Published by :
https://www.ijert.org/
An International Peer-Reviewed Journal

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

Decentralized Academic Certificate Verification System Using Blockchain

Hemachandiran A
(Student)
Department of Information Technology
Alpha College of Engineering Chennai,
India

Ms. S. Sumalatha
Assistant Professor
Department of Information Technology
Alpha College of Engineering Chennai,
India

***Abstract*—Blockchain-based certificate verification systems provide a secure and decentralized approach for validating academic credentials. By leveraging immutable ledgers and cryptographic hashing, these systems ensure data integrity and prevent unauthorized modifications. This approach eliminates dependency on centralized authorities, enabling transparent, tamper-proof, and real-time verification of certificates.This paper presents a secure and decentralized framework for academic certificate verification by leveraging Blockchain and distributed storage systems. Traditional certificate validation mechanisms rely on centralized infrastructures, which are vulnerable to forgery, unauthorized modification, and operational inefficiencies. To overcome these limitations, the proposed system integrates the Polygon blockchain, InterPlanetary File System (IPFS), and SHA-256 hashing to ensure data immutability, integrity, and secure storage.An enhanced authentication mechanism based on email One-Time Password (OTP) verification is incorporated to strengthen user identity validation during registration and login processes. The system implements role-based access control for administrators, students, and verifiers, enabling secure certificate issuance and efficient real-time validation through QR code-based verification. Experimental evaluation demonstrates that the proposed system significantly improves reliability, reduces verification time, and provides strong resistance against data tampering compared to traditional approaches.Overall, the proposed solution offers a scalable, cost-effective, and trustworthy framework for digital credential management, making it suitable for real-world deployment in academic and organizational environments.**

***Index Terms*—Blockchain, IPFS, Smart Contracts, Certificate Verification, SHA-256, Email OTP Authentication**

I. Introduction

Academic credentials play a critical role in validating an individual's educational qualifications and professional eligibility across academic institutions, industries, and governmental organizations. However, the rapid digitization of records and increasing global mobility have exposed significant vulnerabilities in traditional certificate management systems. Conventional verification mechanisms rely on centralized databases, manual approval processes, and institutional intermediaries, making them inefficient, time-consuming, and highly susceptible to security breaches.

One of the most pressing challenges in existing systems is the proliferation of fraudulent certificates, which undermines trust in educational institutions and recruitment processes. According to recent studies, certificate forgery has increased significantly due to the ease of digital manipulation and lack of standardized verification frameworks. Furthermore, centralized systems introduce a single point of failure, making them vulnerable to cyberattacks, unauthorized modifications, and data loss. These limitations highlight the urgent need for a secure, transparent, and decentralized approach to credential verification.

Emerging technologies such as Blockchain have introduced a paradigm shift in data integrity and trust management. Blockchain enables a decentralized and immutable ledger where data, once recorded, cannot be altered without consensus, thereby ensuring tamper-proof storage. However, storing large certificate files directly on-chain is inefficient and costly. To address this, decentralized storage solutions like InterPlanetary File System (IPFS) are utilized to store certificate data off-chain while maintaining secure references on the blockchain.

In addition, modern systems require robust user authentication mechanisms to prevent unauthorized access. Traditional password-based systems are inadequate in protecting sensitive academic data. Therefore, this work integrates multi-factor authentication using email-based One-Time Password (OTP) to enhance identity verification and system security.

This paper proposes a decentralized academic certificate verification system that integrates blockchain, IPFS, and cryptographic hashing (SHA-256) to ensure data integrity, security, and scalability. The system enables institutions to issue tamper-proof digital certificates, while verifiers can instantly validate authenticity using QR codes and blockchain records. By eliminating reliance on centralized authorities, the proposed solution significantly reduces verification time, enhances transparency, and provides a scalable infrastructure for real-world deployment.

The main contributions of this work include:

1) Decentralized Certificate Management: The primary contribution lies in the design and implementation of a secure and decentralized academic certificate verification system leveraging Blockchain technology. The proposed system eliminates the dependency on centralized au-

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

thorities by enabling a trustless verification mechanism, where certificate authenticity can be validated directly through immutable blockchain records.

2) Hybrid Storage Architecture: The system introduces an efficient hybrid storage architecture through the integration of the InterPlanetary File System (IPFS). Instead of storing large certificate files directly on the blockchain, which is computationally expensive and inefficient, the certificates are securely stored in IPFS, and only their corresponding content identifiers and cryptographic hashes are recorded on the blockchain.
3) Robust Authentication Mechanism: This work incorporates a robust authentication mechanism using email-based One-Time Password (OTP) verification to strengthen system security. Unlike conventional password-based systems, the OTP-based approach provides an additional layer of protection by ensuring that only authorized users can access or interact with the system.
4) Smart Contract Automation: The system employs smart contract-based automation to manage certificate issuance, validation, and revocation processes. These smart contracts, deployed on the blockchain, ensure that all operations are executed in a transparent, secure, and tamper-proof manner without requiring third-party intervention.

