International Journal Of Engineering Research And Development
e- ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 21, Issue 4 (April 2025), PP 110-119

Student Certificate Verification System

Asst. Prof. Aarti Abhyankar[1],
Ammar Ansari[2], Zaid Khan[3], Shreyansh Mishra[4], Maksud Shaikh[5]
[123]*Bachelor of Engineering in Information Technology*
[4]*Assistant Professor, Department of Information Technology*
K. C. College of Engineering and Management Studies and Research, Thane, Maharashtra, INDIA

ABSTRACT: *The absence of a centralized system for storing and verifying student certificates in educational institutions poses significant challenges, including document falsification and inefficiencies in validation. This paper presents the development of a Student Certificate Verification web application designed to ensure authenticity and streamline certificate management.*
The system comprises two panels: one for students and another for faculty. Students can upload their certificates, which are then accessible to faculty members for verification. The verification process is facilitated through QR code scanning, enabling automatic extraction of embedded links to redirect faculty to the course provider for validation.
For certificates lacking QR codes, the system integrates advanced image analysis techniques to detect tampering. Histogram analysis is employed to assess pixel distribution and identify modifications, particularly in textual regions such as student names. Additionally, edge detection is utilized to highlight structural inconsistencies within the certificate, improving the identification of alterations.
By incorporating QR code verification, histogram analysis, and edge detection, this project provides a comprehensive and automated solution to certificate tampering. The proposed system enhances academic record integrity by offering a secure, efficient, and centralized platform for certificate submission and validation in educational institutions.
Keywords: Certificate verification, QR code authentication, image analysis, edge detection, histogram analysis, academic integrity, document tampering detection.

Date of Submission: 05-04-2025 Date of acceptance: 15-04-2025

I. INTRODUCTION

In the digital era, educational institutions handle vast amounts of student data, including academic certificates that validate achievements. However, many institutions still lack a centralized system for storing and verifying certificates, leading to significant challenges. A major issue is certificate tampering, where students manipulate their documents—such as altering names or grades—before submission. This not only compromises the integrity of academic records but also places an additional burden on faculty members who rely on manual verification processes.

To address these challenges, this paper proposes a Student Certificate Verification System, a secure and automated solution for verifying student certificates. The system consists of two primary user interfaces: a student panel and a faculty panel. Students can upload their certificates, which are then accessible on both dashboards. Faculty members can initiate verification through a "Verify" button, which triggers a backend process to extract embedded QR code links, redirecting them to the original course provider for authentication.

For certificates lacking QR codes, the system incorporates advanced image analysis techniques to detect tampering. Histogram analysis examines pixel data to identify irregularities, particularly in textual regions such as student names. Edge detection further enhances the verification process by identifying structural inconsistencies that indicate possible alterations. By comparing pixel distributions and edge variations across different sections, the system effectively detects document modifications.

This project provides a comprehensive and automated solution to the problem of certificate falsification and the absence of a centralized verification system in educational institutions. By integrating QR code extraction, histogram analysis, and edge detection, the proposed system ensures the authenticity, reliability, and security of academic records while offering an efficient and accessible verification process for both students and faculty.

Additionally, the system reduces human intervention, minimizing errors and making the verification process faster. It enhances institutional credibility by maintaining tamper-proof academic records. With increasing cases of academic fraud, such a system is essential for strengthening trust in digital certifications and ensuring transparency in student evaluations.

II. LITERATURE SURVEY

Several approaches have been proposed to ensure the authenticity and security of academic certificates. This section reviews existing methods, highlighting their advantages and limitations.

2.1 Decentralized Certificate Validation using Hyperledger Fabric

A privacy-preserving system utilizing Hyperledger Fabric stores certificates on a distributed ledger, ensuring authenticity and immutability through blockchain technology. This approach increases trust among stakeholders by reducing the risk of unauthorized access and data breaches. The distributed nature of the system minimizes single points of failure and secures certificate data. However, high setup costs, technical complexity, and specialized infrastructure requirements make it difficult for smaller institutions with limited budgets to implement.

2.2 Certificate Authentication via Machine Learning

This study employs machine learning algorithms to analyze documents and authenticate them, detecting forgeries without the need for QR codes. By training on large datasets, the system can identify tampered areas within certificates, such as altered grades or student names. The flexibility of this approach allows it to handle various document formats. However, the effectiveness of machine learning models is highly dependent on the availability of large, high-quality datasets. Regular updates are also required to keep up with evolving forgery techniques.

