International Journal of Information Technology & Computer Engineering

ISSN 2347–3657

Volume 14, Issue 1, 2026

Student Certificate Verification System Using Blockchain And Ai

T Santosh[1], Gundlapally Akshaya[2], Thota Deekshitha[3], Dandeboina Mamatha[4]

[1]Associate Professor; Department Of Information Technology Bhoj Reddy Engineering College For Women Hyderabad India.

[2,3,4]B.Tech Students; Department Of Information Technology Bhoj Reddy Engineering College For Women Hyderabad India.

Mail Id; thotadeekshitha928@gmail.com[3]

Abstract

In the digital era, ensuring the authenticity of academic certificates has become essential to prevent fraud, maintain institutional credibility, and streamline verification processes. Conventional verification methods rely on manual procedures and centralized databases, which are time-consuming, error-prone, and vulnerable to tampering. These challenges often lead to certificate forgery, administrative inefficiencies, and reduced trust among stakeholders.This paper proposes a secure and automated academic certificate verification system that integrates Blockchain technology with Artificial Intelligence (AI). Blockchain provides a decentralized and immutable ledger for storing certificate hashes, ensuring transparency, data integrity, and tamper-proof record management. AI-based algorithms are incorporated to analyze certificate data, identify anomalies, and detect potential fraudulent entries before certificates are committed to the blockchain network.A user-friendly web interface developed using HTML, CSS, and Bootstrap enables institutions to issue digital certificates and allows employers or verification authorities to authenticate them instantly using hash-based validation. The system also incorporates decentralized storage through IPFS, smart contract-driven automation, and certificate revocation mechanisms to enhance security and control. The integration of blockchain immutability, AI-driven validation, and a lightweight web interface ensures scalability, efficiency, and practical deployment in academic environments. This approach provides a reliable solution for trusted digital credential verification.

Keywords: *Blockchain, Academic Certificate Verification, Artificial Intelligence, Smart Contracts, IPFS, SHA-256, Digital Credentials, Decentralized Ledger, Fraud Detection, Proof-of-Authority.*

Introduction

Academic certificate verification is an essential process for validating student credentials in higher education and employment scenarios. Traditional verification methods depend heavily on physical documents and manual confirmation from issuing institutions. These approaches are often inefficient, prone to human error, and susceptible to forgery or unauthorized modifications. Additionally, centralized digital databases may face security threats, increasing the risk of data manipulation and loss of trust.To overcome these limitations, this work proposes a Blockchain and Artificial Intelligence–based certificate verification system. Blockchain technology enables decentralized and immutable storage of certificate records using cryptographic hashing techniques, ensuring that once issued, certificates cannot be altered. Artificial Intelligence complements blockchain by analyzing certificate data prior to storage, identifying inconsistencies, and minimizing the chances of fraudulent submissions.The proposed system also includes a web-based interface developed using HTML, CSS, and Bootstrap. Through this interface, institutions can securely issue digital certificates, while employers and other stakeholders can verify credentials instantly using unique hash values stored on the blockchain. The combination of blockchain security, AI-based validation, and an accessible web platform results in a scalable and transparent solution that enhances trust in academic credential verification.

Purpose of the Project

The main objective of this project is to design and implement a secure certificate verification system using blockchain and AI technologies. Blockchain provides a decentralized and tamper-resistant ledger for storing certificate information, eliminating risks associated with forgery and unauthorized modification. Artificial Intelligence enhances the system by detecting anomalies, recognizing suspicious patterns, and validating certificate data prior to blockchain storage.The system enables educational institutions to issue digital certificates securely and allows employers to verify credentials instantly without relying on intermediaries. Additionally, the framework supports certificate revocation, scalability, and reliable verification, ensuring transparency and trust among institutions, students, and recruiters.

Existing System

Current academic certificate verification methods primarily rely on paper-based documents or centralized digital repositories. Paper certificates are vulnerable to loss, damage, or forgery, while centralized systems are susceptible to cyberattacks and unauthorized data manipulation. Verification

often requires manual communication with issuing institutions, resulting in delays that may extend to several days or weeks.Furthermore, most existing systems lack intelligent mechanisms to detect fraudulent certificates. The absence of automated validation and real-time verification reduces efficiency and undermines confidence in credential authenticity. These shortcomings highlight the necessity for a decentralized and automated solution.

