AN ONLINE ACADEMIC DOCUMENTS AND CERTIFICATE VERIFICATION SYSTEM VIA SECURE USABLE AUTHENTICATING ARTFORMS

[1]Annie O. [2]Egwali, Franklyn C. Egwali, and [2*]John Ogene
[1]Department of Computer Science, University of Benin, Benin City, Nigeria.
[2]Department of Fine and Applied Arts, University of Benin, Benin City, Nigeria.

Abstract
The increasing global demand for higher education has led to a surge in fake degrees and certificates. Counterfeiters are scanning and printing sensitive documents, posing a challenge to the integrity of the academic community. Traditional verification methods are insecure and time-consuming, resulting in various risks for organizations. This research aim is to develop a secure online system that uses art-based graphical passwords to verify academic documents and certificates. The system targets employers, organizations, graduates, and institutions. The Transcript and Certificate Verification System (TCVS) adopted an Agile development methodology. The system will be developed as an online platform, leveraging authentication techniques commonly used in computer security. The research aims to deliver a secure online system that utilizes art-based graphical passwords for the verification of academic documents. It will provide a reliable and efficient method for authentication and validation, reducing the prevalence of forged certificates. The development of an online system using art-based graphical passwords has the potential to address the challenges posed by fake degrees and certificates. It offers a secure and efficient verification method, safeguarding the integrity of academic credentials. Employers, organizations, graduates, and institutions can benefit from increased reliability and confidentiality, protecting their reputation.

Keywords: Certificate Verification, Artforms, Fake Certificates, Verification, Risks, Forgery, Authentication

Introduction

Many factors have led to reduced operational efficiency in student services in many institutions. One of the most significant factors is the verification process for educational certificates and related documents. The certificate issued by educational institutions is one of the most important documents for a graduate. It is a proof of the graduate's qualification and can be used anywhere. However, due to identity theft, advances in printing and photocopying technologies, academic degrees are subject to corruptions, forgeries, and imitations. The problem statement highlights the reliance on manual verification procedures, leading to a lack of instant document authentication and difficulties for recruiters and employers in validating academic certificates. Certificates issued by many institutions have been forged. Fake certificates can be created easily and the quality of a fake certificate can now be as good as the original which makes these forgeries difficult to detect. Some employers concern comes or sends delegate to schools to verify a particular certificate, however, some employer never did and this has resulted in the acceptance of forged certificates.

Paper verification sets aside a long process to handle certificate verification on the grounds that the certificates need to return to the issuing institutions which is tedious and time wasting. To this end, the certificates end up not getting verified or are delayed due to long process. Certificate verification is necessary to ensure that the holder of the certificate is genuine and that the certificate itself comes from the right source.

Some universities have implemented online certificate verification systems, but existing methods are often insecure and time-consuming. The verification of certificates is a challenge for the verifier (the prospective employer who wants to verify the certificate). Employers need to authenticate the certificate from the certificate issuing authority. Presently, employers and other institutions takes much time for certificate verification to check the originality of the certificate. The overall certificate verification process also takes longer time to complete the selection process.

Also for automated online certificate verification systems, there is increased risk of unauthorized access through stolen identities which has potentially resulted in a direct loss of highly sensitive information. Researchers have proposed various systems to address these shortcomings, emphasizing the need for enhanced security measures and comprehensive applications. To counter identity attacks, most online systems employ the pedestrian predominant textual password authenticating model. However, although ubiquitous, textual passwords have lots of drawbacks from a usability perspective. This has resulted in the proposal and deployment of several other authentication models like token, graphical and biometric models, which have some deployment, security and usability drawbacks.

A past study on graphical password models make use of diverse composition of artform interfaces that have different security levels and that have a positive or negative effect on user's ability to remember their generated passwords (Egwali & Ogene, 2020). The study correlated artistic design elements of artforms and usable design elements of recognition based graphical password models (RGPM) in computer security. Results from the study revealed that using the principles of art was effective and reliable in a multifactor authenticating model level of security, usability and memorability as a result of a derivation of these artforms from standardized artform design principles. The strength of these artform authenticating models should be deployed in a real life setting that is both secured and usable.

The justification of the study is supported by Emele, oguoma, Uka and Nwaoha, (2020), who argue that existing online certificate verification systems lack sufficient security measures against forged university transcripts. Oyediran, Elegbede, Olusanya, Awokola, and Sodipo (2021) recommend enhancing the certificate verification system by reinforcing encrypted codes with tamper-resistant information. There are several units in an Institution, but this study focuses on certificate verification. This research will propose and design a secure online academic documents and certificate verification system via a secure usable artforms multifactor authenticating model using the University of Benin (UNIBEN) as a case study. The system will verify graduation certificates and preserve the confidentiality of the information in them. The system will be designed for employers or recruiters, organizations, graduates and institutions.