2.3 Blockchain-Based Certificate Verification System

A blockchain-based verification system uses Ethereum to generate digitally hashed certificates, ensuring their authenticity and preventing unauthorized modifications. Blockchain's decentralized nature eliminates the need for centralized storage and provides a transparent and secure verification process. However, the high cost of blockchain infrastructure and the requirement for a separate QR code scanning application introduces complexity for end users, making this solution less practical for widespread adoption.

2.4 Cloud-Based Certificate Repository

A cloud-based certificate repository designed using AWS, Python, React, and DynamoDB allows for global access to certificates. This approach offers seamless storage, retrieval, and verification of academic records, with the added benefits of scalability and high availability. However, reliance on third-party cloud services introduces recurring operational costs, and data privacy concerns must be managed to comply with regulations such as GDPR and FERPA.

2.5 Summary

While blockchain and machine learning-based approaches offer strong security measures, the high infrastructure costs and complexity of implementation hinder their adoption in smaller institutions. Cloud-based solutions provide scalability and ease of access, but data privacy concerns and operational costs need careful management. Thus, a cost-effective, secure, and user-friendly solution is needed to address the growing need for certificate verification in educational institutions.

III. PROPOSED METHODOLOGY

The development of the Student Certificate Verification System follows a structured approach to automate certificate verification while ensuring accuracy and security. This methodology aims to address the challenges faced by educational institutions in maintaining certificate authenticity and preventing tampering.

1. Project Initiation:

In the initial phase, the **problem statement** is clearly defined. Many institutions lack a centralized system for storing and verifying certificates, leading to potential tampering, such as name or grade manipulation. The primary objective is to create a system where students can upload certificates, and faculty can easily verify them through QR code validation or tampering detection.

2. Requirements Gathering:

This phase focuses on gathering input from both students and faculty to define the core features of the system. Discussions with potential users help identify requirements related to ease of use, security, and accuracy. Key functionalities include:

- Certificate upload

- Dashboard views for both students and faculty
- Automated certificate verification methods (QR code scanning and tampering detection)

3. Design and Prototyping:
The design phase involves creating user-friendly interfaces for both students and faculty. Prototypes are developed to visualize the dashboard and certificate verification process. Feedback from users is incorporated into iterative design improvements. The student panel allows users to upload certificates, while the faculty panel provides access for reviewing and verifying uploaded certificates.

4. Development:
The development phase utilizes the MERN stack (MongoDB, Express, React, Node.js) for building the web application. The following functionalities are implemented:

- **User Input and Authentication:** Authentication is performed through a SignUp/SignIn process, distinguishing between students and faculty roles.
- **Certificate Upload**: Students upload their certificates, which are displayed on both their dashboard and the faculty dashboard.
- **Certificate Verification:**
    - QR Code Scanning: The system extracts the embedded QR code and redirects faculty to the course provider for validation.
    - Tampering Detection: For certificates without QR codes, the system utilizes histogram analysis to detect alterations in text (e.g., name changes), by analyzing pixel data.

5. Image Processing and Analysis:

- **QR Code Detection:** For certificates with QR codes, a QR code reader extracts the embedded link for validation.
- **Histogram Analysis:** For certificates lacking QR codes, the system analyzes pixel distributions to detect tampering, especially in text sections like student names.
- **Edge Detection:** Additionally, edge detection techniques are applied to identify structural inconsistencies within the certificate. This method highlights areas with sudden changes in intensity, which are common indicators of tampering, such as modifications in text or graphical elements (e.g., logos or signatures).

6. Output Presentation:
After verification, the system updates the certificate status on both the student's and faculty's dashboards. Faculty members are notified with a clear indication of whether the certificate is valid or tampered.

7. System Flow Chart
The flowchart illustrates the process a user follows when interacting with the certificate verification system. It begins at the home page, where users are prompted to select their role as either a student or faculty member. After selecting their role, students can either sign up or sign in, which directs them to their respective dashboard, while faculty members follow a similar process to access their own dashboard.

Once logged in, both students and faculty have the option to upload a certificate. This can be done through either a QR code scanner or by uploading the certificate file directly.

After the certificate is uploaded, it is displayed for verification. Faculty members can then view the uploaded certificate. The system first checks for the presence of a QR code. If a QR code is found, the system automatically extracts the embedded link and redirects the user for further processing. If no QR code is detected, the system alerts the user and provides information on whether the certificate is authentic or tampered.

This flowchart ensures a clear and straightforward process for both students and faculty to manage and verify certificates efficiently, enhancing the security and integrity of the verification process..