Proposed System

The proposed system integrates blockchain technology with AI-based validation to create a secure certificate verification framework. Blockchain ensures tamper-proof storage of certificate hashes, while AI validates certificate data during issuance. This dual-layer approach improves fraud detection and enhances trust. Institutions can issue digital certificates, and third parties can verify them instantly through blockchain-based validation.

Related Work

Academic certificate verification has attracted significant research attention due to increasing cases of document forgery and unreliable manual validation. Recent advancements in blockchain and AI technologies have enabled the development of secure and automated credential verification systems.Several researchers have explored blockchain-based academic record management. Gupta et al. demonstrated that decentralized ledgers combined with cryptographic hashing can prevent certificate tampering. However, their approach lacks intelligent anomaly detection. The proposed system addresses this limitation by integrating AI-based validation prior to blockchain storage.Gayathiri et al. emphasized the use of hashing algorithms such as SHA-256 to ensure document integrity. While hashing prevents modification after storage, it cannot detect invalid data entered initially. The proposed system incorporates AI validation before hashing, thereby preventing fraudulent certificates from being recorded.Other studies have explored decentralized storage mechanisms such as IPFS for secure document management. These approaches improve scalability and reduce data loss risks. Building on these findings, the proposed architecture stores encrypted certificates in IPFS while maintaining immutable blockchain references.

Requirement Analysis

Requirement analysis is an essential phase in system development that identifies the functional capabilities and performance expectations of the proposed certificate verification system. This phase focuses on defining what the system should accomplish and the quality standards it must satisfy to ensure reliability, security, and scalability. The proposed Blockchain and AI-based certificate verification system requires both functional and non-functional requirements to support secure issuance, validation, and verification of academic credentials. These requirements ensure that the system operates efficiently while maintaining transparency, usability, and robustness across different academic environments.The functional requirements describe the core operations of the system. The system must allow authorized academic institutions to issue digital certificates securely through a web-based interface. Before storing certificates, an AI-based validation module analyzes the document structure, metadata, and formatting to detect inconsistencies or potential fraud. Once validated, certificates are encrypted and stored in decentralized storage such as IPFS, while their cryptographic hash is recorded on the blockchain for capabilities.Non-functional requirements define the quality attributes necessary for efficient system performance. The system must be scalable to handle an increasing number of certificates and verification requests without performance degradation. It should provide fast processing to ensure quick issuance and verification. Security is a critical requirement, requiring encryption, secure authentication, and tamper-proof blockchain storage to protect certificate data. The system must be reliable, ensuring continuous operation and availability of verification services. Maintainability is also important so that updates and improvements can be implemented without disrupting system functionality. Furthermore, interoperability should be supported to allow integration with existing academic portals and third-party verification platforms. The user interface should remain simple and intuitive, enabling users with minimal technical knowledge to interact with the system effectively.

The computational resource requirements define the software and hardware specifications necessary for implementation. The system is designed to operate on a Windows-based environment using Python as the primary programming language. Development can be carried out using Visual Studio Code, while the frontend is built using HTML, CSS, and Bootstrap to ensure responsiveness. AI-based validation is implemented using frameworks such as TensorFlow, Scikit-learn, or PyTorch. Blockchain functionality is supported through the Ethereum platform, and decentralized file storage is managed using IPFS. Web3.js is used for blockchain interaction, and Chart.js may be incorporated for data visualization. The recommended hardware configuration includes an Intel Core i5 processor or higher, a minimum of 8GB RAM, and at least 500GB storage capacity to ensure smooth system performance.

Design

System Architecture

The proposed architecture consists of four major components: user interface, AI validation module,

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 1, 2026

blockchain network, and decentralized storage. Institutions upload certificate data through the web interface. The AI module validates the data and detects anomalies. After validation, certificate hashes are generated and stored on the blockchain, while the encrypted certificate files are stored in IPFS. Verification is performed by comparing hashes retrieved from the blockchain.