Related Works

Dey, Agoke and Shallah (2013) proposed a system that encrypts essential student data like name, roll number, marks, and grades before embedding them into a QR code printed on the student's mark sheet. This approach ensures data confidentiality and prevents unauthorized access or modification. Musee (2015) employed an Agile Methodology approach and Unified

Process modeling to develop a cloud-based prototype for certificate verification offered as a Software-as-a-Service (SaaS) solution. This prototype allowed users to request verification by entering details like institution name, course name, graduation year, and a verification code. The verification process occurred entirely within a private cloud and was accessible online. However, the system's reliance on a Relational Database Management System (RDBMS) limits its horizontal scaling capabilities.

Nwachukwu and Igbajar (2015) proposed an online certificate verification system with a top-down structure and an iterative model. This system can be implemented as a standalone application or integrated into a school's official website. While the system offers functionalities for certificate creation and management, its reliance on a relational database management system (RDBMS) for certificate storage can limit its scalability when dealing with very large datasets. Yusuf, Boukar and Shami-lunu, (2018) developed a system that enables users to define certificate templates without requiring XML knowledge. The system allows for importing student details via excel files, making it partially automated and potentially inefficient.

Singhal and Pavithra (2015) proposed a system that utilizes QR codes and smartphone applications to combat fake degree certificates. The QR code contains a digital signature over student data signed by university authorities. A dedicated smartphone application scans the QR code and verifies the certificate's authenticity. This system offers a faster and more cost-effective method for verification compared to manual verification processes. Obilukwu, Usman and Kwaghtyo (2019) proposed a Certificate Verification System for Institutions (CVSI) that utilizes a Top-Down Design approach with an iterative model. This system employs a NoSQL database (MongoDB) for certificate storage and Hypertext Preprocessor (PHP) for the front-end design. The proposed solution involves three parties: the university, the graduate, and the verifier, working together to achieve accurate certificate verification [6].

Clemens, Fabian and Dominik (2019) presented SPROOF, a public permissionless approach for issuing, managing, and verifying digital documents, offering transparency and integrity of the certificate. Dinesh et al. (2020) developed a Certificate Verification system that leverages blockchain technology. This system offers a verifiable ledger with cryptographic mechanisms to combat counterfeit academic certificates. Blockchain also provides a common platform for storing, accessing documents, and minimizing overall verification time (Nwachukwu and Ijagbar, 2015). Oyediran et al. (2021) developed a certificate verification system that utilizes QR codes to create a simple check for certificate authenticity. This system employs an advanced encryption standard method.

Elva and Besnik (2021) described a system with three main parts: a verification application, a university interface, and an accreditor interface. Their proposed solution aims to eliminate administrative barriers, expedite the deployment, verification, and validation of certificates, and enhance efficiency and security. Additionally, it offers data confidentiality through the use of the AES encryption algorithm before creating transactions and allows for bulk submission of multiple academic certificates.

Methodology

Existing System

University Graduation Result Processing

In the University of Benin (UNIBEN), following Senate approval, raw scores, formatted results (Senate Format), and GPA charts are transferred electronically from the Senate Floor to the Exams & Records office's Senate Matters Unit. This unit stores the approved results in a secure database.

(i) **Result Processing Software**: A dedicated program within the Exams & Records office converts the approved results into two electronic formats:
   a) **Microsoft Word Format:** This format includes student names (with appropriate prefixes like Ms. or Mrs.), course titles, degree classifications, academic sessions, and graduation years.
   b) **Microsoft Excel Format:** This format contains raw scores alongside student names, matriculation numbers, courses, degrees, and degree classifications.

(ii) **Result Distribution and Verification:** The Senate Matters Unit transmits the student names and details in Microsoft Word format to the Certificate Section of the Central Records Processing Unit (CRPU) for certificate preparation. Additionally, a final graduation brochure is printed, with a copy sent to the press.
   The Senate Matters Unit also sends the raw scores in Microsoft Excel format to the CRPU for verification of outstanding student fees. Once verified, the CRPU forwards the cleared results to their Certificate Section for certificate preparation. These certificates utilize a standardized name format: First Name, Middle Name, Last Name.

(iii) **Fee Verification and Certificate Issuance:** The CRPU verifies graduation fees with the student's department. If a student's fees are settled, their results proceed for Senate approval for certificate issuance. However, if fees are outstanding, the student's results are withheld, and the CRPU Certificate Unit holds back the certificate. The student can reclaim their certificate upon presenting proof of fee payment to the CRPU.

(iv) **Data Verification:** Finally, student details from the Microsoft Word format results (provided by the Senate Matters Unit) are cross-checked against the physical certificates received from the CRPU Certificate Section to ensure accuracy.

