Frontiers in Health Informatics
ISSN-Online: 2676-7104
www.healthinformaticsjournal.com
2024; Vol 13: Issue 4
Open Access

Automated Certificate Verification and Management System

Pranjali Bahalkar,Pallavi Shingade,Nakul Gavhane, Vijoy Khatri,Atharv Pote, Saikiran Chilakapati
Dr. D. Y. Patil Institute of Technology
Email: pranjali85bahalkar@gmail.com,Email: pallavi.rshingade@gmail.com
Email: nakulgavhane@gmail.com, Email: vijoykhatri3@gmail.com
Email: atharvapote20@gmail.com, Email: saikiranrch@gmail.com

Cite this paper as: Pranjali Bahalkar,Pallavi Shingade,Nakul Gavhane, Vijoy Khatri,Atharv Pote, Saikiran Chilakapati (2024) Automated Certificate Verification and Management System. *Frontiers in Health Informatics, 13* (4), 142-147

***Abstract*—**The purpose of this project is to clarify the use of the new fully automated system for the verification and management of digital certificates issued by such well-known platforms as Google, Coursera, and Udemy. Our one-of-a-kind approach efficiently extracts and authenticates essential information from certificates through either QR codes or embedded verification links, while also providing strong functionalities for certificates with public key inclusion. Users can create carefully compiled reports and save the certificates in a variety of file types like XLSX and Word. Moreover, future improvements are reviewed such as the smooth connection with Learning Management Systems (LMS), implementing blockchain technology to the verification process to gain trust, real-time alert functions, and full support of multi-languages.

Keywords— Certificate verification, QR code scanning, Blockchain, Public key, Digital certificate management, LMS integration, Security.

I. INTRODUCTION

The online education platforms have grown in popularity, resulting in a rapid increase in the issuance of digital certificates, which are used as official recognition of the skills acquired or courses completed. These certificates are used by learners but are also valuable to employers who want to evaluate whether a candidate is qualified. Yet, a central problem both for the certificate holders and the organizations is the fact of the authenticity and the legitimacy of the digital credentials. The rise of the fake certificates along with the ease of digital manipulation has made it very hard to trust the documents without a reliable verification mechanism.

Our project undertakes the task of overcoming these difficulties through the use of an automated and secure certificate verification system. It is a platform that authenticates digital certificates using QR code scanning and other technologies such as embedded link extraction to get details about the certificate. The system then proceeds to cross-verify the issuing platform's information with the one obtained to ensure that the validity of the certificate is not questionable. As any of these certificates are accepted by major online education platforms such as Google, Coursera, and Udemy, it is a truly versatile. Certified users get an easy-access and manageable environment thanks to the user-friendly system. It also consists of several high-end options that bring an extra layer of security and functionality. One such feature is the verification of a public key, ensuring the certificates are tamper-free by checking them against the cryptic signature of the issuing authority for organizations and institutions that need documentation or audit trails., the system also produces comprehensive verification reports.

Through digital education, these days, we have the demand for more secure verification ways. Keeping this in mind our system is developed with the future in consideration. It could include blockchain-based verification, allowing it to have an unshakeable and decentralized ledger that will store certificate data. This one, therefore, provides an extra layer of security and transparency, which in turn makes it almost impossible to forge or alter verified credentials.

Basically, our project has not only simplified the certificate verification process but also the introduction of high-tech technologies, guarantees the

II. Literature Review

Year	Paper	Technology	Outcome
2008	On Automatic Authenticity Verification of Printed Security Documents	Machine Authentication, SVM	Develops a framework using Support Vector Machines (SVM) with non-linear kernels to automatically verify the authenticity of printed security documents like bank cheques, achieving 99.5% accuracy. The method involves feature extraction from document images and differentiating between genuine and duplicate documents.
2017	Automated Batch Certificate Generation and Verification System	Template-based System, GUI	Introduces a system that facilitates certificate generation and verification without requiring the user to know XML. The system allows users to define and verify certificate templates via a graphical user interface (GUI), aimed at reducing manual effort and speeding up the certificate processing time.
2021	Publication in 2021 International Conference on Computational Techniques, Electronics and Mechanical Systems	Machine Learning	Describes a system using machine learning algorithms for automated document analysis, particularly focusing on preventing errors and fraud in industries with a high volume of document processing by ensuring accuracy and integrity.
2023	Automatic Certificate Verification using Computer Vision	Computer Vision, OCR	Proposes a computer vision system to verify academic certificates by providing a database using OCR (optical character recognition) and detecting labels and details from certificate images. Client-server architecture ensures very quick response time and very fast access.
2023	A Blockchain-Based Verification System for Academic Certificates	Blockchain, Smart Contracts	We are utilizing smart contracts and blockchain technology for the development of a DApp that will be used to verify authentic academic certificates that are secure and transparent. The solution provided by the platform enables the instant and simple verification of credentials through the immutable ledger thus, reducing the time needed for the verification process and increasing the trustworthiness of it.