II. Literature Survey

Recent advancements in blockchain technology have led to significant research in the domain of academic certificate verification systems. Various studies have explored the use of decentralized architectures, smart contracts, and distributed storage to address the limitations of traditional verification methods.

Dheeraj Shukla et al. [1] proposed a blockchain-based academic certificate verification system using the Ethereum platform. Their approach stores certificate data as blockchain transactions, ensuring immutability and resistance to tampering. The system assigns unique identifiers to each certificate, enabling verification by third parties. While the model improves security and eliminates forgery, it primarily focuses on blockchain storage and lacks advanced usability features such as QR-based verification and user-friendly interfaces.

Shraddha H. D and Sushmitha N [2] introduced a system combining blockchain with IPFS for decentralized certificate storage. Their work demonstrates that integrating IPFS reduces storage costs and enhances scalability by storing large certificate files off-chain while maintaining hashes on the blockchain. This approach significantly improves efficiency and transparency compared to traditional systems. However, the system does not incorporate real-time verification mechanisms such as QR codes or strong authentication techniques.

Gangwar et al. [3] proposed a blockchain-based decentralized application (DApp) for certificate verification that integrates smart contracts, IPFS storage, and QR code-based validation. The system enables rapid verification of certificates and reduces dependency on centralized authorities. Experimental results show reduced operational costs and improved verification speed. However, the system lacks multi-factor authentication mechanisms, making it vulnerable to unauthorized access.

Rahman et al. [4] developed a blockchain-based credential verification system utilizing IPFS for storage and hashing techniques for identity generation. In this model, certificates are stored in IPFS, and a unique hash is recorded on the blockchain. The system ensures tamper-proof storage and efficient verification while reducing computational costs. Their results indicate that decentralized storage combined with blockchain significantly enhances reliability and scalability.

A systematic literature review by Rustemi et al. [5] analyzed multiple blockchain-based certificate verification systems and identified key research themes such as security, decentralization, scalability, and usability. The study highlights that blockchain can provide immutable and trustworthy academic records while reducing reliance on centralized authorities. However, it also emphasizes that most existing solutions are still in early development stages and require improvements in usability and real-world deployment.

Ambast et al. [6] proposed a blockchain-based credential verification system using IPFS, focusing on secure data sharing and decentralized storage. Their work highlights the importance of off-chain storage to handle large datasets efficiently while maintaining data integrity through blockchain hashes. The system improves scalability but does not address user authentication challenges.

Additionally, several studies have explored blockchain frameworks for certificate verification that emphasize transparency, immutability, and cost efficiency. These systems demonstrate that blockchain-based solutions eliminate the need for third-party verification and significantly reduce processing time. However, they often lack comprehensive user authentication mechanisms and user-friendly interfaces.

III. Problem Statement

Traditional academic certificate verification systems face significant challenges that limit their reliability, security, and efficiency in modern digital environments. One of the most critical issues is the widespread possibility of certificate forgery and tampering, as digital documents can be easily duplicated, altered, or fabricated using readily available tools. This undermines the credibility of academic credentials and creates serious risks for organizations relying on them for recruitment and validation purposes.

In addition, existing systems are predominantly centralized, meaning that all certificate data is stored and managed by a single authority such as an educational institution or governing body. This centralized architecture introduces a single point of failure, making the system highly vulnerable to cyber-attacks, data breaches, and unauthorized modifications. Any compromise in the central database can lead to large-scale data corruption or loss, affecting the integrity of the entire system.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

Another major limitation is the inefficiency of traditional verification processes, which often involve manual communication between institutions, physical document checks, or email-based confirmations. These procedures are time-consuming, resource-intensive, and prone to human error, resulting in delays and reduced operational productivity. Furthermore, the lack of transparency in such systems makes it difficult for third parties to independently verify the authenticity of certificates without relying on institutional approval.

Security is further weakened by inadequate authentication mechanisms. Many existing platforms rely solely on basic credentials such as usernames and passwords, which are susceptible to phishing, credential theft, and unauthorized access. This exposes sensitive academic data to potential misuse and compromises user privacy.

These challenges collectively highlight the urgent need for a decentralized, secure, and automated certificate verification system. By leveraging advanced technologies such as Blockchain, InterPlanetary File System, and cryptographic hashing techniques like SHA-256, it is possible to ensure data integrity, enhance transparency, eliminate single points of failure, and enable efficient real-time verification of academic credentials.

