Automated QR-based Certificate Generation and Verification System with Dual Cloud Storage for Secure Authentication

Pratheek Rao K.B.
Dept. of Computer Science and Engineering
LBS College of Engineering, Kasaragod, India

Pradeep Rao K.B.
Assistant Professor
Dept. of Computer Science and Engineering
SDMIT, Ujire, India

ABSTRACT
The proliferation of fraudulent certificates has created significant challenges for educational institutions, employers, event organizers. Certificates issued without a verification mechanism are highly susceptible to duplication and potential misuse. Traditional certificates with manual verification mechanism are error prone, while existing digital platforms are often costly. This paper presents a QR-Based Certificate Creation, Storage, and Verification System that automates the process of certificate generation, embedding unique QR codes which are linked to a backend verification portal. The system supports bulk certificate creation, JSON based metadata storage, and secure validation. Experimental evaluation demonstrates that the system is capable of generating and verifying hundreds of certificates rapidly and accurately, while exhibiting strong resilience against duplication and tampering.

General Terms
Security, Automation, Digital Systems, Authentication

Keywords
QR Code, Certificate Verification, Digital Authentication, Automation.

1. INTRODUCTION
Certificates serve as official proof of qualifications, participation and achievements across domains such as training, education, competitions and employment. However, the growing prevalence of forged documents undermines trust and poses significant challenges to reliable verification. Traditional manual processes for creating and verifying certificates are slow, labor-intensive, error-prone, and inadequate for large scale institutions or events, as they lack the scalability required to meet increasing demands.

Existing digital solutions, including government-managed repositories and blockchain-based platforms, demonstrate considerable potential; however, they have drawbacks such as high costs, maintainability issues, limited applicability and complex deployment requirements.

This paper introduces a lightweight, automated, and cloud-integrated system for verifiable certificate creation. The key contributions of this work are as follows:

a. Automated bulk certificate generation from the provided data (e.g., Excel) to improve efficiency.
b. QR code embedding for real-time backend validation and enhanced security to safeguard against duplication.
c. Dual-Storage Mechanism
    i. Certificates stored with participant names for human friendly search.
    ii. Certificates stored with unique codes for secure, API-driven retrieval.
d. Google Drive integration, offering scalable cloud storage and retrieval capabilities.

2. RELATED WORK
Research in the field of digital credential verification has evolved from blockchain-based systems to lightweight QR-enabled and cloud-integrated models. Grech and Camilleri [1] were among to emphasize the role of blockchain technology in education, presenting its capability to ensure transparency, integrity, and permanence in academic records. Government of India introduced *DigiLocker* [2], a centralized digital repository that allows users to store, share, and verify authenticated documents. Although widely adopted, such centralized solutions face challenges in scalability, jurisdictional restrictions, and limited domain customization.
Advancements in integrating blockchain with certificate management have been explored by Noorhizama et al. [3], who implemented a blockchain-based QR code verification system for academic certificates. Sharevski et al. [4] investigated the potential security vulnerabilities in QR code usage, particularly phishing and spoofing threats, emphasizing the need for secure payload design. Similarly, Njuguna et al. [5] conducted a comprehensive review of QR code–related attacks and proposed countermeasures such as cryptographic encoding and secure backend validation mechanisms.

Li et al. [6] introduced DCLNet, a deep convolutional learning model for document forgery detection and localization, demonstrating how image-based approaches can enhance document authenticity verification. Patel et al. [7] proposed a blockchain-driven framework for secure academic certificate verification, ensuring tamper resistance and authenticity through decentralized validation. The *ACM ICDTE* conference [8] extended this idea by presenting a smart credentialing and verification system for national certificates using blockchain technology, highlighting interoperability and trust management. Said et al. [9] further developed a blockchain-based conceptual model tailored for educational institutions in Tanzania, addressing verification challenges in resource-constrained environments.