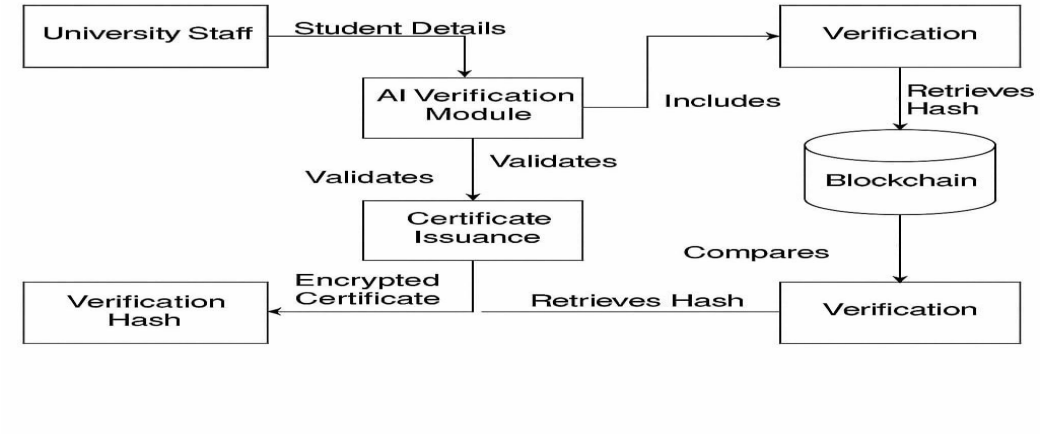


Fig. 1 System Architecture

Technical Architecture

The technical architecture integrates frontend technologies, backend AI modules, blockchain smart contracts, and decentralized storage. The frontend handles certificate issuance and verification. The backend processes certificate data using AI algorithms. Smart contracts manage blockchain transactions and authentication. IPFS stores certificate files, and the blockchain maintains immutable references.

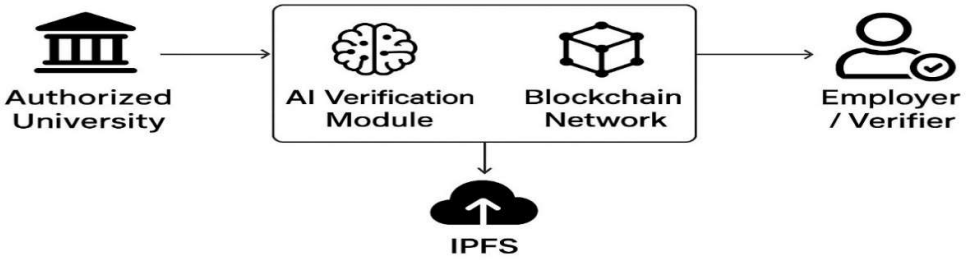


Fig. 2 Technical Architecture

Modules

A module represents an independent functional unit of a software system. The proposed certificate verification system is organized into multiple modules, each responsible for a specific task. This modular design improves scalability, maintainability, and performance. Every module communicates with others to ensure secure certificate issuance, storage, verification, and monitoring. The following modules form the core architecture of the system.

Blockchain Network Module:

The Blockchain Network Module manages all blockchain-related activities, including secure communication, block creation, and smart contract execution. It records certificate transactions on a decentralized and immutable ledger, ensuring transparency and preventing unauthorized changes. Cryptographic mechanisms provide tamper resistance and trust among participants. The module utilizes the Proof-of-Authority (PoA) consensus mechanism, where authorized validator nodes generate and validate blocks. This approach reduces computational overhead and enables faster confirmations, making it suitable for private academic blockchain environments that require reliability and low latency.

Certificate Issuance Module:

The Certificate Issuance Module allows authorized institutional staff to generate digital academic certificates securely. When a certificate is created, the system computes a unique cryptographic hash

representing the certificate content. This hash is stored on the blockchain to maintain authenticity and traceability. Additionally, the certificate is digitally signed using Elliptic Curve Digital Signature Algorithm (ECDSA), ensuring that only authorized issuers can create valid certificates. Any alteration to the certificate invalidates the signature, preventing unauthorized modifications. SHA-256 hashing is used to generate fixed-length hashes, providing strong tamper resistance and data integrity.