Certificate Verification Process

(i) The institution offers two convenient methods for verifying certificates. The first method involves utilizing the services of ETX-NG, a trusted third-party partner of the institution. This collaboration ensures a streamlined, efficient, and cost-effective verification process. Through ETX-NG, individuals can verify various documents such as degree certificates, academic transcripts, and statements of results. To initiate the verification request, individuals need to visit the ETX-NG Exchange website and navigate to the "Certificate Verification Request Forms" section, where they can select the University of Benin. Following the website's instructions, which may include filling out a form and uploading scanned copies of the certificate, individuals can proceed with the verification process. It is important to note that there may be a fee associated with the verification service facilitated by ETX-NG.

(ii) The second method entails direct verification through the institution itself. The university has established a dedicated portal for certificate verification requests, accessible through the UNIBEN certificate verification portal (please note that the

provided link might not be official, but it contains relevant information). Although specific details about the process on this portal are currently unavailable, it typically involves registering on the portal, submitting scanned copies of the certificate and identification documents, paying a processing fee, and selecting a preferred method for receiving the verification results, such as in-person pickup or delivery.

Both methods offered by the institution provide individuals with accessible and reliable means of verifying the authenticity of their certificates. Whether opting for the convenience of ETX-NG or the direct verification through the institution's portal, individuals can confidently ensure the validity of their educational credentials.

3.1.3 Current Transcript Request and Collection Process at the University

Information is provided about transcript requests on the University Alumni website: https://alumni.uniben.edu. The page typically outline the process, fees involved, and available delivery options. An applicant signifies interest by registering into the system. Next, login credentials are sent to the email address provided, and the system sends a confirmation message that the registration was successful. Subsequently, using the credentials provided, the applicant is required to download and fill out the transcript request form completely and accurately. This form usually asks for details like your full name, student matriculation number, ID number, degree earned (if applicable), the number of copies needed, and the recipient's address (if it is an international application, to send it directly to another institution/organization).

Transcript fee varies for the International Application or Local Application and if it is i**n-person or by mail to** the university provided by the applicant. The timeframe to process each request varies depending on the institution's workload. **The** University also typically offer several delivery options for transcripts, the applicant can pick up the transcript in person from the Senate Matter's office by showing a valid ID or the University cam mail the transcript directly to the address provided by the applicant on the request form. This option might take longer depending on the chosen postal service. Tracking the package also depends on the chosen delivering service.

Issues and Challenges of the Existing System

The existing system outlined in the provided content presents several issues and challenges. Here are the identified concerns:

(i) University Graduation Result Processing:

a) **Manual Conversion and Storage**: The process of converting and storing Senate-approved results in a digital format appears to be manual, which increases the risk of errors and inconsistencies. Depending on a program within the Exams & Records office for this conversion introduces potential data inaccuracies.

b) **Multiple Formats**: The system generates results in both Microsoft and Excel formats, leading to confusion and compatibility issues when sharing and handling results across different departments and units.

c) **Verification of School Fees Payment:** The current process of verifying school fees payments by the CRPU Certificate Unit is manual and time-consuming. It involves cross-referencing student details from the results with the CRPU Certificate, causing delays in issuing certificates.

(iii) **Certificate Verification Process:**
Lack of Information: There is a lack of available details regarding the certificate verification process, particularly the direct verification option through the dedicated portal. This absence of information may result in confusion and difficulties for individuals seeking to authenticate their certificates.

(iii) Transcript Request and Delivery:

a) Lack of Clarity: The content does not provide clear instructions on how to initiate a transcript request through the University Alumni website, making it challenging for users to navigate and understand the necessary steps.
b) Incomplete Information: The description of the transcript request process lacks details about processing times, delivery options, and tracking capabilities, leading to confusion and uncertainty for individuals requesting transcripts.

Overall, the existing system would benefit from enhancements in automation, data accuracy, transparency in the verification process, and the provision of clear and comprehensive instructions for transcript requests and deliveries.

The Proposed System
(i) Study Area
The research study area is UNIBEN, established as a model Institution of Higher learning which ranks among the best in the world and responsive to the creative and Innovative abilities of the Nigerian people. The University's mission policies are founded on the principles of fairness and equity, in the task of producing graduates who are worthy in learning and character. The University of Benin (UNIBEN) is a government owned tertiary institution, established on the 23rd of November, 1970. The University was established, first as Midwest Institute of Technology. After attaining the status of a full-fledged university in line with the requirement of the National Universities Commission on the 1st of July, 1971, the name was changed to the University of Benin. The Institution became a federal government owned University on the 1st of April, 1975.

