IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, June 2026
Impact Factor: 8.2

Chain of Trust: Secure and Transparent Digital Certificate Verification Using Blockchain

Prof. Sagar Dhanake[1], Rutuja Ingle[2], Suhani Zodage[3], Akshata Gangurde[4] and Sunakshi Gaikwad[5]
Professor, Department of Computer Engineering, Pune, India[1]
Students, Department of Computer Engineering, Pune, India[2-5]
[1] sagar.dhanake@dypatilef.com[2] rutujaingale059@gmail.com
[3] suhani3858@gmail.com [4] akshatargangurde2217@gmail.com, [5] sunakshigaikwad2@gmail.com
Dr. D. Y. Patil College of Engineering and Innovation, Pune, India.

Abstract: *Since confirming the legitimacy of applicants' cre-dentials is still crucial to preserving the integrity of hiring pro-cedures, the rising prevalence of forged certificates and falsified work experience has become a major problem for businesses, educational institutions, and employers. Due to their manual nature, traditional verification techniques are time-consuming, expensive, and prone to human mistake. As a result, hiring choices may be made inefficiently, unqualified candidates may be accepted, and system trust may be diminished. This project uses blockchain technology and artificial intelligence to create a safe, automated, and transparent platform for certificate generation and verification in order to address these problems. Employee registration is the first step in the process, after which a digital request for an experience certificate is submitted. The request is then sent to the relevant organization for verification via a special dashboard. In order to prevent fraud, authorized workers examine the request and verify the candidate's work history, rejecting any assertions that cannot be independently verified. After verification, the system conducts an AI-driven skill evalu-ation to determine the employee's competencies and produces a comprehensive report to assist in making well-informed decisions. After going through a multi-level review process to guarantee accuracy and accountability, the request is either accepted or denied. If accepted, a digital certificate with an integrated QR code that allows for quick and safe verification is created in a standard format. In order to guarantee immutability and guard against manipulation, the system can also store certificate data on a blockchain network and update the employee's digital profile. Furthermore, a public verification portal enables third parties to instantly verify certificates using a unique identification or a QR code. Overall, while maintaining scalability for applications in the fields of professional certification, employment, and education, this system improves efficiency, increases transparency, lowers fraudulent activity, and fosters trust in certificate verification procedures.*

Keywords: SHA-256, QR codes, blockchain, smart con-tracts, security, and certificate verification

I. INTRODUCTION

Digital certificates have become much more popular in educational institutions and professional associations in recent years. Certificates are frequently used as evidence of academic credentials, abilities, and accomplishments. But the increasing usage of digital documents has also resulted in an increase in unauthorized changes and certificate forgeries, raising grave questions about validity and trust. Traditional certificate ver-ification systems rely on manual validation procedures and are primarily centralized. In addition to taking a lot of time, these techniques are prone to mistakes, data manipulation, and delays. To validate certifications, firms frequently need to get in touch with the issuing authorities, which adds complexity and decreases efficiency. A safe, automatic, and trustwor-thy verification mechanism is therefore desperately needed. Blockchain technology has become a potent remedy for these problems. Data integrity, transparency, and immutability are guaranteed by this decentralized distributed ledger technol-ogy. Because data

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 4, June 2026 Impact Factor: 8.2

cannot be removed or changed once it is saved on the blockchain, it is ideal for secure record-keeping applications like certificate verification. The ”Chain of Trust: Secure and Transparent Digital Certificate Verification System,” which uses blockchain technology to stop certificate fraud, is presented in this paper. A cryptographic hashing algorithm is used in this system to create a distinct digital fingerprint for each certificate. This hash value is kept on the blockchain, making it simple to identify any changes made to the certificate. Furthermore, the system creates a distinct certificate ID and QR code, which enables consumers to swiftly and effectively validate certificates. In order to ascertain authenticity, the system verifies by comparing the created hash with the one kept on the blockchain. This method yields immediate results and does away with the necessity for manual verification.

