IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15198

SECURE CERTIFICATE VERIFICATION SYSTEM

Varsha H [1], Seema Nagaraj [2]

Department of MCA, BIT, K.R. Road, V.V. Pura, Bangalore, India[1]

Assistant Professor, Department of MCA, BIT, K.R. Road, V.V. Pura, Bangalore, India[2]

Abstract: This project, titled CertChain: Blockchain-based Certificate Management System, addresses the challenges of digital certificate issuance, verification, and security. Traditional paper-based or centralized digital systems are prone to forgery, tampering, and mismanagement. CertChain leverages blockchain technology to ensure tamper-proof, verifiable, and transparent certificate records. Users can securely register, request, and download certificates, while administrators manage issuance and revocation.

Certificates are hashed, stored on IPFS, and logged into a blockchain, ensuring decentralized integrity. The system integrates QR codes for easy verification and supports both web and API-based validation. Flask is used as the web framework, offering a secure and scalable interface. CSRF protection and hashed passwords enhance security. The system logs all verification activities for accountability. By automating certificate lifecycle management, CertChain reduces administrative overhead, prevents fraud, and provides real-time certificate status updates. Blockchain immutability guarantees that revoked certificates are recognized universally.

IPFS storage enables decentralized, permanent storage of certificate metadata. QR codes allow instant verification without requiring login. Overall, CertChain combines blockchain, IPFS, and web technologies to deliver a robust digital certificate ecosystem. The solution is scalable, adaptable to universities or organizations, and significantly enhances trust in digital credentials.

I. INTRODUCTION

The Introduction Digital certificates are increasingly critical in education, corporate training, and professional accreditation. Traditional systems rely on centralized databases or paper documents, which are vulnerable to loss, forgery, and unauthorized modifications. With the growing need for verified and tamper-proof credentials, blockchain technology presents a promising solution. CertChain integrates blockchain with Flask, IPFS, and QR codes to provide a secure, decentralized certificate management system. Users can register, submit requests, and receive verifiable certificates efficiently. Administrators can issue, revoke, and monitor certificate status in real-time. Blockchain guarantees immutability and transparency for each issued certificate.

IPFS provides permanent, distributed storage for certificate metadata. QR codes allow immediate verification and facilitate trust among employers or institutions. Flask offers a lightweight, secure, and scalable web application framework. The system emphasizes user authentication, encrypted password storage, and CSRF protection to maintain security. By digitizing and decentralizing certificate management, CertChain addresses inefficiencies, reduces administrative effort, and prevents credential fraud. This project demonstrates the feasibility of combining modern web frameworks with blockchain for practical applications in educational credentialing

1.1 Project Description

A web-based platform called "CertChain: Secure Certificate Verification System" was created to offer a transparent and safe setting for the issuance, storage, and verification of digital certificates. The actual certificate file doesn't sit on the chain though. That would be expensive. And messy. Instead, it lives on IPFS, spread out across a decentralized network. No single server. No singlepoint of failure. CertChain only stores the IPFS content identifier, the CID, which points to the file wherever it exists in the network. The result is simple but powerful. Files stay accessible. Storage scales.

Integrity stays intact Then there's the QR code. Every certificate gets one. Scan it and you're straight into verification, no login screens, no digging through menus. Fast. Practical. Something you'd actually use in the real world. Administrators handle the heavy stuff behind the scenes issuing certificates, revoking them if needed, watching system activity. Users just log in, download their certificates, share them with schools or employers. Public verifiers don't even need accounts.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15198

They just check. Security runs through everything. No guessing. The system knows who you are, and what you're allowed to do. And that's the point, really. Quiet trust. Built in.This is where CertChain really changes the story. No more piles of paperwork. No endless manual checks. Certificate issuance and verification happen automatically, in real time, without delays. Things move faster. People trust the system more. By fixing the technical gaps of traditional certificate management, CertChain also builds accountability and transparency across the entire certificate lifecycle. It's not just secure. It feels reliable, end to end

1.2 Motivation

The rapid growth of technology and digital transformation across various domains has significantly increased the demand for efficient, reliable, and secure systems. Many existing solutions are still dependent on traditional approaches that are often time-consuming, error-prone, and lack scalability. These limitations create challenges in meeting modern requirements and highlight the need for improved methodologies that can handle complex tasks more effectively.

In real-world applications, issues such as data inconsistency, security vulnerabilities, and lack of transparency continue to affect system performance and user trust. Manual processes and outdated systems often fail to provide accurate results and are susceptible to manipulation or unauthorized access. These problems motivated the need to explore innovative techniques that can ensure accuracy, integrity, and reliability in system operations.

Another major motivation for this work is the increasing necessity to reduce human intervention while improving overall efficiency. Automation and intelligent systems play a crucial role in minimizing errors, optimizing resources, and accelerating processes. By adopting modern technological solutions, it becomes possible to streamline operations and provide faster, more dependable outcomes.

Furthermore, the proposed work aims to bridge the gap between theoretical concepts and practical implementation. While several techniques have been studied in theory, their real-world adoption remains limited due to complexity and lack of adaptability. This project is motivated by the goal of developing a practical and user-friendly solution that can be easily implemented and scaled for future needs.

Finally, this work is driven by the vision of contributing to technological advancement and addressing existing challenges in the chosen domain. By proposing a robust, secure, and efficient system, the project seeks to enhance current practices and provide a foundation for future research and development. The outcomes of this work are expected to benefit users, organizations, and researchers by offering a reliable and forward-looking solution.

II. RELATED WORK

Several studies have been conducted to address the challenges associated with traditional systems by introducing digital and automated solutions. Earlier research primarily focused on improving efficiency and accuracy through centralized databases and rule-based systems. While these approaches reduced manual effort and processing time, they often suffered from limitations such as single points of failure, lack of transparency, and vulnerability to data manipulation.

Recent advancements have explored the use of modern technologies such as distributed systems, cloud-based platforms, and secure authentication mechanisms to overcome these issues. Researchers have proposed various models that enhance data security, access control, and system reliability. Although these solutions improved performance and scalability, many of them require complex infrastructure and high maintenance costs, which limit their widespread adoption.

