DOCUMENT GENERATION WITH QR CODE ENCRYPTION FOR ENHANCED FRAUD DETECTION AND VERIFICATION

Emewu, Benedict Mbanefo [1], Okpara Chukwuemeka[2], Okeiyi Euphemia K.[3]

[1, 2] Department of Computer Science, David Umahi University of Health Science, Uburu
[3] Department of Computer Science, Ebonyi State University, Abakaliki.

Abstract- In this twenty first century, the need for secure and reliable document, verification system has become overriding, principally in sectors where the integrity of documents is crucial. Traditional methods of document handling and verification often lack robust security measures, making them susceptible to tampering and unauthorized access. Therefore, a comprehensive web-based solution that not only facilitates document generation but also integrated advanced technologies, QR code encryption, and advanced fraud detection algorithms to address the existing shortcomings in document security to enable fraud detection and document verification process is required. This work focused on developing a web-based document generation system that integrated QR code encryption and a variety of cutting-edged verification technologies. It explored novel approaches such as blockchain technology, decentralized identity, zero knowledge proof, and machine learning for fraud detection. The methodology followed a structured process that involved both front-end and back-end development. The front-end focused on the user interface (UI) design for document generation and verification while the back-end focused on data processing, QR code encryption, blockchain integration, machine learning-based fraud detection, and secure storage. Built using HTML and CSS for intuitive UI design, PHP and Python for back-end processing, JavaScript for dynamic user interaction, and MySQL for robust data management. The system is designed to be versatile and scalable, supporting a wide range of applications, including academic certifications, legal documents, healthcare records, and financial reports. It also addressed critical security challenges in document management and provided a comprehensive framework for fraud detection, real-time verification, and audit tracking. Finally, the system offered a practical and innovative approach to document generation and management, suitable for organizations requiring high levels of document security and integrity.
.

Index Terms- Audit trails, Authentication, Blockchain, Encryption, QR code

I. INTRODUCTION

The security and confidentiality of data are very important for institutions. Meanwhile, data fabrication or falsification of official documents is still common. Validation of the authenticity of documents such as certificates becomes a challenge for various parties, especially those who have to make decisions based on the validity of the document. Scanning-based signatures on printed and digital documents are still relatively easy to counterfeit and yet still difficult to distinguish from the original. The traditional approach is no longer reliable. Solutions to these problems require the existence of data security techniques, seamless online verification of the authenticity of printed documents, and e-certificates quickly.

In some other cases, data confidentiality is not the main issue, such as in the case of the authenticity of a published certificate, ID card, or similar documents. Being easily verifiable and trustable is of more importance, as generally, such documents tend to be open for public sharing. The next level is that all published documents are truly legitimate and clearly distinguishable from modified or falsified versions of the same documents. Here, data security technologies play even more strategic usage. There are many techniques that have been proposed to overcome this issue such as: ink stamps, live signatures, documentation of transactions in third party such as the court or notary (Arko *et al*., 2023; Maysaa *et al*., 2020). There are many usages and applications where quick response (QR) codes are significantly involved such as commercial products, tracking and monitoring labeled goods, marketing and advertising, identification of business cards, as a result, in many other circumstances, where sharing data is needed (Omar and Oleg, 2017; ISO/IEC, 2015). Practically, it is so hard to control considerable quantity of documents quickly using traditional ways. Verification of these documents is quite challenging because they cannot be traced as quickly and accurately (Malsa *et al*., 2021). Thus, a system is needed to inspect the authenticity and validity of document certification rapidly and precisely. Due to the rise in the usage of smart phones with cameras combined with the ease of scanning a QR code using this device, studies have explored the use of QR codes as a cheap alternative to other tag-based systems (Rogel *et al*., 2022). QR code is a two-dimensional barcode that is usually used to encode bits of information represented as black square dots placed on a white square grid (Uzun and Bilgin, 2016). They are designed to decode the data quickly. It is the most popular type of verification system used in the world. It has a wide storage space and fast readability and it brings greater reliability and security in the existing process of issuing degree certificates to university and other level graduating students (Oyediran *et al*., 2021).

Fake degree certificates case cause many problems to the institutions of higher educations. The occurrences of this case affect the institutions' reputation and many reflect to their output to industry. In order to prevent the problem to occur, a certain safety must be applied to new issued official document. This research has the purpose to design new safety measures to prevent documents against illegal replication especially document spoofing by using encrypted data signature.

