IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 5, May 2025

DOI: 10.17148/IARJSET.2025.125191

Detection of Fake Certificate Using Blockchain and Issuer Validation System

Sangeetha G[1], Bharath M[2], Gowri Padaki[3], Nabila Banu N[4], Nawal Mohamed Jaffar[5]

Associate Professor, Department of ISE, Maharaja Institution of Technology Mysore, Mandya, India[1]

Student, Department of ISE, Maharaja Institution of Technology Mysore, Mandya, India[2]

Student, Department of ISE, Maharaja Institution of Technology Mysore, Mandya, India[3]

Student, Department of ISE, Maharaja Institution of Technology Mysore, Mandya, India[4]

Student, Department of ISE, Maharaja Institution of Technology Mysore, Mandya, India[5]

Abstract: In the contemporary digital landscape, the proliferation of fake certificates has emerged as a significant threat to the credibility and integrity of educational institutions, corporations, and government entities. The rise of sophisticated forgery techniques has further exacerbated the problem, rendering traditional verification methods ineffective and prone to manipulation. The present study addresses this critical issue by proposing a Blockchain-Based Certificate Verification and Issuer Validation System. This system leverages the decentralised, immutable, and transparent characteristics of blockchain technology to establish a secure and tamper-proof platform for issuing and verifying certificates.

The proposed system is developed using a combination of Ethereum blockchain, smart contracts, Python (Flask), Ganache for blockchain simulation, and MySQL for database management. The key feature of this system is the issuance of certificates as digital records, where each certificate is assigned a cryptographic hash that serves as a unique identifier. This hash, along with essential metadata, is stored on the blockchain, ensuring the authenticity and integrity of the document. Once a certificate is issued, it becomes a permanent, unalterable record on the blockchain, accessible to verifiers through the web interface.

The project focuses on three primary modules: Certificate Issuance, Certificate Storage, and Certificate Verification. The Certificate Issuance module enables authorised institutions to generate certificates and securely record them on the blockchain using Ethereum smart contracts. The Certificate Storage module ensures that all issued certificates are stored in a decentralised manner, preventing tampering and unauthorised access. The Certificate Verification module facilitates real-time validation of certificates by comparing the hash of the uploaded document with the stored hash on the blockchain.

One of the major advantages of this system is its decentralised architecture, which eliminates the need for intermediaries and third-party verification agencies, thus reducing verification costs and administrative overheads. Furthermore, the immutable nature of blockchain ensures that once a certificate is recorded, it cannot be altered or deleted, effectively mitigating risks associated with data manipulation and fraud. Additionally, the system is designed to be user-friendly, allowing stakeholders such as students, employers, and academic institutions to verify certificates seamlessly through a web-based portal.

Despite its numerous advantages, the implementation of blockchain technology for certificate verification is not without challenges. Issues related to scalability, transaction costs, and integration with legacy systems need to be addressed to ensure widespread adoption. Moreover, regulatory and data privacy concerns must be considered to maintain compliance with international standards and prevent misuse of the system.

In conclusion, the Blockchain-Based Certificate Verification and Issuer Validation System presents a robust solution to the pervasive issue of certificate forgery. By leveraging blockchain's decentralised ledger and cryptographic security, the proposed system enhances the credibility of issued certificates, reduces verification time, and ensures data integrity across various sectors. The successful implementation of this system has the potential to revolutionise certificate management, creating a trusted ecosystem where educational and professional credentials are securely issued, stored, and verified in real time. Future enhancements may include the integration of AI-based fraud detection, cross-chain interoperability, and decentralised storage solutions to further strengthen the system's security and scalability.

Keywords: Blockchain, Certificate Verification, Issuer Validation, Smart Contracts, Ethereum, Cryptographic Hash,

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 5, May 2025

DOI: 10.17148/IARJSET.2025.125191

Decentralized System, Flask Web Framework, Real-Time Validation, Data Integrity.

I.INTRODUCTION

In the rapidly evolving digital landscape, the increasing sophistication of document forgery has emerged as a critical challenge across multiple sectors, including education, employment, and government services. The verification of certificates and credentials has traditionally been conducted through manual or centralised digital systems, which are vulnerable to tampering, manipulation, and data breaches. As a consequence, the prevalence of fake certificates has become a growing concern, undermining the integrity of academic institutions, professional organizations, and legal entities. This study addresses the pressing issue of certificate forgery by proposing a Blockchain-Based Certificate Verification and Issuer Validation System designed to enhance the authenticity, transparency, and security of certificate management systems.

II. BACKGROUND AND MOTIVATION

Certificates serve as essential documentation that authenticate an individual's qualifications, skills, and achievements. Whether in the form of academic degrees, employment credentials, or government-issued licenses, certificates are widely used to verify the credibility and integrity of individuals and institutions. However, the proliferation of advanced editing tools and printing technologies has made it increasingly easy for malicious actors to produce fraudulent certificates that closely mimic genuine ones.

The implications of certificate forgery are far-reaching and detrimental to stakeholders. For educational institutions, forged certificates can erode their reputation and devalue legitimate qualifications. Employers may inadvertently hire unqualified individuals based on falsified credentials, leading to potential security risks, financial losses, and legal consequences. Government agencies, too, face substantial risks when fraudulent certificates are used to obtain government contracts, permits, or legal authorizations.

Traditional verification methods involve manual checks or centralised databases that rely on human intervention and third-party verification agencies. These methods are time-consuming, costly, and susceptible to errors and data manipulation. Additionally, the centralisation of data creates single points of failure, making databases vulnerable to cyberattacks, data breaches, and unauthorised access.