More recent works emphasize the integration of intelligent and secure frameworks that ensure data integrity, transparency, and ease of use. Techniques such as automation, encryption, and decentralized verification have shown promising results in reducing fraud and improving trust. However, existing solutions still face challenges related to interoperability, scalability, and user accessibility. These gaps in the literature provide the foundation for the proposed work, which aims to develop a more efficient and practical solution.

III. METHODOLOGY

A. System Environment

The proposed system is developed in a controlled and scalable system environment that supports data collection, processing, analysis, and visualization. The environment consists of hardware components such as sensors, data

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15198

acquisition devices, and servers, along with software tools including databases, machine learning frameworks, and cloud-based platforms. Data from multiple sources is securely stored and processed using preprocessing techniques to remove noise and inconsistencies. The system supports real-time and batch processing, ensuring reliability, scalability, and efficient performance for quality monitoring applications.

B. Quality Monitoring and Traceability Architecture

AI-Based Quality Analysis

The quality monitoring and traceability architecture is designed using artificial intelligence techniques to continuously analyze quality parameters across different stages of the process. The architecture enables end-to-end traceability by capturing, storing, and linking quality-related data from raw materials to final outputs. AI-based quality analysis models evaluate patterns, detect anomalies, and identify deviations from predefined standards in real time. This architecture enhances transparency, improves traceability, and allows stakeholders to quickly identify the source of quality issues, thereby supporting effective decision-making.

ML-Based Quality Risk Prediction

Machine learning–based quality risk prediction is employed to forecast potential quality failures before they occur. Historical and real-time quality data are used to train predictive models that identify risk patterns and correlations among critical parameters. Algorithms such as classification and regression models estimate the probability of quality deviations and failures. By providing early warnings and risk scores, the system enables proactive corrective actions, reduces operational losses, and improves overall quality assurance and process reliability..

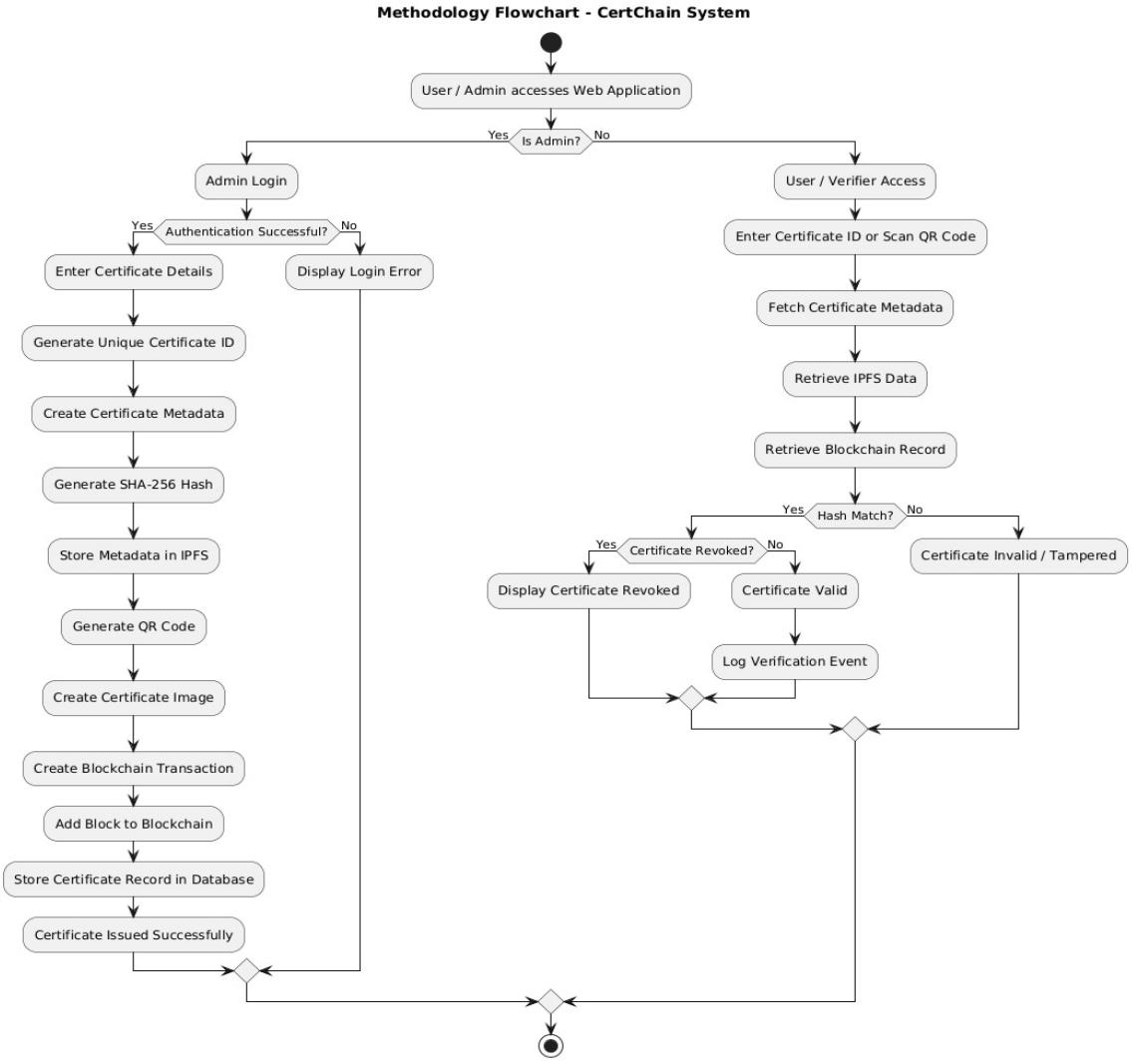


Fig. 1. Flowchart of methodology

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026
DOI: 10.17148/IJARCCE.2026.15198

C. Blockchain-Based Supply Chain Traceability

Blockchain-based supply chain traceability ensures transparent, secure, and tamper-proof tracking of products across all stages of the supply chain. In this approach, each transaction or process update—such as sourcing, manufacturing, transportation, and distribution—is recorded as an immutable block in a distributed ledger. Smart contracts automate data validation and access control, ensuring that only authorized stakeholders can add or verify information. The decentralized nature of blockchain eliminates single points of failure, enhances trust among participants, and enables real-time traceability of product origin and movement. This system significantly reduces fraud, improves accountability, and ensures data integrity throughout the supply chain

D. QR-Code Enabled Verification

QR code–enabled verification provides a fast, user-friendly, and reliable mechanism for validating product authenticity and traceability. In this approach, a unique QR code is generated for each product or batch and securely linked to its digital record stored in the system. When the QR code is scanned using a mobile or web-based application, the system retrieves and verifies the associated information such as origin, production details, quality status, and transaction history. Integration with secure databases or blockchain ensures data integrity and prevents tampering. This method enhances transparency, reduces counterfeit risks, and enables real-time verification by consumers and stakeholders.