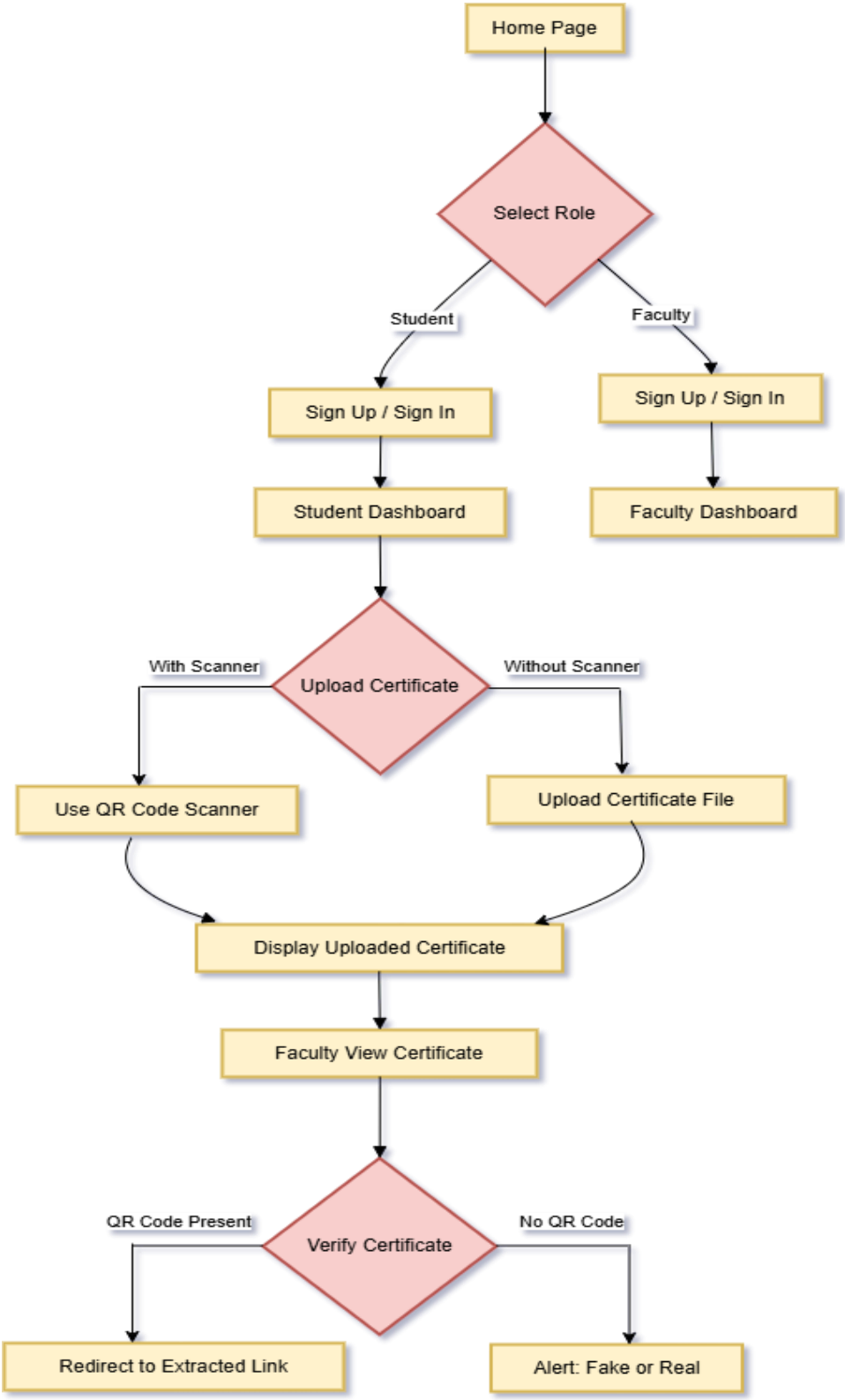

Figure 1: System Flow Chart

IV. IMPLEMENTION

The implementation of the Student Certificate Verification System involves the integration of various technologies and features to automate the certificate verification process. The system is developed using the MERN stack (MongoDB, Express.js, React, Node.js) to ensure a scalable and efficient web application. Advanced image processing techniques such as histogram analysis and edge detection are incorporated to detect certificate tampering. Additionally, QR code extraction enables quick and reliable verification by redirecting faculty to the official course provider for authentication.

