iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** III **Month of publication:** March 2026

DOI: https://doi.org/10.22214/ijraset.2026.77897

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

AI Based Decentralized Academic Credential Verification System Using Blockchain

P. Gayathri Reddy[1], P. Charitha Reddy[2], P. Yoshitha[3], Mr. T Vinay Simha Reddy[4]
CSE-AI&ML, Malla Reddy University, Hyderabad

Abstract: ***The increasing incidents of forged academic certificates and the inefficiencies of traditional verification systems highlight the urgent need for a secure, transparent, and reliable credential management mechanism. Conventional systems are largely centralised, time-consuming, and prone to manipulation, resulting in high administrative overhead and verification delays. We prepared an AI-Based Decentralized Academic Credential Verification System that leverages blockchain technology, smart contracts, and artificial intelligence to provide a tamper-proof platform for issuing, storing, and validating academic records. Artificial Intelligence is integrated to perform anomaly detection during certificate issuance and AI-based facial authentication for students, enhancing security and preventing fraudulent entries before blockchain storage. Students gain permanent, secure access to their verified credentials, while verifiers, such as employers, can instantly authenticate certificates using blockchain records or QR code scanning, eliminating the need for intermediaries. By integrating Ethereum, Solidity, Web3.js, IPFS, React.js, and AI models, the proposed system delivers a decentralized, scalable, and cost-effective solution that enhances trust, reduces verification time, and effectively combats academic credential fraud.***

Index Terms: ***Artificial Intelligence; Blockchain; Decentralized Credential Verification; Academic Certificate Authentication; Smart Contracts; Inter Planetary File System; Fraud Detection***

I. INTRODUCTION

Since ancient times, education has been central to societal advancement, initially taking shape through the direct sharing of wisdom and skills by elders and knowledgeable community members. In these early settings, personal trust served as the main mechanism for validating what was learned. As civilisation progressed, formal educational institutions such as schools and universities emerged, taking on the responsibility of assessing learners and granting official certificates. These credentials gradually became essential proof of academic accomplishments, unlocking opportunities for further study and employment. However, as globalisation and digital learning environments have expanded, the task of authenticating academic qualifications has become increasingly complex, especially where direct social trust is absent.

Today, universities and third-party agencies typically oversee academic records using centralised systems. Unfortunately, these systems face risks like forgery, data loss, unauthorised alterations, and duplication, which can jeopardise both institutional reputation and the value of individual certificates [1][8][9]. Studies indicate that fake academic credentials are a common problem, leading to far-reaching ethical, economic, and social implications [9]. Individuals often require multiple documents for career or educational advancement, but conventional verification processes are inefficient, costly, and time-consuming [1]. The swift adoption of digital certificatesfurther accelerated by the COVID-19 pandemic has exposed additional vulnerabilities in centralised systems, such as limited scalability, cyberattack risks, and single points of failure [1][8]. As a result, there is a pressing need for a secure, tamper-resistant, and automated credential management approach that reduces reliance on central authorities. Technologies like blockchain, when paired with innovative verification techniques, offer decentralised solutions that ensure transparency, data integrity, and trustless authentication of academic records. Adopting such systems can foster greater trust between all parties and dramatically reduce the time required for verifying credentials.

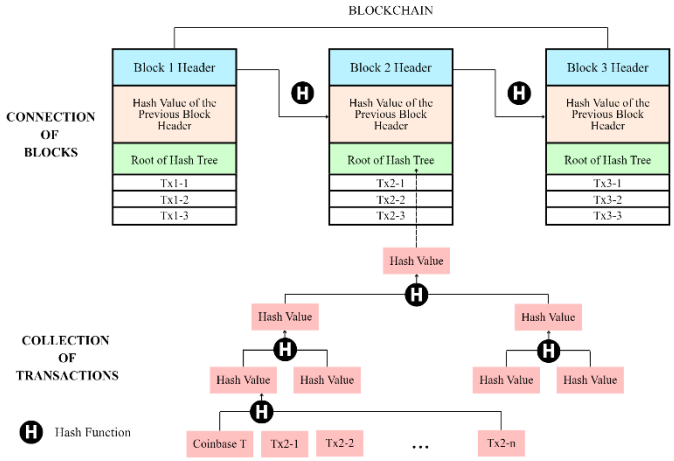


Figure 1:Structure of Blockchain

Blockchain technology, first introduced in 2008 as a peer-to-peer distributed ledger for Bitcoin transactions, offers a promising solution to these challenges through its decentralized and tamper-resistant architecture [4][5]. A credential verification system, as used in education, is a system that verifies the ownership, legitimacy, and integrity of academic records, including degrees and certificates. By spreading trust throughout a network, a decentralised credential verification system removes the need for a single central authority and permits credentials to be independently checked by authorised parties while maintaining transparency and tamper resistance. In a blockchain network, each node maintains a replica of the ledger, and transactions are validated through consensus mechanisms before being permanently recorded using cryptographic techniques such as hash functions and digital signatures [4][6]. Beyond cryptocurrencies, blockchain has demonstrated applicability across various domains including healthcare, supply chains, certificate management, and education due to its properties of immutability, transparency, and auditability [4][6][8]. Furthermore, integration with decentralized storage systems such as IPFS can enhance secure data storage while blockchain ensures traceability and ownership protection of digital records [3]. These properties make blockchain ideal for decentralised academic credential management and verification.