IV. Objectives

The primary objective of the proposed system is to develop a secure, reliable, and scalable academic certificate verification framework that addresses the limitations of traditional approaches. Key goals include:

1) Eliminate Certificate Forgery: A key goal of this work is to eliminate certificate forgery and unauthorized modifications by leveraging the immutability property of Blockchain, ensuring that once certificate data is recorded, it cannot be altered without consensus. This guarantees the authenticity and integrity of academic credentials.
2) Efficient Bulk Certificate Generation: Enable efficient bulk certificate generation through structured datasets such as Excel files, enabling institutions to automate the issuance process and handle large volumes of student records with minimal administrative effort. This significantly improves operational efficiency and reduces manual workload.
3) Enhanced Security: Enhance system security through a robust authentication mechanism based on email One-Time Password (OTP) verification. This approach strengthens user identity validation and prevents unauthorized access, ensuring that only legitimate users can interact with the system.
4) Real-time QR-based Verification: Provide real-time and user-friendly verification through the integration of QR code technology. By scanning a QR code embedded in the certificate, verifiers can instantly access and validate certificate authenticity without relying on manual processes or institutional intermediaries.
5) Data Integrity: Ensure data integrity through the use of cryptographic hashing techniques such as SHA-256. This guarantees that any alteration in certificate data can be immediately detected through hash mismatch during verification.
6) Scalability and Usability: Design the system to be scalable and user-friendly, supporting seamless interaction for administrators, students, and verifiers. By combining decentralized storage using IPFS with blockchain-based validation, ensure efficient performance, reduced operational costs, and adaptability for real-world deployment.

V. Proposed System

The proposed system is designed as a decentralized and secure architecture that integrates Blockchain, InterPlanetary File System, and advanced authentication mechanisms to ensure reliable academic certificate issuance and verification. The system eliminates reliance on centralized authorities by distributing data across a blockchain network while utilizing IPFS for efficient off-chain storage. This hybrid architecture enhances scalability, reduces storage costs, and ensures tamper-proof data management.

A. System Architecture Overview

The system is structured into multiple functional modules, each responsible for specific operations within the framework:

1) Administrative Module: The administrative module serves as the core control unit, allowing authorized personnel to upload student data in bulk using structured datasets such as Excel files. Upon data submission, digital certificates are generated and securely stored in IPFS, which produces a unique Content Identifier (CID) for each certificate. A cryptographic hash of the certificate, generated using SHA-256, along with the corresponding CID, is then recorded on the blockchain to ensure immutability and verifiability.

2) Student Module: The student module provides a secure interface for users to access their certificates. Students can log in to the system using email-based authentication combined with One-Time Password (OTP) verification, ensuring that only authorized individuals can access their records. Once authenticated, users can view, download, and manage their academic certificates in a secure and user-friendly environment.

3) Verifier Module: The verifier module enables third parties, such as employers or institutions, to validate certificates efficiently. Verification can be performed either by entering a unique certificate identifier or by scanning a QR code embedded within the certificate. The system retrieves the corresponding blockchain record, recalculates the hash of the provided certificate, and compares it with the stored hash to determine authenticity. The verification result is then displayed in real time, indicating whether the certificate is valid, invalid, or revoked.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

B. Authentication Mechanism

A significant enhancement of the proposed system is the integration of email-based OTP authentication, which introduces an additional layer of security beyond traditional login mechanisms. In this process, the user initiates authentication by entering their registered email address, after which a time-sensitive OTP is generated and transmitted to the user's email. The user must provide the correct OTP within a predefined time frame to gain access. This approach ensures two-factor authentication, prevents unauthorized access, and strengthens identity validation within the system.

C. Data Flow

The data flow within the system follows a structured and secure pipeline. When a certificate is generated, it is first uploaded to IPFS, which returns a unique CID representing the file. A SHA-256 hash is then computed using the certificate data and associated metadata. This hash is stored on the blockchain through a smart contract, ensuring immutability and transparency. Meanwhile, additional metadata such as student details and certificate references are stored in a relational database (PostgreSQL) to enable efficient querying and system performance. During verification, the system recomputes the hash of the provided certificate and compares it with the blockchain-stored hash to ensure integrity and authenticity.

Overall, the proposed system provides a comprehensive solution that combines decentralized storage, cryptographic security, and automated verification mechanisms to deliver a scalable, efficient, and tamper-resistant academic certificate management platform.

VI. Methodology

The proposed system follows a structured and secure workflow that integrates decentralized storage, blockchain validation, and cryptographic techniques to ensure the authenticity and integrity of academic certificates. The process begins with certificate generation, where the administrator inputs student data through a structured dataset and generates digital certificates in a standardized format. These certificates are then prepared for secure storage and verification within the decentralized framework.