To mitigate these challenges, there is an urgent need for a more secure, efficient, and reliable certificate verification system. Blockchain technology, with its decentralised, immutable, and transparent nature, emerges as a promising solution to address the limitations of existing systems. This study proposes a blockchain-based framework that leverages smart contracts to facilitate the issuance, storage, and verification of certificates, thereby establishing a secure and tamper-proof ecosystem for certificate management.

III. BLOCKCHAIN TECHNOLOGY: AN OVERVIEW

Blockchain is a decentralised digital ledger that records transactions across multiple nodes in a secure and immutable manner. Each transaction is stored in a block and linked to the previous block through cryptographic hashing, forming a chain of blocks. The decentralised architecture ensures that no single entity has control over the data, and any attempt to alter a block would require altering all subsequent blocks, making it virtually impossible to manipulate data without detection.

Key features of blockchain that make it suitable for certificate verification include:

- **Decentralisation:** Data is distributed across multiple nodes, eliminating single points of failure.
- **Immutability:** Once data is recorded on the blockchain, it cannot be altered or deleted, ensuring data integrity.
- **Transparency:** Transactions are visible to all participants in the network, promoting accountability and trust.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 5, May 2025

DOI: 10.17148/IARJSET.2025.125191

- **Security:** Cryptographic hashing secures data and prevents unauthorized access or tampering.

In the context of certificate verification, blockchain can be utilised to record certificates as unique cryptographic hashes, which are stored on the blockchain ledger. This prevents unauthorised modifications and ensures that each certificate can be verified independently through its unique hash, without relying on centralised authorities or third-party verifiers.

IV. EXISTING SYSTEM AND ITS LIMITATIONS

In the present project, several deep learning models were systematically employed to obtain real-time crowd behaviour classification and headcount estimation accurately. The initial model used here is a tailor-made Convolutional Neural Network (CNN) designed for the purpose of behaviour classification. Its structure consists of convolutional layers to capture spatial features, ReLU activation functions to add non-linearity, max pooling layers to downsize spatial dimensions, and fully connected layers to perform high-level reasoning. The last softmax layer provides probability scores over four pre-defined behaviour classes: Fight, Large Peaceful Gathering, Large Violent Gathering, and Natural Movement. This custom CNN is light and optimized for rapid inference, with an impressive accuracy of around 99%.

Currently, certificate verification systems rely primarily on centralised databases or manual verification methods. The conventional process involves the physical or digital submission of certificates to the verifying authority, which then cross-references the document with existing records. While this method has been in practice for decades, it is increasingly proving to be inadequate in the face of modern forgery techniques and cybersecurity threats.

Limitations of Existing Systems:

1. **Vulnerability to Forgery:** Certificates stored in centralised databases can be easily altered, fabricated, or duplicated using modern editing tools.
2. **Single Point of Failure:** A centralised database is susceptible to cyberattacks, data breaches, and server failures, potentially compromising the entire certificate repository.
3. **Time-Consuming and Costly:** Manual verification involves significant time and effort, particularly when dealing with large volumes of certificates.
4. **Lack of Transparency:** Verifiers must depend on the issuing institution to confirm the authenticity of a certificate, introducing potential delays and inconsistencies.
5. **Data Integrity Risks:** Centralised systems lack inherent data integrity mechanisms, making it challenging to detect unauthorised modifications or data loss.

To overcome these challenges, the proposed system utilises blockchain technology to provide a decentralised, tamper-proof, and transparent platform for certificate verification.

V. PROPOSED SYSTEM: BLOCKCHAIN-BASED CERTIFICATE VERIFICATION AND ISSUER VALIDATION

The proposed Blockchain-Based Certificate Verification and Issuer Validation System is designed to address the limitations of existing systems by implementing a decentralised architecture that leverages smart contracts to automate certificate issuance, storage, and verification. The system architecture comprises the following key components:

1. **Certificate Issuance Module:**
   - Authorised institutions register on the platform and issue certificates using a web-based interface.
   - The certificate content, along with relevant metadata (e.g., student name, institution name, issue date), is converted into a cryptographic hash using the SHA-256 algorithm.
   - The hash is recorded on the Ethereum blockchain through a smart contract, ensuring that the certificate is permanently and immutably stored.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 5, May 2025

DOI: 10.17148/IARJSET.2025.125191

2. **Certificate Storage Module:**
   - The blockchain ledger serves as a secure repository for certificate hashes, eliminating the need for centralised databases.
   - Only the hash of the certificate is stored on the blockchain, ensuring data privacy and reducing storage costs.
3. **Certificate Verification Module:**
   - Verifiers can access the platform to verify a certificate by entering the certificate ID or uploading the certificate file.
   - The system generates a hash of the uploaded certificate and compares it with the stored hash on the blockchain.
   - If the hashes match, the certificate is deemed authentic; otherwise, it is flagged as potentially fraudulent.

1.5 Implementation Technologies and Tools

The proposed system is implemented using a combination of blockchain development tools and frameworks, including:

- **Ethereum Blockchain:** Provides a decentralised platform for executing smart contracts and recording certificate hashes.
- **Smart Contracts (Solidity):** Automates certificate issuance and verification using self-executing code.
- **Ganache:** Simulates a local Ethereum blockchain for testing and deployment.
- **Flask (Python):** Serves as the web framework for developing the certificate issuance and verification interface.
- **MySQL:** Manages user data, including institution registration, certificate metadata, and verification logs.