The University, which commenced academic activities at the site of the Old Teachers' Training College on Ekenwan Road which is now one of the campuses of the University with 109 students; but now has an estimated 60,000 students' population that are spread across the two campuses of the University (Ugbowo and Ekenwan campus). The University has 15 Faculties, 1 College and 3 Institutes. Since the establishment of the University, it has continued to break new grounds in the realization of its goals of teaching, learning, research and community service. It undertakes programmes at various levels of graduate and postgraduate, for which students are admitted annually. It is important to note that nearly all courses offered at the University of Benin are, by 2021, fully accredited.

For over five decades of its existence, the University of Benin has grown to mentor other institutions that operate as affiliate institutions to the University. They include: Lagos State University, Akoka, Lagos; College of Education, Warri; College of Education, Asaba; College of Education, Mosogar, and the National Institute for Legislative and Democratic Studies, Abuja.

The University of Benin is also renown for collaborative researches with other universities - nationally and internationally – including the Lancaster University, England. Also, the University has gained national, regional and international recognition with its pioneering drive in several areas; it is the first University in Nigeria to award degrees in Industrial Chemistry, first Nigerian University to develop an indigenous software for the conduct of Computer Based Testing (CBT), first Nigerian University to award Ph.D in Optometry, first University in South South geo-political zone of Nigeria to establish a Faculty of Veterinary Medicine, and in 2011, the University was ranked as the number one University in West Africa by WEBOMETRICS. With an estimated 350,000 alumni, the Institution has continued to display its greatness which is evident in the human capital it has produced for Nigeria and the world.

(ii) Subjects

To establish the Performance Evaluation of the system, the proposed system will be implemented and tested using sample certificates of the University of Benin.

(iii) Data Collection

To enhance the general process of certificate verification, data collected sources will include three parties: the institution, the student graduate and a verifier system.

- ✓ the institution- It is proposed that the university issues a secret certificate verification code number to each graduate to ensure confidentiality. This number is given to the graduate at the point of receiving his/her certificate.
- ✓ the student graduate provides his/her matriculation numbers,
- ✓ Verifier system.

(iv) Data Analysis

This certificate verification system will try to follow the same process as it is in the University of Benin, and it will be online and automated. The research approach signifies a schematic view of the general solution to secure the paper certificates with encryption algorithms and using mobile scanner for authenticity verification. It will include the following phases:

Phase I: Generating the secret QR Code

A secure QR code will be generated based on the references to the student's profile records (Authenticating Credentials, Matric Number, Name, Class of Degree, Department etc.). The secret QR Code generation process will entail the following steps:

Step 1: Data Analysis:

QR codes generally are of four types of data which are; alphanumeric, numeric, Kanji and byte. The data types can be encoded into string of bits 1's and 0's in different ways. However, in this stage, data to be encoded are analyzed to determine the data type and the

proper encoding mode to be adopted. The matric number being considered here will be an alphanumeric data type therefore, the adopted encoding mode will be alphanumeric.

Step 2: Data Encoding:
The secret QR code data encoding process will include amidst others, choosing the error correction level i.e. the probability if extracted character is damaged or disfigured in the attempt to extract character, therefore, Error correction are used to restore the extracted characters. To achieve this, the appropriate error correction level must be selected. The appropriate level for the secret QR code for encoding matric number will be selected. This step will include:

(i) Determining the appropriate data version: QR code could be in different sizes called versions. A numeric mode and a specific version will be adopted
(ii) Determining the mode indicator: 0's and 1's in four-bit sequence will be used to indicate the chosen encoding mode.
(iii) Determining the character count indicator: character count indicator states the total number of characters to be encoded.
(iv) Encoding the input data: the chosen encoding mode will be used to encode the input data.
(v) Breaking up the intermediary bits into 8-bit code words: Since a specific version QR code in numeric mode is being used, 19 total data code words will be needed. The total number of bits needed for the QR code generation will now become 19 * 8 i.e. 152 bits.

Step 3: Error Correction
Errors occur due to inappropriate handling of secret QR code and which may challenge the integrity of the data encoded in the secret QR code; therefore, in the process of data encoding, code words needed to correct the errors are also generated. However, Reed-Solomon error correction technique will be used for error correction. It is the most commonly used error correction techniques which make use of polynomial long division as well as Galois field arithmetic in computing the error correction code words.

Step 4: Developing the mobile application to scan the QR code
A mobile application will be developed to decode, read and translate the encoded data information embedded in the QR code. Java software Development Kit versions 6 (JDK6) containing eclipse Integrated Development Environment (IDE) and Android Development Tools (ADT) eclipse plugin will be used for the mobile application development.

Phase 2: Certificate Verification
Each person or organization that want to verify the certificate can have the Authenticating credentials from the Student and type it into a field named "enter certificate number" and /or scan the embedded secret QR code on the certificate using the QR mobile scanner to establish its authenticity.