Below are the system imgaes:

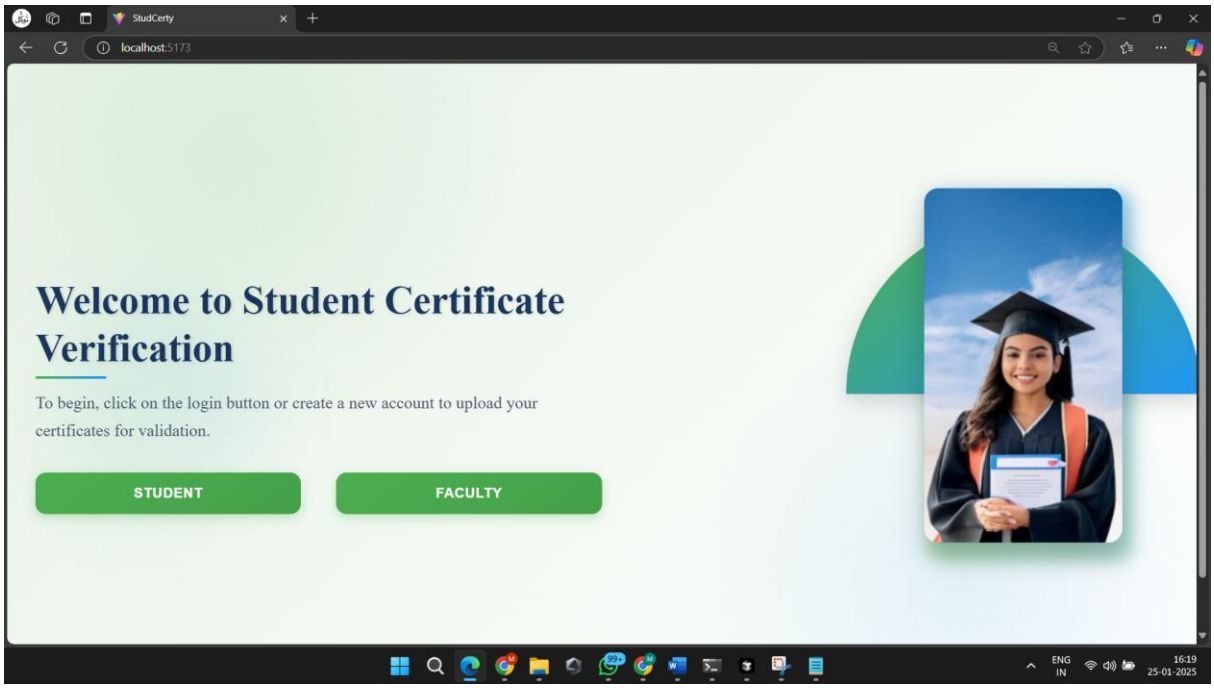

Figure 2: Home Page

1. Student Panel

The **Student Panel** serves as the primary interface for students to upload and manage their certificates. It ensures that students can easily navigate the verification process by providing clear options and functionalities. The panel categorizes certificates into two sections for efficient handling:

- **Upload Certificate with QR Code**: This section allows students to quickly upload certificates that contain an embedded QR code. The system extracts the QR code and verifies it by redirecting faculty members to the course provider for validation.
- **Upload Certificate without QR Code**: In cases where the certificate lacks a QR code, students can upload the document for analysis. The system then utilizes image processing techniques, including **histogram analysis** and **edge detection**, to detect tampering or alterations in the certificate, particularly in text sections like student names or grades.

The **Student Dashboard** (Fig No. 3) provides a clear, user-friendly interface where students can upload, view, and track the status of their certificates. The dashboard allows for easy access to the verification process and keeps students informed about whether their certificates are valid or flagged for potential tampering. Additionally, students can manage and review their submission history, ensuring a comprehensive and transparent verification process.