Once generated, the certificates are uploaded to the Inter-Planetary File System (IPFS), a distributed file system that stores data in a content-addressable manner. Each uploaded certificate is assigned a unique Content Identifier (CID), which serves as a permanent reference to the file. This approach ensures efficient storage while avoiding the high cost associated with storing large files directly on the blockchain.

To guarantee data integrity, a cryptographic hash of the certificate is generated using the SHA-256 algorithm. The hash is computed based on the certificate content along with its associated CID, producing a unique fixed-length output that acts as a digital fingerprint of the certificate. Due to the deterministic and tamper-sensitive nature of the hashing process, any modification in the certificate results in a completely different hash value, thereby enabling reliable detection of data alterations.

The generated hash is then securely stored on the blockchain through a smart contract deployed on the Polygon network. By leveraging Blockchain, the system ensures immutability, transparency, and decentralized access to verification data. The smart contract maintains a mapping between certificate identifiers and their corresponding hash values, enabling efficient retrieval and validation.

During the verification phase, the system performs a recomputation of the hash using the certificate provided by the verifier. This newly generated hash is compared with the hash stored on the blockchain to determine authenticity. If both values match, the certificate is considered valid; otherwise, it is flagged as invalid. Additionally, the system checks the revocation status of the certificate to ensure that previously invalidated certificates are not accepted, thereby supporting full lifecycle management.

To enhance system security, an authentication layer based on email One-Time Password (OTP) verification is integrated into the workflow. Before accessing sensitive operations such as certificate retrieval or validation, users must authenticate themselves by entering a valid OTP sent to their registered email address. This ensures secure identity verification and prevents unauthorized access to the system.

A. Smart Contract Design and Implementation

The core functionality of the proposed system is implemented using a smart contract deployed on the Polygon blockchain network, enabling secure, transparent, and automated management of academic certificates. The smart contract is developed using Solidity and deployed through the Hardhat framework, ensuring efficient development, testing, and deployment.

The smart contract is designed to maintain a structured representation of certificate data, including attributes such as certificate identifier, student identifier, IPFS CID, cryptographic hash, and revocation status. These attributes are stored within a mapping structure that associates each certificate ID with its corresponding data, enabling constant-time access and efficient retrieval during verification.

Access control is enforced within the smart contract to ensure that only authorized administrators can perform critical operations such as certificate issuance and revocation. This prevents unauthorized modifications and preserves the integrity of the system. The issuance function records certificate details on the blockchain, ensuring immutability, while the revocation function allows administrators to invalidate certificates by updating their status without altering historical data.

The verification function is designed to provide a secure and efficient mechanism for validating certificates. It retrieves the stored certificate data from the blockchain, verifies its existence, checks its revocation status, and performs a hash comparison between the stored hash and the hash generated from the input certificate. This entire process is executed in

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

a trustless environment, eliminating the need for third-party intermediaries.

B. Certificate Verification Algorithm

Algorithm 1 Smart Contract-Based Certificate Verification

Require: certificateId, inputCertificateFile
Ensure: verificationStatus $\in$ {VALID, INVALID, REVOKED}
Step 1: Retrieve the certificate record using the given certificate identifier
Step 2: Check whether the certificate exists
if certificate record is empty **then**
  return INVALID
end if
Step 3: Verify the revocation status of the certificate
if certificate is revoked **then**
  return REVOKED
end if
Step 4: Generate the hash of the input certificate using SHA-256
Step 5: Retrieve the stored hash value from the blockchain
Step 6: Compare the generated hash with the stored hash
if both hash values are equal **then**
  return VALID
else
  return INVALID
end if

1) Algorithm Explanation: The certificate verification algorithm (Algorithm 1) ensures authenticity, integrity, and non-repudiation through blockchain immutability and cryptographic validation. The process retrieves certificate data from the blockchain and validates its existence. If the certificate is found, the system checks the revocation status to ensure it has not been invalidated.

Subsequently, a cryptographic hash is generated using SHA-256 and compared with the stored blockchain hash. Both hashes are converted to byte arrays and processed using keccak256 for secure Solidity-compatible comparison. A match confirms authenticity and returns VALID status, while any mismatch indicates tampering and returns INVALID. This approach provides high security while maintaining computational efficiency.

The certificate verification algorithm is designed to ensure authenticity, integrity, and non-repudiation through a combination of blockchain immutability and cryptographic validation techniques. The process begins by retrieving the certificate data associated with the provided certificate identifier from the blockchain. If no corresponding record is found, the certificate is immediately classified as invalid.

Once the certificate is retrieved, the system evaluates its revocation status. If the certificate has been marked as revoked by an authorized administrator, it is considered invalid regardless of any further validation steps. This mechanism ensures proper lifecycle management and prevents the reuse of invalidated credentials.