AI Verification and Anomaly Detection Module:
This module incorporates artificial intelligence techniques to analyze certificate data before blockchain storage. It identifies anomalies, inconsistencies, or suspicious entries to prevent fraudulent records from being permanently recorded. The system uses Isolation Forest for unsupervised anomaly detection, which isolates abnormal data points such as unusual verification attempts or abnormal certificate attributes. Additionally, a Random Forest classifier is used to learn patterns from historical verification data and classify requests as legitimate or suspicious. These models continuously improve with new data, enhancing fraud detection accuracy over time.

Certificate Storage Module:
The Certificate Storage Module stores certificate files in a decentralized storage environment such as IPFS. Instead of saving complete certificates on-chain, only the hash and IPFS content identifier are stored on the blockchain. This approach reduces blockchain storage overhead while maintaining secure access to certificate data. The module also employs Keccak-256 hashing within smart contracts for generating identifiers and mapping storage locations. This ensures collision-resistant indexing and efficient certificate retrieval.

Verification Module:
The Verification Module enables employers, institutions, or third parties to validate certificate authenticity. During verification, the system recalculates the certificate hash using SHA-256 and compares it with the hash stored on the blockchain. If both values match, the certificate is confirmed as genuine. This process allows instant validation without manual intervention and significantly reduces verification time.

Certificate Revocation Module:
The Certificate Revocation Module provides administrators with the ability to revoke certificates that are invalid, outdated, or incorrectly issued. Once revoked, the certificate status is updated on the blockchain, making the change visible to all verifiers. The module uses Merkle Tree structures to organize certificate hashes efficiently. Merkle Proofs allow verification of certificate existence or revocation using minimal data, ensuring scalability even with large datasets.

Dashboard and Visualization Module:
The Dashboard Module offers a graphical interface for monitoring system operations. It displays issued certificates, verification logs, revocation records, and blockchain activity. Interactive charts and tables provide administrators with insights into system performance. This improves usability and simplifies management of the entire certificate verification ecosystem.

Implementation
The system implementation relies on several software libraries and frameworks to support blockchain, machine learning, and web application functionalities.

TensorFlow is used as a machine learning framework for building predictive models and supporting intelligent validation features. It provides tools for model training, deployment, and scalability across platforms. Scikit-learn is employed for implementing classical machine learning algorithms such as Isolation Forest and Random Forest, offering efficient data preprocessing and evaluation utilities. PyTorch is included to support flexible deep learning experimentation and GPU-accelerated computations where required.

Ethereum serves as the blockchain platform for executing smart contracts and maintaining decentralized certificate records. It enables transparent and secure transaction handling without relying on centralized authorities. IPFS is used for decentralized storage of certificate files, ensuring content-addressable retrieval and high availability. Chart.js provides visualization capabilities for displaying certificate statistics, system activity, and verification logs in an interactive dashboard. Web3.js acts as the communication layer between the frontend application and blockchain network, allowing smart contract interaction and transaction submission.

Pseudocode Description
The application initialization module sets up the Flask server, loads blockchain and AI components, and configures database connectivity. The routing module manages user authentication, certificate issuance, verification, and revocation operations. When issuing a certificate, the system first validates data using the AI module. If approved, the certificate data is uploaded to IPFS, and a new blockchain block is created containing the certificate hash and metadata.

The blockchain core consists of block and chain modules. Each block contains certificate data, timestamp, IPFS identifier, previous hash, validator identity, and revocation status. The chain module initializes the genesis block and handles new block additions while maintaining integrity through SHA-256 hashing.

The AI validation module loads a trained anomaly detection model and evaluates certificate attributes such as attendance and CGPA. Suspicious entries

are flagged before blockchain insertion. The training module uses Isolation Forest to learn normal patterns from sample data and stores the trained model for runtime use.

The IPFS handler module calculates file hashes, stores certificate files in a decentralized manner, and returns content identifiers for retrieval. During verification, the system compares the submitted certificate hash with blockchain records. If a match is found, the certificate is validated; otherwise, it is marked invalid. The revocation mechanism updates blockchain entries to prevent further use of revoked certificates.

Testing

System testing was conducted to ensure that each functional component of the proposed certificate verification system operates correctly and meets the design requirements. The testing process covered user authentication, certificate issuance, AI-based validation, blockchain storage, IPFS upload, verification, and revocation mechanisms. During user registration, valid input data resulted in successful account creation, confirming that the registration module correctly stores user details. Similarly, login testing verified that users with valid credentials could access the system without errors.