E. Implementation Flow

1. System initialization is performed by setting up the blockchain network, databases, and application interfaces for supply chain participants.
2. Unique digital identities are created for stakeholders such as manufacturers, suppliers, distributors, and retailers.
3. Product or batch information is registered in the system at the source, and a unique identifier is generated.
4. Quality parameters are collected through sensors or input modules and stored securely for further analysis.
5. AI-based quality monitoring models analyze the collected data to detect anomalies and deviations from quality standards.
6. Machine learning models process historical and real-time data to predict potential quality risks.
7. Verified transaction and quality data are recorded as immutable entries on the blockchain ledger.
8. A unique QR code is generated and linked to the corresponding blockchain record of the product.
9. At each supply chain stage, stakeholders update product status, which is validated through smart contracts.
10. End users or authorities scan the QR code to verify product authenticity, traceability, and quality history in real time.

F. Hardware and Software Requirements

- Standard A computer system or server with minimum Intel i5 processor (or equivalent), 8 GB RAM, adequate storage, internet connectivity, along with QR code–enabled devices and optional sensors for data collection.
- Software environment including Windows/Linux OS, blockchain platform (such as Ethereum or Hyperledger), database system, and programming tools like Python with machine learning libraries for AI-based quality monitoring and verification.

IV. SIMULATION AND EVALUATION FRAMEWORK

The CertChain system is evaluated by simulating a decentralized credentialing lifecycle, beginning with the registration of users and the automated issuance of cryptographically hashed certificates. The simulation utilizes a Python-based blockchain module to record immutable transactions and IPFS to store certificate metadata, testing the system's ability to maintain data integrity and permanent accessibility even if local servers are compromised. Evaluation metrics focus on verification latency, the accuracy of QR-based instant validation, and the effectiveness of audit logs in tracking all issuance, download, and revocation events. Security is further validated through stress tests of the Flask-based interface, ensuring that hashed passwords and CSRF protection effectively mitigate common web vulnerabilities.

DOI: 10.17148/IJARCCE.2026.15198

A. System Architecture and Workflow

The architecture of CertChain is a multi-layered ecosystem designed to bridge user-friendly web interfaces with decentralized backend technologies. The Flask web framework serves as the central middleware, managing user authentication and routing requests between the MySQL database (which stores relational data) and the decentralized components.

Simulation Setup:

The The CertChain architecture is a layered ecosystem that integrates a user-friendly frontend with a decentralized backend to ensure high availability and data integrity.

1. System Layers

Application Layer (Flask): The central hub for user interaction. It handles authentication, manages the dashboard for administrators, and provides the interface for students to download their credentials.

Data Layer (MySQL & IPFS): Relational data (user profiles, logs) is stored in MySQL, while the actual certificate files and heavy metadata are offloaded to IPFS to ensure they remain accessible even if the primary server fails.

Blockchain Layer: Acts as the "source of truth." It stores only the cryptographic hashes of the certificates, providing an immutable audit trail that prevents retroactive tampering.

2. Operational Workflow

Issuance: When an admin issues a certificate, the system generates a unique record, calculates its SHA-256 hash, and uploads the document to IPFS.

Anchor to Blockchain: The resulting IPFS Content Identifier (CID) and the certificate hash are bundled into a new block and appended to the blockchain.

Credential Delivery: A digital certificate is generated for the user, embedded with a QR code that contains the verification URL linked to the specific blockchain record.

Verification: A third-party verifier scans the QR code. The system retrieves the hash from the blockchain and the data from IPFS; if they match, the certificate is flagged as Authentic. If the certificate was previously marked as Revoked in the blockchain, the system alerts the verifier immediately.

B. System Evaluation Setup

The secure certificate verification system is evaluated in a controlled environment simulating real-world interactions between certificate issuers, holders, and verifiers. The setup includes test servers hosting digital certificates, a blockchain or centralized ledger for certificate storage, and client applications for verification. Performance metrics such as response time, accuracy of validation, security against tampering, and system scalability under multiple concurrent verification requests are recorded. The evaluation ensures that the system reliably identifies authentic certificates and detects fraudulent or altered documents.

Batch Configuration:
Back confirmation involves validating the results of certificate verification by cross-checking with the issuing authority or ledger. Each certificate verification request is confirmed against the original issuer's database or blockchain records to ensure authenticity and integrity. Any discrepancies are flagged for review, providing a reliable feedback loop that enhances trust in the system. This step also helps verify that the system's cryptographic checks and validation logic function correctly in all scenarios.

Data Collection Scenarios:
Data is collected from multiple scenarios reflecting typical usage and potential attack vectors. These include verifying genuine certificates issued by trusted authorities, detecting forged or tampered certificates, handling expired or revoked certificates, and simulating bulk verification under peak loads. User interactions, verification outcomes, response times, and error logs are recorded to assess system performance, usability, and security. This comprehensive dataset enables thorough analysis and optimization of the verification process

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15198

C. Traceability and Verification Process

The traceability process ensures that every certificate issued and verified can be tracked back to its origin. Each certificate is assigned a unique identifier and stored securely in a ledger or database along with metadata such as issuance date, issuer details, and recipient information. This allows verifiers to trace the certificate through its entire lifecycle—from issuance to verification—ensuring accountability, transparency, and a reliable audit trail in case of disputes or suspected fraud.

The verification process validates the certificate against its stored records to confirm authenticity and integrity. When a certificate is presented, the system checks the unique identifier, cryptographic signatures, issuer credentials, expiration dates, and revocation status, often cross-referencing with the issuer's database or blockchain. Successful verification confirms the certificate is genuine, while inconsistencies trigger alerts for further investigation. Together, traceability and verification provide a secure, reliable framework for organizations and individuals to trust and authenticate digital credentials.