One of the principal weakness of all encryption systems is that the form of the output data (the cipher text), if intercepted, alerts the intruder to the fact that the information being transmitted may have some importance and that it is therefore worth attacking and attempting to decrypt it.

In order to provide strong encryption data, this research integrated the following new verification technologies: blockchain verification, advanced encryption standard (AES), timestamping services, and machine learning for fraud detection, multifactor authentication, (MFA), API integration for document verification services, audit trails and logging. These technologies will significantly enhance the security, reliability, and fraud detection capabilities of the web-based document generation project with QR code encryption. Furthermore, novel scopes the research explored include: smart contracts integration, zero knowledge proofs (ZKPs), decentralized identity (DID), interoperability with existing systems, artificial intelligence for document analysis, geo-location verification, temporal blockchain anchoring, and multi-party computation (MPC). This scope leverages emerging technologies and address specific changes in document verification, fraud detection, and user privacy, enhancing the capabilities and utility of this project in innovative ways.

The objectives of this research include:

i. Develop a secure web-based platform for document generation, encryption and authentication.
ii. Integrate advanced verification technologies for document encrytion.
iii. Explore novel scopes such as blockchain technology, machine learning, zero knowledge proof, decentralized identity, and temporal anchoring for document security and verification.
iv. Implement comprehensive logging and audit trails.

II. CONCEPT OF DOCUMENT SECURITY AND FRAUD DETECTION

In the digital age, the security and integrity of documents have become increasingly crucial. As more business operations and personal transactions migrate online, the risk of document fraud has escalated significantly. Fraudulent documents can be used to enable identity theft, financial crimes, and illicit activities, causing substantial financial and reputational damage to individuals and organizations alike (Ashifa and Sathya, 2019, Tripathi, 2023, ID-Pal, 2024).

Document fraud has evolved alongside technological advancements, making it increasingly difficult to detect. Criminals leverage tools such as data scraping and image editing software to create convincing forged documents that can bypass manual inspection. This poses significant challenges for organizations responsible for verifying the authenticity of documents, such as financial institutions, government agencies, embassies and human resource departments. The consequences of document fraud can be severe, ranging from financial losses and legal liabilities to reputational damage and regulatory penalties. Detecting fraudulent documents often requires a meticulous, time-consuming process that is prone to human error (Vallesky, 2024). Furthermore, the global nature of modern business operations and the ease of digital document sharing amplify the risk of cross-border document fraud.

To effectively combat the growing threat of document fraud, organizations must embrace advanced technologies that automate and enhance the document verification process. Artificial intelligence and machine learning (ML) have emerged as powerful tools in the fight against document fraud (ID-Pal, 2024; Vallesky, 2024).

The use of AI and geo-location verification may raise concerns about data privacy, particularly when dealing with sensitive personal information. Organizations must ensure that they comply with relevant data protection regulations and obtain user consent for data collection and processing (Ashifa and Sathya, 2019).

QR code encryption is if employed to verify document authenticity will quickly execute the action, allowing users to scan codes and retrieve validation information instantly. Some advanced systems integrate blockchain technology, creating immutable ledgers for tracking document history, enhancing trust, and ensuring transparency.

Fraud prevention is another key feature, with machine learning algorithms often utilized to detect unusual patterns or alterations in documents. This real-time detection provides added protection in fast-paced environments, such as legal and financial sectors.

Figure 1 below shows common QR code patterns

Figure.1: Sample generated document with encrypted QR code

III. SYSTEM ANALYSIS

The system centers around the use of encrypted QR codes embedded within documents. These QR codes contain unique identifiers and metadata, such as creation date and digital signatures, which allow for easy verification. When scanned, the QR codes instantly provide the authenticity of the document by cross-referencing the data with a blockchain ledger, ensuring that

any unauthorized changes or manipulations are detected in real-time. Blockchain's decentralized nature makes it ideal for this purpose, as it creates an immutable record of document transactions, which can be transparently verified at any point without the risk of tampering.

The research also incorporates machine learning to enhance fraud detection. By training models on historical data, the system is able to identify suspicious patterns and potential anomalies that may indicate fraudulent activity. This adaptive capability allows the system to continuously improve its fraud detection accuracy over time, making it more efficient and reliable.