III. Methodology

The Automated Certificate Verification and Management System has been developed to provide a simple, secure, and efficient way of checking the digital certificates issued by various online education platforms. The procedure for building this system has a number of steps, and each uses different technologies and frameworks to deliver the functionality required. The sections given below outline the steps that are involved:

i) Requirement Gathering and Analysis

The first stage is initiated by users, educational institutions, and the employers who delineate the core functions they are looking for. The system is intentionally designed to support certificates from the most popular online education platforms such as Google, Coursera, and Udemy. Besides, technologies such as QR code scanning, public key verification, blockchain integration, and report generation were also highlighted by the users and stakeholders.

ii) System Design

The framework as a whole consists of three main components:

a) Frontend Interface: The certificate's upload should be secure and fast. The web dashboard has advanced search and filtering functions for Efficiently managing certificates.

b) Back-end Processing: This method requires the use of a QR code extracted link and the public key to validate it to the issuing organizations servers.

c) Data Storage and Security: It makes sure that certificate data is securely stored by using encryption and has an audit trail for any modifications made to the certificates.

iii) QR Code and Link Extraction

The basic business is a procedure of extracting the details of the certificates from a QR code or the links which are embedded in the certificates. The backend now uses QR code readers and optical characters recognition (OCR) software to decode the certificate data. The next step is to send an API call to the issuing platform to verify the authenticity of the document.

4. Public Key Verification

For the ones that possess a public key, the Public Key Infrastructure (PKI) method is utilized for cryptographic validation. By doing this, the RSA algorithm is used to authenticate the certificate:

- RSA Encryption:

- Cipher: C = M^e mod n

- Plaintext: M = C^d mod n

- One of the alternatives to Elliptic Curve Cryptography (ECC) is the case when high performance is needed and small resource requirements are available.

5. Blockchain Integration

Immutability of the verification history is achieved through storing the certificate's hash on a private blockchain. The internet creates Merkle trees which, in case of data corruption, can be proved by blockchain users. The blockchain is secured by the SHA-256 hashing algorithm which uses a proof-of-authority (PoA) consensus method to validate the network relationship quickly and privately.

6. Report Generation

As soon as the verification process is completed, the system issues reports in XLSX or Word formats. These details include the certificate holder's name, course description, and verification status. The report generation tool is highly beneficial for employers and educational institutions dealing with big batches of certificates.

7. Testing and Validation

The implementation of the system is validated through the various test cases that resemble the different formats and types of certificates, thus, certifying that the system can work through different kinds of QR codes, public key validations, and API responses from the certificate issuing entities. Security validation exercises are done through tests that secure the data problems from the mishandling of data.

8. User Interface Development.

A front-end, user-oriented interface is made by means of HTML, CSS, and JavaScript, while the Node.js frameworks provide the needed backend support. The UI facilitates users to upload, verify, and manage certificates with a very little technical know-how. Moreover, it includes instant alerts and smart tools to help in grouping of certificates.

9. Deployment

The system is cloud-based making it easy for users to scale and access the platform. An API Gateway is utilized for the communication between users and the backend

10. Custom Algorithm

In addition to that, the proposed system is to be equipped by utilizing a custom software created to improve the certificate verification to be more secure and also to detect the fraud. The built model will apply deep learning methods and natural language processing (NLP) techniques to detect the subtle changes of the certificate texts, if any, and find out the underlying differences. In this way, it will not only help to solve data discrepancies but also will be the contributor to the reliability and assurance of the overall system, thus making the verification process more secure and trustworthy.

-Support Vector Machines (SVM)

Support vector machines (SVMs) are the main document-authentication mechanism employed in state-of-the-art verification systems since their excellent ability to perform the classification task. Decision boundary of a binary SVM classifier is the following equation:

$f(x)= w(T) + b$

Where:

- w: Weight vector
- x: Input feature vector
- b: Bias term.

The aim of SVM is to boost the margin M between the decision boundary and the closest data points. A margin can be derived from the following line:

$M = 2 / ||w||$

Maximizing the margin leads to better generalization and robust classification.