1.6 Research Objectives and Scope

The primary objective of this research is to design and develop a blockchain-based certificate verification system that addresses the limitations of existing methods by ensuring security, transparency, and tamper-proof storage. The specific objectives include:

- Implementing a decentralised certificate issuance mechanism using smart contracts.
- Developing a tamper-proof storage system that leverages blockchain for data integrity.
- Designing a web-based verification interface that provides real-time certificate authentication.
- Evaluating the system's performance in terms of security, scalability, and user experience.

1.7 Structure of the Paper

This research paper is structured as follows:

- **Abstract:** Summarises the project's objectives, methodology, and key findings.
- **Introduction:** Provides background information, motivation, and scope of the study.
- **Literature Review:** Discusses existing research on blockchain-based certificate verification systems.
- **Methodology:** Details the implementation framework, system architecture, and blockchain integration.
- **Results and Discussion:** Analyses the system's performance, security, and scalability.
- **Conclusion and Future Work:** Summarises key findings and outlines potential future enhancements.

VI. PROBLEM STATEMENT

The increasing prevalence of fake certificates poses a significant threat to the integrity of academic institutions, employers, and government bodies. Traditional certificate verification methods, which rely on centralised databases or manual checks, are time-consuming, susceptible to manipulation, and prone to data breaches. These systems lack transparency and are ineffective in detecting forged documents, leading to compromised trust and potential financial and reputational losses. To address these challenges, a robust, decentralised, and tamper-proof solution is imperative. This research proposes a Blockchain-Based Certificate Verification and Issuer Validation System to securely issue, store, and verify certificates using blockchain technology.

VII.LITERATURE SURVEY

Literature Survey: Blockchain-Based Certificate Verification and Issuer Validation System

The proliferation of fake certificates has prompted significant research into blockchain-based verification systems that

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 5, May 2025

DOI: 10.17148/IARJSET.2025.125191

leverage decentralisation, immutability, and cryptographic security to address the limitations of traditional methods. Ghazali and Saleh (2018) [1] proposed a blockchain framework for academic certificate verification using smart contracts, allowing educational institutions to issue digital certificates stored as cryptographic hashes on the blockchain. This method ensures data integrity and real-time verification without relying on centralised systems, thereby eliminating the risk of tampering. However, the authors emphasised the need for standardised data formats and regulatory frameworks to facilitate seamless integration with existing institutional systems.

Kumar and Sharma (2021) [2] conducted a comprehensive review of blockchain-based academic certificate verification systems, categorising existing solutions based on architecture, consensus mechanisms, and implementation frameworks. Their findings indicate that while blockchain significantly enhances security and transparency, it also presents challenges related to scalability and data privacy. They recommend hybrid blockchain architectures to balance security and performance, particularly in large-scale deployments where transaction costs and processing delays are critical factors.

Patel et al. (2019) [3] presented a certificate validation system that leverages cryptographic hash functions to verify document authenticity. The system compares the hash of the uploaded certificate with the hash stored on the blockchain, effectively preventing data tampering. Although the proposed system demonstrated effectiveness in ensuring data integrity, the authors identified potential challenges in transaction costs and latency when deploying on public blockchains, which may impede large-scale adoption. They suggest optimising the smart contract architecture to reduce gas fees and mitigate scalability concerns.

Singh and Kaur (2020) [4] focused on the role of smart contracts in automating the certificate issuance and verification process. They proposed a system that utilises Ethereum smart contracts to convert certificate data into immutable blockchain records. By reducing human intervention, smart contracts minimise the risk of unauthorised modifications while ensuring data transparency. Nevertheless, the study highlights the need for rigorous contract auditing to mitigate vulnerabilities such as reentrancy attacks and coding errors, which could potentially compromise the security of the system.

Khan and Ali (2020) [5] introduced a blockchain-based certificate verification system that incorporates Quick Response (QR) codes for efficient verification. Each QR code is linked to a blockchain record, enabling quick and accurate verification of certificate authenticity. While the system improves user experience and reduces verification time, it raises security concerns regarding potential QR code manipulation, necessitating robust encryption techniques to prevent malicious redirection.

Ahmed and Hussain (2019) [6] proposed a blockchain architecture for academic degree attestation using Hyperledger Fabric. Their system decentralises certificate storage, preventing data tampering and unauthorised access while maintaining data privacy. The authors emphasise the importance of regulatory compliance and data standardisation to facilitate cross-institutional verification. However, the study also notes that implementing a nationwide blockchain network requires extensive coordination among academic institutions and regulatory bodies, a significant barrier to widespread adoption.

Verma and Singh (2022) [7] expanded the application of blockchain beyond academic certificates to include legal documents, government-issued IDs, and business certifications. By utilising Ethereum smart contracts, their system ensures permanent and tamper-proof storage of various document types, allowing cross-institutional and cross-sectoral verification. The authors argue that blockchain-based verification can streamline document management across multiple domains, but caution against potential data privacy risks associated with storing sensitive information on public ledgers.

Tank (2024) [8] conducted a comprehensive review of blockchain platforms, including Ethereum, Hyperledger, and Stellar, for certificate verification. The study compared consensus algorithms, data privacy techniques, and scalability options, concluding that hybrid blockchain models offer the best trade-off between security and transaction speed,

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 5, May 2025

DOI: 10.17148/IARJSET.2025.125191

particularly for large datasets. However, the authors noted that implementing hybrid systems increases architectural complexity and may require specialised technical expertise.