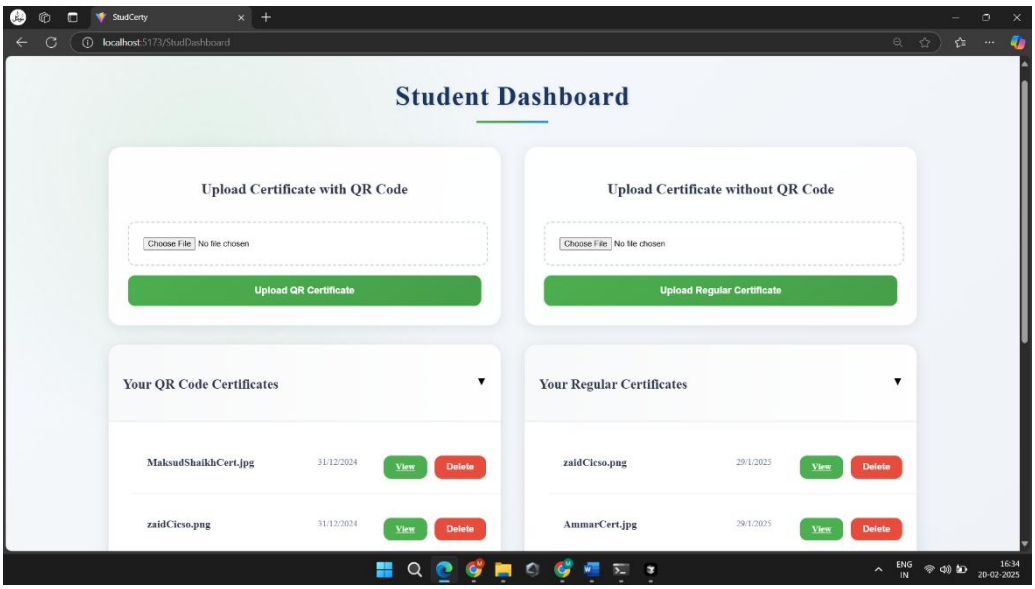

Figure 3: Student Dashboard

2. Faculty Panel

The Faculty Panel allows faculty members to efficiently verify student certificates using automated QR code scanning or tampering detection techniques. Upon logging in, faculty can access a dashboard that categorizes certificates into two sections:

- **Certificates with QR Code** – Enables quick verification by extracting embedded QR codes and redirecting to the course provider's database.
- **Regular Certificates** – Uses image processing techniques such as histogram analysis and edge detection to detect tampering.

The Faculty Dashboard (Figure No. 4) provides an intuitive interface for managing certificate verification, reducing manual workload, and ensuring academic integrity.

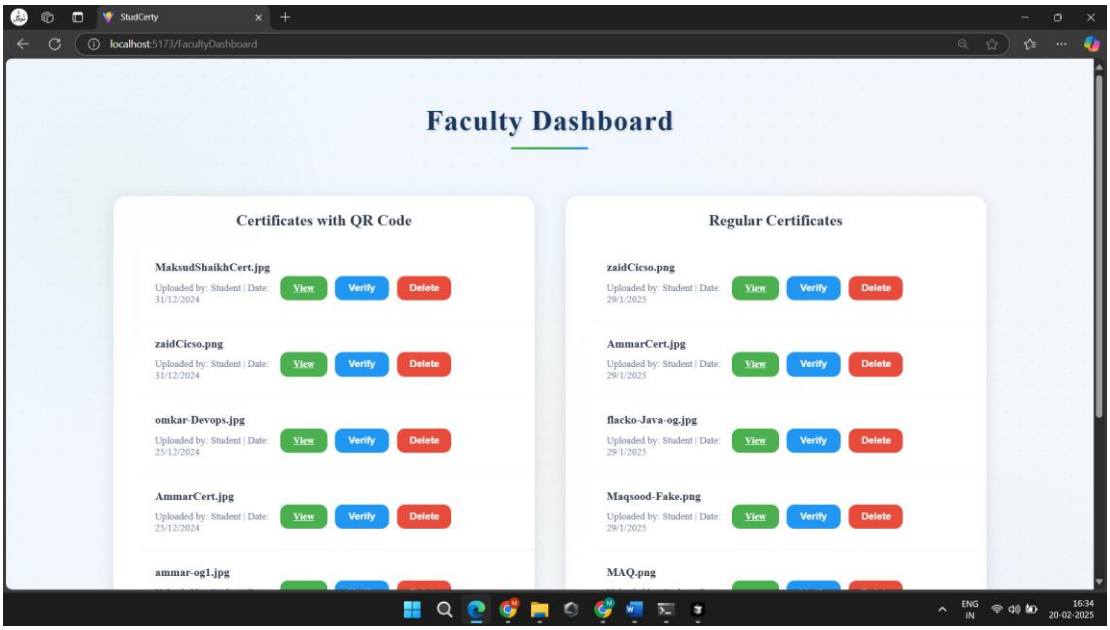

Figure 4: Faculty Dashboard

Faculty Verification: Faculty members can verify certificates with a single click using QR code scanning.

Figure No 5: Certificate Verification – Displays the faculty dashboard where the "Verify" button is clicked for certificate validation.

Tampering Detection: Tampering detection using histogram analysis operates seamlessly in the background, providing results instantly. Edge-based processing techniques are employed to enhance the analysis by quickly identifying tampered regions in real-time during certificate upload and verification.

Certificate Authentication: When a certificate is verified as authentic, faculty can confirm its status.

Fig No 6: Verification Redirect – Shows the redirect process to the course provider's website for certificate verification after the "Verify" button is clicked.

