International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 11 | Nov - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

Secure Academic Certificate Vault: A Web-Based Approach to Academic Document Authentication

K.Tamil Selvi [1]
Assistant Professor,
Department of Computer Science & Engineering,
(An Autonomous Institution),
Adhiyamaan College of Engineering,
(An Autonomous Institution), Hosur, India

Thirunavukarasan Y [1]
YokeshrajS[2]
Tamilarasan J[3]
Adhiyamaan College of Engineering
UG Scholars,
Department of Computer Science & Engineering,
Hosur, India

Abstract - This paper introduces the Secure Academic Certificate Vault, an innovative and reliable web-based application developed to overcome the increasing challenges of fake, tampered, or lost academic certificates in the education and recruitment sectors. In most institutions, certificate verification still relies on manual and time-consuming processes that are prone to human error and manipulation. With the growing sophistication of digital forgery, there is a pressing need for a secure, automated, and verifiable approach to certificate management. The proposed system provides a centralized digital vault where educational institutions can securely upload, store, and manage student certificates in a verified digital format. Once a certificate is uploaded, it is automatically assigned a unique, non-sequential Certificate ID and a dynamic QR code, which serve as permanent and tamper-proof identifiers for verification. The QR code enables quick and transparent validation of credentials by employers or verifiers without requiring direct contact with the issuing institution. The system is built on a robust technology stack that includes Spring Boot for backend operations and secure API management, React.js for a responsive and user-friendly interface, and PostgreSQL for efficient and safe data storage. To ensure data protection and proper access control, the system implements Role-Based Access Control (RBAC) for three key user roles: Institution/Admin, Student, and Employer/Verifier, ensuring that each stakeholder can perform only their designated functions. Additionally, the platform incorporates an audit logging module that tracks every transaction and verification request, providing complete traceability and accountability. The implementation of this system demonstrates a significant improvement in the accuracy, speed, and reliability of certificate verification. By eliminating manual dependencies and introducing digital transparency, the Secure Academic Certificate Vault restores trust between educational institutions and employers while promoting efficiency and integrity in academic document verification. Overall, this solution presents a scalable and secure alternative to traditional verification systems, aligning with modern digital transformation trends in the education sector.

Keywords - Academic verification, QR code authentication, certificate management, web application security, role-based access control, data integrity

I . INTRODUCTION

Background and Motivation

The authenticity of academic certificates plays a crucial role in maintaining trust within both the education system and the job market. In today's competitive environment, organizations and employers rely heavily on verified credentials to assess a candidate's qualifications. However, with the rise of easily accessible digital editing tools, it has become increasingly simple to forge or alter certificates, leading to widespread incidents of fake or tampered documents. This growing issue not only damages the credibility of educational institutions but also undermines fair recruitment practices and the value of genuine qualifications.

Educational institutions and employers are forced to spend significant time and effort verifying certificates through manual methods such as email communication, document scanning, and cross-verification of physical records. These processes are often slow, inconsistent, and prone to errors, creating unnecessary delays in recruitment and academic verification cycles. As a result, the need for a secure, transparent, and automated system that can validate academic credentials in real time has become essential. Such a solution would not only enhance the efficiency of verification but also restore confidence in the authenticity of academic records across institutions and industries.

Problem Statement

The primary problem this research addresses is the lack of a centralized, tamper-proof, and real-time verification system for academic credentials. Current verification approaches are fragmented and largely depend on manual workflows or disconnected systems that lack transparency and standardization. Moreover, existing systems often rely on static identifiers like serial numbers or registration IDs, which can easily be duplicated or falsified.

This situation gives rise to several critical issues:

- **Vulnerability:** Once issued, certificates can be forged, altered, or misused without effective means of detection.
- **Inefficiency:** Traditional verification processes consume considerable time and manpower, making them unsuitable for large-scale or time-sensitive recruitment.
- **Accountability Gap:** There is limited traceability of who verified a document, when, and under what conditions, making it difficult to maintain audit integrity.

Proposed Solution and Key Objectives

To address these challenges, this research proposes the **Secure Academic Certificate Vault (SACV)** — a centralized, web-based solution designed to securely manage, verify, and authenticate academic certificates. The system is engineered to ensure end-to-end transparency and data integrity across the certificate lifecycle.