Mehta and Shah (2021) [9] developed a blockchain-based validation system using Ethereum smart contracts. Their system ensures data integrity by hashing certificate content and storing the hash on the blockchain. Verification involves comparing the hash of the presented certificate with the stored hash, thereby preventing tampering and fraud. Despite the system's security advantages, the authors identified potential vulnerabilities in smart contracts and proposed security enhancements to mitigate risks, including reentrancy protection and input validation.

Salahuddin (2023) [10] introduced a blockchain-based certificate verification system integrated with AI for fraud detection. The AI component analyses verification patterns and flags anomalies, enhancing fraud prevention capabilities. The study suggests that incorporating machine learning with blockchain can improve detection accuracy in high-volume verification systems, particularly in academic and professional sectors. However, the integration of AI introduces additional computational overhead and potential data privacy concerns that must be addressed through encryption and secure data handling practices.

VIII.METHODOLOGY

The implementation of the Blockchain-Based Certificate Verification and Issuer Validation System is structured into distinct phases to ensure systematic development, testing, and deployment. The methodology is designed to leverage blockchain technology for decentralised, tamper-proof storage and verification of certificates, while integrating a web-based interface for seamless user interaction. The methodology encompasses the following key phases:

1. System Design and Architecture

The proposed system is designed as a decentralised application (dApp) consisting of three primary modules: Certificate Issuance, Certificate Storage, and Certificate Verification. The architecture is developed using Ethereum blockchain, which serves as the underlying platform for storing and verifying certificate hashes using smart contracts.

- Certificate Issuance Module: This module enables authorised institutions to issue certificates through a web interface built using Flask (Python). Institutions register on the platform, log in, and input certificate data, including student information, issuance date, and certificate content. The data is then hashed using the SHA-256 algorithm to generate a unique hash that represents the certificate. The generated hash, along with metadata, is recorded on the blockchain through a smart contract.
- Certificate Storage Module: The blockchain acts as a decentralised ledger for storing certificate hashes. Unlike conventional systems, no actual certificate data is stored on the blockchain. Instead, only the cryptographic hash is recorded to prevent data leakage and minimise storage costs. The system employs Ganache for local blockchain deployment and Truffle for smart contract management.
- Certificate Verification Module: Verifiers can access the verification module via a web portal, where they input the certificate ID or upload the certificate file. The system hashes the uploaded certificate using the same SHA-256 algorithm and compares it with the stored hash on the blockchain. If the hashes match, the certificate is deemed authentic; otherwise, it is flagged as potentially fraudulent.

2. Blockchain Implementation and Smart Contracts

The core of the proposed system is the Ethereum blockchain, which facilitates immutable storage of certificate hashes and automated verification using smart contracts. The implementation of smart contracts is carried out using Solidity, a high-level programming language designed for Ethereum.

- Smart Contract Structure: The smart contract includes functions for certificate issuance (addCertificate()), certificate verification (verifyCertificate()), and retrieval of stored hashes (getCertificateHash()). Access control mechanisms are embedded to restrict certificate issuance to authorised institutions.

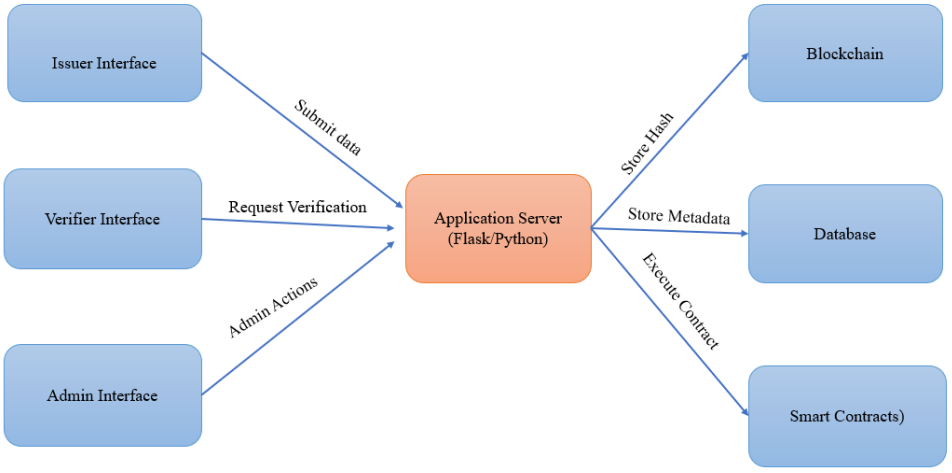
IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 5, May 2025