The certificate issuance test confirmed that valid student information leads to successful certificate generation. The AI validation test ensured that abnormal values, such as CGPA greater than the allowed limit or attendance exceeding the defined range, were detected and blocked before storage. Testing of the IPFS upload module demonstrated that valid certificate data generates a unique content identifier, confirming decentralized storage functionality. The blockchain storage test validated that new blocks containing certificate data are correctly added to the chain.

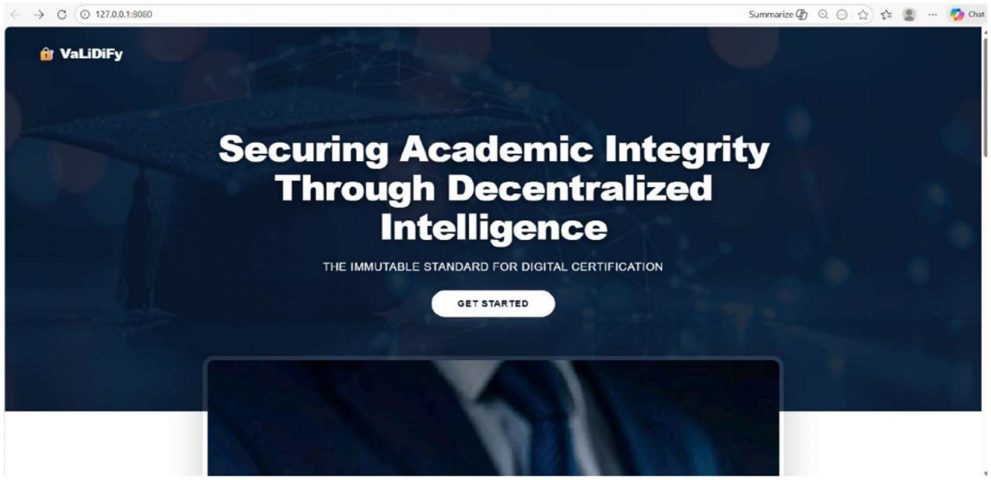
The verification module was tested by providing a valid certificate hash, and the system successfully displayed certificate details, confirming authenticity. The revocation module was also evaluated, and the system correctly updated certificate status when an administrator revoked a certificate. All test cases produced expected results, indicating that the system functions reliably across all modules.

Validation

Input validation mechanisms were implemented to ensure data integrity and prevent incorrect information from entering the system. During user registration, all required fields were validated to confirm completeness and correctness before storing the data. Login validation ensured that the provided email and password matched existing records. Certificate input validation restricted CGPA values to a maximum of 10 and attendance values to 100, preventing invalid entries.

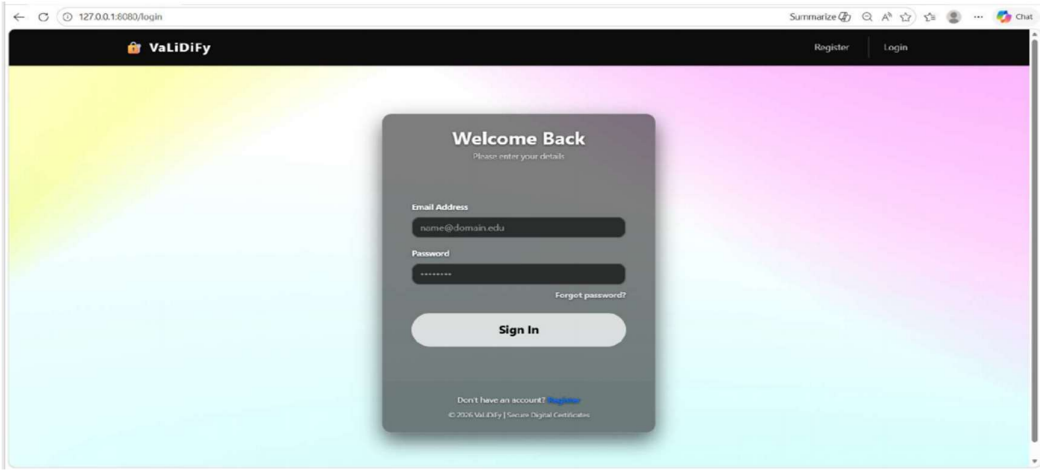
The AI validation module analyzed certificate attributes to detect abnormal patterns and blocked suspicious data. The IPFS upload process verified that certificate data followed a valid JSON format before generating a storage hash. Blockchain validation ensured that each certificate hash remained unique to prevent duplication. Certificate verification validation compared the submitted hash with blockchain records to confirm authenticity. Additionally, revocation validation restricted certificate revocation privileges to authorized administrators only. These validation checks improved system security, reliability, and accuracy.