The system, will adopt the use of a NoSQL database (MongoDB) to store certificate details. The verification process is same as in the existing system, however, the implementation using a NoSQL database is a unique and key feature of the proposed model to improve on the

established existing system. It will use Java-Script Object Notation (JSON) to represent a schema-less arrangement. This database will consists of collections which host a group of MongoDB documents with different fields. The choice of MongoDB which is a document-oriented NoSQL database is considered here due to its Flexibility, Scalability, and partition tolerance, all of which makes it efficient even when data becomes very large as a result of the indexing capability of MongoDB. Figure 1 shows the proposed system architecture.

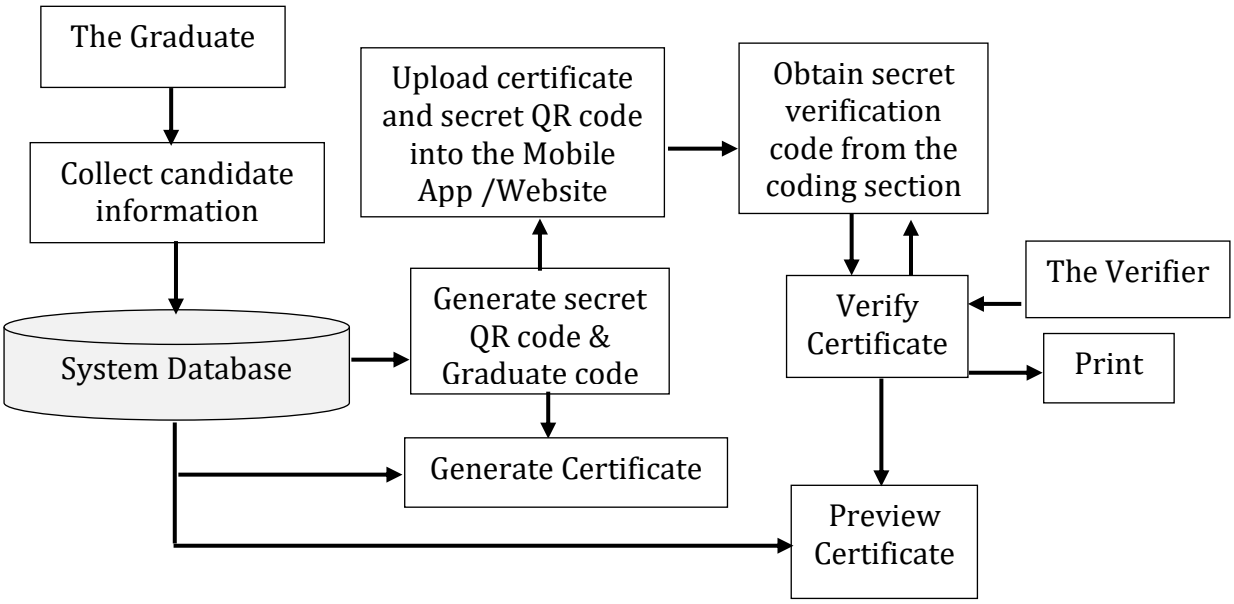

Figure 1: Architecture of Certificate Verification

Implementation

The Transcript and Certificate Verification System (TCVS) adopted an Agile development methodology, known for its flexibility and emphasis on continuous improvement based on user feedback. Specifically the Scrum framework, to ensure flexibility and continuous improvement based on user feedback. New features are incorporated throughout short development cycles called sprints. This iterative approach allows for new features and functionalities to be readily incorporated throughout the development process.

TCVS System Requirements

TCVS can be successfully implemented by meeting the following software and hardware requirements:

Software Requirements

- **Server-side:**
  - **Operating System (OS):** Ubuntu Server 20.04 LTS (Long Term Support) - a reliable and secure Linux distribution for server environments.
  - **Web Server:** Apache - a free and open-source web server software known for its stability and performance.
  - **Application Server:** uWSGI - a production web server gateway interface (WSGI) implementation in C that efficiently serves Python web applications.

  - **Python 3.9:** A high-level, general-purpose programming language used for TCVS's server-side development.
  - **Django Framework 3.2:** A high-level Python web framework that provides structure, security features, and simplifies common web development tasks.
  - **PostgreSQL 14 Database Management System (DBMS):** An open-source relational database management system that stores student information, transcript data, and other system records.
- **Client-side:**
  - Modern web browser (Google Chrome, Mozilla Firefox, Microsoft Edge) with JavaScript enabled - TCVS is a web application accessible through any modern web browser that supports JavaScript for interactive functionalities.