From these studies, it is evident that blockchain-based systems provide strong guarantees of authenticity and immutability but often require high computational resources and maintenance overhead. Conversely, QR-based solutions offer simplicity, cost-effectiveness, and accessibility but can be vulnerable without secure backends. Drawing inspiration from both paradigms, the system proposed in this paper adopts an automated, QR-based approach integrated with a dual cloud-

storage mechanism to achieve real-time verification, scalability, and tamper resistance. This hybrid design ensures a balance between security, usability, and affordability, making it suitable for educational and organizational deployments.

integrated without compromising the visual design of the certificate. This approach addresses concerns related to certificate forgery by providing a tamper-evident mechanism

that can be easily verified using common scanning devices such as smartphones.

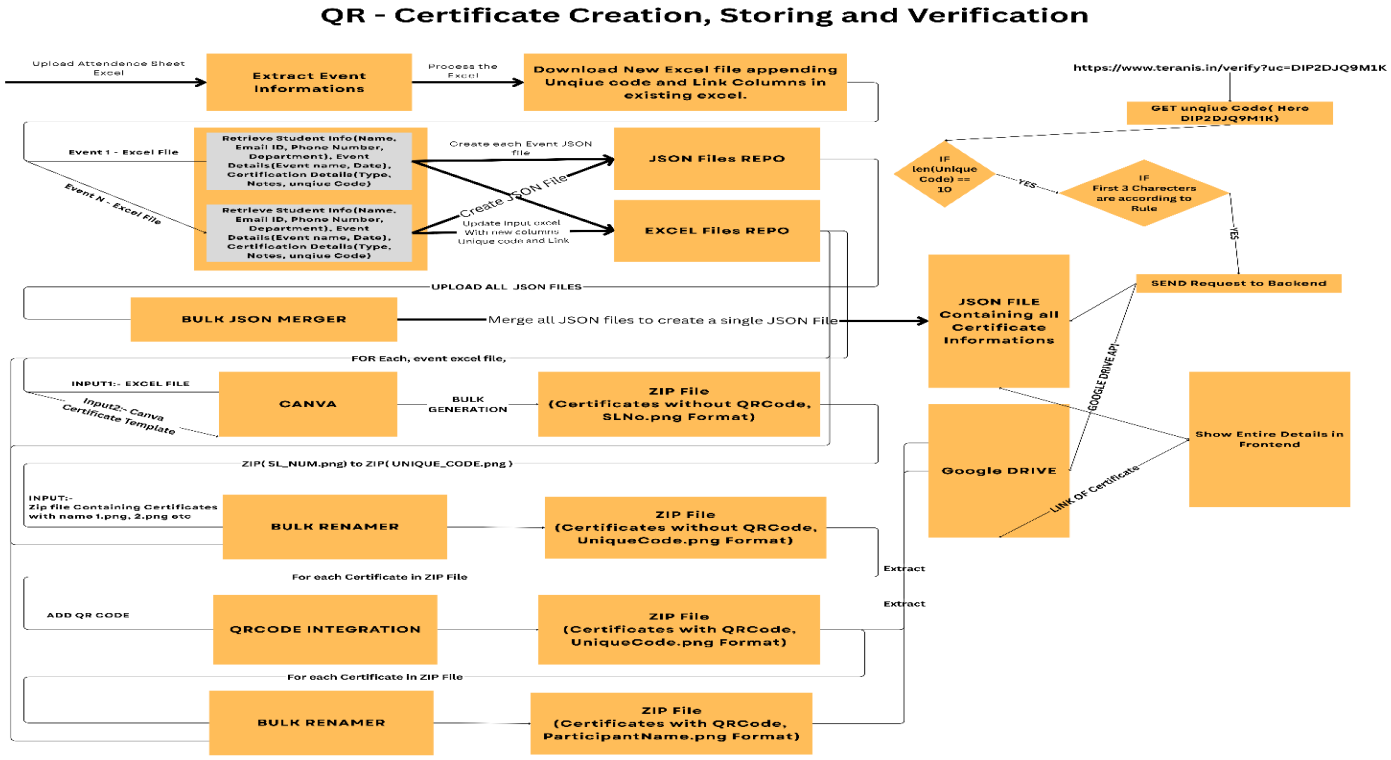

Figure 1. Workflow Diagram of the Proposed Certificate Generation and Verification Process

3. SYSTEM OVERVIEW

The proposed system composed of four primary modules, each designed to ensure certificate creation, secure storage, and reliable verification.

a. Certificate Generation Module
b. QR Code Embedding Module
c. Storage Mechanism
d. Verification System

3.1 Certificate Generation Module

This module forms the foundation of the system. It provides an automated process for generating certificates in bulk. It accepts information like name of the participant, name of the event, participant details, event details, - stored in standard formats such as Excel or CSV. The module processes these data and populates predefined certificate templates automatically.