$(1/2) ||w||^2$

Subject to the constraint:

$y_i * (w^T * x_i + b) >= 1$ for all i

Where y_i represents the label of the i-th data point. This framework was used in the 2008 study to classify security documents like bank cheques with a remarkable accuracy of 99.5%.

-Optical Character Recognition (OCR)

Optical Character Recognition, is the key module in new automated certificate verification systems. The year 2023 research states that OCR, along with data derived from computer vision techniques, was used to extract text from student certificates. The core method of the OCR is template matching, that is, a certificate image is correlated with the already set reference at the beginning. The cross-correlation is explained by the following equation:

The primary functionality of OCR is **template matching**, which involves computing cross-correlation to compare the certificate image with predefined patterns. The cross-correlation is defined by the equation:

$R(x, y) = \Sigma\Sigma T(i, j) * I(x + i, y + j)$

Where:

• T(i, j): Represents the predefined text pattern (template).
• I(x + i, y + j): Refers to the subsection of the certificate image centred at (x, y).

In the output, sample size of the correlation coefficient at each pixel is obtained and thus can be used to point out the matched areas between the template and the image. This approach provides a high degree of precision in text extraction when the certificate turns out to be physically flawed or differently designed. The OCR-based system has excellent performance and reliability in certificate verification tasks when it runs in a client-server network architecture.

-Blockchain Hashing Mechanisms

HTML/The crypto security of the blockchain system relies on hashing in 2023.Each of the certificates is a hash that is unique with the rest of them by using such algorithms as/XML

SHA-256:H(x)=SHA-256(x)

where the certificate data corresponds to the value of x. Hashing preserves the integrity of the certificate, and at the same time, smart contracts automate the verification process without human intervention, which in turn, cuts down the time and bolsters the trustworthiness intensively.

IV. Comparative Analysis

It happened in 2023, for the first time in the history of any technology, as the system became able to recognize and get the figures that were in the certificates and the centralized database confirmed that. Through a computer vision and OCR application used to validate the certificates for the first time in the year 2023, this technology was embraced on a large scale. The verification precision has undoubtedly reached a new level but at the same time, it carries this disadvantage of the centralized storage of data that can be hacked. Next year, 2023, a new verification scheme was introduced which relied on the blockchain technology whereby smart contracts were employed to ensure that the academic certificates were recorded on a ledger that could not be altered. So far, safety and visibility have improved tremendously, but a few more things are still needed like public key cryptography protection and certificate validation notifications which is not yet available.

The proposed project, building upon the gains made so far, is an automated certificate checking and management system that uses advanced technologies including QR codes and embedded link extractions to collect and send the information to platforms such as Google, Coursera, and Udemy certificates for verification automatically. It has a infrastructure scheme (PKI) that allows for the verification of public key embedded certificates, making certificates' authenticity secure. The system utilizes verification data inscription technology in the blockchain through a non-reproducible ledger which brings more certainty to the process while the invoice function makes it easy for users to classify certificate data in XLSX and Word formats. Moreover, the system will formulate links with Learning Management Systems (LMS) to make the certificate validation process more efficient. Planned improvements include real time alerts for expired or invalid certificates which, will provide users, and employers with instant notifications as well as multi-language support to make the platform accessible to global users. Blockchain technology will add another layer of security to the system by using a public key cryptography scheme that enables redirect management.

This combination will generate certificates that have a verifiable history which cannot be altered. The user interface thus will be made user-friendly such that users may well upload & manage used materials with proper search and filtering options. The other side of the AI is the technology based on it, which will be used in real time to warn the system of any possible malicious activities through anomaly detection in certificate structure and metadata thus improving fraudulent certificates detection.

To sum up, this project extends the prevalent machine learning, OCR, and blockchain technologies by integrating new features such as real-time verification, multi-platform integration, and enhanced security with the help of public key cryptography. Our project, which fills in the gaps that were found in the previous ones, intends to deliver a complete, easily operated, and safe platform for the digital certificate verification and management that will be adaptable to the highly developed and digital education landscape.

The proposed project, building upon the gains made so far, is an automated certificate checking and management system that uses advanced technologies including QR codes and embedded link extractions to collect and send the information to platforms such as Google, Coursera, and Udemy certificates for verification automatically. It has a infrastructure scheme (PKI) that allows for the verification of public key embedded certificates, making certificates' authenticity secure. The system utilizes verification data inscription technology in the blockchain through a non-reproducible ledger which brings more certainty to the process while the invoice function makes it easy for users to classify certificate data in XLSX and Word formats. Moreover, the system will formulate links with Learning Management Systems (LMS) to make the certificate validation process more efficient. Planned improvements include real time alerts for expired or invalid certificates which, will provide users, and employers with instant notifications as well as multi-language support to make the platform accessible to global users. Blockchain technology will add another layer of security to the system by using a public key cryptography scheme that enables redirect management.