II. OBJECTIVES

The main goal of the suggested system is to use blockchain technology to create a trustworthy and safe certificate verification system. By using cryptographic hashing techniques, the system seeks to avoid unwanted alterations and certificate forgeries. By keeping certificate hashes on a decentralized blockchain network, it guarantees data integrity and im-mutability. Additionally, the system is built to reduce reliance on manual and centralized verification procedures by offering quick and automatic verification through the use of QR codes and unique certificate identifiers. Enabling transparent and reliable validation for institutions and organizations is another key component of the suggested solution. Additionally, it has a revocation mechanism to render compromised or inaccurate certificates invalid. All things considered, the system is meant to be effective, scalable, and appropriate for practical uses.

III. LITERATURE REVIEW

Blockchain technology has been investigated in a number of studies to solve ineffective verification mechanisms and certificate forgery. Decentralized solutions are required since traditional systems are centralized, time-consuming, and ma-nipulable. [1] presents a blockchain-based certificate authen-tication system that uses distributed ledgers to securely store and verify certificate data. Similarly, decentralized document verification systems and its practical uses are covered in [2]. A blockchain-based certificate validation method is suggested in
[3] to guarantee authenticity and stop manipulation. The work in [4] focuses on developing blockchain-based safe document verification solutions. The significance of automation and transparency in certificate verification systems is emphasized by research in [5] and [6]. Additionally, a blockchain-based architecture for digital certificate validation is presented in [7]. While [8] suggests an incentive-based certification system, [9] presents DocCert, a blockchain-based document authentica-tion system. In a similar vein, [10] introduces a blockchain-based system for degree verification and accreditation. Apart from these works, [11] suggests a cryptographic hashing-based blockchain-based certificate verification method. While
[12] addresses safe data sharing in decentralized settings,
[13] shows how smart contracts automate validation proce-dures. Hashing and smart contracts are important elements in verification systems, according to a systematic review in [14]. Improving transparency and combining blockchain with IPFS for effective storage are the main goals of research in
[15] and [16]. While [17] presents the idea of decentralized ledgers, [18] investigates blockchain applications in education. Furthermore, verified credentials and decentralized identity are covered in [19]. Additional research on blockchain ap-plications in education is presented in [20], and EduCTX for safe academic credit management is presented in [21]. Scalability, affordability, and real-world integration are still issues despite these developments. By offering a scalable and secure certificate verification mechanism, the suggested system overcomes these drawbacks.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, June 2026
Impact Factor: 8.2

IV. SYSTEM ARCHITECTURE

The suggested approach uses blockchain technology to offer a safe, transparent, and impenetrable method for digital certifi-cate verification. The architecture uses a modular design with several interdependent parts that guarantee effective certificate creation, storage, and validation.

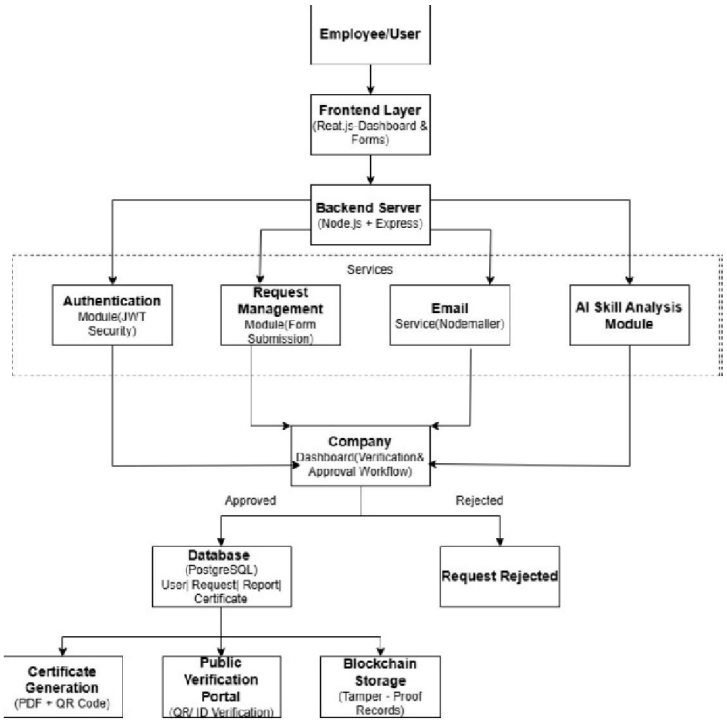

Fig. 1: Architecture of Blockchain-Based Certificate Verification System

Fig. 1 depicts the system's general structure. Users, issuing companies, the blockchain network, and the application layer are all included.