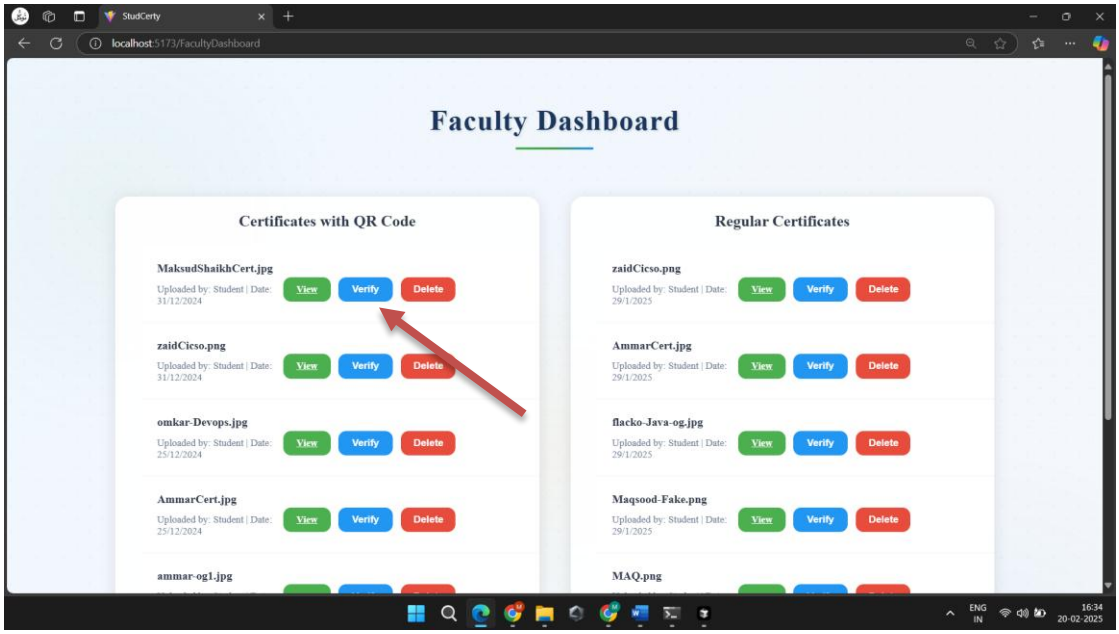

Figure 5. Certificate Verification

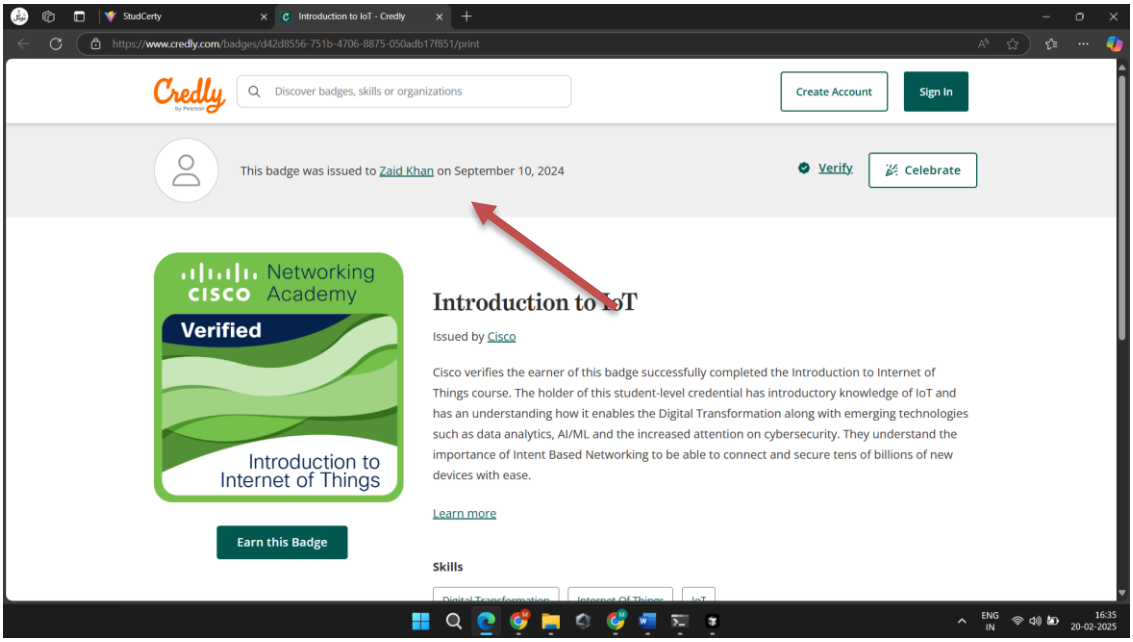

Figure 6: Verification Redirect

Fig No 7: Authenticating Non-QR Certificate – Displays the faculty dashboard where a certificate without a QR code is verified, showing an alert that the certificate is authentic after clicking the "Verify" button.