Subsequently, the system generates a cryptographic hash of the input certificate using the SHA-256 algorithm. This hash is then compared with the original hash stored on the blockchain during the certificate issuance phase. To perform this comparison securely within the Solidity environment, both hash values are converted into byte arrays and processed using the keccak256 hashing function, which is native to Ethereum-based systems and optimized for gas efficiency.

The final verification decision is based on the outcome of this comparison. A match between the computed hash and the stored hash confirms that the certificate is authentic and unaltered, resulting in a valid status. Conversely, any mismatch indicates potential tampering, leading to an invalid classification. This approach ensures a highly secure and reliable verification process while maintaining computational efficiency.

VII. System Architecture

The proposed system architecture is designed as a multi-layered framework that integrates frontend interfaces, backend services, blockchain infrastructure, and decentralized storage to enable secure and efficient academic certificate verification. Each layer in the architecture is responsible for specific functionalities, collectively ensuring seamless interaction, data integrity, and system scalability.

A. Frontend Layer

The frontend layer is developed using modern web technologies such as React, providing an interactive and user-friendly interface for administrators, students, and verifiers. This layer facilitates user interactions, including certificate generation, authentication, and verification processes. It acts as the entry point of the system, enabling users to communicate with backend services through secure API calls.

B. Backend Layer

The backend layer is implemented using Spring Boot, which handles business logic, request processing, and communication between different components of the system. It acts as an intermediary between the frontend and other layers, ensuring secure data transmission and enforcing application-level validation. The backend is responsible for processing certificate data, managing authentication workflows, generating hashes, and interacting with both the blockchain network and storage systems.

C. Blockchain Layer

The blockchain layer utilizes the Polygon network, which serves as a decentralized ledger for storing certificate hashes and verification data. By leveraging Blockchain, this layer ensures immutability, transparency, and resistance to tampering. Smart contracts deployed on the blockchain manage certificate issuance, revocation, and verification, enabling trustless and automated operations without reliance on centralized authorities.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

D. Storage Layer

The storage layer is divided into two components to optimize performance and scalability. Certificate files are stored in the InterPlanetary File System (IPFS), which provides decentralized and content-addressable storage. Each file stored in IPFS generates a unique Content Identifier (CID), ensuring permanent and tamper-resistant access. In parallel, a relational database such as PostgreSQL is used to store metadata, including student details, certificate references, and system logs. This hybrid storage approach balances efficiency, scalability, and data accessibility.

The overall workflow of the system follows a structured data flow across these layers. User requests initiated from the frontend are processed by the backend, which performs necessary validations and operations. Certificate files are uploaded to IPFS for decentralized storage, while their corresponding cryptographic hashes are recorded on the blockchain to ensure integrity. Metadata related to certificates and users is stored in the database for efficient retrieval.

During verification, the system retrieves data from these layers, recomputes the hash, and compares it with the blockchain record to determine authenticity. This integrated workflow ensures secure, real-time, and reliable certificate validation within a decentralized environment.

VIII. Experimental Setup

The proposed system is implemented using a combination of modern web technologies, blockchain infrastructure, and decentralized storage solutions to ensure efficiency, scalability, and security.

A. Blockchain Infrastructure

The deployment of smart contracts is carried out on an Ethereum-compatible environment, specifically utilizing the Polygon Mumbai Testnet, which provides a cost-effective and scalable platform for blockchain-based applications. The choice of Polygon enables reduced transaction fees and faster confirmation times compared to traditional Ethereum mainnet deployments.

The smart contract development and deployment process is facilitated using the Hardhat framework, which provides a robust environment for compiling, testing, and deploying Solidity-based contracts. This framework supports efficient debugging and simulation of blockchain interactions, ensuring the reliability of contract execution.

B. Frontend and Backend Implementation

The frontend of the system is developed using React.js, which offers a dynamic and responsive user interface for administrators, students, and verifiers. It enables seamless interaction with backend services and provides an intuitive platform for certificate generation, authentication, and verification.

The backend is implemented using Spring Boot with Java, which handles application logic, API management, and communication between different system components. It acts as a bridge between the frontend, blockchain network, and storage layers, ensuring secure and efficient data processing.