The key objectives of the SACV are as follows:

- **Automated Management:** Enable institutions to easily upload and manage digital certificates, either individually or in batches, ensuring secure issuance and organized storage.

- **Data Integrity:** Protect the confidentiality and integrity of stored certificate data using robust cryptographic techniques and a secure database framework.

- **Secure Verification Mechanisms:** Implement a dual-layer verification process, including a unique, non-sequential Certificate ID and a dynamically generated QR code for real-time authentication.

- **Role-Based Access Control (RBAC):** Enforce strict user access policies, granting specific permissions to Institution/Admin, Student, and Employer/Verifier roles, ensuring that each stakeholder accesses only the data relevant to their role.

- **Comprehensive Audit Trail:** Maintain an immutable log of all system interactions — including uploads, verifications, and access events — to ensure transparency and accountability at every stage.

Paper Organization

The remainder of this paper is structured as follows:
Section II reviews related work and existing approaches to digital document verification. Section III describes the architecture and design principles of the proposed system, including the technologies used. Section IV details the implementation and functionality of the key system modules for each user role. Section V presents the experimental results, performance evaluation, and security validation. Finally, Section VI concludes the paper and highlights potential directions for future development and improvement.

II. LITERATURE REVIEW: RELATED WORK AND CRITIQUE

Research on secure academic credential systems has evolved around the use of unique identifiers and cryptographic methods to prevent forgery and ensure document authenticity. Among these, QR code-based verification has gained significant attention due to its simplicity and accessibility. However, a closer look at existing approaches reveals that many solutions focus narrowly on the verification mechanism while overlooking essential aspects like usability, scalability, and administrative control. The Secure Academic Certificate Vault (SACV) aims to bridge these gaps by combining technical robustness with practical, institution-level management features.

1. Singhal, A. & Pavithra, R.S. (2015) – Degree Certificate Authentication using QR Code and Smartphone

This study introduced a system that integrates QR codes into degree certificates, allowing verification through a dedicated mobile application linked to a central database. The approach successfully automated basic verification, reducing manual intervention and serving as an early step toward digital validation.
Critique: Despite its usefulness, the reliance on a proprietary mobile app limits accessibility for verifiers who may use different platforms or devices. This dependency also adds unnecessary friction to the process, making it less practical for widespread adoption. In contrast, SACV removes this dependency by enabling verification through any standard web browser or QR scanner, ensuring universal access.

2. Egwali, A. O., Egwali, F. C., & Ogene, J. (2025) – The Transcript and Certificate Verification System (TCVS) utilizing Art-Based Graphical Passwords for Secure Verification

This research presents an innovative verification platform that uses art-based graphical passwords as the primary method of authentication. The system was designed to counteract the increasing prevalence of fake academic credentials by introducing an additional layer of visual security.
Critique: While creative, the reliance on non-standard authentication methods introduces complexity for users and requires prior training or familiarity with the system. The focus on login security rather than

document authenticity limits its real-world practicality. SACV instead prioritizes direct document validation using secure QR code verification that does not require any specialized knowledge or user credentials for third-party verification.

3. Alsuhibany, S. A. (2025) – Innovative QR Code System for Tamper-Proof Generation and Fraud-Resistant Verification

This paper proposed embedding digital watermarking into QR codes, combined with neural network-based verification to strengthen tamper resistance. It advanced the technical aspect of QR security and introduced an intelligent layer of fraud detection.

Critique: While technically sound, this approach focuses heavily on the low-level security of QR generation and ignores the operational needs of educational institutions, such as role-based data access and verifiable audit logging. SACV integrates both technical and organizational security by combining QR-based verification with a structured access control model and institutional audit trails.

4. Ma, G. & Zhang, L. (2024) – Application of Two-Dimensional Code Technology in College Student Archives Management

This study explored how two-dimensional (QR) code technology could improve student file management and retrieval efficiency within college archives. It highlighted the organizational benefits of using QR codes for better storage and record access.

Critique: Although effective for internal administrative use, the system lacks features for external verification, which is essential in combating certificate fraud. SACV extends this concept by introducing a real-time, externally accessible verification portal for employers and verifiers, while maintaining the same efficiency for institutional management.