Using blockchain-based decentralised application (DApp) technology, this study suggests a decentralised credential verification framework to overcome the drawbacks of conventional credential verification systems. The suggested method reduces dependency on centralised authorities while facilitating the safe issuance, storage, and verification of academic credentials. By incorporating QR codes and blockchain-backed verification, the system aims to reduce verification time, operational cost, and the risk of credential forgery, while improving transparency and trust among stakeholders such as students, institutions, and employers [1][8]. The creation of a secure blockchain-based credential management system, the automation of verification procedures using DApp technology, and the incorporation of decentralised principles to improve scalability and dependability are the primary contributions of this work.

The remainder of this paper is organized as follows: Section 2 reviews related work, Section 3 discusses existing systems, Section 4 presents the proposed framework, Section 5 analyzes results, and Section 6 concludes the paper with future directions.

II. LITERATURE REVIEW

The decentralised, transparent, and tamper-resistant characteristics of blockchain technology have attracted significant attention from the research community. The foundational concept of blockchain was first introduced by Nakamoto [2] through Bitcoin, a peer-to-peer electronic payment system enabling trustless transactions without intermediaries. Building on this concept, Zheng et al. [1] and Holotescu [4] analysed the core architecture, key features, and challenges of blockchain technology, highlighting its potential applications beyond cryptocurrencies, including secure data storage and decentralised verification systems, while also identifying limitations such as scalability, security, and consensus efficiency. Further, Kuo et al. [11] compared different blockchain platforms and demonstrated how architectural variations influence system performance and security in sensitive application domains. In the education sector, blockchain has been widely explored for academic credential management and verification. Alammary et al. [8] conducted a comprehensive review of blockchain applications in education and identified certificate issuance and verification as among the most promising use cases.

Similarly, Bokariya and Motwani [5] proposed a decentralised credential verification approach aimed at reducing reliance on centralised authorities and mitigating certificate forgery, while Kumar et al. [9] and Pathak et al. [10] examined blockchain-based academic certificate verification systems, emphasising the role of immutable ledgers in enhancing trust and reducing administrative overhead. Several studies have focused on automating credential verification using decentralised applications and smart contracts. Cheng et al. [12] introduced an Ethereum-based digital certificate system that assigns unique identifiers and QR codes to certificates for secure and transparent verification. The effectiveness of smart contract-based certificate issuance and validation was further demonstrated by Gundgurti et al. [14] and Gayathiri et al. [15], who showed that automation improves efficiency while preserving data integrity. Additionally, Shawon et al. [21] proposed a decentralised application architecture that enables employers and students to verify academic credentials without dependence on institutional databases. Prior research has also addressed critical concerns such as certificate revocation, privacy preservation, and verification efficiency. Vidal et al. [17] examined blockchain-based certificate revocation mechanisms, emphasising the importance of maintaining up-to-date credential status, while Chen et al. [16] proposed CertChain, a blockchain-based certificate audit framework focused on public verifiability and operational efficiency. Furthermore, Tariq et al. [18] introduced Cerberus, a blockchain-based degree verification system supporting selective data disclosure and real-world threat modelling, whereas Wang et al. [19] and Yao et al. [20] presented privacy-preserving certificate transparency and validation schemes using cryptographic techniques such as Merkle hash trees. Collectively, these studies demonstrate that blockchain-based credential verification systems offer enhanced security, transparency, and trust compared to conventional centralised approaches; however, many existing solutions address privacy, revocation, and verification as isolated components, indicating a research gap in developing an integrated, scalable, and user-friendly decentralised credential verification framework.

III. EXISTING SYSTEM

Academic credential issuance and verification in modern educational institutions are predominantly managed through centralized systems overseen by universities, examination boards, or authorized third-party agencies. Student academic records and certificates are stored in institutional databases, while verification requests are processed either manually or through institution-specific online portals. Employers or external organizations must contact the issuing authority to authenticate credentials, making the entire process highly dependent on institutional availability and administrative workflows.