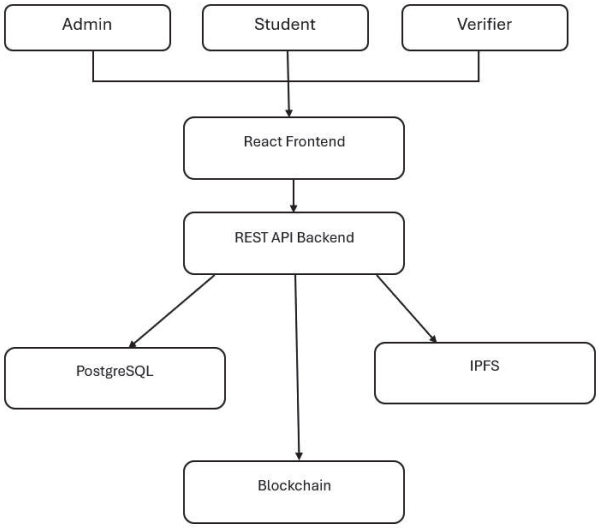

Fig. 1. System Architecture Diagram

C. Storage and Authentication

For decentralized file storage, the system utilizes the InterPlanetary File System (IPFS) through the Pinata service, enabling reliable and persistent storage of certificate files. Each file stored in IPFS generates a unique content identifier, which is later used for verification purposes.

In addition, a PostgreSQL database is employed to store metadata such as student information, certificate references, and system logs, ensuring efficient data retrieval and management.

Authentication within the system is implemented using an email-based One-Time Password (OTP) mechanism, which enhances security by providing multi-factor authentication. Furthermore, wallet integration is achieved using MetaMask, allowing secure interaction with the blockchain network for executing smart contract functions such as certificate issuance and verification.

D. Testing Environment

The system is evaluated in a controlled testing environment using simulated datasets that replicate real-world academic records. This setup enables comprehensive testing of system functionalities, including certificate generation, storage, authentication, and verification, ensuring the robustness, accuracy, and performance of the proposed solution under realistic conditions.

IX. Results and Discussion

The proposed system was evaluated based on key performance metrics, including security, efficiency, and usability, to

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

assess its effectiveness in comparison with traditional certificate verification methods. The experimental results demonstrate that the integration of Blockchain, decentralized storage, and secure authentication mechanisms significantly enhances the overall system performance.

A. Certificate Verification Performance

The system achieves instant certificate verification by eliminating manual validation processes and enabling direct comparison with immutable blockchain records. Unlike conventional systems, where verification requires institutional approval and time-consuming communication, the proposed approach provides real-time validation with minimal latency. Additionally, no instances of data tampering were observed during testing, confirming the robustness of the cryptographic integrity ensured through hashing and blockchain immutability.

B. Authentication and Security

The incorporation of email-based One-Time Password (OTP) authentication strengthens access control by preventing unauthorized interactions with the system. This ensures that only authenticated users can access or verify certificates, thereby enhancing data security and user trust. Furthermore, the system supports efficient bulk certificate generation and processing, enabling institutions to handle large datasets with reduced administrative overhead.

C. Comparative Performance Analysis

A comparative performance analysis reveals that the proposed system significantly outperforms traditional methods across multiple parameters. Verification time is drastically reduced due to automation and decentralized validation, while security is enhanced through cryptographic techniques and blockchain-based storage. Unlike traditional systems that lack tamper resistance, the proposed model ensures that any modification in certificate data is immediately detectable. Additionally, the authentication mechanism is considerably stronger due to the integration of OTP-based verification, as opposed to conventional password-based systems.

The performance comparison clearly indicates that the proposed system provides lower verification time, higher security, complete tamper resistance, and stronger authentication mechanisms, making it a more reliable and efficient solution for academic certificate validation.

X. Gas Cost Analysis

The efficiency of blockchain-based systems is largely determined by the gas consumption associated with smart contract execution. Gas represents the computational cost required to perform operations on blockchain networks such as Ethereum and Polygon. In the proposed system, gas consumption was analyzed for key operations, including contract deployment, certificate issuance, verification, and revocation.

The results indicate that contract deployment incurs the highest gas cost due to the initialization and storage of smart contract logic on the blockchain. In contrast, certificate issuance requires moderate gas consumption as it involves storing certificate hashes and associated metadata. Verification operations are comparatively lightweight, as they primarily involve hash comparisons without extensive state modifications. Similarly, revocation functions consume moderate gas as they update the status of existing records.

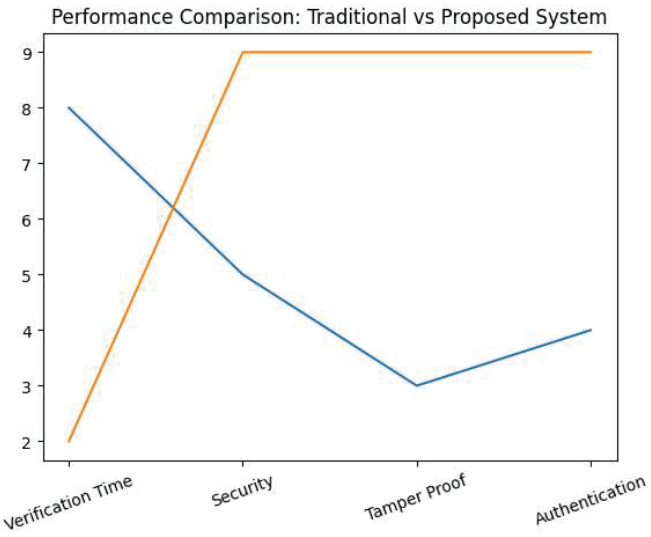

Fig. 2. Performance Comparison: Traditional vs Proposed System

The gas cost can be mathematically expressed as:

$$\text{Total Gas Cost} = \text{Gas Used} \times \text{Gas Price} \quad (1)$$

where the gas used represents the number of computational steps required for execution, and the gas price denotes the cost per unit gas measured in Gwei.

In the experimental setup, contract deployment required approximately 983,758 units of gas, with an average gas price of 25 Gwei, resulting in a total cost of approximately 0.025 MATIC. This demonstrates that deploying and operating the system on the Polygon network is significantly more cost-effective compared to Ethereum mainnet. The results also highlight that verification operations are optimized for minimal gas consumption, making the system suitable for large-scale and frequent validation scenarios.

Overall, the analysis confirms that the proposed system achieves a balance between security and cost efficiency, ensuring practical feasibility for real-world deployment.

A. Gas Consumption Breakdown

TABLE I
Gas Consumption Breakdown for Key Operations

Operation	Gas Used (Approx.)
Contract Deployment	∼983,758
Certificate Issuance	∼120,000
Certificate Verification	∼25,000
Revocation Function	∼40,000

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

XI. Mathematical Model of Certificate Verification System

The proposed system can be formally represented using cryptographic and functional models that define certificate structure, hashing mechanisms, and verification logic. A certificate can be represented as a tuple consisting of its essential attributes:

$$C = (ID, SID, CID, H, R) \tag{2}$$

where ID denotes the certificate identifier, SID represents the student identifier, CID corresponds to the IPFS content identifier, H is the cryptographic hash, and R indicates the revocation status.

The integrity of the certificate is ensured using the SHA-256 hashing function:

$$H = \text{SHA256}(C_{\text{file}}) \tag{3}$$

where C_{file} represents the certificate file. This function generates a unique fixed-length output that acts as a digital fingerprint of the certificate.

The blockchain storage mechanism can be modeled as a mapping function that associates certificate identifiers with their corresponding hash values:

$$B(ID) \rightarrow H \tag{4}$$

During verification, the system evaluates the authenticity of a certificate using the following function:

$$V = \begin{cases} \text{Valid} & \text{if } H_{\text{input}} = H_{\text{blockchain}} \wedge R = \text{false} \\ \text{Revoked} & \text{if } R = \text{true} \\ \text{Invalid} & \text{otherwise} \end{cases} \tag{5}$$

This model ensures that certificate validity is determined based on both hash integrity and revocation status.

From a security perspective, the probability of hash collision in SHA-256 is extremely low and can be expressed as:

$$P(\text{collision}) \approx 2^{-256} \tag{6}$$

This guarantees a negligible likelihood of two different certificates producing the same hash, thereby ensuring strong cryptographic security. The integration of SHA-256, blockchain immutability, and decentralized storage through InterPlanetary File System collectively strengthens the reliability and trustworthiness of the system.

XII. Conclusion

As a component of this research study , we introduced a decentralized academic certificate verification system that integrates blockchain technology, decentralized storage, and secure authentication mechanisms to address the limitations of traditional verification approaches. By leveraging the immutability of Blockchain and the scalability of IPFS, the proposed system ensures tamper-proof storage, transparent verification, and efficient data management.

The incorporation of cryptographic hashing techniques guarantees data integrity, while the implementation of email-based OTP authentication enhances system security by preventing unauthorized access. The system enables real-time certificate validation, significantly reducing verification time and eliminating dependence on centralized authorities.

Experimental results demonstrate that the proposed solution achieves superior performance in terms of security, efficiency, and reliability compared to conventional methods. Additionally, the use of the Polygon network ensures cost-effective deployment and scalability, making the system suitable for real-world applications.

Future work may focus on integrating advanced identity management techniques, such as decentralized identity (DID) frameworks, and expanding interoperability with other blockchain networks to further enhance system capabilities. Overall, the proposed system provides a robust, scalable, and secure solution for digital credential verification in modern academic ecosystems.