5. Wellem, T., Nataliani, Y., & Iriani, A. (2023) – Academic Document Authentication using ECDSA and QR Code

This research combined QR codes with Elliptic Curve Digital Signature Algorithm (ECDSA) to ensure document authenticity through cryptographic signing. The approach guarantees that once signed, the data cannot be altered without detection.

Critique: Despite offering strong cryptographic protection, implementing ECDSA requires a complex key management system, which can be expensive and difficult for many institutions to maintain. Moreover, the system focuses mainly on document signing rather than end-to-end management, lacking features such as audit logging and access control. SACV builds on this by offering a more practical enterprise-ready solution that integrates cryptographic security with operational features like RBAC and detailed audit trails.

Synthesis of Research Gap and SACV Contribution

The collective review of existing research highlights that while QR code-based verification is a reliable foundation, most systems fail to deliver a complete enterprise-level solution that combines usability, scalability, and operational security. The major gaps observed include:

- **Accessibility and Usability:** Many systems depend on complex or proprietary technologies—such as custom apps, graphical passwords, or costly cryptographic frameworks—reducing accessibility for end users.
- **Administrative and Security Management:** Most existing models do not include essential features like Role-Based Access Control (RBAC) or non-repudiable audit logs, which are vital for institutional accountability.
- **Real-Time Centralization:** There is a lack of real-time integration with secure databases that can

confirm the current status of a certificate, such as whether it remains valid or has been revoked.

The Secure Academic Certificate Vault (SACV) effectively addresses these gaps through a comprehensive, web-based approach that blends technology and institutional needs. By utilizing Spring Boot for backend stability and PostgreSQL for secure, transactional data storage, the system ensures high availability and integrity. SACV integrates strict RBAC enforcement for controlled user access, provides instant real-time verification directly linked to the central database, and maintains a transparent, non-repudiable audit trail for all user activities. This combination delivers a complete, scalable, and secure solution tailored for modern academic institutions and verification agencies.

III. SYSTEM ARCHITECTURE AND DESIGN

The Secure Academic Certificate Vault (SACV) is designed as a secure, scalable, and modular three-tier web application that ensures efficiency, reliability, and data integrity. The architecture follows an enterprise-grade layered model that separates the presentation, application, and data layers. This modular approach enhances maintainability, allows independent scaling of each component, and supports future system expansion without compromising performance or security.

3.1 Three-Tier Architecture Overview

The architecture, illustrated in *Figure 1*, is composed of three main layers, each with clearly defined responsibilities:

Presentation Layer (Frontend):
This layer forms the system's interactive interface, developed using React.js for its dynamic and responsive features. The user interface adapts based on the user's role—Institution/Admin, Student, or Employer/Verifier—ensuring a seamless and secure experience. The frontend communicates exclusively with the backend through secure RESTful APIs, preventing direct data access and minimizing exposure of sensitive operations to the client side. By implementing strict session management and input validation, the presentation layer ensures that all data exchanges remain secure and well-structured.

Application and Logic Layer (Backend):
At the core of the system lies the Spring Boot framework, responsible for managing business logic, authentication, and certificate lifecycle operations. This layer performs several critical tasks, including Role-Based Access Control (RBAC) enforcement, certificate ID and QR code generation, and secure database communication. The Certificate Management Service handles the complete document workflow—from upload to verification—while the Authentication and RBAC module ensures that users operate strictly within their designated permissions. By decoupling services, the system maintains both flexibility and security, supporting concurrent operations without affecting system integrity.

Data Layer:
The data layer is responsible for storing and maintaining all certificate-related information and ensuring transaction-level consistency. It is divided into two secure components:

- PostgreSQL Database: Used for structured data storage such as certificate metadata, student and institution information, and audit logs. PostgreSQL was chosen for its ACID compliance (Atomicity, Consistency, Isolation, Durability), which guarantees reliable and error-free transactions.

- Secure Object Storage: Dedicated to storing binary files such as PDF certificates. Each stored document is linked to its corresponding metadata through a unique identifier and stored path, preventing unauthorized modification or access.

This multi-layered architecture ensures high system resilience, fault isolation, and data confidentiality while providing a smooth verification experience for all stakeholders.

3.2 Role-Based Access Control (RBAC) Design

Security within SACV is governed by a Role-Based Access Control (RBAC) model implemented using Spring Security. This framework ensures that every user action aligns with their assigned privileges, maintaining a strict separation of duties and minimizing the risk of data exposure or misuse.