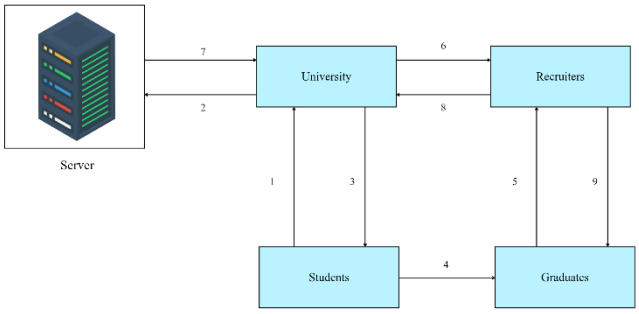


Figure. 2: Existing Framework

Although many institutions have transitioned from paper-based certificates to digital formats, most existing systems continue to rely on centralized servers and trusted intermediaries. This centralized architecture introduces multiple concerns related to security, scalability, and operational efficiency. Centralized databases represent a single point of failure and remain vulnerable to cyberattacks, unauthorized access, and data tampering, especially during system outages or technical disruptions.

The verification process in current systems is often time-consuming and labor-intensive. Institutions must manually retrieve records, authenticate certificates, and respond to verification requests, which significantly increases administrative workload and operational costs.

For students seeking employment or higher education across multiple organizations or geographical regions, repeated verification requests further amplify delays and inefficiencies. Moreover, the absence of standardized credential formats restricts interoperability among institutions.The major limitations of existing credential verification systems include:

- Centralized control over certificate issuance and verification, leading to dependency on a single authority
- Manual or semi-automated verification processes, resulting in delays and increased administrative overhead
- Susceptibility to data breaches and manipulation, as credentials are stored in centralized databases
- Limited scalability and interoperability, particularly for cross-institutional and international verification
- Vulnerability to certificate forgery and duplication due to exploitable system weaknesses
- Insufficient privacy control, where students have minimal authority over how their credentials are shared
- Inefficient revocation and update mechanisms, making it difficult to maintain certificate validity over time

IV. PROPOSED SYSTEM

To address the shortcomings of centralised credential management systems, the proposed methodology introduces a decentralised academic credential verification framework powered by blockchain and AI. Without depending on reliable third-party middlemen, the system makes it possible to securely issue, store, and verify academic credentials. The suggested method guarantees transparency, immutability, privacy, and intelligent validation of academic records by combining blockchain technology, decentralised storage, and artificial intelligence.

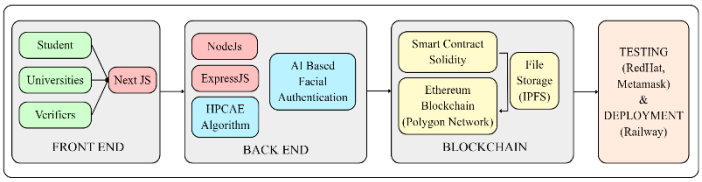


Figure.3: Proposed Architecture for Decentralized Application

This structure prevents fraudulent certificate generation and ensures institutional validity by limiting the issuance of academic credentials to authorised universities. The InterPlanetary File System (IPFS), which offers decentralised, tamper-resistant storage, is used to securely store and process certificates when they are granted. Using smart contracts implemented on the Polygon-based Ethereum network, a cryptographic hash and issuer metadata, including the certificate ID, issuing authority, and timestamp, are stored on the blockchain for every certificate. Employers and academic organisations may quickly confirm the legitimacy of certificates without getting in touch with the university that issued them thanks to the QR code that is incorporated in each credential and connected to its blockchain record.

The system integrates AI-based identification and integrity verification algorithms to improve security and trust. To make sure that only the rightful owner may use the credential, students use live face recognition to authenticate themselves. To identify manipulation or fake certificates, AI-driven picture integrity analysis and watermark verification are also used. To find illegal or questionable activity, an AI-based anomaly detection module continuously examines access patterns. A Hybrid Principal Component Analysis (HPCAE)-based dimensionality reduction technique is used to optimise certificate data before to blockchain anchoring. This technique reduces storage overhead while maintaining crucial credential attributes.

The entire system is designed as a web-based decentralised application (DApp) with role-based access for administrators, universities, students, and verifiers. Web 3.0 technologies were used to construct the DApp, and wallet-based authentication makes it possible to interact with blockchain smart contracts in a safe and easy way. By automating the procedures of credential issue, verification, and revocation, smart contracts guarantee uniformity and do away with manual involvement. All things considered, the suggested approach offers a scalable, effective, and safe decentralised option for verifying academic credentials, greatly lowering administrative burden, fraud, and verification time while enhancing transparency and confidence.

A. System Architecture

This credential verification platform is organised with separate layers and modules to ensure it is secure, scalable, transparent, and easy to deploy.

The architecture includes a user-friendly web portal, a powerful backend enhanced by artificial intelligence, a blockchain layer that leverages decentralised storage, and individual modules for both testing and deployment, as shown in the system diagram. This setup allows credentials to be issued automatically, stored safely, and verified quickly, all without the need for a central authority, drawing inspiration from previous education systems that use blockchain.