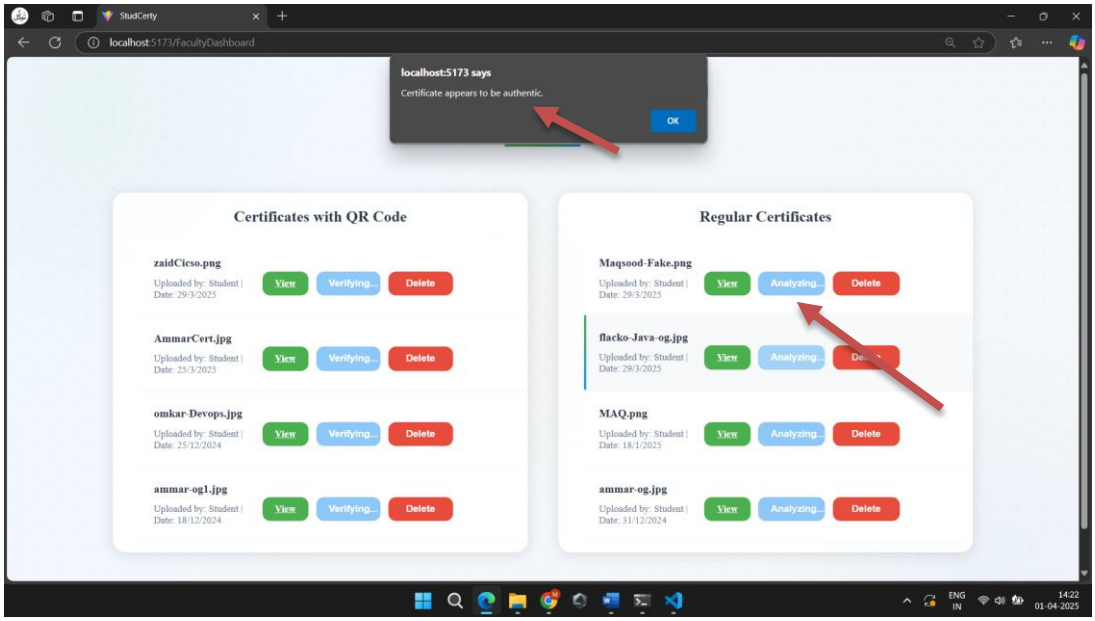

Figure 7: Authenticating Non-QR Certificate

V. RESULT ANALYSIS

Test Case Name	Input	Expected Output	Pass/Fail
Student Login/Signup	Enter valid student credentials or fill the signup form	Successfully logged in or signed up, redirected to the student dashboard	Pass
Faculty Login/Signup	Enter valid faculty credentials or fill the signup form	Successfully logged in or signed up, redirected to the faculty dashboard	Pass
Upload Certificate with QR Code	Click on the Upload button and select a valid certificate with a QR code	Successfully uploaded and listed	Pass
Verify Certificate with QR Code	Click on the Verify button for the uploaded certificate	Redirects to the course provider's page using the scanned QR code	Pass
Upload Certificate without QR Code	Click on the Upload button and select a valid certificate without a QR code	Successfully uploaded and listed	Pass
Verify Certificate without QR Code	Click on the Verify button for the uploaded certificate	Certificate is verified using combined histogram analysis and edge detection; verification status is displayed	Pass
Upload Invalid Certificate with QR Code	Click on the Upload button and select an invalid or corrupted certificate with a QR code	Error message displayed: "Invalid or corrupted QR code"	Pass
Histogram and Edge Analysis for Unaltered Certificate	Upload an unaltered certificate image without a QR code	Both techniques confirm no manipulations; successfully verified	Pass
Histogram and Edge Analysis for Altered Certificate	Upload a certificate with painted or altered text area or edges	Combined techniques detect manipulations; fake certificate detected and flagged	Pass
Display Uploaded Certificates on Student Dashboard	Login as a student and upload certificates	Uploaded certificates are visible in the student dashboard	Pass

Display Uploaded Certificates on Faculty Dashboard	Login as a faculty member and view certificates uploaded by students	Certificates uploaded by students are visible for verification	Pass
File Format Validation	Upload files in unsupported formats (e.g., .exe, .mp3)	Error message displayed: "Invalid file format. Please upload a PDF or image file."	Fail
File Size Validation	Upload a file exceeding the maximum size limit	Error message displayed: "File size exceeds the maximum allowed limit."	Pass
Verify QR Code Scan Redirection	Upload a valid certificate with a QR code, click the Verify button	Redirects to the course provider URL after successful QR code scan	Pass

VI. Future Enhancement

- **Blockchain Integration –** Implementing blockchain technology will provide a decentralized and tamper-proof ledger for secure certificate storage and verification. This will eliminate the risk of data manipulation and enhance trust in the system.