The RBAC model defines three primary roles, each with specific permissions and restrictions:

- Institution/Admin: Responsible for uploading new certificates, managing student records, and maintaining metadata. Administrators can view audit logs and oversee verification activities. However, once a certificate is issued, they cannot alter its core data—preserving document immutability and ensuring historical accuracy.

- Student: Students can view and download their verified certificates and generate temporary verification links or QR codes for sharing. Their access is limited to their own records; they cannot view or modify data belonging to others.

- Employer/Verifier: Employers or third-party verifiers access the system through a public verification portal. By scanning the QR code or entering the certificate's unique ID, they can instantly verify the document's authenticity and view its validity status (e.g., VALID or REVOKED). Importantly, they cannot access personal metadata, audit records, or internal storage locations, thereby maintaining the privacy and integrity of institutional data.

This layered access model ensures that sensitive operations remain protected while still allowing transparent verification to legitimate stakeholders.

3.3 Data Model and Security Mechanisms

The SACV data model prioritizes data confidentiality, integrity, and immutability. Several mechanisms are employed to safeguard stored data:

- User Security: All passwords in the USER_MASTER table are encrypted using the BCrypt hashing algorithm with random salting, effectively protecting against brute-force and rainbow table attacks.

- Certificate Metadata Management: The CERTIFICATE_MASTER table contains all essential details related to each document, including its unique identifier (CERT_ID), basic metadata, and an encrypted reference to the file's storage path in the object storage system.

- Data Immutability: Once a certificate is committed to the system, its metadata cannot be altered.

Only the status field (e.g., VALID, REVOKED) is updatable, preserving the authenticity and historical traceability of all issued certificates. This principle guarantees that no document can be retroactively modified or deleted, reinforcing trust in the verification process.

Collectively, these measures establish a secure, verifiable chain of custody for every document from issuance to verification.

3.4 Certificate Generation and Linkage Module

One of the core components of SACV is the Certificate Generation and Linkage Module, which automates the creation and secure storage of digital certificates. This process is initiated when an institution admin uploads a certificate PDF through the platform.

1. PDF Hashing: Upon upload, the system generates a SHA-256 cryptographic hash of the certificate file. This hash acts as a unique digital fingerprint, ensuring that any modification to the document can be instantly detected.
2. Unique ID Generation: A non-sequential and cryptographically secure Certificate ID (CERT_ID) is created using randomization techniques. This identifier is unique for every certificate and forms the backbone of the verification process.
3. QR Code Encoding: A dynamic QR code is generated, embedding a secure verification link that references the certificate ID (e.g., https://sacv.edu/verify?id=[CERT_ID]). This enables immediate validation by scanning the code using any standard smartphone camera or QR reader.
4. Secure Storage: The original PDF is transferred to the object storage system, while its metadata and storage path are committed to the PostgreSQL database in a single atomic transaction, ensuring data consistency and eliminating synchronization errors.
5. Audit Logging: Every operation—upload, verification, or modification of status—is automatically recorded in the AUDIT_LOG table. This log provides an immutable record of all actions for future review, ensuring full accountability and transparency.

By integrating these steps, SACV guarantees both data integrity and traceability, creating a secure, verifiable digital ecosystem for academic document management