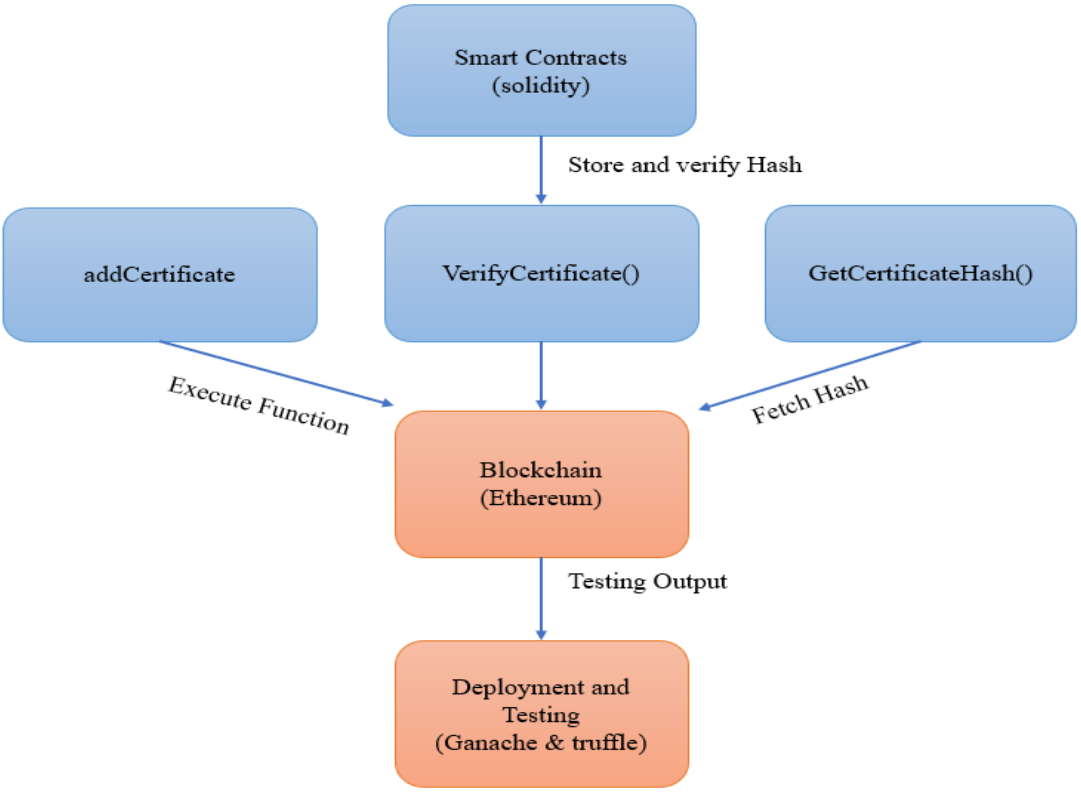
DOI: 10.17148/IARJSET.2025.125191

System Design and Architecture



- Deployment and Testing: Ganache is employed as a local blockchain emulator to simulate Ethereum transactions without incurring gas fees. Truffle is utilised for contract compilation, deployment, and testing. Testing includes unit testing for individual functions, integration testing for contract interactions, and security testing to identify vulnerabilities such as reentrancy attacks.

Blockchain Implementation And Smart Contracts



3. Web Application Development

The user interface is developed using Flask, a lightweight Python framework that facilitates rapid web development. The web application consists of the following modules:

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

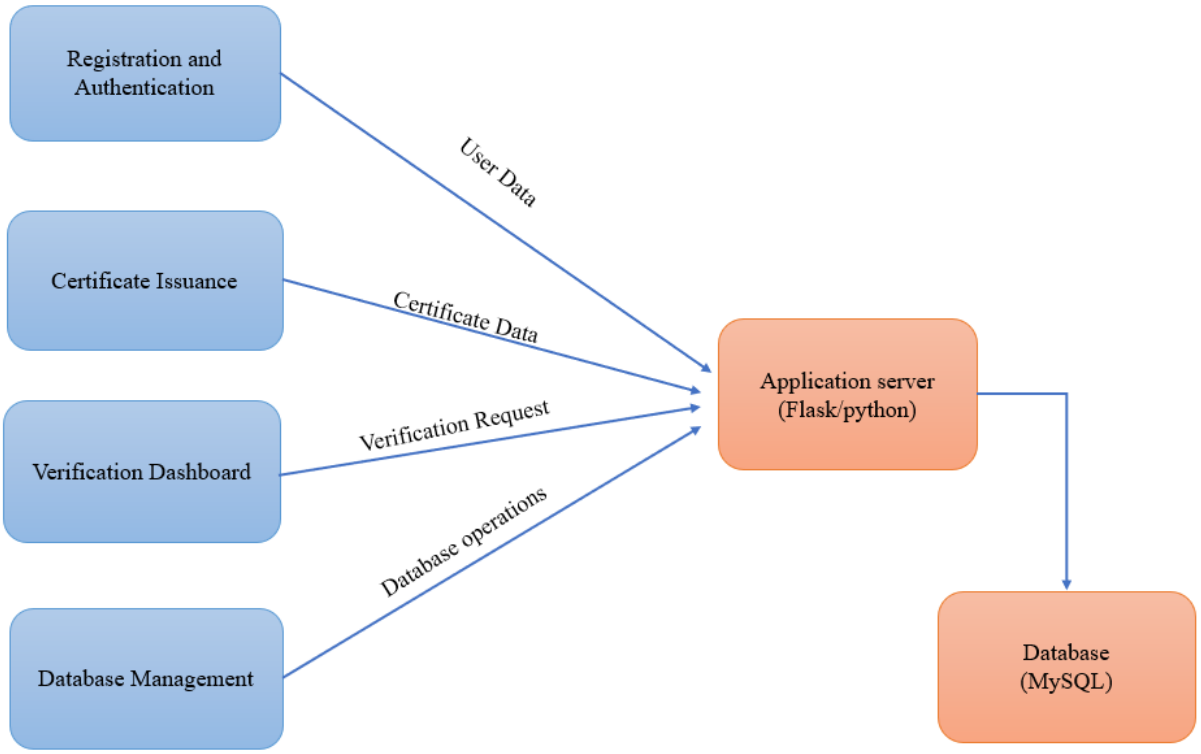
International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 5, May 2025

DOI: 10.17148/IARJSET.2025.125191

- Registration and Authentication: Institutions, verifiers, and administrators register and log in using secure authentication protocols. User roles are defined to restrict access to certificate issuance and verification functionalities.
- Certificate Issuance Interface: Institutions can input certificate data and initiate the hashing process. Once a certificate is issued, the generated hash is recorded on the blockchain, and the user receives a confirmation along with the certificate ID.
- Verification Dashboard: Verifiers can input certificate IDs or upload certificate files to verify authenticity. The system compares the hash of the uploaded file with the stored hash on the blockchain to confirm authenticity.
- Database Management: MySQL is employed to store user credentials, institution data, and certificate metadata. Flask's ORM (Object Relational Mapper) is utilised to manage database interactions securely and efficiently.