- **Mobile Application –** Developing Android and iOS apps will enable on-the-go certificate verification for students and faculty, ensuring seamless access to the platform anytime and anywhere. The mobile app will also include features like instant QR scanning and real-time status updates.

- **Support for More Documents –** Expanding the system to verify additional academic records, such as diplomas, transcripts, and degrees, will enhance its usability and make it a comprehensive solution for educational institutions. This will allow organizations to streamline multiple verification processes within a single platform.

- **AI-Based Tampering Detection –** Integrating machine learning models will significantly improve forgery detection accuracy and efficiency by identifying even subtle manipulations. AI-driven analysis will continuously learn from new data, making the system more adaptive to evolving document fraud techniques.

- **Multi-Language Support –** Adding multiple language options will make the system accessible to a global audience, improving adoption across different regions and institutions. This will ensure that users from diverse linguistic backgrounds can navigate and utilize the platform effectively.

- **Cloud-Based Storage** – Implementing a cloud-based storage solution will enhance data accessibility, scalability, and security. This will ensure that certificates are stored securely and can be retrieved from anywhere, reducing dependency on local storage and minimizing the risk of data loss

VII. DISCUSSION AND CONCLUSION

This project effectively addresses the prevalent issue of certificate tampering and the absence of a centralized verification system in educational institutions. By implementing an automated and user-friendly platform, it streamlines certificate submission and verification for both students and faculty. The integration of QR code scanning for instant validation, along with histogram analysis and edge detection for tampering detection, significantly enhances the reliability and authenticity of academic certificates.

Furthermore, the system ensures data security and privacy through robust encryption techniques, safeguarding sensitive student information. Future enhancements, including blockchain integration for immutable record-keeping, AI-driven tampering detection, and multi-language support, will further strengthen the platform's capabilities and expand its usability across diverse educational institutions.

Overall, the Student Certificate Verification System presents a scalable and efficient solution that not only enhances the integrity and trustworthiness of academic records but also streamlines the verification process. Its adoption can significantly benefit educational institutions by reducing administrative burdens, minimizing fraudulent activities, and ensuring a secure and transparent certificate validation system on a global scale.

REFERENCES

[1] Lisa Patel et al., 2021. Decentralized Certificate Validation using Hyperledger Fabric. A privacy-preserving system utilizing Hyperledger Fabric, storing certificates on a distributed ledger. Complexity and high setup costs may hinder adoption by smaller institutions.

[2] David Chen et al., 2021. Certificate Authentication via Machine Learning. This study analyzes document features with machine learning for authentication, detecting forgeries without QR codes. It requires large datasets and continuous updates for effectiveness.

[3] Amit Sharma et al., 2020. Blockchain-Based Certificate Verification System. Utilizes Ethereum for digitally hashed certificates, ensuring authenticity and immutability. Challenges include the need for a separate QR code scanning app and high implementation costs.
[4] R. Kumar et al., 2019. Cloud-Based Certificate Repository. Employs AWS, Python, React, and DynamoDB for a scalable cloud repository, offering global access but incurring additional costs for reliance on third-party services.
[5] Jin-chiou et al., 2018. Smart Certificate Authentication System. Developed with HTML, CSS, JavaScript, PHP, and MySQL, this system enables centralized storage and validation of certificates using QR code scanning. It mitigates risks of forgery but is limited when QR codes are absent.
[6] A. Kumar et al., 2017. "Certificate Authentication using QR Codes and Blockchain." This paper discusses the integration of QR codes with blockchain technology for enhancing the security and traceability of academic certificates.
[7] R. Smith et al., 2016. "Secure Digital Certificates for Educational Institutions." This study outlines the development of a secure digital certificate system that uses cryptographic techniques to ensure the authenticity and immutability of certificates issued by educational institutions.
[8] J. Taylor et al., 2015. "Verification of Academic Credentials using Image Analysis." This paper presents a method of verifying academic certificates by analyzing the image content, identifying inconsistencies that may indicate tampering or forgery.
[9] C. Harris et al., 2014. "Using Cryptographic Hash Functions for Secure Certificate Verification." The study investigates the use of cryptographic hash functions to secure certificates, ensuring that certificates remain tamper-proof and their validity can be easily verified.
[10] L. Thomas et al., 2013. "Design of a Digital Certificate Management System." Focuses on the design of a centralized digital certificate management system for educational institutions, improving certificate issuance, verification, and storage processes.