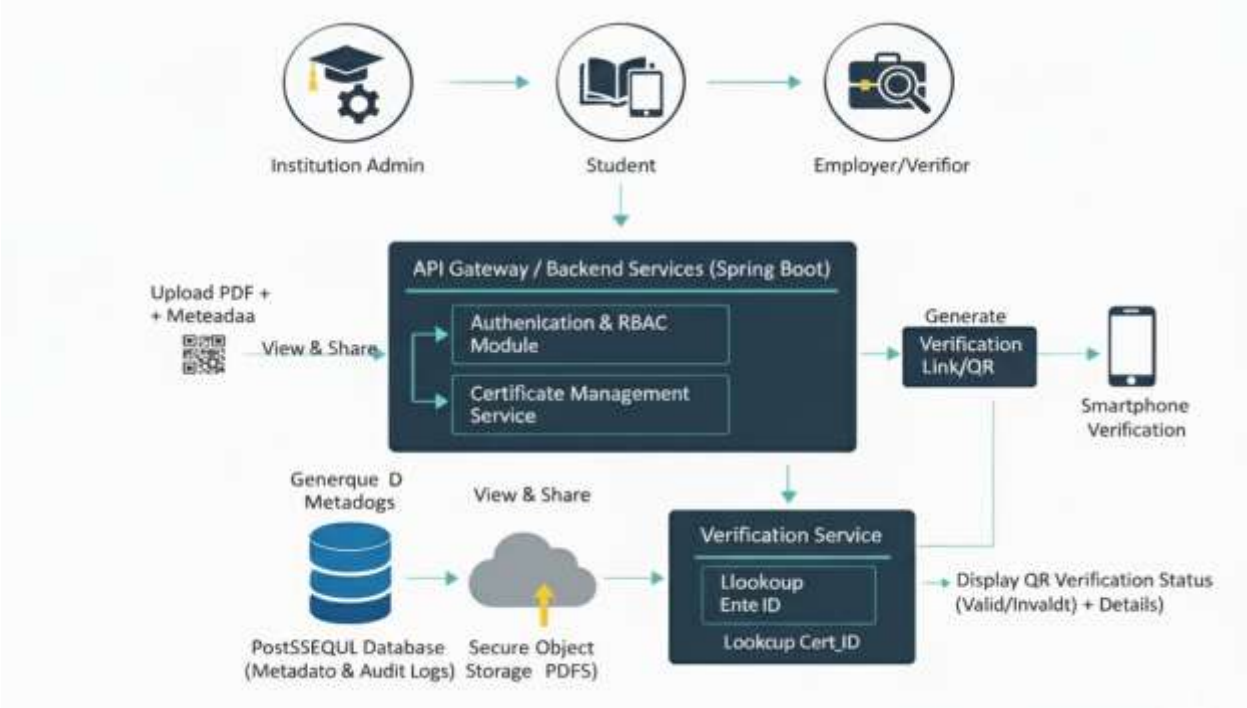

Figure 1:Dataflow and Architecture

IV. IMPLEMENTATION AND MODULES

This section details the operational workflows and the key software modules developed to service the three distinct user roles within the SACV.

4.1 Institution/Admin Dashboard and Upload Module

The Admin interface serves as the control panel, using JWT managed by Spring Security for session management.

- Batch and Single Upload: The interface supports both single file uploads and a batch upload facility where metadata can be supplied via a CSV file, automating the data entry for large-scale issuance.

- Server-Side Validation: The Spring Boot service performs rigorous validation (data types, student ID validity, file type).

- Certificate Creation Trigger: Successful validation triggers the Certificate Generation and Linkage Module.

4.2 Student Access and Sharing Module

The student dashboard is designed for secure retrieval and controlled sharing of personal credentials.

- Secure Download Feature: When a student requests a PDF download, the Spring Boot application generates a temporary, time-limited, and tokenized download link. After a short expiration period or one use, the link becomes invalid, preventing file path leakage and unauthorized sharing.

- Sharing Mechanism: The student can initiate a share request, prompting the system to generate a unique, persistent verification URL that can be shared. This URL, when clicked, acts exactly like scanning the printed QR code, directing the verifier to the public portal for instant validation.

4.3 Employer/Verifier Authentication Module

The verification process is designed to be frictionless and instantaneous, without requiring the employer to register or login (unauthenticated access).

- Verification Flow (Dual Path):

  - QR Code Verification (Primary Path): The Employer scans the QR code printed on the document. The embedded URL automatically opens the verification portal and populates the Unique Certificate ID.

  - Manual Verification (Secondary Path): The Employer manually enters the Unique Certificate ID on the public-facing verification page.

- Real-time Server Query: The Spring Boot service receives the CERT_ID via the API endpoint, queries the CERTIFICATE_MASTER table in PostgreSQL, and verifies two conditions: a) the ID exists, and b) the certificate is marked as VALID.

- Result Display: The portal instantly displays the verification result (e.g., "Certificate VALID" or "Certificate REVOKED") along with truncated essential details (e.g., Student Name, Course, Issue Date) to confirm the match, without revealing sensitive student data or full grades.

4.4 The Audit and Logging System

The SACV incorporates a mandatory, non-repudiable audit logging system that is central to the system's accountability and integrity.