The following essential elements allow the system to func-tion:

1. Layer of Users: Students or staff who request certificates and verifiers who validate them make up this tier. A web-based interface is used by users to communicate with the system.

2. Layer of Application: Submission, processing, and verification of certificates are handled by the application layer. It consists of the backend logic, dashboard interface, and APIs that control communication between various modules.

3. Module for Hashing: The SHA-256 hashing technique is used to process certificate data in order to create a distinct digital fingerprint. This guarantees that a slight alteration in the data will produce an entirely new hash.

4. Layer of the Blockchain: Smart contracts are used to store the generated hash on the blockchain network. This guarantees immutability, which means that once recorded, the data cannot be changed or tampered with.

5. Module for Verification: The system recalculates the hash from the supplied certificate and compares it with the blockchain hash that has been recorded during verification.

The certificate is considered genuine if both match; if not, it is marked as invalid.

6. Integration of QR Codes: A QR code containing a unique identification is placed in every certificate. By directly connecting to the stored blockchain data, this allows for rapid and secure verification.

All things considered, the design guarantees safe data pro-cessing, does away with manual verification, and offers a quick and dependable method for certificate authentication.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, June 2026
Impact Factor: 8.2

V. DESIGN AND IMPLEMENTATION

The suggested system's implementation focuses on offering a safe and intuitive platform for blockchain-based certificate creation and verification. The system uses several interfaces to assist its organized workflow.

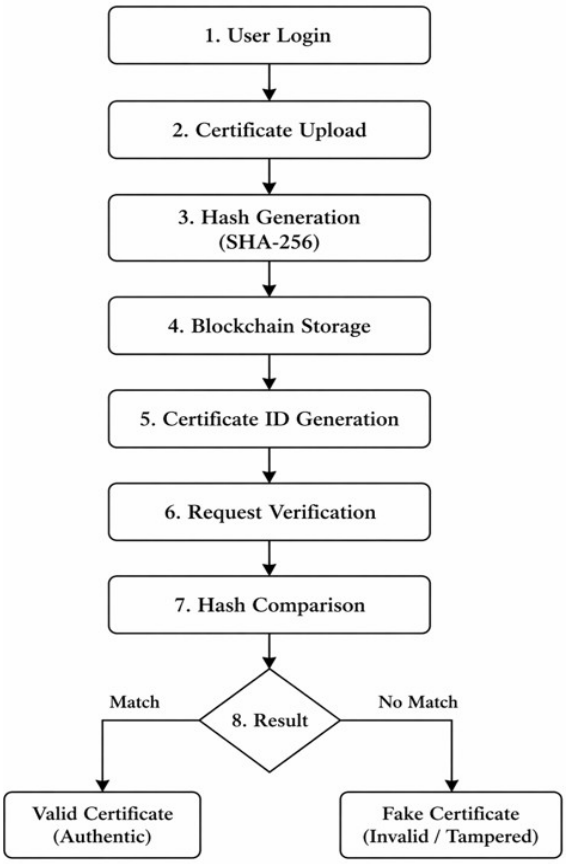

Fig. 2: System Workflow

Fig. 2 depicts the system's whole operational flow. Using the application interface, the user first submits certificate data. After processing the input, the system creates a SHA-256 hash value that serves as a distinct digital fingerprint. To guaran-tee immutability, this hash is safely kept on the blockchain network. The stored data is connected to a distinct certificate ID and QR code. The system recalculates the hash from the supplied certificate and compares it with the blockchain record during verification. The certificate is deemed legitimate if both values match; if not, it is deemed invalid. A safe and automated verification procedure is guaranteed by this workflow.