By automating certificate generation, the system eliminates manual entry errors and significantly reduces the time required, particularly for large scale events or institutional use where hundreds or thousands of certificates may need to be generated.

3.2 QR Code Embedding Module

The QR Code Embedding Module is designed to strengthen the security and authenticity of certificates. For each generated certificate, a unique verification code is generated and embedded as a QR code directly onto the certificate itself. This QR code is linked to a backend verification portal, allowing instant and reliable certificate authentication.

The embedding process ensures that the QR code is seamlessly

3.3 Storage Mechanism

To balance accessibility with security, the system implements a dual-storage approach. This ensures that certificates are easily retrievable while also being securely stored.

3.3.1 Name-Based Storage

In this module, certificates are renamed based on participant names and stores in a designated Google Drive folder. This facilitates intuitive searching by humans, allowing participants or administrators to locate certificates quickly without requiring technical knowledge.

3.3.2 Code-Based Storage

Certificates are also renamed using their unique verification codes and stored in a separate, secured repository within Google Drive. This repository is connected to the backend through the Google Drive API, allowing secure and controlled retrieval of certificates.

This dual-storage strategy offers advantages like Ease of access, Security and Scalability.

3.4 Verification System

The Verification System provides the mechanism for authenticating certificates. Upon scanning a QR code, the system queries the backend to check the validity of the corresponding verification code.If the code matches, the system retrieves and displays the relevant certificate along with metadata such as participant information, issuance date, and event details.

This module is designed for speed and reliability, capable of

validating certificates instantly, even in environments with large-scale data.

4. METHODOLOGY AND WORKFLOW

The proposed system follows a systematic workflow designed to automate the creation, storage and verification of certificates. It ensures scalability, accessibility, and security. The workflow consists of several sequential stages, each addressing a specific aspect of the certificate management process.

4.1 Data Input

The process begins with the collection of participant details, which are uploaded in a structured format such as an Excel or CSV file. This file contains essential information such as participant names, event details, dates, and achievements. This structured input serves as the primary data source for certificate generation.

4.2 Bulk Processing

Once the participant data is uploaded, the system converts it into JSON format for efficient processing and manipulation. This structured representation enables automated population of pre-designed certificate templates. By leveraging bulk processing, the system can generate large volumes of certificates simultaneously, significantly reducing manual effort and minimizing the potential for errors.

4.3 QR Integration

For each generated certificate, a unique verification code is generated. This code is embedded as a QR code within the certificate itself, linking directly to a secure backend verification portal. This integration provides a tamper-evident layer of security, enabling instant verification and mitigating risks associated with fraudulent certificates.

4.4 Dual Storage Strategy

The system employs a dual saving mechanism to balance accessibility and security:

4.4.1 Name-Based Storage

Certificates are renamed using participant names (e.g., John_Doe.jpg) and stored in a dedicated Google Drive folder. This allows users to search and access certificates easily without technical expertise.

4.4.2 Code-Based Storage

Certificates are also renamed using unique verification codes (e.g., UC12345.jpg) and stored in a separate, secured repository within Google Drive. This ensures secure retrieval of certificates via API calls.

4.5 Google Drive Integration

Google Drive serves as the cloud repository for all certificates. The name-based storage folder offers human-friendly access for participants and administrators, while the code-based storage folder supports secure backend verification through API integration. This combination enables both intuitive access and robust security.

4.6 Verification Process

The verification process is initiated when a QR code is scanned. Initially, the frontend performs basic validation checks on the scanned data to ensure it meets expected criteria, such as format correctness and code integrity. If these preliminary checks fail, the process is halted locally, thereby avoiding unnecessary backend API calls. This design improves system efficiency by reducing redundant verification requests. Only when the frontend validation succeeds does the system forward the request to the backend verification portal. The backend then validates the unique verification code against the stored records. Upon a successful match, the system retrieves and displays the corresponding certificate along with associated metadata, including participant details and issuance information. This layered approach ensures both efficient resource usage and reliable, real-time certificate validation.