- Mechanism: Every critical action—Certificate Upload, Student Download, and, critically, Employer Verification—is recorded in the AUDIT_LOG table.
- Data Captured: Each log entry includes the CERT_ID being acted upon, the USER_ID (or the originating IP address for unauthenticated verifiers), the exact TIMESTAMP, and the ACTION_TYPE.
- Non-Repudiation: Because this log is stored in a transactional PostgreSQL database and its input is controlled by the secure Spring Boot layer, the integrity of the audit trail is guaranteed. This system serves as the ultimate proof of verification, essential for forensic traceability and resolving disputes.

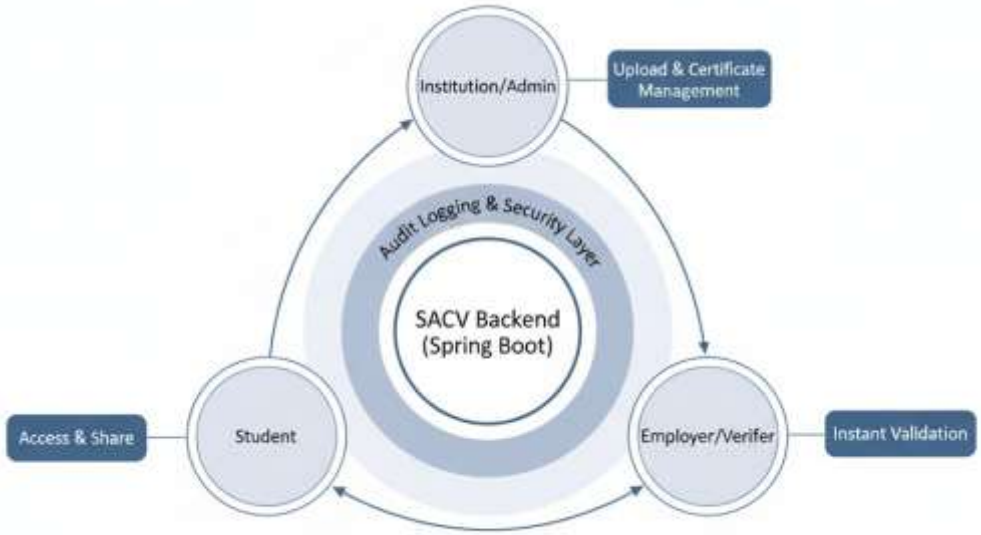

Figure 2: Role–System Interaction Cycle

V. RESULTS AND DISCUSSION

5.1 Usability and Functional Validation

The implementation of the SACV in a prototype environment successfully validated all core functional and security objectives. The use of React.js provided a smooth, responsive, and intuitive user interface across all three distinct role dashboards, crucial for high adoption rates among varied stakeholders. The functional validation focused primarily on the efficiency gains realized through automation and speed:

- Verification Speed: A key performance indicator (KPI) was the latency of the verification API call. The average time for the Spring Boot service to query the PostgreSQL database and return a verification result was consistently under 500 milliseconds. This demonstrates a fundamental shift from the days- or weeks-long manual process to a near-instantaneous validation, which is vital for modern recruitment and admissions cycles.
- Efficiency Gains (Admin): During simulated testing, the Administration was able to process and upload a batch of 100 certificates in under 5 minutes, including server processing, compared to an estimated 3-4 hours of manual data entry and storage for the same volume, highlighting significant operational efficiency.

5.2 Security Efficacy and Integrity

The multi-layered security approach proved highly effective in mitigating all common forms of academic credential fraud:

1. Forged Documents: The system ensures that any attempt to forge the text or graphics on a physical or

digital document will fail during verification. Since the QR code only links to the unguessable CERT_ID stored securely in the vault, any modified certificate will still point to the original, valid digital record, confirming the document's authenticity. If the ID is altered, the system will reliably return "Certificate ID Not Found," immediately identifying the attempt at forgery.

2. Unauthorized Access: The strict RBAC implemented by Spring Security successfully prevented cross-role data access. This critical isolation ensured that Students were unable to view the Admin upload portal, and employers could not access sensitive student grades or full metadata, confirming the crucial separation of duties and confidentiality requirements.