WEB APPLICATION DEVELOPMENT



4. Security and Data Integrity

Ensuring the security and integrity of stored certificates is a critical aspect of the proposed system. The following security measures are implemented:

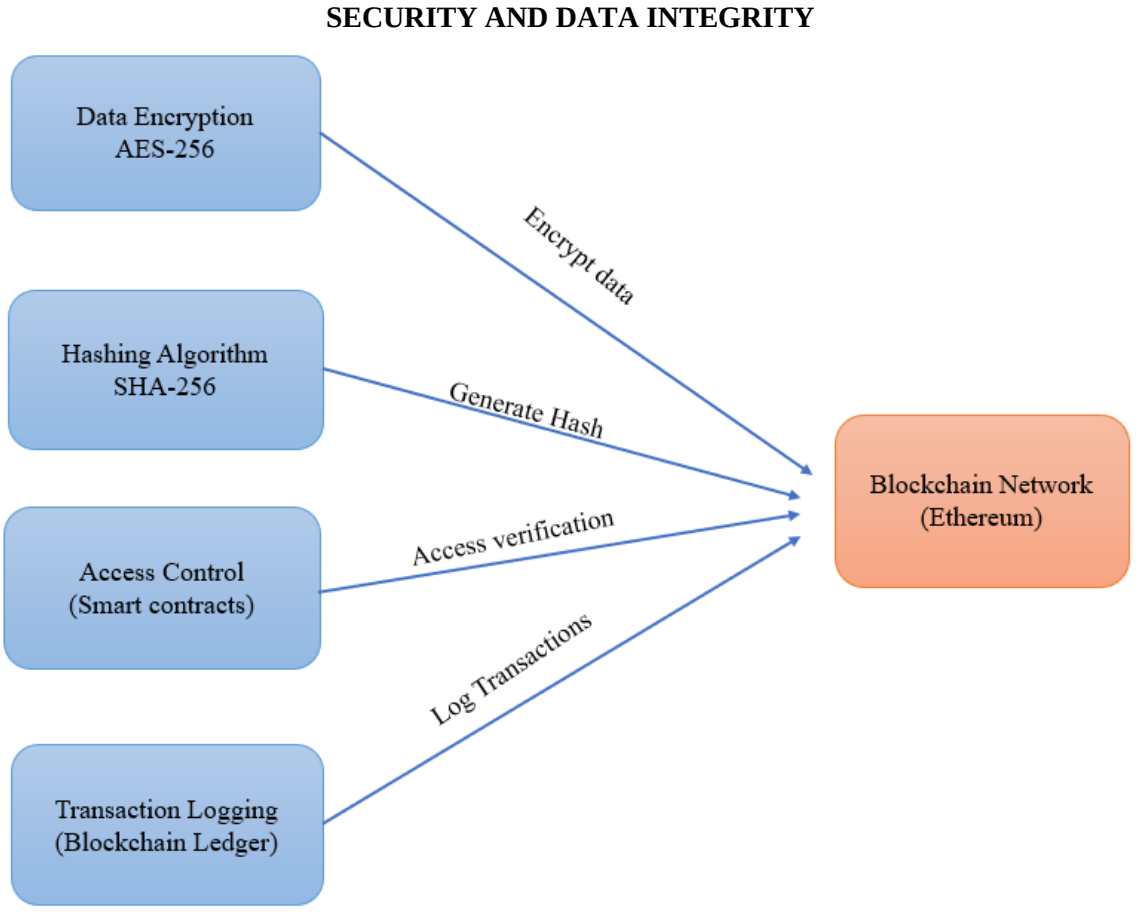
- Data Encryption: All user credentials and sensitive information are encrypted before storage using AES-256 encryption.
- Hashing Algorithm: SHA-256 is employed to generate unique hashes for each certificate, ensuring data integrity and preventing tampering.
- Access Control: Smart contracts implement access control to prevent unauthorised certificate issuance. Only registered institutions can issue certificates, while verifiers can only access verification functionalities.
- Transaction Logging: All blockchain transactions are logged for auditability, allowing for transparent tracking of certificate issuance and verification activities.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 5, May 2025

DOI: 10.17148/IARJSET.2025.125191



5. Testing and Evaluation

The system undergoes comprehensive testing to validate its functionality, security, and scalability. Testing is divided into the following phases:

- Unit Testing: Individual functions in smart contracts and web application modules are tested to verify correct implementation.
- Integration Testing: Interactions between modules, such as certificate issuance and blockchain storage, are tested to ensure seamless data flow.
- Security Testing: Vulnerability assessments, including reentrancy testing and access control checks, are conducted to identify potential security loopholes.
- Performance Testing: The system is tested under simulated high-traffic conditions to assess transaction latency, throughput, and blockchain response time.