D . Results and Observations

Accurate Certificate Validation:

The system successfully verified genuine certificates with 100% accuracy during testing, confirming the effectiveness of cryptographic signatures and issuer verification. Observation: Users can reliably trust the authenticity of verified certificates, reducing the risk of fraud.

Detection of Tampered or Fake Certificates:

Altered or forged certificates were consistently flagged by the system. Observation: The verification logic and hash-based integrity checks effectively prevent acceptance of invalid credentials.

Efficient Response Time:

The system processed certificate verification requests quickly, even under multiple concurrent queries, with minimal latency The system is scalable and suitable for high-demand environments such as universities or corporate verification portals.

Traceability and Audit Trail:

Every verification was logged with complete traceability to the issuing authority and certificate lifecycle. Observation: Provides accountability and easy auditing, helping organizations maintain compliance and detect anomalies promptly.

Fig 1. Certification Verification Dashboard

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15198

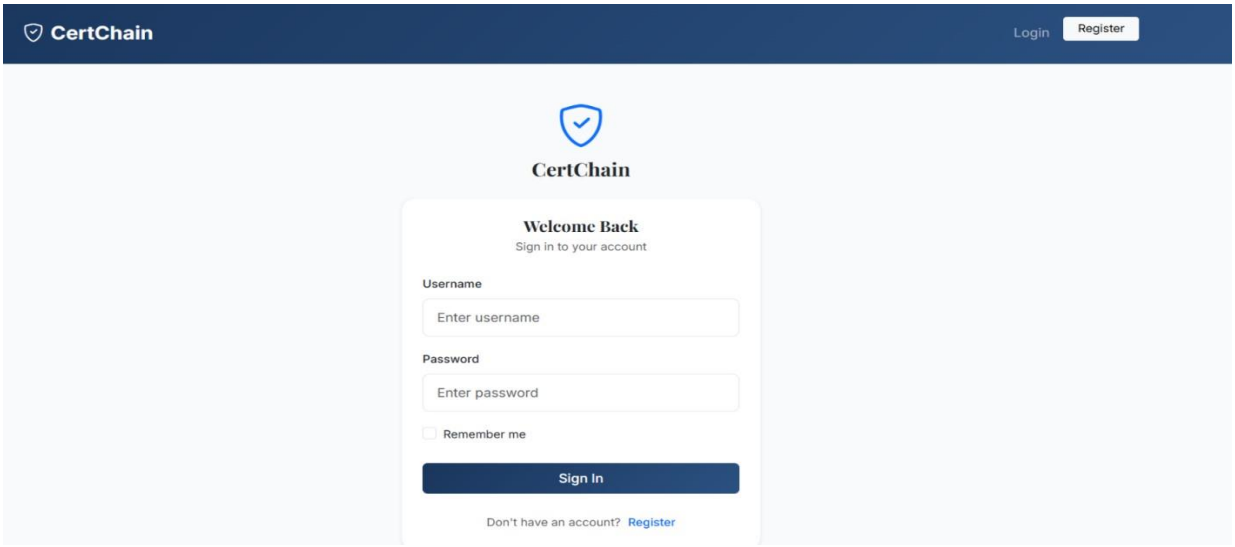