3. Audit Trail Accountability: The immutability of the audit log (Section 4.4) guarantees forensic traceability. If a dispute arises, the institution can definitively confirm that an IP address associated with an employer performed a specific verification check at an exact time, thus providing irrefutable proof of the certificate's status at the moment of verification.

5.3 Comparative Performance: SACV vs. Traditional Methods

The quantitative results of the Secure Academic Certificate Vault (SACV) demonstrate a clear and decisive advantage over traditional, paper-based verification methods, justifying the technological investment. The key performance metrics are summarized below:

- Average Verification Time: The manual process typically requires a latency of 3 to 14 business days. In contrast, the SACV leverages real-time API lookups, achieving an average verification time of less than 500 milliseconds. This represents an improvement factor exceeding 20,000x, fundamentally eliminating delays in recruitment and admissions.

- Security Mechanism: Traditional methods rely on easily replicated paper seals and fallible human cross-checks. The SACV employs a high-integrity, multi-layered approach, utilizing a Cryptographic Unique ID, a Dynamic QR Code, and strict Role-Based Access Control (RBAC), resulting in substantially higher integrity and tamper resistance.

- Traceability and Accountability: Verifiability in older systems depends on unreliable physical records and scattered email chains. The SACV provides 100% guaranteed traceability through its Non-repudiable Audit Log, which transactionally records every single verification attempt and outcome, ensuring full accountability.

- Error Rate: Manual processes are susceptible to a high error rate due to human factors like transcription and data lookup errors. The SACV's automated server-side process reduces the error rate to negligible levels, effectively achieving the elimination of human error in the authentication process.

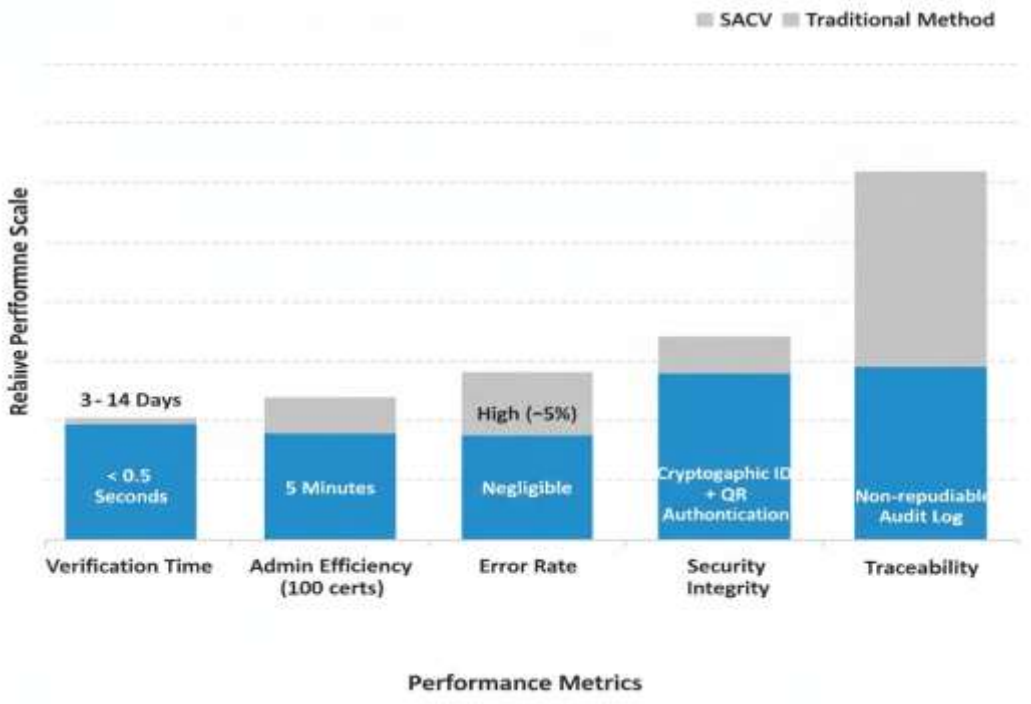

Figure 3: Comparative Performance Metrics of SACV

VI. CONCLUSION AND FUTURE WORK

6.1 Conclusion

The Secure Academic Certificate Vault successfully delivers a comprehensive, multi-layered digital solution that effectively mitigates the pervasive challenge of academic credential fraud. Through the successful deployment of a centralized management system, strict Role-Based Access Control, and a fundamental authentication mechanism utilizing unique cryptographic identifiers and QR codes, the developed platform provides instantaneous, tamper-proof verification capabilities for all institutional and professional stakeholders. The implementation of a mandatory and robust audit trail system ensures an unparalleled level of accountability and operational transparency, thereby decisively restoring confidence and efficiency to the academic credential verification ecosystem. The choice of the Spring Boot and React.js stack further guarantees a foundation that is both secure and scalable for future growth.