The front end, built with Next.js, acts as the main point of interaction for students, educational institutions, and credential verifiers. This interface enables universities to distribute certificates, students to check their achievements, and employers or organisations to validate those credentials. Digital wallet authentication restricts access to approved users, and the interface works smoothly with backend services to interact with blockchain components efficiently [21], [22]

At the core, the backend developed with Node.js and Express.js handles the platform's logic, processes API calls, and ensures safe communication between the user interface, artificial intelligence modules, and the blockchain. This part of the system uses the HPCAE algorithm to make data handling more efficient. A standout feature is the facial recognition module powered by AI, which ensures that only verified students can access their certificates, adding a further layer of protection beyond basic logins.

The blockchain component acts as the trust foundation for the entire platform. It operates on Ethereum and takes advantage of the Polygon network for rapid and low-cost transactions, all while preserving a decentralised environment. Smart contracts written in Solidity control the creation, validation, and possible revocation of credentials. To provide transparency and permanence, only hashed versions of certificates with key details like certificate ID, issuer address, timestamp, and status are kept on the blockchain [5], [20]. This approach helps prevent tampering and ensures that verification is trustworthy and straightforward.

B. WorkflowImplementatio

The workflow starts when a recognized educational institution logs into the decentralized application by confirming its identity through a blockchain wallet. This secure authentication step validates the institution's authority and sets up a transparent, traceable environment for all future operations. Once inside, the institution uses a unified system that merges blockchain, decentralized storage, and artificial intelligence. This integration enables the complete automation of the academic credential lifecycle, covering everything from issuing to storing and verifying records. This digital transformation replaces slow, manual, and error-prone paper processes, providing faster, more reliable, and more secure credential management at every step.

To enhance system security, the application uses several authentication layers, such as multi-factor verification and AI-driven anomaly detection, to block unauthorized users and flag unusual activity. After clearing these safeguards, the institution can upload student credentials for processing. Artificial intelligence is then used to prepare the uploaded data—by checking its integrity, optimizing storage, embedding digital watermarks, and, if needed, using steganography to hide sensitive information. These steps ensure the data is both authentic and efficiently stored for future reference.

After these preparations, the credential is stored in the Inter Planetary File System (IPFS), a decentralized storage solution. IPFS assigns a unique content-based hash to every credential, serving as its permanent digital fingerprint. This hash both connects the credential to its storage location and acts as an unchangeable reference for any future checks or validation, making tampering easy to detect

After the credential has been stored, a smart contract automatically generates a QR code linked to the blockchain record and records a cryptographic hash of the certificate along with key metadata, including the certificate ID, issuing institution, and timestamp. For added security, the system relies on AI-powered biometric authentication for users. When verification is needed, the smart contract compares the hash from IPFS to the one on the blockchain, ensuring that the most current and legitimate version is always used. If the hashes match, the certificate is confirmed as authentic. The application also supports transparency and auditing with analytics, anomaly detection, and verification logs. Students access their records securely through the system, and employers or educational bodies can verify credentials using either the certificate ID or the provided QR code.

Algorithm 1: Creating the Degree Certificate

```
1: Input: PassingYear, NameOfDegree, StudentName, Division, RollNo, Stream, CertificateNo
2: if adminList[msg.sender] == true then
3:     require PassingYear.length > 0
4:     require NameOfDegree.length > 0
5:     require StudentName.length > 0
6:     require Division.length > 0
7:     require RollNo.length > 0
```

```
8:    require Stream.length > 0
9:    require CertificateNo.length > 0
10:   if all requirements satisfied then
11:       certificateMapped[CertificateNo] = studentData[Input]
12:       emit CertificateCreated(CertificateNo, StudentName, NameOfDegree)
13:   else
14:       revert “Not allowed to create certificate”
15:   end if
16: end if
```

Output:The platform generates a new certificate record and logs an event capturing the certificate number, student’s name, and their awarded degree.

Algorithm 2: Verifying a Degree Certificate

```
1: Input: CertificateNo, CertificateFileHash
2: require verifierList[msg.sender] == true
3: if certificateMapped[CertificateNo] exists then
4:    storedHash = blockchainMapping[CertificateNo].hash
5:    if storedHash == CertificateFileHash then
6:       emit CertificateVerified(CertificateNo, true)
7:       return "Certificate is authentic"
8:    else
9:       emit CertificateVerified(CertificateNo, false)
10:      return "Certificate verification failed"
11:   end if
12: else
13:   revert "Certificate does not exist"
14: end if
```

Output**:**The outcome shows whether the certificate is valid and logs a verification event for audit and tracking.

Once a credential is registered on the blockchain, students must verify their identity using biometric methods powered by artificial intelligence, such as facial recognition, before they can access their records. This ensures that only the rightful owner can view or use the certificate. Employers or educational organizations looking to confirm a credential can use the decentralised application to scan a QR code or input a unique certificate ID. The smart contract within the platform retrieves the stored hash from the blockchain and checks it against the hash created by the version stored on IPFS. If the two hashes match, the certificate is proven to be genuine, allowing for verification without the need for intermediaries and protecting against tampering. In addition, the platform keeps a comprehensive log of verification attempts and analytics involving students, employers, and educational institutions, which increases accountability, auditability, and confidence in the system.