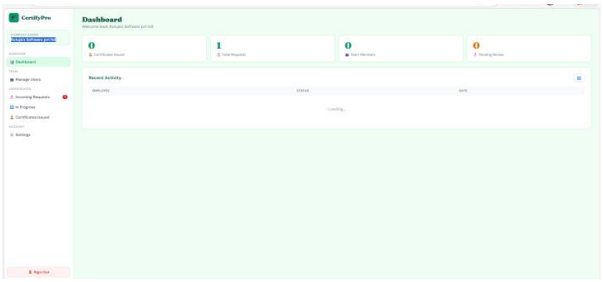

Fig. 3: Interface of the Dashboard

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, June 2026
Impact Factor: 8.2

Fig. 3 displays the dashboard that administrators use to handle certificate requests, check information that has been submitted, and accept or deny applications.

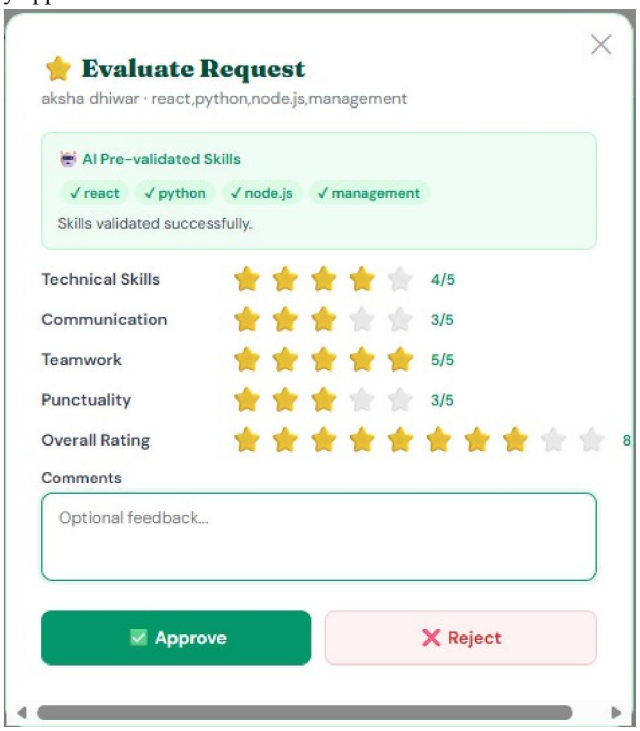

Fig. 4: Portal for Verifying Certificates

Fig. 4 shows the verification portal where users can utilize a unique certificate identifier or a QR code to validate certifi-cates. has been written. In order to facilitate rapid and easy verifi-cation, the system also incorporates QR code generating. By reducing unnecessary calculations and guaranteeing effective blockchain interface, the system also emphasizes performance optimization. Sensitive data is protected by security techniques like input validation, access control, and secure API connec-tivity. Overall, the implementation guarantees that the system is safe, dependable, and appropriate for deployment in various domains in the actual world.

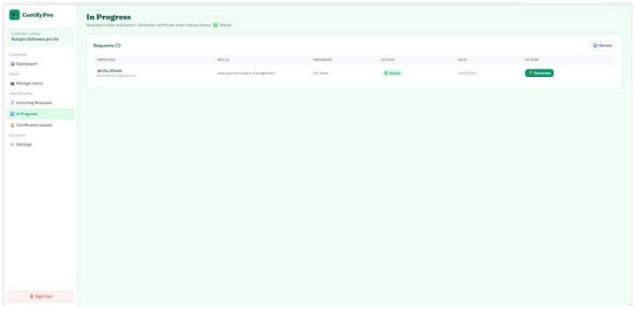

Fig. 5: Interface for Certificate Generation

Fig. 5 symbolizes the process of creating a certificate fol-lowing successful issuing authority verification and approval.