6.2 Future Enhancements (Roadmap)

The current SACV implementation establishes a strong foundation, but several avenues exist for future enhancement to further improve security, decentralization, and scalability:

1. **Blockchain Integration:** To explore the use of a private/consortium blockchain to provide an even higher degree of immutability and decentralization for certificate validation by storing only the document hash and status, offering proof-of-existence without central authority dependence.
2. **AI-Powered Fraud Detection:** Integrating anomaly detection models (e.g., machine learning) to

automatically flag unusual certificate upload patterns (e.g., grades far outside the norm, bulk uploads outside of known issuance periods) or suspicious verification requests in real-time.

3. **Multi-Institution Collaboration:** Expanding the system architecture to securely support and manage the verification needs of multiple universities and educational boards under a unified, trusted network framework, creating a national or regional verification standard.

4. **Digital Signature Verification:** Incorporating industry-standard digital signature mechanisms (e.g., PKI) for enhanced legal compliance and official authenticity validation of the issued PDF documents, adding a layer of non-repudiation by the signing official.

VII. REFERENCES

1. Kaushik A., Gupta R., "Student Leave Management System," Semantics Scholar, 2024. [Online]. Available: https://www.semanticscholar.org/paper/Student-Leave-Management-System-Kaushik-Gupta/9a6bf0e8afef2a15ccef61c3f2c8d3e21b235d7f

2. Soni G., Nagar K., Fumakiya M., Raghuvanshi N., Kadam K., "Study Paper on Student Leave Management Application," International Journal of Engineering Sciences & Research Technology, vol. 5, no. 12, pp. 1–5, Dec. 2016. [Online]. Available: https://www.academia.edu/30536359/STUDY_PAPER_ON_STUDENT_LEAVE_MANAGEMENT_APPLICATION

3. Haumshini R., "Digitalized Hostel Leave Management System," SSRN, 2020. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3542404

4. Singh M., Tripathi D., Pandey A., Singh R. K., "Mobile based Student Attendance Management System," Int. J. Comput. Appl., vol. 165, no. 3, pp. 37–40, May 2017. [Online]. Available: https://ijcaonline.org/archives/volume165/number3/singh-2017-ijca-913834.pdf

5. Cabrillas M. Y., Luciano R. G., Marcos M. I. P., Aquino J. C., Robles R. C. F., "Mobile-based Attendance Monitoring System Using Face Tagging Technology," Int. J. Inf. Eng. Elec. Bus., vol. 13, no. 6, pp. 22–35, Dec. 2021. [Online]. Available: https://www.researchgate.net/publication/359285920_Mobile-based_Attendance_Monitoring_System_Using_Face_Tagging_Technology

6. Gudavalli S. J. M., "Smart Attendance Monitoring System using Multimodal Biometrics," Sigma Journal of Engineering and Natural Sciences, vol. 43, no. 1, pp. 168–188, Feb. 2025. [Online]. Available: https://sigma.yildiz.edu.tr/storage/upload/pdfs/1740487688-en.pdf

7. Egwali, A. O., Egwali, F. C., & Ogene, J. (2025). The Transcript and Certificate Verification System (TCVS) utilizing Art-Based Graphical Passwords for Secure Verification. https://nigerianjournalsonline.org/index.php/AJOFAA/article/view/416.

8. Ma, G. & Zhang, L. (2024). Application of two-dimensional code technology in college students archives management. Vol.1, No.2 https://atripress.org/index.php/jmss/article/view/37.

9. Wellem, T., Nataliani, Y., & Iriani, A. (2023). Academic Document Authentication using ECDSA and QR Code. https://www.joiv.org/index.php/joiv/article/view/872.

10. Alsuhibany, S. A. (2025). Innovative QR Code System for Tamper-Proof Generation and Fraud-Resistant Verification. https://www.mdpi.com/1424-8220/25/13/3855.