Screenshots



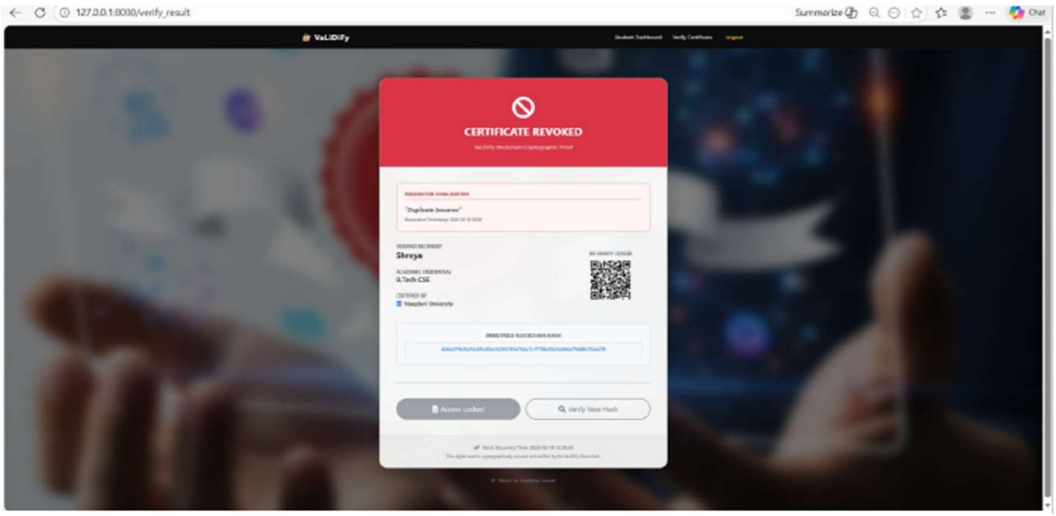
Screenshot 1: VaLiDiFy system homepage displaying project interface.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 1, 2026



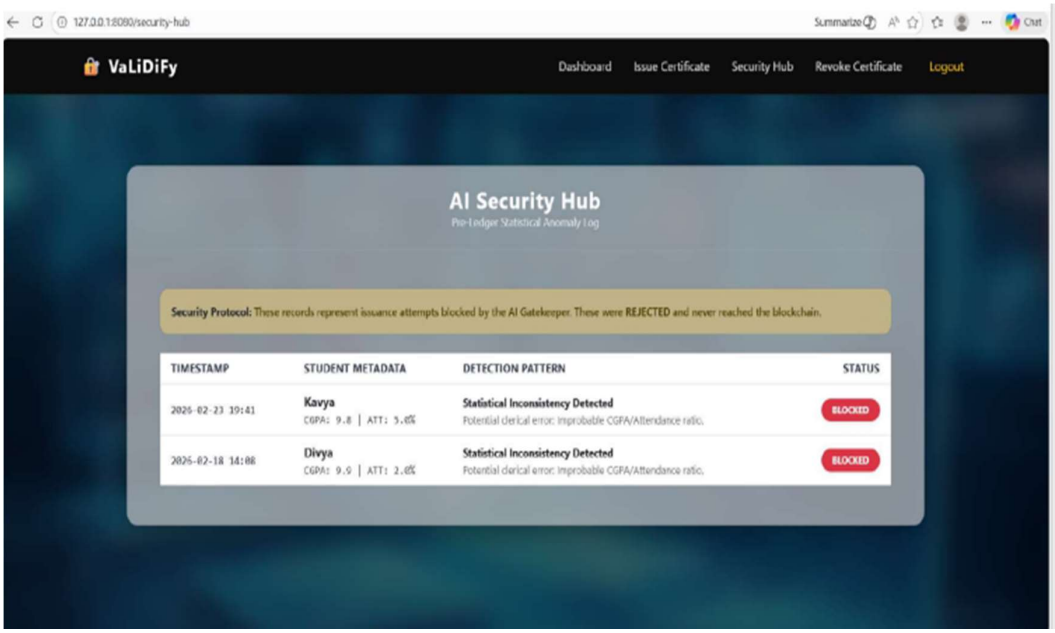
Screenshot 2: User login page.