This decentralised system provides a trustworthy and streamlined way for students, educational institutions, and employers to manage and validate credentials. By automating the verification process, the platform removes the need for manual review, lightens administrative tasks, and ensures continuous, secure access to academic records. The solution supports immediate updates to credentials, enables revocation when necessary, and logs every change immutably on the blockchain for absolute traceability. Data shared across the network is protected with robust encryption, and artificial intelligence is used to monitor for any suspicious activity or unauthorized access. The architecture is highly adaptable and can work in conjunction with AI-enabled hiring platforms, digital identification wallets, third-party decentralised services, and scalable blockchain layers to accommodate future requirements.

V. RESULT AND DISCUSSIONS

The workflow diagrams provide a clear illustration of how the proposed decentralized academic credential verification system operates in practice, highlighting the separation between credential issuance and verification processes. System execution results show that student and university interactions are tightly secured via authentication and automated validation. When a student requests a credential, the issuing authority submits all relevant degree information through the DApp.

The generated certificate, which includes a QR code, undergoes AI-based HPCAE anomaly detection to confirm the authenticity of both student details and the certificate itself. Only certificates that successfully pass this validation are uploaded to the blockchain, effectively filtering out invalid, duplicate, or inconsistent credentials at the point of issuance.

The final degree certificate provided to the student contains both the blockchain transaction hash and a QR code, verifying its successful registration. Any authentication or anomaly detection failure leads to denial of access or certificate re-issuance, thereby ensuring robust issuance control. Figures 4 and 5 illustrate the student-university and verifier workflows, respectively

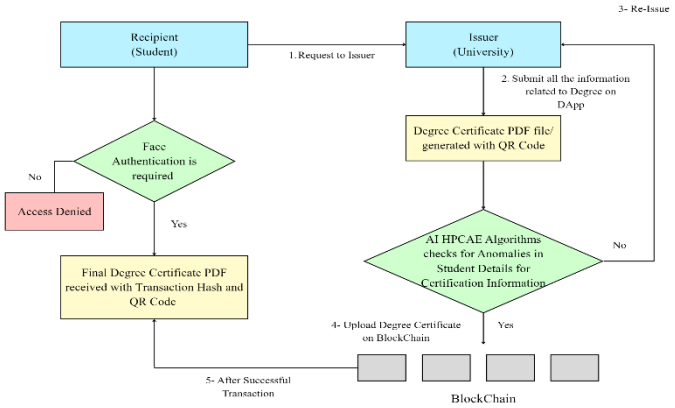


Figure.4: WorkFlow Diagram student and university

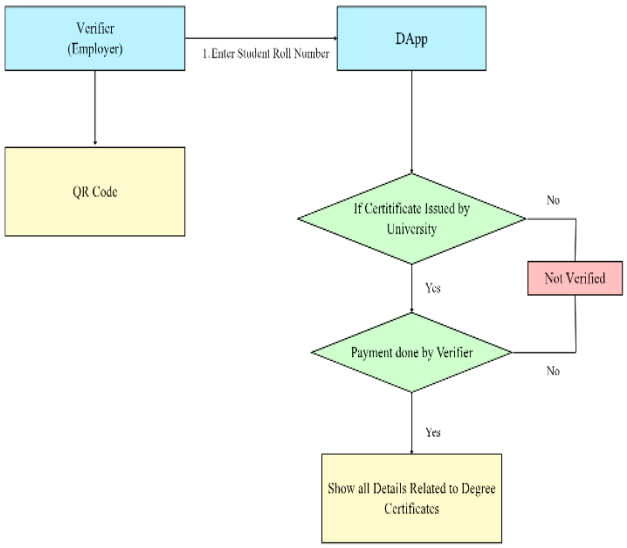


Figure. 5: WorkFlow Diagram Verifier

Verification workflow results demonstrate the system's efficiency and reliability. The DApp initially checks whether the certificate was issued by a recognized institution. When an employer or verifier enters the student roll number or scans the QR code, unregistered or forged certificates are instantly flagged as unverified. The system retrieves all degree-related data directly from the blockchain after the verifier completes the required transaction and issuer validation. This approach significantly reduces verification time and eliminates the need for direct contact with educational institutions. The findings highlight that verification decisions are made instantly, transparently, and without human intervention. Overall, these integrated workflows confirm that the proposed system boosts efficiency, security, and authenticity, while providing real-time verification and tamper resistance, two major advantages over traditional centralized systems