DOI: 10.48175/IJARSCT-36536

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 6, Issue 4, June 2026
Impact Factor: 8.2

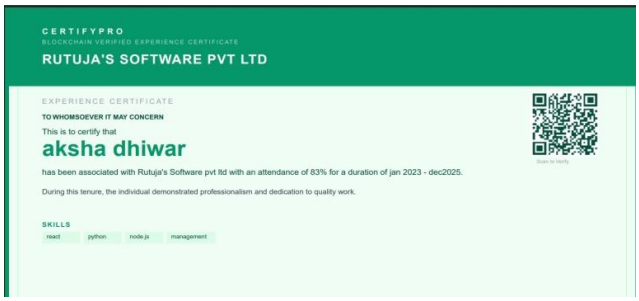

Fig. 6: Generated Digital Certificate with QR Code

Fig. 6 shows the final certificate that was produced together with a QR code, allowing for safe and quick blockchain verification.

A. Working Description of the System

TABLE I: System Working Description

Step	Description
1	The user enters certificate info into the system.
2	The system produces a SHA-256 hash value.
3	The hash is safely kept on the blockchain.
4	A distinct certificate ID is produced.
5	A QR code is made for confirmation.
6	Hash comparison is used to verify the certificate.
7	The system shows the outcome (Valid/Invalid).

B. Specifics of Implementation

A modular design is used in the system's implementation to provide scalability and maintainability. Both administrators and end users will find the frontend interface easy to use. Hashing, certificate processing, and blockchain network connectivity are handled by the backend. Hash values are safely stored and validation logic is enforced through the use of smart contracts. These agreements guarantee that data cannot be altered without the required authorization once it

C. Algorithm

1) Enter info about certificates into the system.
2) Create a SHA-256 certificate hash.
3) Hash value storage on a blockchain
4) Create a QR code that is connected to the certificate ID
5) Check the hash values to validate the certificate.

By doing away with manual verification procedures, the solution guarantees quick, safe, and impenetrable certificate validation.

VI. RESULTS

The suggested approach was successfully put into practice and assessed to confirm its efficacy in the creation and valida-tion of secure certificates. The outcomes show notable gains in efficiency, security, and dependability over conventional verification techniques. By enabling automatic certificate gen-eration, the technology minimizes human mistake and manual labor. A certificate is instantly processed using a cryptographic hashing technique and safely stored on the blockchain when it is issued. This guarantees that the certificate data is un-changeable and impervious to manipulation. The verification procedure was found to be quick and effective during testing. By entering the unique

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 4, June 2026 Impact Factor: 8.2

certificate ID or scanning the QR code, certificates might be verified instantly. By spotting discrepancies in hash values, the system correctly identified any alteration in certificate data, stopping fraudulent activity. Administrators had an efficient platform to handle requests, examine information, and accept or reject applications thanks to the dashboard interface. When compared to conventional verification methods, this optimized workflow dramatically decreased processing time. Furthermore, the system remained transparent at every stage, enabling stakeholders to indepen-dently confirm the authenticity of certificates without depend-ing on a central authority. Data integrity was guaranteed by the blockchain integration, while accessibility and usability were improved by the usage of QR codes. Overall, the findings demonstrate that the suggested system accomplishes safe, effective, and scalable certificate verification, making it appropriate for implementation in government agencies, business settings, and educational institutions.

TABLE II: Evaluation of System Performance

Parameter	Observation
Generation Time of Certificates	¡ 5 seconds
Time of Verification	Instant
Generation Time of Hash	¡ 1 second
Accuracy of theSystem	High
Strong Security Level (SHA-256 + Blockchain)	

Table II demonstrates the purposed system's performance evaluation.

VII. PERFORMANCE ANALYSIS

Verification time, security, and scalability were used to as-sess the system's performance. Because the blockchain-based solution allows for rapid validation through hash comparison, the average verification time was much shorter than with manual methods. Strong protection against data manipulation and unauthorized changes is ensured by the use of blockchain storage and SHA-256 hashing. Forgery is easily recognized since even little changes in certificate data produce entirely different hash results. Blockchain's decentralized structure promotes scalability by enabling participation from several institutions without degrading performance. Easy connection with current platforms and upcoming additions is another benefit of the modular system design.