Screenshot 3; Generated digital certificate.



Screenshot 4: Revoked certificate result.

International Journal of Information Technology & Computer Engineering
ISSN 2347–3657
Volume 14, Issue 1, 2026



Screenshot 5: AI anomaly detection page.

Conclusion

The proposed blockchain-based certificate verification system integrated with artificial intelligence provides a secure and efficient alternative to traditional verification methods. By storing certificate records on a decentralized and immutable blockchain ledger, the system eliminates risks associated with document forgery and unauthorized modifications. The integration of AI techniques enhances system intelligence by detecting anomalies and preventing suspicious entries before they are recorded permanently. This proactive approach strengthens data integrity and improves trust among stakeholders.

The developed platform enables instant certificate verification through hash comparison, significantly reducing manual effort and processing time. The use of decentralized storage further ensures long-term accessibility and resilience against data loss. Additionally, the user-friendly interface and dashboard simplify system management for administrators and institutions. The proposed framework supports digital transformation by replacing paper-based verification processes and promoting secure digital credential management. Overall, the system demonstrates a scalable and reliable solution capable of improving transparency, efficiency, and security in academic certificate verification.

Future Scope

The proposed system can be further enhanced by integrating additional technologies and expanding its applicability. Future improvements may include biometric authentication and digital identity frameworks to strengthen user verification and reduce identity fraud. Integration with national and international academic databases could enable cross-border certificate verification, supporting global education and employment opportunities. Smart contracts may also be extended to automate certificate issuance, validation, and revocation with minimal manual intervention.

The system can be expanded to support verification of professional certifications, licenses, and skill-based credentials beyond academic records. Advanced artificial intelligence models, including deep learning approaches, may improve fraud detection accuracy and adapt to emerging forgery techniques. Developing mobile applications and cloud-based deployment can enhance accessibility and scalability. With these enhancements, the system has the potential to evolve into a comprehensive and universally accepted digital credential verification ecosystem that ensures trust, security, and efficiency.

References

[1] Cheng, Wei, Zhang, Li, and Liu, Yang, “Smart Contract-Based Certificate Issuance and Verification System,” *International Journal of Blockchain Applications*, 2020.

[2] Gupta, Rahul, Sharma, Ankit, and Verma, Neha, “Blockchain-Based Academic Record Verification Using Cryptographic Hashing,” *Proceedings of the International Conference on Emerging Technologies*, 2019.

[3] Gayathiri, S., Priya, K., and Kumar, Ramesh, “Secure Hashing Techniques for Digital Certificate Verification Systems,” *Journal of Information Security and Applications*, 2021.

[4] Akanksha Jadhav and Ramesh D. Jadhav, "Decentralized Storage Using IPFS for Secure Certificate Management," *International Journal of Computer Science and Engineering*, 2022.
[5] Jason Brownlee, *Machine Learning Mastery with Python*, Machine Learning Mastery Publications, 2017.
[6] Kumar, Sandeep, Reddy, Mahesh, and Singh, Amit, "Exploratory Data Analysis and Secure Credential Verification Using AI and Blockchain," *IEEE Access*, 2022.
[7] Nakamoto, Satoshi, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Cryptography Mailing List*, 2008.
[8] Buterin, Vitalik, "Ethereum: A Next-Generation Smart Contract and Decentralized Application Platform," *Ethereum White Paper*, 2014.
[9] Zheng, Zibin, Xie, Shaoan, Dai, Hongning, Chen, Xiangping, and Wang, Huaimin, "Blockchain Challenges and Opportunities: A Survey," *International Journal of Web and Grid Services*, 2018.