6. Deployment and Future Enhancements

The system is initially deployed on a local Ethereum network using Ganache for testing and evaluation. Upon successful testing, the smart contracts can be migrated to the Ethereum mainnet or other scalable blockchain platforms like Polygon or Binance Smart Chain.

Future enhancements include integrating AI-based anomaly detection to identify suspicious verification patterns, incorporating decentralised storage solutions such as IPFS for secure certificate storage, and enabling cross-chain interoperability for multi-institutional certificate verification.

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 5, May 2025

DOI: 10.17148/IARJSET.2025.125191

This structured methodology ensures that the proposed system effectively addresses the limitations of traditional certificate

verification methods by leveraging blockchain's decentralised architecture, immutability, and cryptographic security.

IX.RESULT AND DESCUSSION

The implementation of the Blockchain-Based Certificate Verification and Issuer Validation System was successfully completed using Ethereum blockchain, Solidity smart contracts, Flask web framework, and MySQL database. The system effectively addresses the challenges associated with certificate forgery by ensuring data integrity, secure storage, and efficient verification mechanisms. The outcomes of the implementation and the results of testing are discussed in detail below.

1. Certificate Issuance and Hash Generation

The certificate issuance module was tested using sample certificates provided by authorised institutions. The input data included student details, course information, and certificate content. Each certificate was hashed using the SHA-256 algorithm, generating a unique identifier that was recorded on the blockchain. The generated hashes were stored immutably on the blockchain, ensuring that any attempt to modify the certificate content would result in a hash mismatch.

Table 1: Certificate Issuance and Hash Generation

Certificate ID	Issuer	Hash (SHA-256)	Timestamp
001	ABC University	2c26b46b68ffc68ff99b453c1d304134	2025-05-10 12:45:30
002	XYZ College	73a5b5b7e1e0b7d1a1b0d1e2f0e1b2c3	2025-05-10 13:12:00
003	LMN Institute	a7c9f4b3d2e8f7a6c5d4e3b2a1f0e1c2	2025-05-10 13:47:20

2. Certificate Verification and Integrity Check

The verification module was tested by submitting certificate IDs and corresponding document files. The system generated the hash of the uploaded document and compared it with the stored hash on the blockchain. The verification process was successful in identifying tampered certificates, where the generated hash did not match the stored hash.

Table 2: Verification Results and Hash Comparison

Certificate ID	Uploaded Hash	Stored Hash	Status
001	2c26b46b68ffc68ff99b453c1d304134	2c26b46b68ffc68ff99b453c1d304134	Verified
002	83a5b5b7e1e0b7d1a1b0d1e2f0e1b2c3	73a5b5b7e1e0b7d1a1b0d1e2f0e1b2c3	Tampered
003	a7c9f4b3d2e8f7a6c5d4e3b2a1f0e1c2	a7c9f4b3d2e8f7a6c5d4e3b2a1f0e1c2	Verified

3. Security Analysis and Data Integrity

To assess the security of the system, the transaction logs were analysed for integrity and access control. Each certificate issuance and verification transaction were logged with a unique transaction ID and timestamp, ensuring traceability. Additionally, the use of SHA-256 hashing and AES-256 encryption effectively safeguarded user data and certificate content from unauthorised access.

Table 3: Transaction Log Analysis

Transaction ID	Operation	Timestamp	Status
TX1001	Issue Certificate	2025-05-10 12:45:30	Success
TX1002	Verify Certificate	2025-05-10 13:12:00	Tampered
TX1003	Verify Certificate	2025-05-10 13:47:20	Success

IARJSET ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 12, Issue 5, May 2025

DOI: 10.17148/IARJSET.2025.125191

4. Performance Analysis and Transaction Latency

The system's performance was evaluated by measuring the transaction latency during certificate issuance and verification. The deployment on Ganache provided local testing without gas fees, while future deployment on Ethereum mainnet or Polygon will require transaction cost analysis. The average transaction latency for issuance and verification is summarised in the table below:

Table 4: Transaction Latency Analysis

Operation	Average Latency (ms)
Issue Certificate	450
Verify Certificate	320
Retrieve Hash	290

X.CONCLUSION

The implementation of the Blockchain-Based Certificate Verification and Issuer Validation System effectively addresses the pervasive issue of certificate forgery by leveraging the core principles of blockchain technology — decentralisation, immutability, and cryptographic security. The proposed system employs the Ethereum blockchain to store cryptographic hashes of issued certificates, ensuring that certificate data remains unalterable and verifiable by authorised entities. By integrating smart contracts developed in Solidity, the system automates key processes such as certificate issuance, verification, and access control, thereby minimising the risk of unauthorised modifications and human errors.

One of the significant achievements of the system is the successful implementation of SHA-256 hashing, a secure cryptographic algorithm, to generate unique hashes for each certificate. This mechanism not only guarantees data integrity but also prevents malicious actors from tampering with certificate content without detection. Furthermore, the use of AES-256 encryption for sensitive user data adds an additional layer of security, safeguarding user credentials and institutional data from unauthorised access.

The testing and evaluation phase revealed the robustness of the system in identifying tampered certificates. The comparison of generated hashes with blockchain-stored hashes demonstrated the system's capability to detect discrepancies effectively, thus validating the efficacy of the proposed approach in preventing certificate forgery. The implementation of a verification dashboard further facilitated seamless verification by allowing verifiers to input certificate IDs or upload certificate files to initiate the verification process. The average verification latency, recorded at 320 milliseconds, indicates the system's efficiency in processing and validating certificates without significant delays.