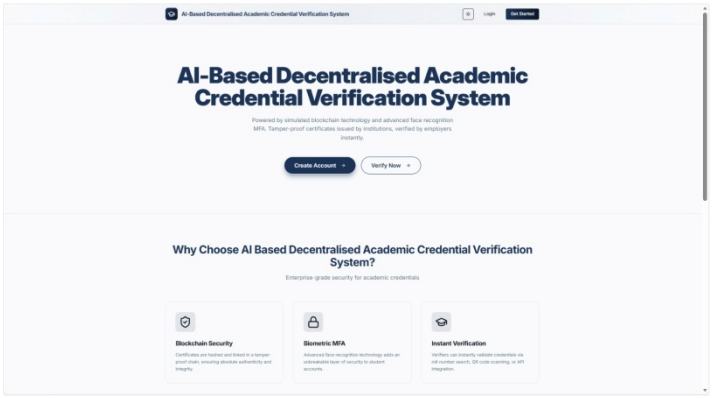


Fig. 6: Main Page

The main page serves as the entrance to the decentralized credential verification platform, outlining its objectives and emphasizing key features such as decentralized storage, blockchain-based security, AI-assisted authentication, and instant verification. Administrators, students, and verifiers can access the appropriate login modules from this page, which clearly communicates the platform's goals and benefits while ensuring ease of use and accessibility

Figure 7 shows the admin login process, where only authorized university administrators can access the system. Authentication relies on secure credentials and wallet-based verification, ensuring that only trusted institutions manage or issue credentials within the decentralized environment. This controlled access fosters institutional accountability and prevents unauthorized creation of fake credentials.

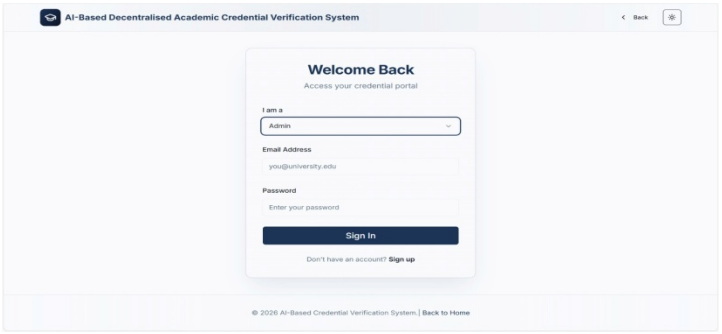


Fig. 7: Admin Login

The system can only be accessed by authorised university administrators using the admin login. Only reputable organisations are able to handle or provide academic credentials thanks to the use of wallet-based verification and secure login credentials. By using a controlled access strategy in a decentralised setting, fake credentials cannot be created by unauthorised parties and institutional accountability is encouraged.

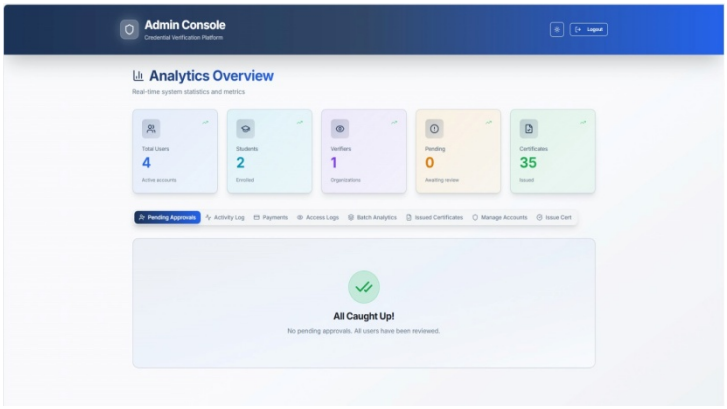


Fig. 8: Admin Console

The admin console, depicted in Figure 8, acts as the central hub for managing and issuing academic credentials. Administrators can generate degree certificates with QR codes, enter student details, and initiate blockchain transactions through this interface. The console also displays analytics on issued certificates, transaction status, and system activity. Before anchoring records on the blockchain, the system applies AI-based anomaly detection and validation to maintain certificate integrity.

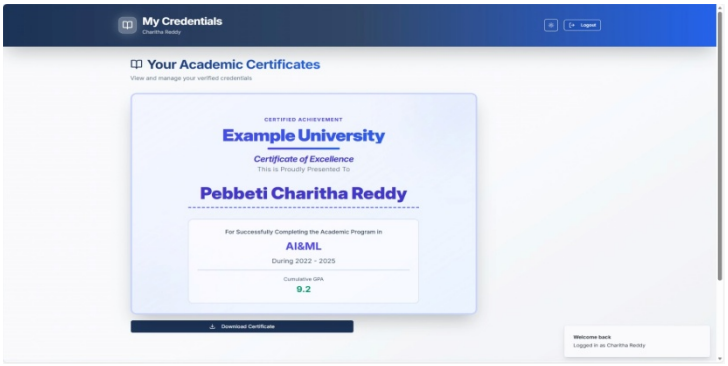


Fig. 9: Student Dashboard

The student dashboard, accessible after successful login with AI-based facial verification, allows students to securely view their academic credentials, including transaction hashes and QR codes, as shown in Figure 9. Students do not need to retain physical copies since certificates are stored on IPFS and validated via blockchain, ensuring perpetual access, privacy, and ownership.