Hardware Requirements

- **Processor:** Minimum 4 cores, ideally 8 cores (e.g., Intel Xeon E-2388G or AMD Ryzen 7 3800X)
- **Memory (RAM):** Minimum 16 GB, recommended 32 GB (e.g., 4x 4GB DDR4 ECC RAM or 4x 8GB DDR4 ECC RAM)
- **Storage:** Minimum 500 GB Solid-State Drive (SSD) with additional storage for backups (e.g., 2x 500GB SSD in RAID 1 configuration for redundancy + separate hard disk drive for backups)
- **Network Interface Card (NIC):** A gigabit Ethernet NIC for efficient data transfer.
- **Uninterruptible Power Supply (UPS):** Protects the server from power outages and prevents data loss.

Development Phases

The development team started with Requirement Analysis, which involved workshops with representatives from students, external universities, and university administration. User stories were created to capture specific functionalities and user needs. Next came the Design phase, where wireframes and mockups were created to define the user interface (UI) for each user role. The system architecture was also designed with scalability and security in mind. The system was then built using using Python, Django framework, and PostgreSQL database. A relational database was chosen to store student information, transcript data, and other system records.

Rigorous testing (Unit testing, integration testing, and User Acceptance Testing) ensured the system functioned as intended. UAT involved students, external universities, and admins to guarantee the system met their specific needs and was user-friendly. Finally, TCVS was deployed in a staged manner. A pilot launch for a limited group of users was conducted before a wider rollout to the entire university community.

System Evaluation

Several methods were used to evaluate TCVS. The evaluation methods included User Acceptance Testing (UAT) which provided valuable insights into the system's usability from a real-world perspective. Performance Testing measured response times and ensured the system could handle anticipated user load. Security Testing assessed the system's vulnerability to cyberattacks and ensured data security. Surveys and Interviews gathered feedback from students and external universities.

The evaluation results indicated that TCVS successfully achieved its objectives of streamlining transcript and certificate requests and verification. The system proved to be user-friendly, secure, and scalable. Based on the feedback received, minor improvements were implemented to enhance the user experience. TCVS is expected to continue to improve efficiency and transparency within the transcript and certificate verification process at the University of Benin.

3 Results

The University of Benin Transcript and Certificate Verification System (TCVS) is a web application designed to simplify the process of requesting and verifying academic transcripts and certificates See figure 2). It caters to three distinct user groups: Students, External Universities, and Admins, each with specific functionalities.

4.1 User Roles and Functionalities

Students can register for an account or proceed directly to request a transcript/certificate if already registered .

Figure 2: Home Page

Students login credentials include the use of artforms that are effective and reliable in a multifactor authenticating model that increases the level of security (see figure 3), also included are a username and password with an additional layer of security through Multi-Factor Authentication (MFA), and a one-time password (OTP) sent to their email for verification.

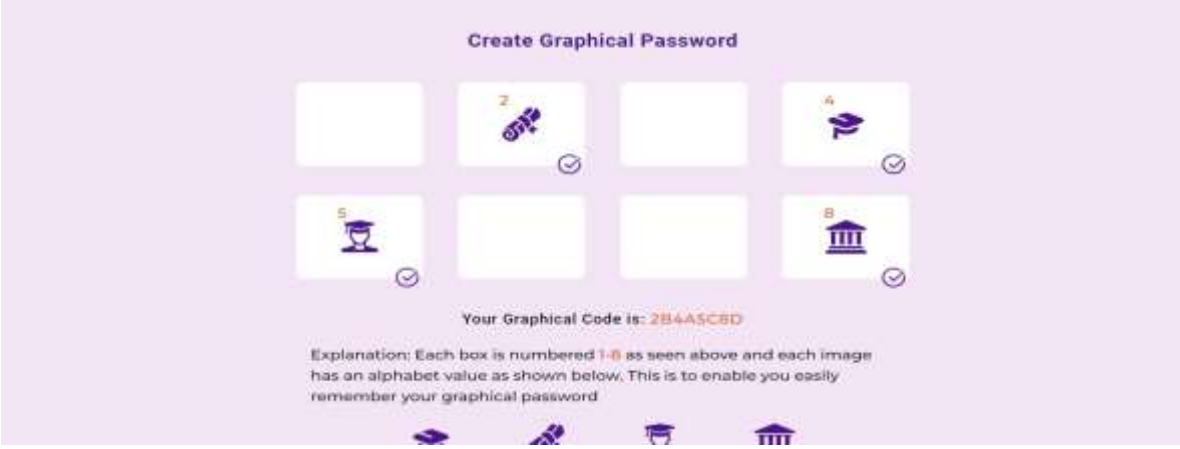

Figure 3: Artforms Graphical Authentication Page

The Student Dashboard (accessible after successful login) serves as a central hub for managing requests and profile information. Here, students can update details like faculty, department, and graduation session. Uploading required documents is crucial before initiating a transcript/certificate request, which can be for their own use or to grant access to an external university. Both functionalities require a holder fee payment processed through the integrated payment system. Students can track the progress of their requests, exchange messages with admins, and view their payment history. Once the transcript/certificate is ready, students can access it using a unique access code provided by the admins.

