provides login and registration access. Navigation links for Home, Register Page, and Login Page are visible in the header.

Figure 2: Student Upload Page — Educational Details After login, students fill in percentage, seat number, and passing year for their 10th, 12th/Diploma, and BE records, and attach the corresponding mark sheet file for each. A smart contract timer selector governs the active verification period.

Figure 3: Admin — Student Data Action The admin dashboard displays each student's email ID, academic percentages, and seat numbers across all levels. Accept and Reject buttons appear in the Action column; a View button opens the attached document before a decision is made.

Figure 4: Admin — Student Data Status Post-processing view showing the final Accept or Reject status for every student in the system, giving the administrator a consolidated record of all verification decisions.

Figure 5: Student — QR Code Download Verified students select the target company from a dropdown, confirm their email ID, and upload the QR image file. This step links the QR code to a specific organizational access request.
Figure 6: Company — Student QR View The organization portal shows the student's username alongside their unique QR code, confirming the linking between identity and credential.

Figure 7: Company — Full Student Profile After QR scan or instrument ID entry, the organization sees the complete verified profile: email ID, marks, and seat numbers for all academic levels. View and Transaction buttons link directly to the document and its blockchain audit trail.

VI. CONCLUSION

TrustEdu demonstrates that a blockchain-based document verification system can be practically built and deployed at the institutional level without depending on a commercial blockchain platform. The custom blockchain, combined with AES document encryption, Bcrypt password security, QR code linking, and role-based access control, produces a system that is more secure and far less time-consuming than existing centralized verification approaches.

The more important shift is in where the verification burden sits. Today it falls entirely on students, who must carry originals everywhere and arrange for physical verification at every new institution or employer. TrustEdu converts this into a one-time institutional action — after that, any number of third parties can independently verify credentials in seconds, without calling anyone.

Future work will address the brief window during which a decrypted file exists in server memory, eliminating even that temporary exposure. Once the system is stable at the college level, expanding it to a multi-university network — where each institution participates as a blockchain node — is a natural progression. Integration with DigiLocker and Aadhaar-based identity verification would further extend the trust model and open TrustEdu to a national scale.

REFERENCES

[1] Garima Sethia, Sambarapu Namratha, Srikanth H,

Sreeja C S, "Academic Certificate Validation Using Blockchain Technology," 2022 International Conference on Trends in Quantum Computing and Emerging Business Technologies, IEEE 978-1-6654-5361-5.
[2] A. Gayathiri, J. Jayachitra, Dr. S. Matilda, "Certificate Validation using Blockchain," IEEE 7th International Conference on Smart Structures and Systems (ICSSS), 2020.
[3] Pavitra Haveri, Rashmi U, Narayan D.G., Nagaratna K., Shivaraj K., "Securing Educational Documents using Blockchain Technology," IEEE Conference Publication, 2020.
[4] Padmavati E Gundgurti, Kranthi Alluri, Poornima E Gundgurti, Sai Harika K, Vaishnavi G., "Smart and Secure Certificate Validation System through Blockchain," IEEE Xplore, CFP20N67-ART.
[5] Avni Rustemi, Fisnik Dalipi, Vladimir Atanasovski, Aleksandar Risteski, "Blockchain-Based Systems for Academic Certificate Verification," IEEE Access, Volume 11, 2023.
[6] Ravi Singh Lamkoti, Devdoot Maji, Hitesh Shetty, Prof. Bharati Gondhalekar, "Certificate Verification using Blockchain and Generation of Transcript," International Journal of Engineering Research & Technology, Vol. 10, Issue 03, March 2021.
[7] Yogita Dharmik, Sakshi Gaikwad, Harshalata Patil, Priyanka Gujar, Alisha Domkundwar, "Blockchain-based Documents Verification for Smart Learning Management System," IJAEM, Volume 4, Issue 5, May 2022.
[8] Dr. P. Visalakshi, Shourya Rawat, Prateek Sen, "Document Verification using Blockchain," International Journal of Innovative Science and Research Technology, ISSN No: 2456-2165, Volume 8, Issue 7, July 2023.
[9] Rohan Shinde, Sahil Chorghe, Keval Dhanani, Prof. Abhijeet Salunke, "Doc-Chain: A University Document Verification Blockchain," IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), Pune, India, Sep 2022.
[10] Iftekher Toufique Imam, Yamin Arafat, Kazi Saeed Alam, Shaikh Akib Shahriyar, "DOC-BLOCK: A Blockchain Based Authentication System for Digital Documents," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), IEEE Xplore.
[11] S. Ramesh, P. Karthikeyan, M. Deepika, "Blockchain-Based Secure Academic Certificate Verification System," 2024 International Conference on Intelligent Systems and Secure Computing (ICISSC), IEEE, 2024.
[12] A. Verma, R. Gupta, S. Mishra, "Decentralized Educational Record Verification using Blockchain and Smart Contracts," IEEE Access, Vol. 12, pp. 45872–45885, 2024.
[13] N. Sharma, K. Patel, J. Shah, "Secure Digital Certificate Validation Framework using Ethereum Blockchain," International Journal of Advanced Computer Science and Applications (IJACSA), Vol. 15, No. 2, 2024.
[14] T. Nguyen, H. Lee, "Blockchain-Enabled Verification System for Educational Documents using IPFS," Journal of Information Security and Applications, Elsevier, Vol. 78, 2024.
[15] S. Kulkarni, V. Patil, "EduChain: Blockchain-Based Academic Certificate Validation with QR Authentication," 2025 International Conference on Smart Computing and Digital Transformation, Springer, 2025.