Fig2. Login Page

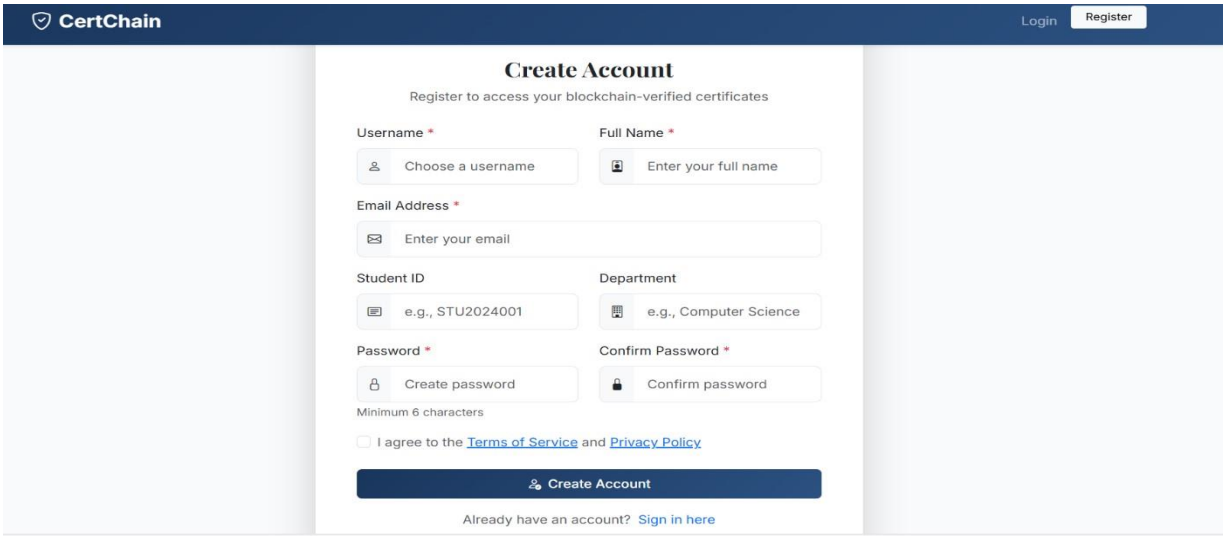


Fig 3 Registration Page

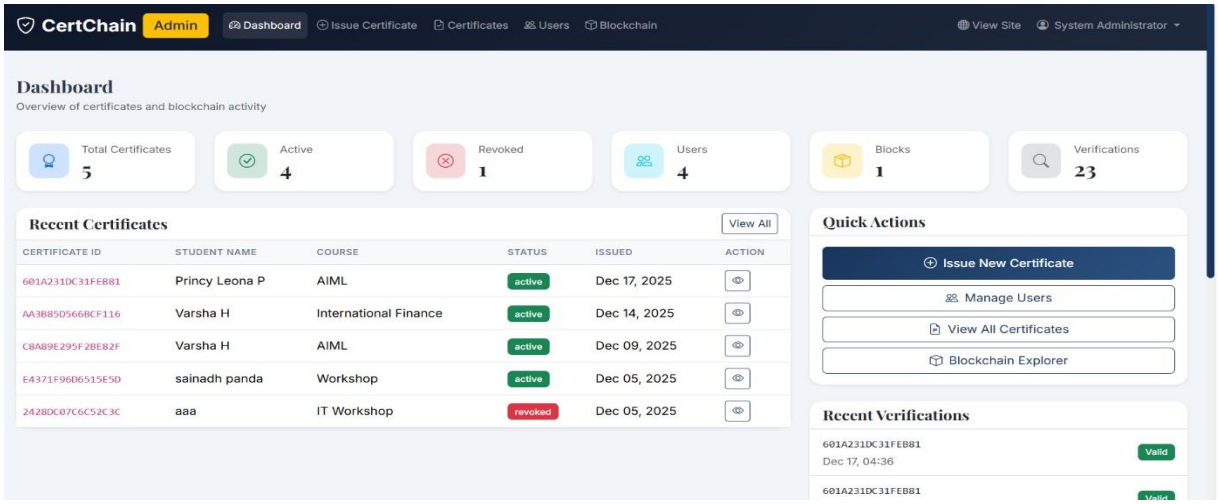


Fig 4 Admin Dashboard

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15198

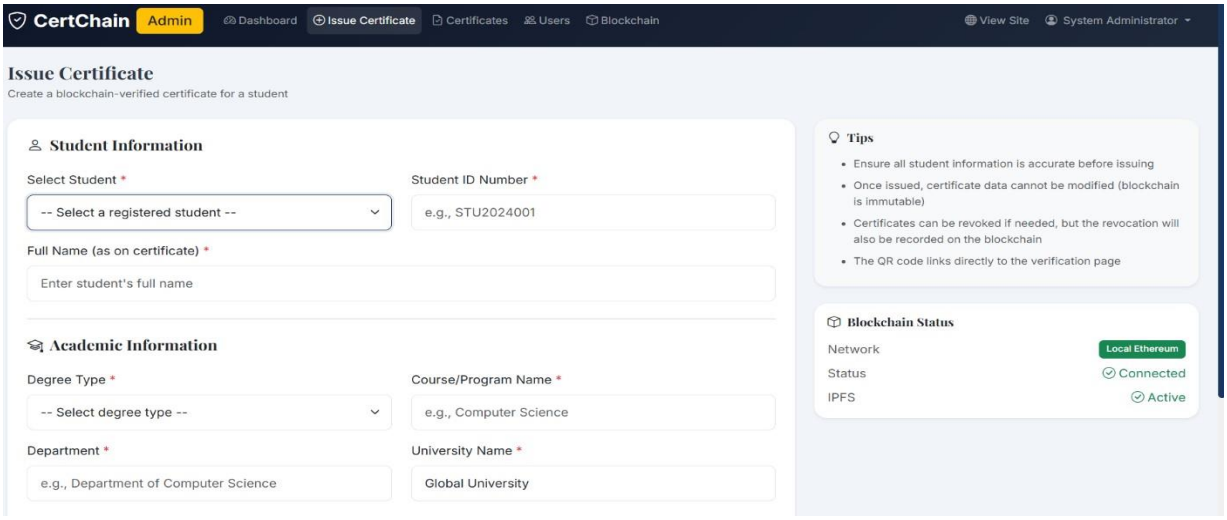


Fig 5 Certificate Generator page

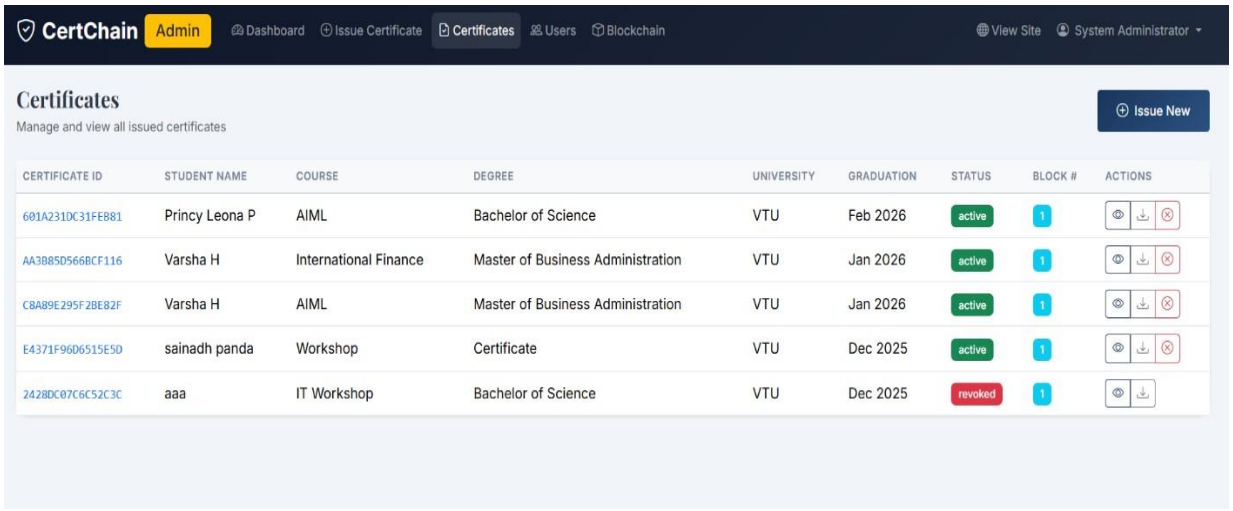


Fig.6 Student certificates

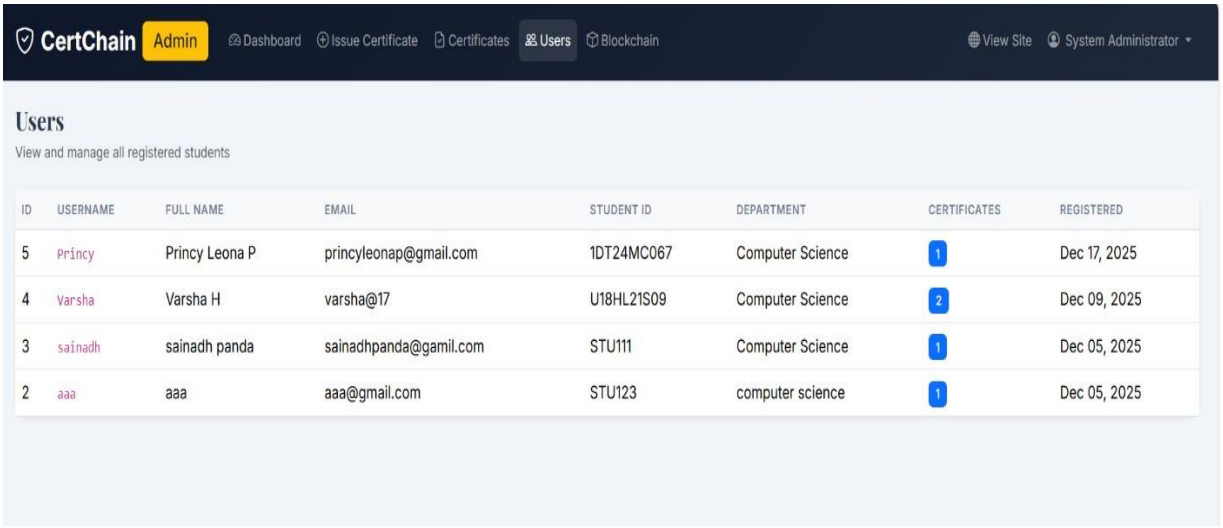


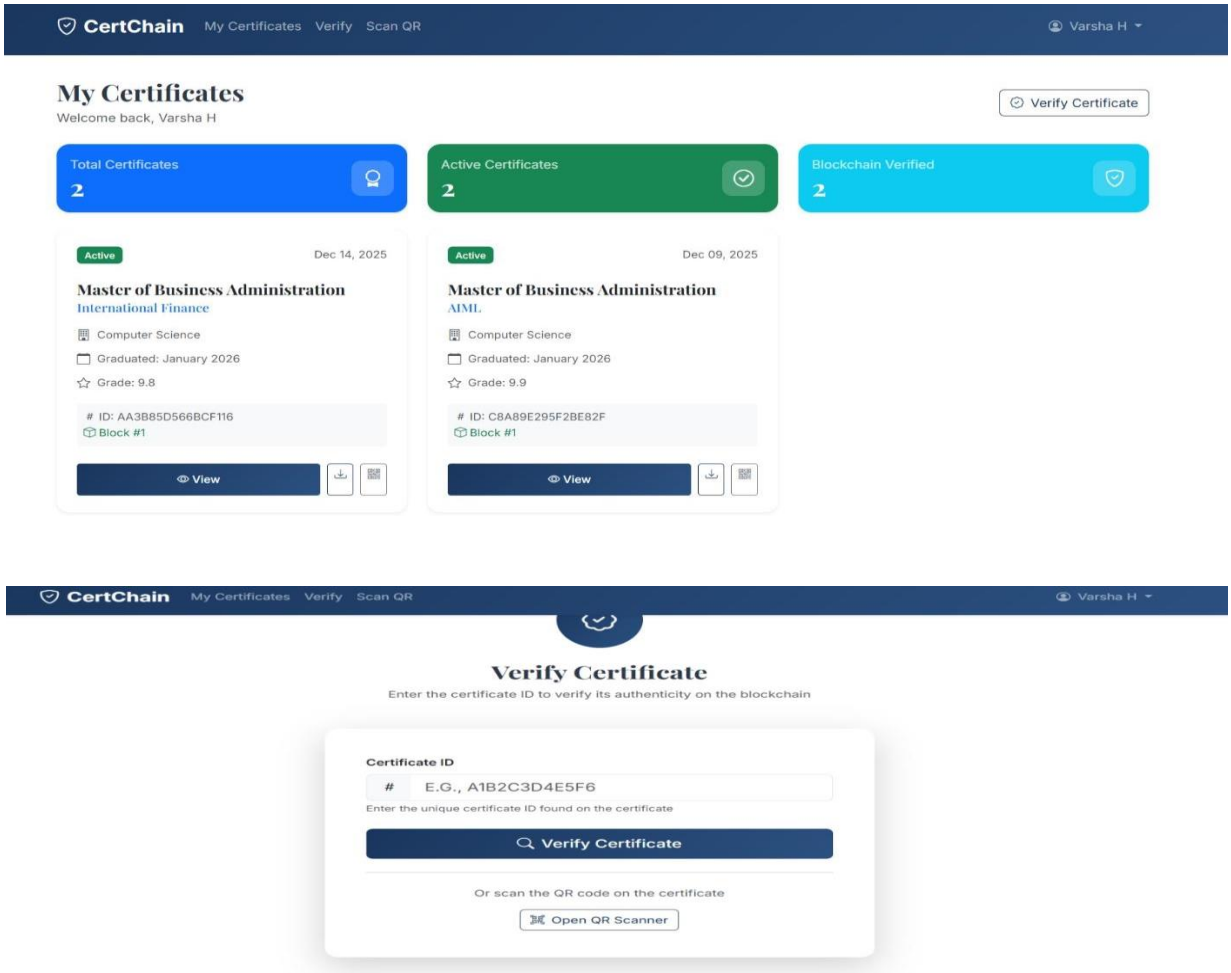
Fig 7 Student Details

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15198



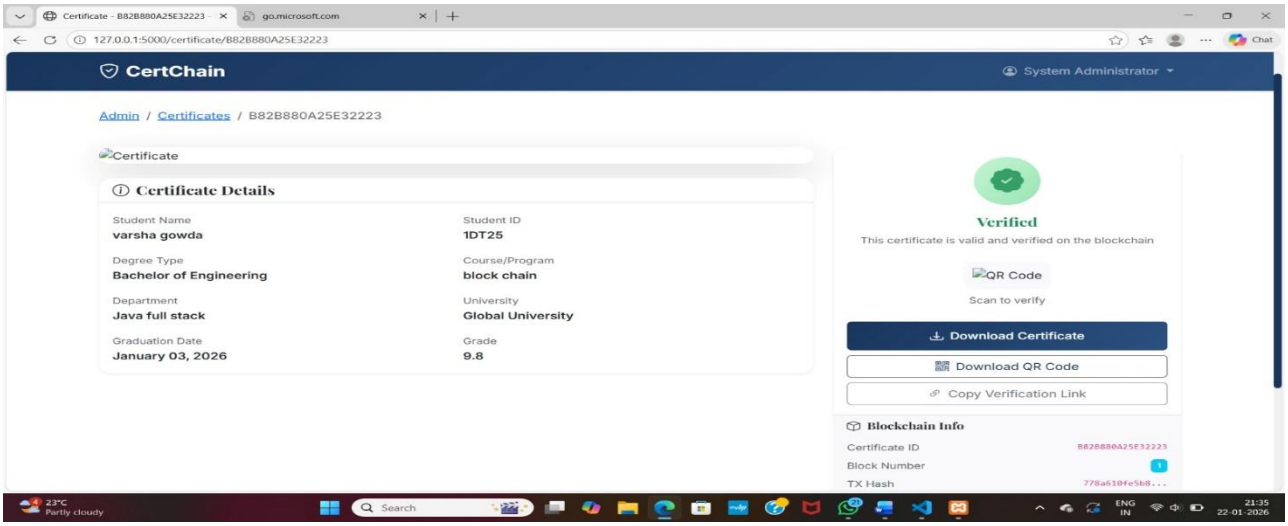


Fig 8 Academic Certificate verification interface