- **External Universities** can initiate a request for a student's transcript/certificate through the Landing Page (Figure 4). This involves providing their university email address, student name, and a letter of request. Upon verification by the admins, external universities receive login credentials to access the system and verify the authenticity of the student's transcript/certificate using an access code.

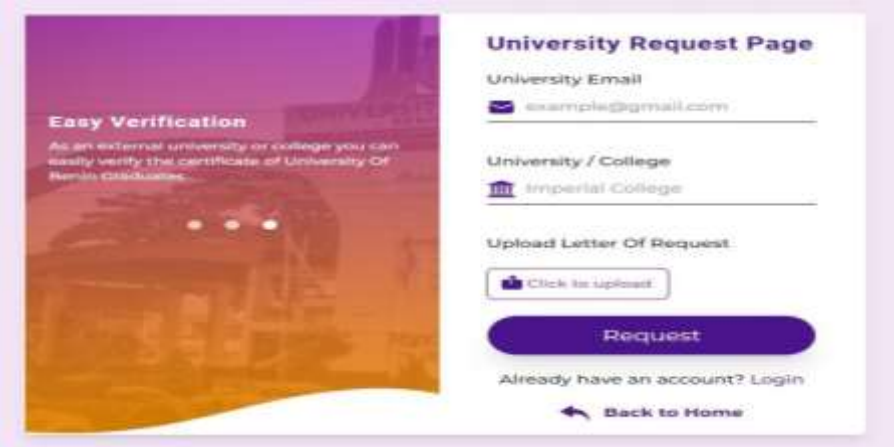

Figure 4: University Request Page

- **Admins (with Role-Based Access Control)** have functionalities tailored to their specific roles. CRPU Certificate Unit Admins can view student requests (Figure 5), including details like documents, messages, and replies to student inquiries. CRPU

Unit Admins, on the other hand, can download the Excel format uploaded by Exams and Records Admins. These Excel documents might contain a list of student requests or verification reports. Exams and Records Admins hold the responsibility of uploading the initial Microsoft Word and Excel documents required by other admins.

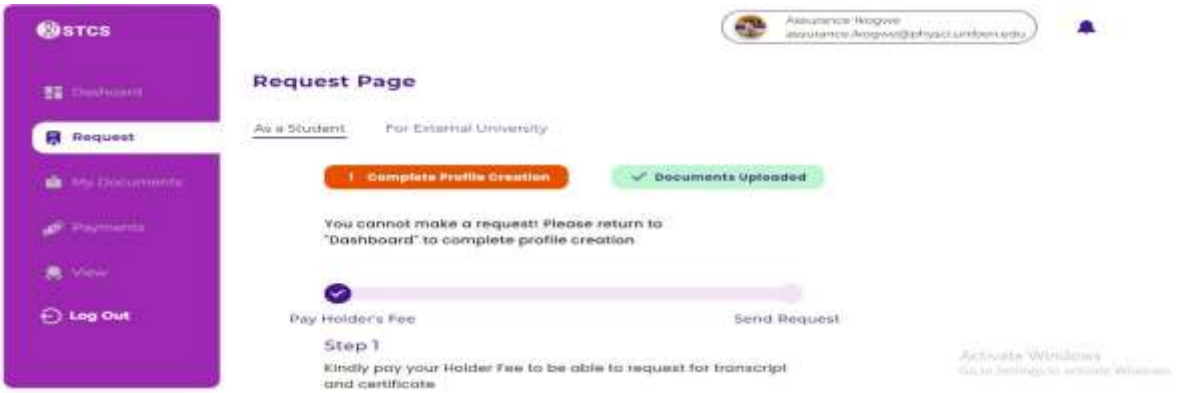

Figure 5: Request Page

Common functionalities shared by all admin roles include viewing university requests for verification, managing other admin accounts, viewing messages sent by them to students, and sending general announcements to all registered students.

- **Evaluation Results:** The UAT results indicated 95% user satisfaction with the system's ease of use and functionality. Performance Testing showed response times averaging 2 seconds under anticipated user load, and security testing identified no critical vulnerabilities. Feedback from students and external universities was overwhelmingly positive, highlighting the efficiency and transparency of the transcript verification process. Overall, the evaluation confirmed that TCVS successfully achieved its objectives.

Discussion

The discussion centered on a web application called the University of Benin Transcript and Certificate Verification System (TCVS). The research explored its functionalities, implementation process, and evaluation results. TCVS caters to students, external universities, and administrators with specific features for each group. Students can request transcripts/certificates, upload documents, track progress, and access verified documents. External universities can initiate verification requests and access transcripts with a verification code. Admins can manage requests, verify documents, and communicate with users.