The front-end of the system is designed using HTML, CSS, and JavaScript, providing a user-friendly interface for generating and verifying documents. On the back end, PHP and Python (Flask) handle the secure communication and processing, while MySQL is used for secure, encrypted storage of documents and audit logs.

Proposed System Users

The following are the proposed users of the web-based application with a few of their functions within the application:

a. Admin
   i. Update Application
   ii. Generate documents
   iii. Encrypt document
   iv. Verify documents
b. User
   i. Search Document
   ii. View document
   iii. Verify document

The figure 1 shows the activities that can be performed by the administrator

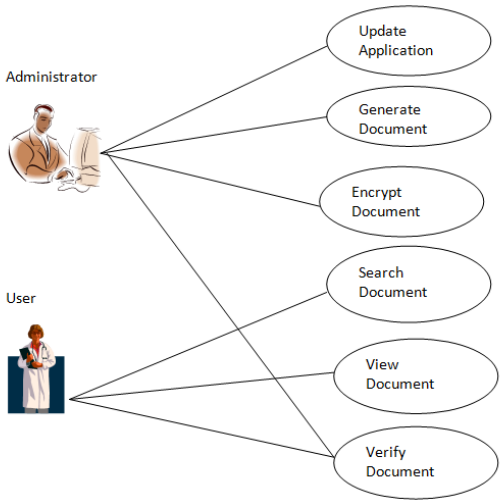

Figure 1 Use Case Diagram

This is a visual representation of an information system to communicate connections between the data structures is as shown in figure 2

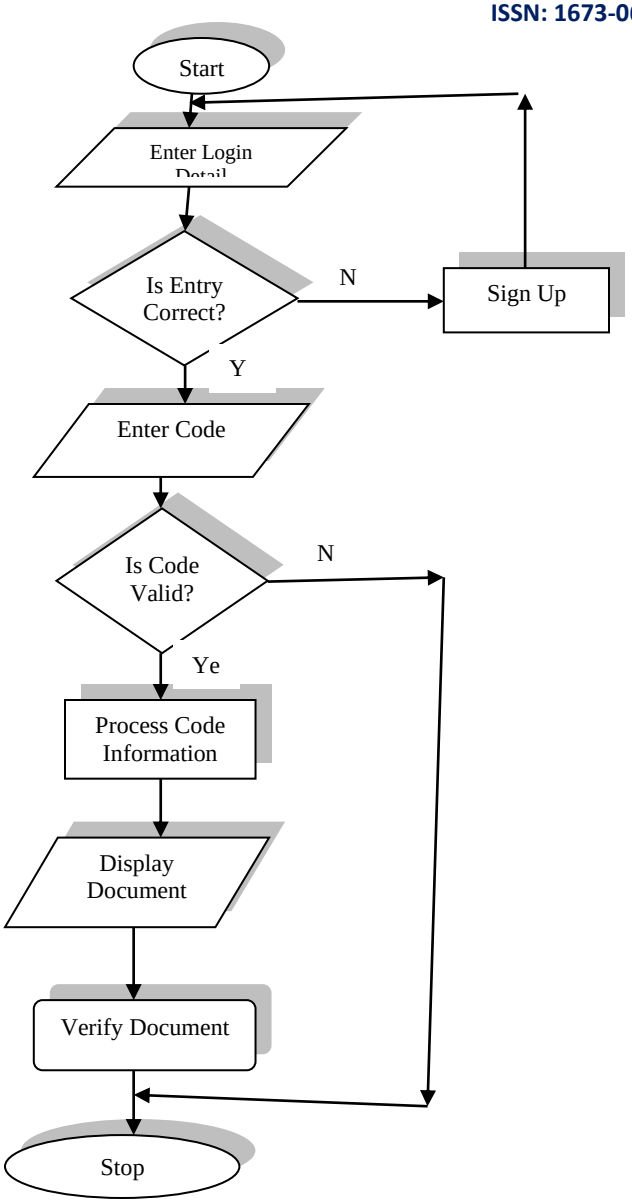

Figure 2 System Flow Chart

IV. METHODOLOGY

The research methodology for the project was designed to ensure a comprehensive, secure, and scalable system. The approach followed a structured plan that incorporated various technologies and tools to achieve document generation, verification, fraud detection, and encryption. Below is a detailed breakdown of the methodology, including system design, development phases, technology integration, testing, and evaluation.