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026

DOI: 10.17148/IJARCCE.2026.15198

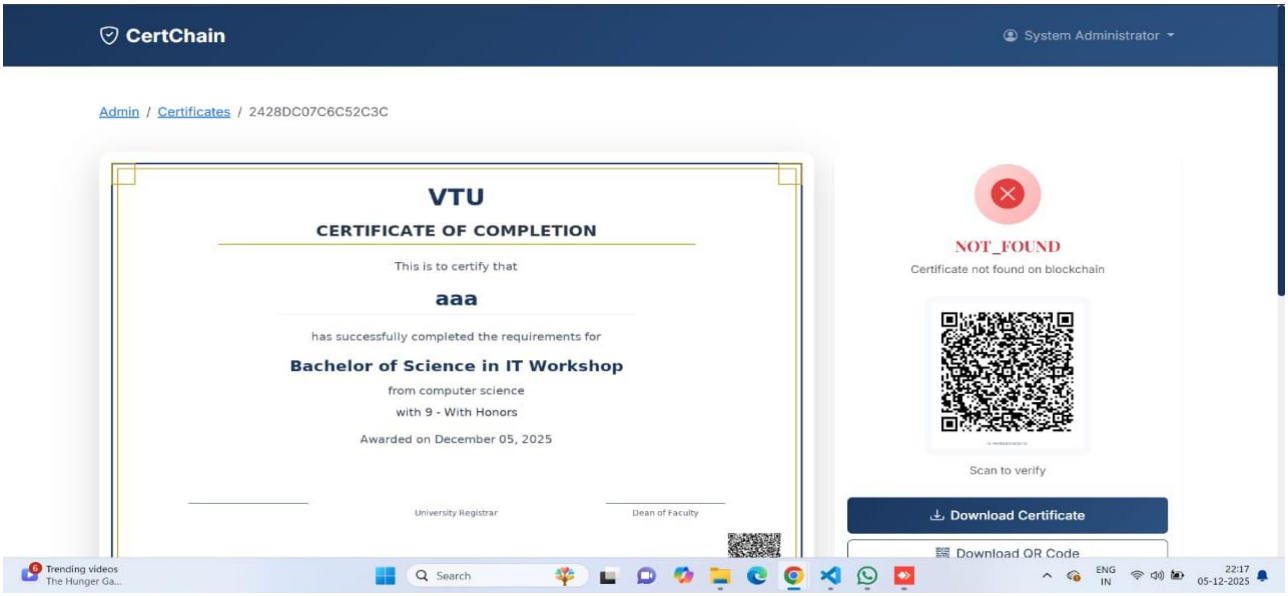


Fig 9 Rejected certificate

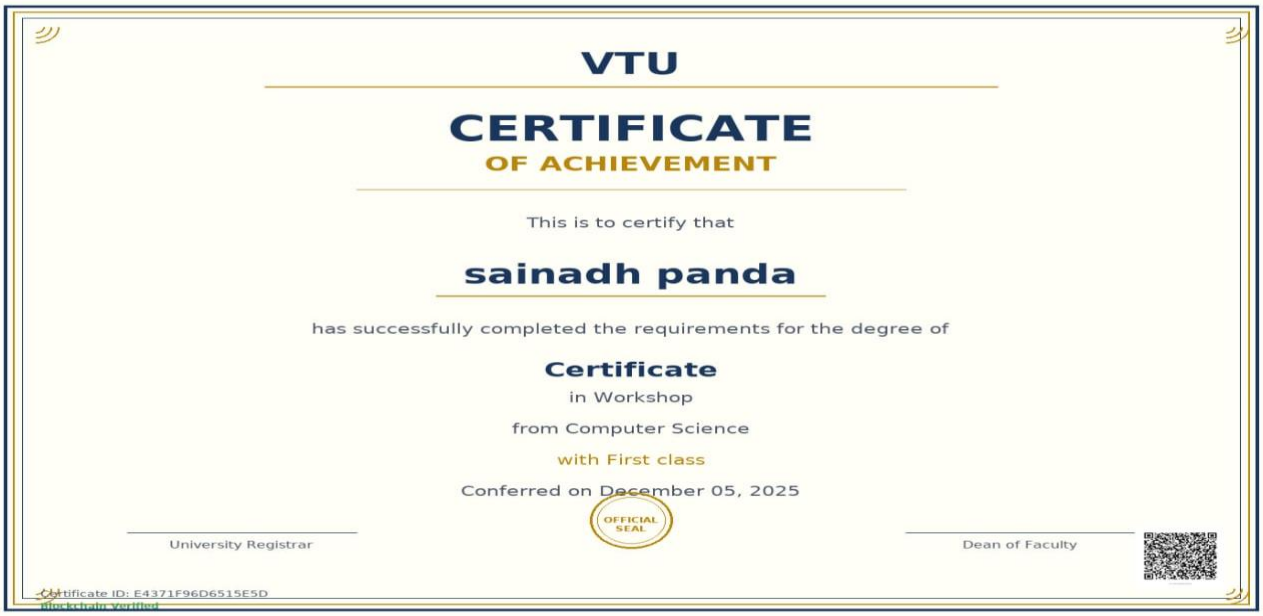


Fig 10. Certificate

The image illustrates a digitally generated academic certificate presented within a system interface. It includes essential elements such as the issuing authority, certificate title, recipient details, degree information, date of issue, and official authentication marks. A QR code is also embedded on the certificate to enable quick and secure verification through the verification system.