TABLE III: Comparison of Traditional vs Proposed System

Feature	**Traditional System**	**Proposed System**
Verification Method	Manual	Automated
Processing Time	High	Low
Security Level	Moderate	High (Blockchain-based)
Data Integrity	Vulnerable	Tamper-proof
Transparency	Limited	High
Fraud Detection	Difficult	Easy
Storage	Centralized	Decentralized
Verification Speed	Slow	Instant

Table III contrasts the suggested system with conventional verification techniques.

VIII. LIMITATIONS AND CHALLENGES

A. Complexity of Blockchain Integration:

It took meticulous planning and testing to implement smart contracts and guarantee correct blockchain interaction.

B. Cost and Delay of Transactions:

Depending on the network being used, blockchain operations may result in transaction fees and latency.

C. Data Privacy Issues:

Care must be taken while handling sensitive data to protect privacy and uphold transparency.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 4, June 2026 Impact Factor: 8.2

D. Problems with Scalability:
Optimization and effective system design are necessary to handle massive amounts of data and heavy user traffic.

IX. APPLICATIONS

1) Verification of Academic Certificates: Eliminates fake degrees and mark sheets by enabling educational institutions to securely issue and validate certificates.
2) Recruitment and Background Verification: Enables businesses to quickly confirm a candidate's credentials, increasing hiring accuracy and cutting down on verifi-cation time.
3) Validation of Government Documents: helps Ensure authenticity and stop fraud by supporting safe authenti-cation of official documents like licenses and certificates.
4) Systems of Professional Certification: Enables the reliable issuing and verification of certifications for skill-based courses and training programs.
5) Platforms for Online Education: Uses transparent and safe verification to guarantee the legitimacy of certifi-cates given by e-learning systems.
6) Verification Across Institutions: Allows several orga-nizations to verify certificates independently of a central authority on a single decentralized platform.
7) Verification of Global Credentials: Supports interna-tional career and educational prospects by offering a trustworthy method for international certificate verifica-tion.

X. CONCLUSION

This study described the design and implementation of a blockchain-based digital certificate verification system that is transparent and safe. The problems of certificate fraud, slow manual verification, and mistrust of centralized systems are all addressed by the suggested method. Each certificate is transformed into a distinct digital fingerprint and saved on a blockchain network using cryptographic hashing algorithms, guaranteeing data integrity and immutability. The solution removes the need for human validation by enabling rapid and trustworthy verification using QR codes and distinct certificate identifiers. Additionally, incorporating automated procedures increases productivity and lowers the possibility of human error. The suggested approach improves certificate manage-ment's security, transparency, and trustworthiness, making it appropriate for use in the fields of professional certification, education, and employment.
This work's main contributions are:
1) A Blockchain-based architecture for certificate verifica-tion that guarantees safe and impenetrable storage of certificate information.
2) QR codes and unique identifiers are used in an au-tomated verification system for immediate validation. To preserve data integrity and stop unwanted changes, cryptographic hashing algorithms are integrated.
3) A Transparent, scalable system architecture that lessens reliance on centralized authorities.

XI. FUTURE WORK

1) Integration of Scalable Blockchain: Enhancing the system's scalability, transaction efficiency, and practical deployment capabilities by incorporating cutting-edge blockchain platforms like Ethereum or Hyperledger.
2) IPFS-based Decentralized Storage: Utilize IPFS to safely store certificate files while preserving only hash values on the blockchain, which will lower storage overhead and increase efficiency.
3) AI-Based Fraud Detection: AI-powered fraud identi-fication using machine learning techniques to automat-ically identify fraudulent certificate generation patterns and questionable activity.
4) Ecosystem of Multi-Institution: Expand the system's functionality to accommodate numerous universities and organizations, allowing for a single, uniform framework for certificate verification.
5) API for RESTful Integration: Create secure and strong RESTful APIs so that external systems, like businesses and government portals, may instantly verify certificates.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 6, Issue 4, June 2026 Impact Factor: 8.2

6) **Integration of Decentralized Identity (DID):** To en-able safe and user-controlled identity management, in-corporate decentralized identity (DID) techniques.