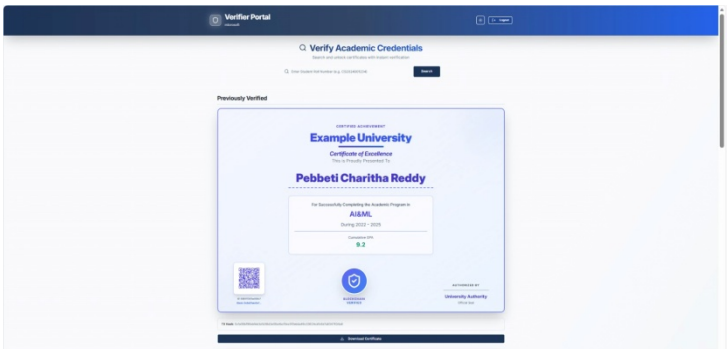


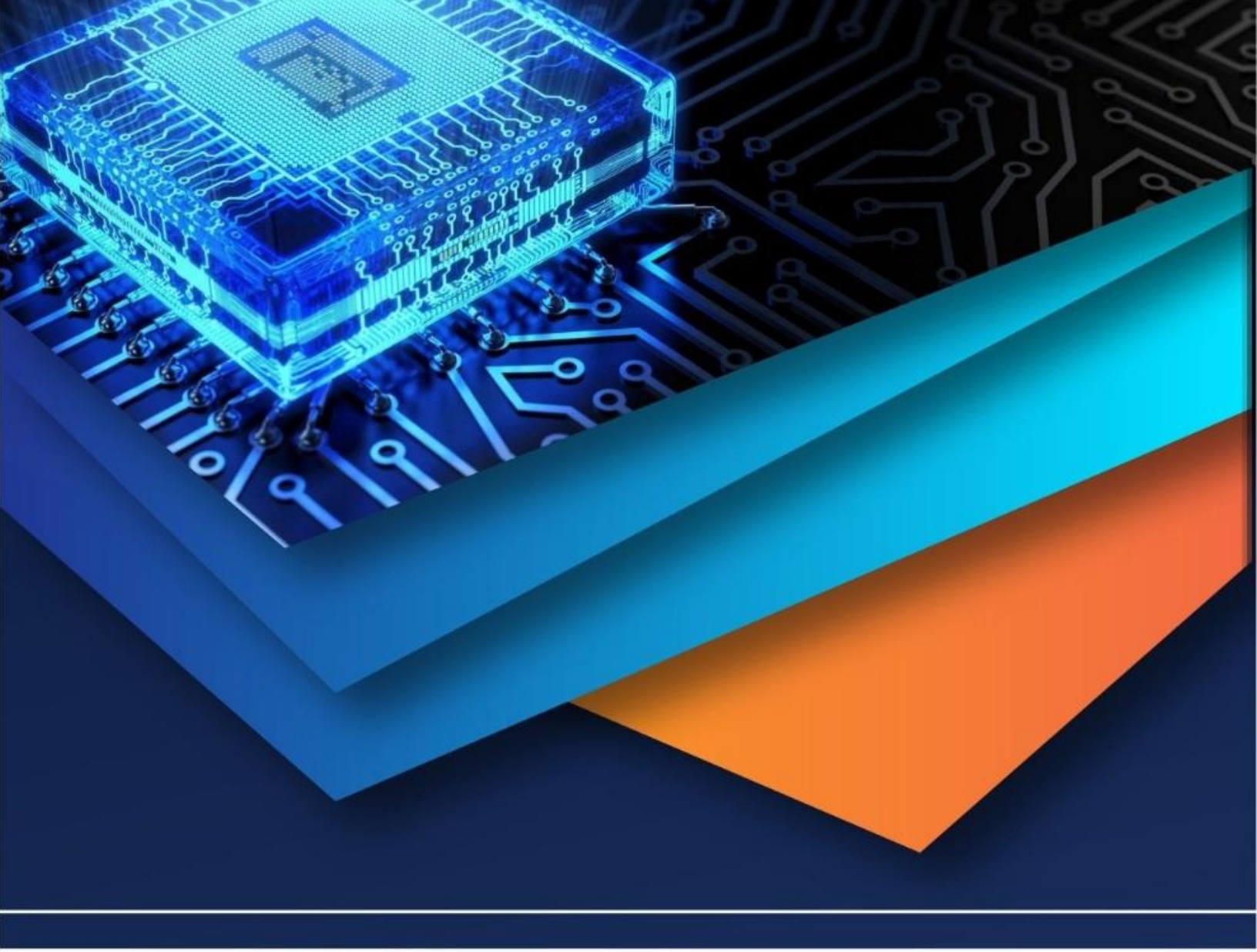
Fig. 10: Verifier Dashboard

The verifier dashboard is designed for employers and institutions to authenticate academic credentials. Verifiers can quickly check whether a certificate was issued by an authorized university and registered on the blockchain by scanning the QR code or entering the student roll number. Full credential details are displayed if the certificate is valid; otherwise, it is marked as unverified. This transparent and secure interface eliminates the need for manual verification, facilitating rapid and trustworthy validation processes.