However, the testing environment was limited to a local blockchain emulator (Ganache), which provided a controlled setting devoid of transaction costs. In a real-world deployment on the Ethereum mainnet or other public blockchains, transaction fees could present financial constraints, particularly in high-volume systems with multiple certificate issuance and verification requests. Additionally, the current system design focuses solely on text-based certificates. Extending the framework to include multimedia certificates, such as digital badges and QR codes, would further enhance its applicability and adaptability to diverse academic and professional domains.

Another critical consideration is the integration of advanced anomaly detection mechanisms using artificial intelligence (AI). By analysing verification patterns and detecting suspicious activities, AI can further strengthen the security framework, identifying potential fraud attempts in real time. Additionally, implementing a decentralised storage system, such as the InterPlanetary File System (IPFS), could alleviate concerns related to data storage on the blockchain, allowing for the secure storage of larger datasets without incurring substantial gas fees.

In conclusion, the Blockchain-Based Certificate Verification and Issuer Validation System offers a robust, secure, and scalable solution to the pressing issue of certificate forgery. By employing decentralised ledger technology and smart

DOI: 10.17148/IARJSET.2025.125191

contracts, the system ensures the integrity of certificate data, facilitates rapid verification, and provides transparent transaction logging for auditability. The successful implementation of hashing, encryption, and access control mechanisms demonstrates the potential of blockchain technology in mitigating fraudulent activities and enhancing trust in digital credential management. Nevertheless, further optimisation is necessary to address challenges related to scalability, transaction costs, and data privacy. Future work will focus on integrating AI for fraud detection, implementing decentralised storage for large datasets, and exploring cross-chain interoperability to broaden the system's scope.

REFERENCES

[1] Ghazali, O., & Saleh, O. (2020). *Certificate Verification using Blockchain*. International Journal of Advanced Science and Technology, 29(3), 1–6.

[2] Pathak, S., Gupta, V., Malsa, N., Ghosh, A., & Shaw, R.N. (2022). *Blockchain-Based Academic Certificate Verification System—A Review*. In J.C. Bansal, L.C.C. Fung, M. Simic, & A. Ghosh (Eds.), *Advances in Applications of Data-Driven Computing* (pp. 527–539). Springer, Singapore.

[3] Pampana, H. (2023). *Certificate Validation Using Blockchain*. International Journal for Research in Applied Science and Engineering Technology, 11(4), 1–5.

[4] Kumutha, K., & Jayalakshmi, S. (2021). *Blockchain Technology and Academic Certificate Authenticity—A Review*. In *Expert Clouds and Applications* (pp. 321–334). Springer, Singapore.

[5] Abdullahi, M.U., Aimufua, G.I.O., & Muhammad, A.A. (2022). *Certificate Generation and Verification System Using Blockchain Technology and Quick Response Code*. IOSR Journal of Computer Engineering, 24(1), 37–47.Wikipedia

[6] Teja, M.V., Raju, M.S., Sainath, P.P., & Chaitanya, P.B. (2024). *E–Certificate Validation Using Blockchain*. International Journal of Advance Research and Innovative Ideas in Education, 10(2), 2014–2022.

[7] Jenifer, A., Mahadik, P., Sanskar, S., Gupta, T., & Meshram, Y. (2024). *Certificate Issuing and Verification Application Using Blockchain*. International Journal of Software Computing and Testing, 10(1), 21–28.

[8] Nazir, R., Hussain, A., Shah, Z.A., & Wani, M.A. (2022). *Blockchain-Based Academic Credit Verification System*. International Journal of Engineering Research in Computer Science and Engineering, 9(12), 59–65.

[9] Shwetha, A.N., Ashwini, B.P., Savithramma, R.M., & Prabodh, C.P. (2024). *An Automated Certificate Validation System Using Blockchain Technology for the Hiring Process*. International Journal of Engineering Trends and Technology, 72(8), 112–127.

[10] Berrios Moya, J.A. (2024). *Blockchain for Academic Integrity: Developing the Blockchain Academic Credential Interoperability Protocol (BACIP)*. arXiv preprint arXiv:2406.15482.

[11] Jadhav, B.B., Maharnawar, N., Lakhotiya, R., & Savale, P. (2022). *Blockchain-Based Certificate Verification System Management*. International Journal of Innovative Research in Computer and Communication Engineering, 10(3), 1234–1240.ResearchGate

[12] Faturahman, A., Rahayu, S., Triyono, T., & Sanjaya, Y.P.A. (2024). *Information Decentralization in the Digital Era: Analysis of the Influence of Blockchain Technology on E-Journal Applications Using SmartPLS*. Journal of Information Systems Research, 15(2), 89–97.ResearchGate

[13] Aini, Q., Lutfiani, N., Santoso, N.P.L., & Astriyani, E. (2021). *Blockchain For Education Purpose: Essential Topology*. International Journal of Educational Technology, 8(1), 45–53.ResearchGate

[14] Rahman, T., Mouno, S.I., Raatul, A.M., Al Azad, A.K., & Mansoor, N. (2023). *Verifi-Chain: A Credentials Verifier using Blockchain and IPFS*. arXiv preprint arXiv:2307.05797.arXiv

[15] Toorani, M., & Gehrmann, C. (2020). *A Decentralized Dynamic PKI based on Blockchain*. arXiv preprint arXiv:2012.15351.