7) **Support for Mobile Application:** Deploy a mobile application that makes it simple to issue, manage, and verify certificates by scanning QR codes.

REFERENCES

[1] M. M. Rahman et al., "Blockchain-based certificate authentication system with enabling correction," Journal of Computer and Commu-nications, vol. 11, pp. 73–82, 2023.

[2] A. Mishra et al., "Blockchain-based decentralized document verification and its applications," Journal of Information Systems Engineering and Management, vol. 10, no. 1, 2025.

[3] A. S. Babu et al., "Certificate validation using blockchain," International Research Journal on Advanced Engineering and Management, vol. 2, no. 12, 2024.

[4] K. Dongare et al., "Verification and validation of certificate using blockchain," IJRASET, vol. 13, no. 11, 2025.

[5] D. Shukla et al., "A blockchain-based system for digital certificate verification," IJERT, vol. 11, no. 5, 2024.

[6] R. Sharma and P. Gupta, "Blockchain-based certificate verification system," International Journal of Engineering Research and Technology, 2024.

[7] A. Rustemi et al., "A systematic literature review on blockchain-based systems for academic certificate verification," IEEE Access, vol. 11, 2023.

[8] V. Kumar et al., "Blockchain-based document verification system using smart contracts," Procedia Computer Science, vol. 218, pp. 457–465, 2023.

[9] S. Wang et al., "Blockchain-based digital certificate authentication system," IEEE Access, vol. 9, pp. 12 345–12 358, 2021.

[10] J. Chen et al., "A blockchain-based approach for secure academic credential verification," IEEE Transactions on Education, vol. 65, no. 2, pp. 266–273, 2022.

[11] R. Kumar and A. Singh, "Secure academic certificate verification using blockchain technology," International Journal of Information Security, vol. 20, no. 3, pp. 345–356, 2022.

[12] K. Gupta and R. Singh, "Secure certificate verification system using blockchain and qr code," International Journal of Computer Applica-tions, vol. 183, no. 45, 2021.

[13] M. Patel and S. Shah, "Smart contract-based certificate verification system," Procedia Computer Science, vol. 173, pp. 200–207, 2020.

[14] S. Aggarwal et al., "Blockchain for secure digital certificates: A review," Journal of Network and Computer Applications, vol. 187, 2021.

[15] T. Rahman et al., "Verichain: A credentials verifier using blockchain and ipfs," arXiv preprint arXiv:2307.05797, 2023.

[16] S. Dhanake, R. Wakchaure, V. Shinde, S. Ghungarde, and L. Sonawane, "Cybersecurity in automotive vehicles," International Journal of Cre-ative Research Thoughts, vol. 13, no. 11, 2025.

[17] A. Wasnik and S. Pathak, "Detecting mental illness using face recog-nition techniques," in Communication in Computer and Information Science. Springer, 2025, pp. 195–206.

[18] S. Dhanake, S. Gaikwad, S. Zodage, R. Ingale, and A. Gangurde, "Chain of trust: Secure and transparent digital certificate validation," Journal of Emerging Technologies and Innovative Research, vol. 12, no. 11, 2025.

[19] S. Dhanake, S. Suse, R. Shaikh, N. Rathod, and A. Sawane, "Cyber bullying detection on social media using nlp," International Journal of Research and Analytical Reviews, vol. 12, no. 4, 2025.

[20] S. Dhanake, A. Kedari, A. Kole, A. Latane, and S. Kakade, "Virtual clin-ical trial simulator using synthetic patient data," International Journal of Scientific Development and Research, vol. 10, no. 11, 2025.

[21] S. Dhanake, A. Nakhate, P. Kalbhor, M. Magar, and Y. Jadhav, "Secured university result system using cryptographic techniques," International Journal for Science and Advance Research In Technology, vol. 7, no. 6, 2021