A. System Design

The system was divided into front-end and back-end components. The front-end focused on the user interface (UI) design for document generation and verification while the back-end focused on data processing, QR code encryption, blockchain integration, machine learning-based fraud detection, and secure storage.A multi-tier architecture was developed, involving user interfaces, application logic, and secure database.

B. Front-End Development

The technology used included HTML, CSS, JavaScript. Thus, a simple, intuitive UI that allows users to input document data and generate QR codes was designed. Also, a developed functionality for scanning QR codes for document verification using standard mobile devices and desktop platforms was achieved.

C. Back-End Development

A secure document generation, encryption, storage, and verification processes was implemented. The technology used included PHP, Python (Flask), and MySQL. For document generation, PHP and Python scripts were used to generate documents in various formats (e.g., PDFs) with embedded QR codes. Generated QR codes were encrypted using advanced encryption standards (AES-256). Each code contained metadata about the document, ensuring tamper-proof verification.MySQL was used to store documents and QR codes in an encrypted format. Documents were securely stored with access control mechanisms, ensuring only authorized users could retrieve or modify the documents. Python's Flask framework was used to integrate a private blockchain for tracking document transactions. The blockchain recorded every action (generation, modification, verification) related to each document, ensuring an immutable history.

D. QR Code Encryption and Blockchain Integration

The tools used included QR code generation libraries, AES encryption, blockchain libraries (e.g., Hyperledger, Ethereum).A custom encryption algorithm was applied to the generated QR codes. The metadata within the QR code, such as document ID, creation date, and a digital signature, was encrypted before being embedded in the QR code. A private blockchain was set up to store document transactions. Each time a document was generated, a transaction was created in the blockchain, ensuring an immutable audit trail. QR codes were verified by comparing the data against the blockchain ledger.

E. Machine Learning-Based Fraud Detection

The technology used was Python (scikit-learn, TensorFlow), historical data of document transactions. A dataset of past document transactions and known fraud cases was collected and used to train the machine learning models. Several algorithms, such as decision trees, support vector machines (SVM), and neural networks, were evaluated to detect patterns indicative of fraud. Models were trained to identify anomalies, unusual access patterns, or tampering in documents. The system continuously updated itself by learning from new data over time.

F. Integration of Advanced Technologies and Novel Scopes

a. Blockchain simulation: Develop Python scripts to simulate blockchain behavior for document hashing and verification.
b. Machine learning: Implement Python scripts with Flask for server-side machine models (e.g. TensorFlow) for fraud detection.
c. API integration: Integrate PHP cURL library for API calls for external document verification services.
d. Audit trails and logging: PHP scripts to log document-related activities into MySQL database tables.
e. Smart contract simulation: Develop Python scripts to simulate smart contract behavior for automated document verification.
f. Zero-knowledge proofs (ZKPs): Implement Python scripts to demonstrate the use of ZKPs for privacy-preserving document verification.
g. Decentralized identity (DID): PHP scripts to integrate DID protocols securely linking user identities to documents.
h. Temporal blockchain anchoring: Develop Python scripts to anchor document timestamps on MySQL for immutable record-keeping.

Multi-party computation (MPC): Implement Python scripts with Flask for secure MPC protocols for collaborative document verification.

Table 3.1: Table illustrating a product backlog creation

ID	USER STORY
a-001	Create a database as well as all the tables required by the proposed system.
a-002	Create a log-in page with user authentication features (authorization code and hardware token)
a-003	Link the log-in page with the database table for users of the proposed system.

Figure 4.5 shows a generated document during the application testing encrypted with a QR code for verification and authentication