References

[1] D. Shukla, P. Rajput, P. Jadhav, N. Jadhav, and J. Thakur, "Blockchain-Based Academic Certificate Verification System," 2023.
[2] S. H. D and S. N, "Secure Academic Certificate Authentication Using Blockchain and IPFS," 2025.
[3] J. B. Moya, J. Ayoade, and M. A. Uddin, "ZKBAR-V: Blockchain-Based Academic Record Verification," 2025.
[4] A. Grech and A. F. Camilleri, "Blockchain in Education," Joint Research Centre, European Commission, 2017.
[5] M. Sharples and J. Domingue, "The Blockchain and Kudos: A Distributed System for Educational Record," 2016.
[6] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
[7] V. Buterin, "Ethereum Whitepaper: A Next-Generation Smart Contract Platform," 2014.
[8] G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," 2014.
[9] M. Swan, *Blockchain: Blueprint for a New Economy*, O'Reilly Media, 2015.
[10] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, 2016.
[11] N. Szabo, "Smart Contracts: Building Blocks for Digital Markets," 1996.
[12] L. Luu et al., "Making Smart Contracts Smarter," *ACM CCS*, 2016.
[13] M. Bartoletti and L. Pompianu, "An Empirical Analysis of Smart Contracts," 2017.
[14] A. Mavridou and A. Laszka, "Tool Demonstration: FSolidM for Smart Contract Development," 2018.
[15] S. Tikhomirov et al., "SmartCheck: Static Analysis of Ethereum Smart Contracts," 2018.
[16] J. Benet, "IPFS - Content Addressed, Versioned, P2P File System," 2014.
[17] Protocol Labs, "IPFS Documentation," 2023.
[18] Q. Xia et al., "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain," *IEEE Access*, 2017.
[19] H. Xu et al., "BlendCAC: A Blockchain-Enabled Decentralized Capability-Based Access Control," *IEEE Access*, 2018.
[20] Z. Zheng et al., "Blockchain Challenges and Opportunities: A Survey," *IJWGS*, 2018.
[21] M. Turkanovic et al., "EduCTX: A Blockchain-Based Higher Education Credit Platform," *IEEE Access*, 2018.
[22] P. R. W. et al., "Blockchain for Secure Academic Credential Verification," *IEEE*, 2019.
[23] R. Chen et al., "A Blockchain-Based System for Academic Certificates," *IEEE*, 2020.
[24] A. Alammary et al., "Blockchain-Based Applications in Education: A Systematic Review," *Applied Sciences*, 2019.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 05 , May - 2026

[25] S. R. Pokhrel and J. Choi, "A Decentralized Approach for Academic Credential Verification," *IEEE*, 2020.
[26] W. Stallings, *Cryptography and Network Security*, Pearson, 2017.
[27] B. Schneier, *Applied Cryptography*, Wiley, 1996.
[28] NIST, "SHA-256 Standard," 2015.
[29] C. Paar and J. Pelzl, *Understanding Cryptography*, Springer, 2010.
[30] D. Eastlake and P. Jones, "US Secure Hash Algorithm (SHA)," RFC 3174.
[31] M. Bellare and P. Rogaway, "Entity Authentication and Key Distribution," 1993.
[32] IETF, "Time-Based One-Time Password Algorithm (TOTP)," RFC 6238.
[33] D. M'Raihi et al., "HOTP: An HMAC-Based One-Time Password Algorithm," RFC 4226.
[34] A. Das et al., "Two-Factor Authentication Using OTP," *IEEE*, 2018.
[35] S. Gupta et al., "Secure OTP Authentication System Using Email Verification," 2021.
[36] ISO/IEC, "QR Code Standard," 2015.
[37] T. Pavlidis et al., "Barcodes vs QR Codes," *IEEE Computer*, 2012.
[38] Y. Liu et al., "QR Code-Based Authentication System," *IEEE*, 2019.
[39] R. Want, "An Introduction to RFID Technology," *IEEE Pervasive Computing*, 2006.
[40] H. Kato and K. Tan, "QR Code Reader Technology," *IEEE*, 2007.
[41] M. Crosby et al., "Blockchain Technology: Beyond Bitcoin," 2016.
[42] K. Croman et al., "On Scaling Decentralized Blockchains," 2016.
[43] S. Underwood, "Blockchain Beyond Bitcoin," *IEEE IT Professional*, 2016.
[44] A. Dorri et al., "Blockchain in IoT: Challenges and Solutions," *IEEE*, 2017.
[45] X. Xu et al., "A Taxonomy of Blockchain-Based Systems," *IEEE*, 2017.
[46] Y. Zhang et al., "Blockchain-Based Data Integrity Verification," *IEEE*, 2019.
[47] J. Sun et al., "Secure Data Sharing Using Blockchain," *IEEE*, 2020.
[48] H. Lin and L. Liao, "Blockchain-Based Secure Authentication," *IEEE*, 2017.
[49] S. Singh and N. Singh, "Blockchain: Future of Trust," *IEEE*, 2016.
[50] A. Reyna et al., "On Blockchain and Its Integration with IoT," *IEEE*, 2018.