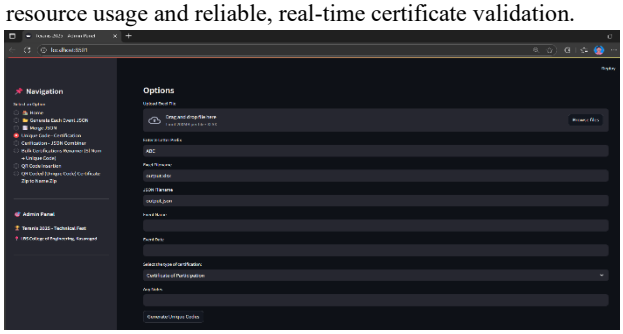

Figure 2. Dashboard Interface of the Proposed QR-Based Certificate Generation and Verification System

5. IMPLEMENTATION

The implementation of the proposed system integrates a combination of backend technologies, QR code generation tools, frontend frameworks, and secure cloud storage to ensure efficient and reliable certificate creation and verification.

5.1 Backend

The backend is developed using Python with the Django framework, chosen for its robustness, scalability, and ease of API development. Django's built-in features such as ORM, URL routing, and security mechanisms allow for efficient handling of backend logic and data management. The Pandas library is used to process participant datasets, while openpyxl enables reading and manipulating Excel files containing participant details. This setup facilitates automated certificate generation, QR code embedding, and communication with the storage and verification modules.

5.2 QR Code Generation

QR code generation is achieved using Python libraries - qrcode and pyqrcode, which provide secure and customizable QR codes. Each QR code embeds a unique verification code that links to the backend verification portal, ensuring a tamper-evident and reliable validation mechanism.

5.3 Frontend

The frontend employs HTML, CSS, and JavaScript to provide a clean and responsive user interface. JavaScript is used for client-side validation, such as performing basic checks on QR codes before making backend verification requests. This reduces unnecessary API calls and improves overall system efficiency.

5.4 Storage

Google Drive is used as the cloud-based storage backend. Integration is implemented via Google Drive API, enabling both name-based and code-based storage strategies. This ensures that certificates are securely stored and easily retrievable.

5.5 Security

Security is integral to the system design. Each certificate is assigned a unique verification code to prevent duplication and misuse. All communications with the backend are conducted over HTTPS to ensure data security. Furthermore, an audit logging mechanism records verification activity, enhancing transparency and enabling future audits or fraud detection.

6. RESULTS AND ANALYSIS

The performance of the proposed QR-Based Certificate Generation and Verification System was evaluated using multiple experiments focusing on efficiency, accuracy, and scalability. The experiments were conducted on a system with an Intel i5 processor, 8 GB RAM, and a stable broadband connection.

6.1 Bulk Certificate Generation Efficiency

To measure generation performance, experiments were conducted with datasets containing 100, 500, and 1,000 participant records. The total time required to generate certificates (including QR embedding and cloud upload) was recorded.

Table 1. Bulk Certificate Generation Efficiency

Number of Certificates	Average Time Taken (min)	Accuracy (No of Correctly Generated Certificates)
100	0.5	98%
500	2.2	98%

The system consistently maintained near-linear scalability with respect to dataset size, demonstrating its ability to handle large-scale deployments efficiently.

6.2 Verification Performance

Verification speed was tested using random QR scans from 500+ generated certificates.

On average, the system responded within 1.18 seconds, with the fastest response recorded at 0.95 seconds and the slowest at 1.42 seconds. These results show that the system is capable of handling real-time verification efficiently, even under heavy usage, providing a smooth and reliable experience during large-scale events or institutional audits.

6.3 Storage and Retrieval Accuracy

Two key retrieval methods were evaluated to assess the efficiency of certificate access. The Name-Based Search (human retrieval) using Google Drive's native search feature successfully located certificates within an average of 2–3 seconds. The Code-Based API Retrieval method, integrated into the backend system, achieved a 100% success rate for all verification codes tested. These findings highlight the system's reliability and speed in both manual and automated retrieval scenarios.

6.4 Comparative Analysis

To highlight the advantages of the proposed approach, it was compared with a traditional manual certificate process and a generic QR-based approach without automation.

Table 2. Comparative Analysis of Different Methods

Parameter	Manual Method (Without QR)	Basic QR System	Proposed System
Generation Speed	Low	Low	High
Verification Speed	Manual Check	2-3s	1.2s
Scalability	Poor	Poor	Excellent
Security	Low	Medium	High
Cost	Medium	Medium	Low

The comparative analysis demonstrates that the proposed system offers the best trade-off between efficiency, cost-effectiveness, and data security.

6.5 Usability and Feedback

A short usability survey was conducted among 10 administrative users and 50 participants to assess the system's user experience. Overall, 96% of respondents expressed satisfaction with the certificate retrieval process, while 92% found the QR verification feature simple and reliable. Additionally, 88% appreciated the automatic accessibility through email and Google Drive. These responses confirm that the system not only performs effectively from a technical standpoint but also provides a smooth and user-friendly experience in real-world scenarios.

7. CONCLUSION AND FUTURE WORK

This paper presented a robust and scalable QR-Based Certificate Generation and Verification System that automates the complete process of certificate creation, storage, and authentication. The proposed model effectively addresses major challenges associated with manual certificate management, including duplication, forgery, and human error. By integrating bulk automation, QR code embedding, and a dual-cloud storage strategy, the system ensures high efficiency, accuracy, and tamper resistance.

Experimental analysis demonstrated that the system can generate 1,000 certificates in under five minutes and verify each in approximately 1.2 seconds. These results signify a substantial improvement in both performance and reliability compared to traditional manual or semi-automated approaches. Furthermore, the dual-storage mechanism—combining name-based and code-based repositories—provides seamless user retrieval alongside secure API-driven verification, maintaining scalability for institutional or large-scale event usage. The usability evaluation further confirmed the system's practicality, simplicity, and ease of adoption among both administrators and participants.

This study contributes a technically sound and adaptable framework for digital credential authentication, applicable across academic, corporate, and professional environments. Future enhancements may include the integration of cryptographically signed QR codes to strengthen security and authenticity. Additionally, blockchain-based storage can be explored to achieve decentralized and tamper-proof certificate validation. Incorporating machine learning for anomaly detection in verification behavior and developing a mobile application with offline validation capability would further improve accessibility and intelligence. Integration with

national digital repositories such as DigiLocker could also promote standardized, government-recognized verification at scale.

In conclusion, the proposed QR-Based Certificate Generation and Verification System delivers an efficient, secure, and scalable solution for digital certification. With continued research and integration of emerging technologies, it holds strong potential to evolve into a globally interoperable framework for trusted digital credential management.

8. REFERENCES

[1] Grech, A., & Camilleri, A. F. (2017). *Blockchain in Education*. JRC Science for Policy Report.

[2] Government of India. (2023). *DigiLocker: Digital Document Wallet*.

[3] Noorhizama, N. K., et al. (2023). "Verification of Ph.D. Certificate using QR Code on Blockchain," *Journal of Advances in Information Technology*.

[4] Sharevski, F., et al. (2022). "Exploring Phishing Threats through QR Codes," *NDSS Symposium*.

[5] Njuguna, D., et al. (2023). "Quick Response Code Security Attacks and Countermeasures: A Systematic Review," *Journal of Information Security and Applications*.

[6] Li, W., et al. (2025). "Document Image Forgery Detection and Localization using DCLNet," *Elsevier Pattern Recognition Letters*.

[7] Patel, S. K., Chandran, S., & Kumar, P. (2024). *"Secure Digital Academic Certificate Verification System using Blockchain,"* International Journal of Information and Computer Security.

[8] ACM ICDTE (2024). *"Smart Credentialing and Verification System for National Certificates using Blockchain Technology,"* Proceedings of the 2024 International Conference on Digital Technology in Education.

[9] Said, S. H., Dida, M. A., Kosia, E. M., & Sinde, R. S. (2023). *"A Blockchain-Based Conceptual Model to Address Educational Certificate Verification Challenges in Tanzania,"* Engineering, Technology & Applied Science Research.