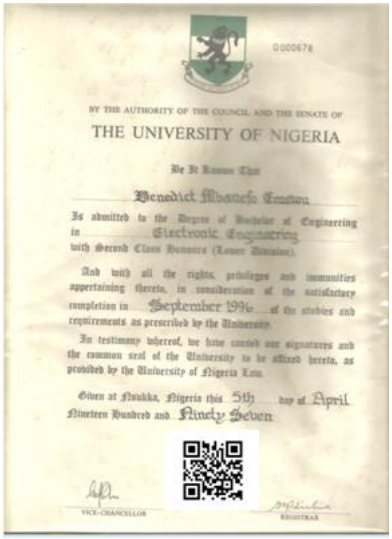
BY THE AUTHORITY OF THE COUNCIL AND THE SENATE OF
THE UNIVERSITY OF NIGERIA
Be It Known That
Benedict Mbanefo Emeka
is admitted to the Degree of Bachelor of Engineering
in Electronic Engineering
with Second Class Honours (Lower Division).
And with all the rights, privileges and immunities appertaining thereto, in consideration of the satisfactory completion in September 1996 of the studies and requirements as prescribed by the University.
In testimony whereof, we have caused our signatures and the common seal of the University to be affixed hereto, as provided by the University of Nigeria Law.
Given at Nsukka, Nigeria this 5th day of April
Nineteen Hundred and Ninety Seven
VICE-CHANCELLOR
REGISTRAR

Figure 4.5: Sample of Generated Document

V. CONCLUSION

i. Enhanced Security: The development of a web-based document generation platform, combined with QR code encryption and blockchain-based decentralized verification, significantly enhances the security and integrity of online document transactions.

ii. Fraud Prevention: The use of machine learning algorithms for fraud detection improves the accuracy of identifying fraudulent activities, while multi-factor authentication and API integration bolster the system's reliability and user trust.

iii. Real-Time Verification and Transparency: The platform's focus on real-time verification, along with comprehensive audit trails and logging mechanisms, reinforces transparency and accountability in document handling.

.

APPENDIX

REFERENCES

1. Arko, D., Karunia, S. L., Linda, E. E., and Aldi, D. (2023). Blockchain-based e-certificate verification and validation automation architecture to avoid counterfeiting of digital assets in order to accelerate digital transformation. [Unpublished manuscript].
2. Ashifa, O., and Sathya, E. (2019). Document fraud detection. *International Journal of Scientific Research in Computer Science, Engineering, and Information Technology*, **5**(2).
3. ID-Pal. (n.d.). Introducing ID-detect: Boosting document fraud detection. Retrieved from https://id-pal.com/introducing-id-detect-boosting-document-fraud-detection/
4. ISO/IEC. (2015). Automatic identification and data capture techniques-QR code bar code semiology specification.
5. Malsa, N., Vyas, J., Gautam, R., Shaw, N., and Ghosh, A. (2021). Framework and smart contract for blockchain enabled certificate verification system using robotics. *Stud. Comput. Intell.*,**960**, 125-138.
6. Maysaa, A. N., Eman, T. J., and Haider, M. A. (2020). QR code based two-factor authentication to verify paper-based documents. *TELKOMNIKA Telecommunication, Computing, Electronics and Control*, **18**(4), 1834-1842.
7. Omar, L., and Oleg, S. (2017). Binary large object-based approach for QR code detection in uncontrolled environments. *Hindawi Journal of Electrical and Computer Engineering*, **2017**, 1-15.
8. Oyediran, M. O., Elegbede, A. W., Olusanya, O. O., Awokola, J. A., and Sadipo, Q. B. (2021). Design and implementation of a certificate verification system using quick response (QR) code. *LAUTECH Journal of Computing and Informatics*, **2**(1), 35-40.
9. Rogel, L. Q., and Theda, F. G. Q. (2022). Document verification using quick response code with modified secure hash algorithm-1 and modified blowfish algorithm. *Indonesian Journal of Electrical Engineering and Computer Science*, **28**(1), 470-479.
10. Tripathi, A. (n.d.). What is document fraud and how to prevent it? Retrieved from https://www/docsumo.com/blog/document-fraud-prevention
11. Uzun, V., and Bilgin, S. (2016). Evaluation and implementation of QR code identity tag system for healthcare in Turkey. *SpringerPlus*.
12. Valleskey, B. (n.d.). Document Fraud: Definition, detection, and prevention. Retrieved from https://www.inscribe.ai/fraud-detection/document-fraud

AUTHORS

First Author – Emewu, Benedict Mbanefo, Ph.D, David Umahi Fedral University of Health Science, Uburu, Nigeria.
Second Author – Okpara, Chukwuemeka, Ph.D, David Umahi Fedral University of Health Science, Uburu, Nigeria.
Third Author – Okeiyi Euphemia K., M.Sc, Ebonyi State University, Abakaliki

Correspondence Author – Emewu, Benedict Mbanefo