The system was built using an Agile development methodology (Scrum) for flexibility and user feedback integration. Secure technologies and a relational database were used. The deployment was staged, starting with a pilot group. The system received positive feedback on usability, performance, and security through various testing methods (UAT, performance testing, security testing) and user surveys.

While successful, TCVS has limitations. Future plans include integrating with student information systems for automatic data retrieval, expanding supported document types, developing a mobile app, and implementing additional security features. TCVS likely offers advantages in user-friendliness, security, and transparency. TCVS has broader implications beyond the university. It improves efficiency for universities, enhances security against transcript fraud, facilitates international student mobility, and serves as a model for other institutions.

Conclusion

The University of Benin Transcript and Certificate Verification System (TCVS) demonstrates the power of user-centered design and Agile development methodologies. This web application streamlines the transcript verification process for students, external universities, and administrators, improving efficiency and transparency. The positive evaluation results highlight the system's usability, performance, and security. While limitations exist, such as the need for data integration and a mobile app, future enhancements are planned to address them. TCVS not only benefits the University of Benin but also presents broader implications for the educational landscape. It promotes efficiency, strengthens security against fraud, and fosters international student mobility. By serving as a successful model, TCVS paves the way for similar advancements in transcript verification systems across institutions.

Funding Acknowledgements: This research was sponsored by the Tertiary Education Trust Fund (TETFUND), which included the study design, data collection, analysis and interpretation of data.

References

Clemens, B. K. Fabian and Dominik, E. "SPROOF: A platform for issuing and verifying documents in a public blockchain", *5th International Conference on Information Systems Security and Security,* ISBN: 978-989-758-359-9, ISSN: 2184-4356, Vol. 1, pp. 15-25, 2019, Prague, Czech Republic, Published by Scitepress Digital Library, DOI: 10.5220/0007245600150025.

Dey, S. Asoke N. and Shalabh, A. (2013). "Confidential Encrypted Data Hiding and Retrieval Using QR Authentication System", *IEEE International Conference on Communication Systems and Network Technologies (CSNT)*.

Dinesh, K., Senthil, P., and S, K. D. (2020). "Educational Certificate Verification System Using Blockchain", International Journal of Scientific and Technology Research Volume 9, Issue 03, March 2020 Issn 2277-8616 82 ijstr,www.ijstr.org

Egwali, A. Egwali, F.and Ogene, J. (2020) "An Appraisal of Artform as Usable Design Elements of RGPM", *The Pacific Journal of Science and Technology.* Vol 21, No. 2, pp. 170 – 180.

Elva, L. and Besnik, S. (2021). "Development and Evaluation of Blockchain based Secure Application for Verification and Validation of Academic Certificates", *Annals of Emerging Technologies in Computing (AETiC) 5 (2)*

Emele, I., Oguoma, S., Uka, K. and Nwaoha, E. (2021). "An Enhanced Web Base Certificate Verification System", *Open Access Library Journal*, **7**, 1-15. doi: 10.4236/oalib.1106342.

Musee, M. (2015) "An academic certification verification system based on cloud computing environment", Vol 3, No. 1, pp. 55-88. Retrieved from http://erepository.uon,bi.ac.ke/bitstream/handle/11295/90179/Musee_An%20Academic%20Certification%20Verification%20Sytem%20Based%20On%20Cloud%20Computing% 20Environment.pdf?sequence=3&isAllowed=y.

Nwachukwu K.and Igbajar, A. (2015). "Designing an Automatic Web-Based Certificate Verification System for Institutions", *Journal of Multidisciplinary Engineering Science and Technology,* Vol 2, No. 12, 3159-0040. Retrieved from https://www.jmest.org/wp-content/uploads/JMESTN42351206.pdf

Obilikwu, P., Usman, K. and Kwaghtyo, K. D (2019). "A Generic Certificate Verification System for Nigerian Universities", International Journal of Computer Science and Mobile Computing, IJCSMC, Vol. 8, Issue. 10, pp.137 – 148.

Oyediran, M. Elegbede, A. Olusanya,O. Awokola J. and Sodipo, Q. (2021) "Design and Implementation of a Certificate Verification System using Quick Response (QR) Code", *LAUTECH Journal of Computing and Informatics (LAUJCI)* – ISSN: 2714-4194 Volume 2 Issue 1, – www.laujci.lautech.edu.ng

Singhal, A. and Pavithr, R. S. (2015). "Degree Certificate Authentication using QR Code and Smartphone", International Journal of Computer Applications, Vol. 120, No. 16, 0975–8887. Retrieved from https://docshare01.docshare.tips/ files/29369/ 293691731.pdf

Yusuf, D., Boukar M., and Shamiluulu, S. (2018). "Automated Batch Certificate Generation and Verification System", Conference Paper. Retrieved from https://www.researchgate.net/publication/324531116_ICECCO