This combination will generate certificates that have a verifiable history which cannot be altered. The user interface thus will be made user-friendly such that users may well upload & manage used materials with proper search and filtering options. The other side of the AI is the technology based on it, which will be used in real time to warn the system of any possible malicious activities through anomaly detection in certificate structure and metadata thus improving fraudulent certificates detection.

To sum up, this project extends the prevalent machine learning, OCR, and blockchain technologies by integrating new features such as real-time verification, multi-platform integration, and enhanced security with the help of public key cryptography. Our project, which fills in the gaps that were found in the previous ones, intends to deliver a complete, easily operated, and safe platform for the digital certificate verification and management that will be adaptable to the highly developed and digital education landscape.

V. Conclusion

The automated management and verification certification system responds to the fact that there is an increasing demand for a secure, efficient and reliable certification of digital certificates issued by platforms such as Google, Coursera, and Udemy. As the online education sector keeps growing, the issue of the authenticity of the digital credentials becomes very important not only for learners but also for employers. Our proposal constitutes a detailed answer by adding the extraction and validation of the certificate details through QR code and embedded links, thereby ensuring data accuracy and consistency.

The system establishes a benchmark for the digital certificate management by involving the implementation of such features as public key verification, blockchain's transparency, and real-time notifications. Besides hacking protection, this system offers yet another way of organizing and managing your verified certificates, thanks to the new report generation feature. Besides, the possible integration of Learning Management System (LMS) and multi-language support opens its applicability to education institutions and learners all over the world.

Safety is the primary aim at every stage of the system's development. Usage of encryption methods and secure API communication guarantees that the information about certificates is treated with utmost care. Blockchain technology makes the system more reliable by providing a ledger of certificate records that cannot be changed. Verified credentials come with a watermark that cannot be forged or altered in any way without being detected, hence making it impossible for anyone to modify them without being caught.

Among the future enhancements that will make the system stronger are the use of AI-insurance algorithms, support of more platforms, and the formation of educational ecosystems. Technology advancement will be of great importance for employers to determine the platform's suitability in relation to digital education media, and for issuing and authenticating digital certificates in a safe, quick, and reliable manner. To be precise, our system of issuing digital certificates is completely secure.

VI. References

[1] Anderson, R. (2019). Blockchain for Academic Credential Verification: A Secure Approach. *International Journal of Blockchain Applications*, 12(4), 45-60.
[2] Gupta, S., & Patel, M. (2020). Public Key Infrastructure and Digital Certificate Validation in E-Learning Platforms. *Journal of Cryptographic Security*, 14(2), 101-118.
[3] Johnson, K. (2022). Automation in Digital Certificate Management and Verification. *Proceedings of the International Conference on Digital Education Systems*, 9(2), 89-97.
[4] Lee, D., & Kim, S. (2021). QR Code Authentication for Digital Certificates in Online Learning Platforms. *Journal of Educational Technology Research*, 11(3), 211-225.
[5] Pranjali Bahalkar, Dr Prasadu Peddi, Dr. Sanjeev Jain," AI-Driven Career Guidance System: A Predictive Model for Student Subject Recommendations Based on Academic Performance and Aspirations", Frontiers in Health Informatics, ISSN-Online: 2676-7104, Vol. 13 No. 3 (2024).
[6] Miller, J., & Zhang, Y. (2023). Enhancing Digital Credential Security with Blockchain and Public Key Integration. *Journal of Emerging Technologies in Higher Education*, 15(1), 67-82.
[7] Roberts, T. (2020). LMS Integration for Automated Certificate Issuance and Verification. *Educational Technology Review*, 8(5), 133-145.
[8] Singh, R., & Verma, P. (2023). Leveraging Blockchain for Transparent Certificate Verification Systems. *Journal of Information Security and Cryptography*, 16(3), 56-74.
[9] Wang, H. (2021). Digital Certificate Authentication Using QR Codes and Embedded Links. *Journal of Online Education and Learning Systems*, 14(1), 90-104.
[10] Zhang, Q. (2022). The Role of Public Key Cryptography in Verifying Online Credentials. *Journal of Digital Identity and Security*, 10(4), 88-99.
[11] Pranjali Kothawade, & Suhas Patil (2019). Collective Data-Sanitization For Personal Information Protection, 9(2), 89-93. DOI: https://doi.org/10.52783/anvi.v28.1915