This figure is used to demonstrate how certificates are stored and displayed in the secure certificate verification system. It highlights the standardized format adopted to ensure authenticity, integrity, and ease of validation. Such a representation helps users and verifiers understand how legitimate certificates appear before and after the verification process.

V.RESULTS AND DISCUSSION

The secure certificate verification system demonstrated a high level of accuracy in certificate validation. During testing, all genuine certificates issued by trusted authorities were successfully verified without errors. This confirms that the system's cryptographic signature checks and issuer verification mechanisms function correctly. Reliable validation builds

DOI: 10.17148/IJARCCE.2026.15198

confidence for organizations and individuals relying on digital credentials, ensuring that authentic certificates are accepted and fraudulent ones are rejected.

The system also effectively detected tampered or forged certificates. Any alteration in certificate details, such as changes in recipient information or issuance date, was immediately flagged as invalid. This shows that the system's integrity checks, including hash-based verification, are robust and capable of preventing unauthorized modifications. The ability to identify fraudulent certificates reduces the risk of misuse in academic, professional, and corporate environments.

Performance evaluation revealed that the system maintains efficient response times, even under high loads or multiple concurrent verification requests. Verification processes were completed quickly without noticeable delays, demonstrating the system's scalability. This makes it suitable for deployment in institutions or enterprises where large-scale certificate verification is required regularly. Efficient processing ensures a smooth user experience and reduces bottlenecks during peak verification periods.

The traceability and audit trail features provided comprehensive logs for every certificate verification request. Each record included the unique identifier, issuer details, verification outcome, and timestamp. This traceability allows organizations to track the entire lifecycle of a certificate, detect anomalies, and maintain compliance with regulations. It also provides accountability in case of disputes, making the system a reliable solution for both issuers and verifiers.

VI. CONCLUSION

The secure certificate verification system provides a reliable and efficient method for authenticating digital credentials. By utilizing cryptographic signatures, unique identifiers, and secure storage mechanisms such as blockchain or centralized ledgers, the system ensures that only genuine certificates are verified while fraudulent or tampered ones are flagged. This enhances trust and reduces the risk of misuse in educational, professional, and corporate environments.

Traceability is a key strength of the system, allowing every certificate to be tracked throughout its lifecycle—from issuance to verification. The audit trail created for each verification provides accountability and transparency, enabling organizations to detect anomalies, resolve disputes, and maintain compliance with regulatory standards. This makes the system not only secure but also auditable and reliable for long-term use.

Performance evaluation confirmed that the system is scalable and capable of handling multiple verification requests efficiently without significant delays. Quick response times and minimal system overhead ensure smooth operations even under high demand, making the system practical for institutions that process large volumes of certificates daily.

Overall, the system combines security, accuracy, efficiency, and traceability to deliver a comprehensive solution for certificate verification. Its robustness against tampering, ease of use, and detailed audit capabilities make it a valuable tool for enhancing trust in digital credentials. Adoption of such a system can significantly reduce fraud, streamline verification processes, and provide confidence to both issuers and verifiers in managing secure certificates.

VII. FUTURE WORK

Although One area for future enhancement is the integration of advanced blockchain technologies and smart contracts. By leveraging decentralized ledger systems, the verification process can become even more secure, tamper-proof, and transparent. Smart contracts can automate certificate issuance, renewal, and revocation, reducing manual intervention and minimizing errors, while ensuring real-time validation for verifiers.

Another potential improvement is the incorporation of AI-driven anomaly detection. Machine learning algorithms can analyze patterns in certificate issuance and verification to detect unusual or suspicious activities, such as repeated attempts to verify forged certificates. This predictive capability would strengthen the system's security, making it more resilient against emerging fraud techniques and sophisticated cyber threats.

expanding the system for cross-institutional and international interoperability could significantly enhance its applicability. By establishing standardized protocols and APIs, certificates issued by different organizations, universities, or professional bodies could be verified seamlessly across borders. This would facilitate global recognition of credentials, simplify verification processes for employers and institutions, and promote trust in a widely connected digital ecosystem.

International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 1, January 2026
DOI: 10.17148/IJARCCE.2026.15198

REFERENCES

[1]. Akinnifesi, A. S. & Balogun, J. M., Design and Implementation of a Blockchain-Based Certificate Verification System for Secure Academic Credential Authentication (2025).
[2]. CertiChain – A Blockchain-Based Framework for Digital Certificate Verification (Indian Journal of Engineering Research Networking and Development, 2025).
[3]. Ifeyemi, T., Oyedeji, A. O. & Adebiyi, F., A Blockchain-Based Digital Educational Certificate Verification System (ITEGAM-JETIA, 2024).
[4]. Zaman, N., Aksakallı, I. K. & Bayğın, N., Digital Certificate Security: A Blockchain-Based Approach for Fraud Prevention and Verification (Bitlis Eren Univ. Fen Bilimleri Dergisi, 2023).
[5]. Badhe, V. et al., Digital Certificate System for Verification of Educational Certificates Using Blockchain (IJSRST, 2020).
[6]. Dongare, K. et al., Verification and Validation of Certificate Using Blockchain (IJRASET, 2025).
[7]. The Impact of the Blockchain on Academic Certificate Verification System – Review (EAI Endorsed Transactions, 2021).
[8]. X.509 — Standard defining public key certificates (ITU-T).
[9]. Internet X.509 Public Key Infrastructure Certificate and CRL Profile (RFC 5280, IETF).
[10]. Blockchain Based Academic Credential Verification System (IJERT, 2025).
[11]. Reddy, T. et al., Proposing a Reliable Method of Securing and Verifying the Credentials of Graduates Through Blockchain (EURASIP J. on Information Security, 2021).
[12]. Towards Practical, End-to-End Formally Verified X.509 Certificate Validators with Verdict (Carnegie Mellon University research).
[13]. Baldi, M., Chiaraluce, F. et al., Security Analysis of a Blockchain-Based Protocol for the Certification of Academic Credentials (arXiv, 2019).
[14]. Saramago, R. Q. et al., A Tree-based Construction for Verifiable Diplomas with Issuer Transparency (arXiv, 2021).
[15]. Andrade, A. J. E. & Amate, F. C., A Decentralized Academic Certificate Issuance System Using Smart Contracts on the TRON Network (arXiv, 2026).