REFERENCES

[1] A. Gangwar, R. Kumar, and S. Verma, "Blockchain-Based Credential Verification System,"Int. J. Computer Applications (IJCA), vol. 186, no. 26, 2024.
[2] M. R. Umale, P. Tiwari, M. Singh, Y. Singh, and S. Sunil, "Decentralized Document Verification Using Blockchain," Journal of Emerging Technologies and Innovative Research (JETIR), vol. 12, no. 2, 2025.
[3] D. C. Onwubiko, N. H. Odikwa, I. K. Ukabuiro, and S. A. Agomah, "Secure Academic Certificate Verification Using Blockchain Technology," IRE Journals, 2023.
[4] S. Mehta, A. Mishra, B. Oza, S. Kumar, and H. Kasturiwale, "Blockchain-Based Decentralized Document Verification and Its Applications," 2024.
[5] A. Sapkota and P. Herbke, "A Survey on Blockchain-Based Identity and Credential Verification Systems," arXiv preprint, 2024.
[6] A. Farabi, I. Khandaker, Nusrat Jahan, J. Ahsan, and I. K. Shanto, "ShikkhaChain: A Blockchain-Powered Academic Credential Verification System for Bangladesh," 2025.
[7] J. Okocha, I. Adigwe, and A. Adebiyi, "A Critical Review of Blockchain in Certificate Verification Systems: Dissecting the Pros, Cons, and Merger with AI,"NIPES J. Sci. Technol. Res., vol. 7, no. 1, Oct. 2025, doi: 10.37933/nipes/7.4.2025.SI42.
[8] J. A. Berrios Moya, J. Ayoade, and M. A. Uddin, "A Zero-Knowledge Proof-Enabled Blockchain-Based Academic Record Verification System,"Sensors, vol. 25, no. 11, art. 3450, May 2025, doi: 10.3390/s25113450.
[9] S. K. Shawon, H. Ahammad, S. Z. Shetu, M. Rahman, and S. A. Hossain, "Diucerts dapp: A blockchain-based solution for verification of educational certificates," in 2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT), pp. 1–10, IEEE, 2021.

[10] A. Alammary, S. Alhazmi, M. Almasri, and S. Gillani, "Blockchain-based applications in education: A systematic review," Applied Sciences, vol. 9, no. 12, p. 2400, 2019.
[11] M. S. Zulfiker, N. Kabir, A. A. Biswas, P. Chakraborty, andM. M. Rahman, "Predicting students' performance of the private universities of Bangladesh using machine learning approaches," International Journal of Advanced Computer Science and Applications, vol. 11, no. 3, pp. 672–679, 2020.
[12] K. D. Kumar, P. Senthil, and D. Kumar, "Educational certificate verification system using blockchain," International Journal of Scientific & Technology Research, vol. 9, no. 3, pp. 82–85, 2020.
[13] E. Nyaletey, R. M. Parizi, Q. Zhang, and K.-K. R. Choo, "Blockipfs-blockchain-enabled interplanetary file system for forensic and trusted data traceability," in 2019 IEEE International Conference on Blockchain (Blockchain), pp. 18–25, IEEE, 2019.
[14] E. P. Fedorova and E. I. Skobleva, "Application of blockchain technology in higher education," European Journal of Contemporary Education, vol. 9, no. 3, pp. 552–571, 2020.
[15] S. Yao, J. Chen, K. He, R. Du, T. Zhu, and X. Chen, "Pbcert: Privacy-preserving blockchain-based certificate status validation toward mass storage management," IEEE Access, vol. 7, pp. 6117–6128, 2018.
[16] Wang, J. Lin, Q. Cai, Q. Wang, D. Zha, and J. Jing, "Blockchain-based certificate transparency and revocation transparency," IEEE Transactions on Dependable and Secure Computing, vol. 19, no. 1, pp. 681–697, 2020.
[17] P. P. Bokariya and D. Motwani, "Decentralization of credential verification system using blockchain," International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol. 10, no. 11, 2021.
[18] O. S. Saleh, O. Ghazali, and N. B. Idris, "A new decentralized certification verification privacy control protocol," in 2021 3rd International Cyber Resilience Conference (CRC), pp. 1– 6, IEEE, 2021.
[19] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey,"International journal of web and grid services, vol. 14, no. 4, pp. 352–375, 2018.
[20] O. S. Saleh, O. Ghazali, and N. B. Idris, "A new decentralized certification verification privacy control protocol," in 2021 3rd International Cyber Resilience Conference (CRC), pp. 1– 6, IEEE, 2021.
[21] P. Vallejo Seade, "Asset tokenization in real estate through the means of token standards available on the ethereum blockchain," 2022.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY