BENIN JOURNAL OF PHYSICAL SCIENCES
BJPS Vol. 1(2), December, pg. 75-90 (2024)
ISSN 3043-6931(Print)
3043-694X(Online)
www.bjps.org.ng

DocVerify: A Service-Oriented Model for Academic Credential Integrity

F. O. OLIHA

Department of Computer Science, University of Benin, Nigeria

Received: 21/10/2024 ***Accepted:*** 11/12/2024

Abstract

The integrity of academic credentials has become a critical issue, especially in developing countries like Nigeria, where cases of certificate forgery and delays in transcript generation have been on the rise. In response to this credential pandemic, this study projects a service-oriented model – DocVerify for academic certificate verification within Nigerian academic institutions. A design science research methodology was adopted, combining the service-oriented architecture modelling language and the software-oriented heterogeneous architecture and platforms engineering approach. The methodology focused on the design of service models with a scenario-based evaluation using test parameters from already graduated participants. The model demonstrated integrity in the signature and verification services of academic credentials. The outcome established that once a certificate is issued and verified, it cannot be altered, indicating a significant reduction in the incidence of fraudulent certificates in circulation. The findings highlighted high satisfaction with the system's usability and adaptability toward restoring trust in academic qualifications issued by Nigerian universities. Furthermore, the reduction in administrative burden is a critical outcome of the system's implementation, aligning with global trends toward the automation of administrative processes in education. The study concludes with implications that the service-oriented verification model offers a viable solution for combating certificate forgery and improving academic credential verification processes. Future research should focus on addressing the identified limitations of DocVerify to facilitate wider adoption.

Keywords: Academic integrity, Academic credentials, Certificate verification, Document signature, SoaML.

1. INTRODUCTION

Academic certificate forgery and ineffective verification systems present significant challenges to educational institutions and employers globally as

*Corresponding author e-mail: oliha_festus@uniben.edu

revealed in the study by Nwaocha and Oloyede (2022). It was highlighted that most institutions, particularly in Nigeria do not have automated systems for the verification of academic credentials, and this easily permits forged certificates and delays in transcript generation (Gairola et al., 2024). In other literary works, it has been established that these institutions depend mostly on manual (or semi-automated) processes that are not only inefficient but also susceptible to fraud (Omogbhemhea and Akpojarob, 2018; Noorhizam et al., 2023; Umar et al., 2023). Moreso, Fortune, et al. (2024) extended this, noting that transcript generation and request in Nigeria is often a slow and cumbersome process. They further highlighted that graduates frequently encounter delays that can span several months, making it difficult for them to pursue further studies or secure employment. This is sad as institutions that still rely on traditional methods find it difficult to meet the increasing demand for secure, verifiable academic credentials (Kareem and Shakir, 2023; Al Ahmed et al., 2024). As a result, it is a widely acknowledged fact, that academic institutions in Nigeria face growing concerns about the authenticity of certificates and processing of transcripts (Ugochukwu et al., 2013; Kumutha and Jayalakshmi, 2022; Fortune et al., 2024; Sozon et al., 2024), and this further impedes the global recognition of their graduates' qualifications.

In existing and related literature, verification approaches often fail due to inadequate infrastructural challenges, particularly those encountered in developing regions; these challenges include the absence of centralized databases, poor infrastructure, and limited access to reliable digital solutions (Omogbhemhea and Akpojarob, 2018; Sultana et al., 2023). They are not just peculiar to the Nigerian case – the issue of certificate verification has gained global attention due to the rising cases of academic fraud, citing some developing countries in Asia like Bangladesh (Al Ahmed et al., 2024), Singapore (Kumutha and Jayalakshmi, 2022), etc. To mitigate these issues, academic institutions across the globe have increasingly adopted digital verification systems, employing technologies such as blockchain, cloud-based services, and decentralized databases (Effiong et al., 2022; Fortune et al., 2024). With the availability of these technological tools, various solutions have been proposed to enhance the verification and authentication of academic certificates for academic institutions seeking to maintain credibility and trust in their academic credentials (Ugochukwu et al., 2013; Omogbhemhea and Akpojarob, 2018; Nwaocha and Oloyede, 2022; Effiong et al., 2022; Umar et al., 2023; Fortune et al., 2024).

For instance, Sy et al. (2024) highlighted the development of EduCredPH, a system introduced in Asia to address challenges in educational credential verification. Although the concept of verification presented in the current study is aligned with such efforts, it does not significantly incorporate blockchain technology. Instead,

this study extends the notion to service orchestration, focusing on their digital management and verification. Similarly, SuperCert, as proposed by Gairola et al. (2023), was developed to foster anti-fraud measures in the verification of educational certificates. Their findings demonstrated the importance of digitalizing academic certificates, particularly through the use of digital signatures, which enhance seamless verification. This approach is particularly relevant to the present study, as digitally signed certificates offer strong protection against alterations, using public and private keys to secure the verification process.

More so, CredChain, introduced by Al Ahmed et al. (2024) for certificate verification in Bangladesh, sought to promote technological proliferation in educational institutions. Their results corroborated the findings of Gairola et al. (2023), acknowledging both the positive and negative impacts of technological applications in academic credential verification. Nonetheless, the present study critically examines these negative implications, aiming to combat fraudulent practices through an advanced technological approach. Another significant method identified in the literature was the use of QR codes for credential verification, as proposed by Noorhizam et al. (2023). QR Code technology provides a unique and efficient mechanism for verification, ensuring the integrity of verified documents. This trend of leveraging technology to counter fraudulent practices, as seen in various research efforts, has proven to be effective in promoting transparency and trust within academic systems. However, in the context of Nigeria, substantial gaps in research and application remain, as many academic institutions are yet to fully embrace technological solutions to address the pervasive fraudulent practices surrounding academic credentials, due to other notable factors bedevilling the adoption of digital verification systems, such as inadequate digital orientation, e-driven motivations, and resistance to change within academic administrative structures (Nwoaocha and Oloyede, 2022).

The present study sees a way to address some of these gaps via a technologically driven verification approach tailored to the fraudulent realities and challenges faced by Nigerian institutions. While this gap significantly motivates the study, it focuses on projecting a service-oriented model for academic credential verification within Nigerian academic institutions with specific markings to the University of Benin. The proposed solution leverages a service-based architecture to enhance the rapidity and timeliness of certificate verification processes, ensuring institutions can efficiently authenticate academic credentials and significantly reduce fraud.

Significantly, the study highlights that the impact of implementing a service-based verification system would not only address the problems associated with certificate forgery but also streamline the generation of academic transcripts. By addressing the issue of certificate forgery and transcript delays, this study has

contributed to the field of academic credential verification services offering a scalable solution to an increasingly national problem. Additionally, a critical outcome of the system's implementation is a tailored solution that considers the unique challenges faced by Nigerian academic institutions, offering a practical alternative to existing verification mechanisms. Other developing nations facing similar challenges in academic document verification could benefit from the study's expansion.

The rest of the paper is organized as follows: Section 2 projects the methods and techniques adopted for the study, highlighting the architecture design and analysis. Section 3 outlined the service integration and orchestration, while section 4 discusses the results and impacts. Conclusion and recommendation ended the paper.

2. MATERIALS AND METHOD

2.1 Study Design

The research employs a design science research (DSR) approach, which is commonly used in information systems research to create innovative solutions for complex problems (Delport et al., 2024; Gledson et al., 2024). The methodology incorporates both a design and evaluation approach, ensuring that the model is fit for implementation in real-world academic environments. DSR was chosen because it allows for the iterative development of a model that can be refined and evaluated based on feedback from stakeholders (Oliha and Usiobaifo, 2024). For a real academic domain, the University of Benin was chosen as a case study. Key stages in the research design include:

1. **Problem Modelling and Motivation:** A comprehensive review of existing literature and consultation with academic administrators of the University of Benin provided a clear understanding of these challenges. Thus, the issues of certificate forgery, delayed transcript generation, and lack of verification infrastructure were well associated with Nigerian academic institutions.
2. **Design and Development**: This stage involves the creation of a model that abstracts the core services of the domain of interest. By this notion, the service-oriented model was developed in this study as depicted in Figure 1, codenamed 'DocVerify', using a combination of cloud-based architecture and web service technologies.
3. **Demonstration and Evaluation**: The last stage of the DSR approach is evaluation. The proposed and developed model is evaluated using metrics such as system usability, certificate services, and verification processes. Feedback was gathered from selected university administrators and IT

personnel, who evaluated the system's ability to meet their operational requirements.

2.2 The Proposed Service-Based Model

The Software-oriented Heterogeneous Architecture and Platforms Engineering (SHAPE) approach was employed in the development of the proposed service-oriented platform. The SHAPE methodology excels in representing system components as services (Andrade and Crnkovic, 2018; Gemlau et al., 2021), leveraging the Service-Oriented Architecture Modeling Language (SoaML) to model service endpoints. Thus, the proposed service model is depicted in Figure 1.

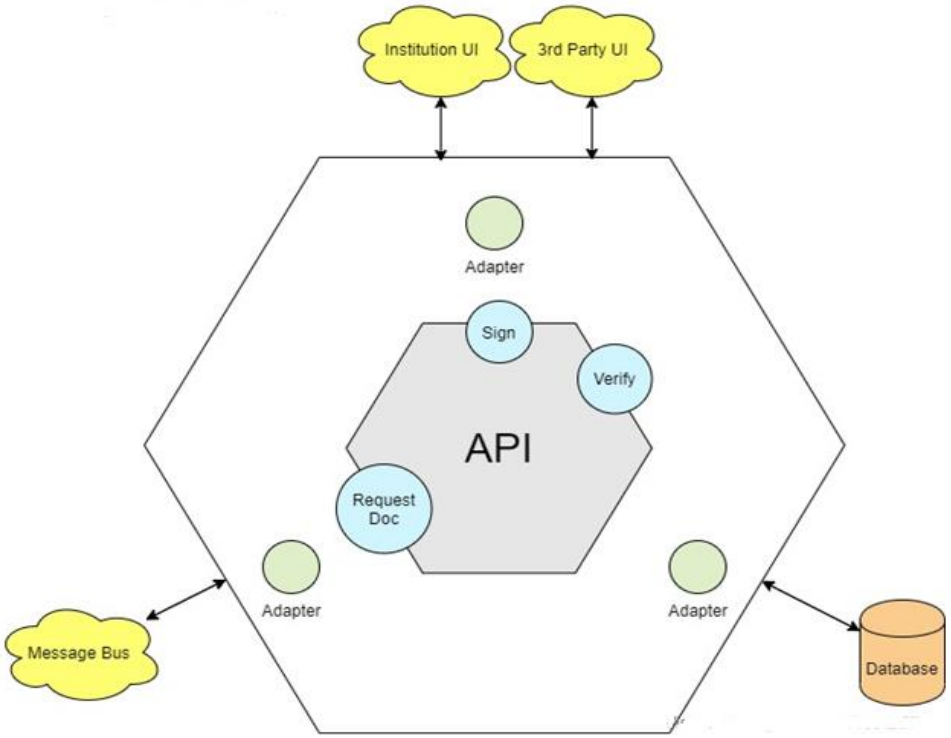


Figure 1: *The Proposed Service-Based Model for Academic Credential Services – DocVerify.*

The proposed architecture employs the hexagonal architectural principle (Gemlau et al., 2021) to abstract the interoperability, integration, and interactivity services of the target domain, specifically focusing on the University of Benin. In specific detail, the service architecture, guided by hexagonal principles and SHAPE methodology, integrates a mechanism where all service logic entering or leaving the application core passes through a port that isolates the application from external technologies, effectively decoupling the business logic from both the persistence and service layers. Consequently, the proposed architecture enables the detachment of external dependencies, allowing for the design of an inner core that seamlessly integrates with various user interfaces, including components for

institutions, databases, messaging systems, and third-party services, as illustrated in Figure 1.

2.3 Service Design Abstraction of the Proposed DocVerify

SoaML was adopted for service design modeling due to its universal standard as a domain-neutral modeling language, utilizing Unified Modeling Language (UML) to architect and model microservices (Elvesæter et al., 2018). It offers a unique perspective, helping to describe and understand services and their architecture using notations like interface, role, connector, capability, usage, exposure, participant, and port (Elvesæter et al., 2018; Yustianto et al., 2018). Figure 2. is a service model for the architectural coupling of how the entities of DocVerify interoperate to achieve a common service value and output as shown in Figure 2.

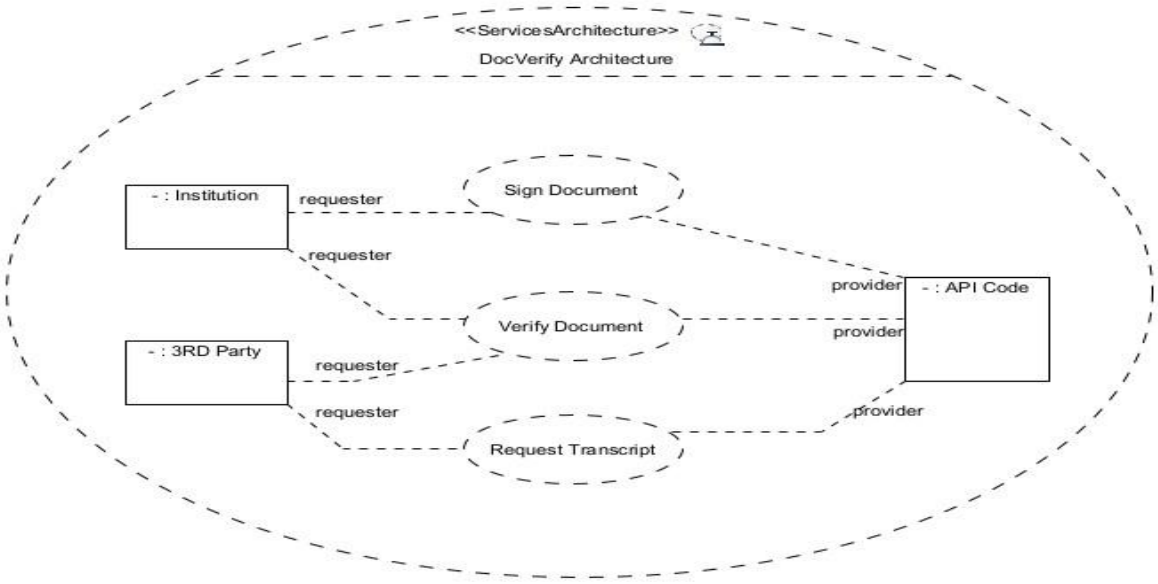


Figure 2: *Service Architecture Diagram for DocVerify.*

As captured in Figure 2., the architectural diagram for the proposed certification verification service entails the role of the requester for both the institution and the 3rd party clients while the role of a provider for the application programming interface (API) component. The architecture provides a service interface where the Institution and 3rd Party clients act as requesters while the API Code stack acts as the provider for the Sign Document service. Similar roles persist for the 'Verify Document' and 'Request Transcript' services for the Institution, 3rd Party, and API stack services.

2.4. Orchestration and Integration Service

In service-oriented computing, services are orchestrated with their dependencies to enable integration and performability across platforms (Oliha, 2022). The orchestration and implementation of the service-based model employed Postman;

a back-end integration tool for service integration and API communication between two or more service components. Postman is best known for its efficiency in modelling service systems and testing service endpoints (Pratik et al., 2022). Three main services were orchestrated for DocVerify namely: Signature, Verification, and Transcript. As depicted in Figure 3., panel A illustrated the various services implemented for the orchestration. The "Authentication" service integrated two service endpoints for registration and login as shown in panel B. These endpoints grant access that authorizes a service/user client to explore the services of DocVerify. With this service, an institution can register and gain access to verification or transcript services.

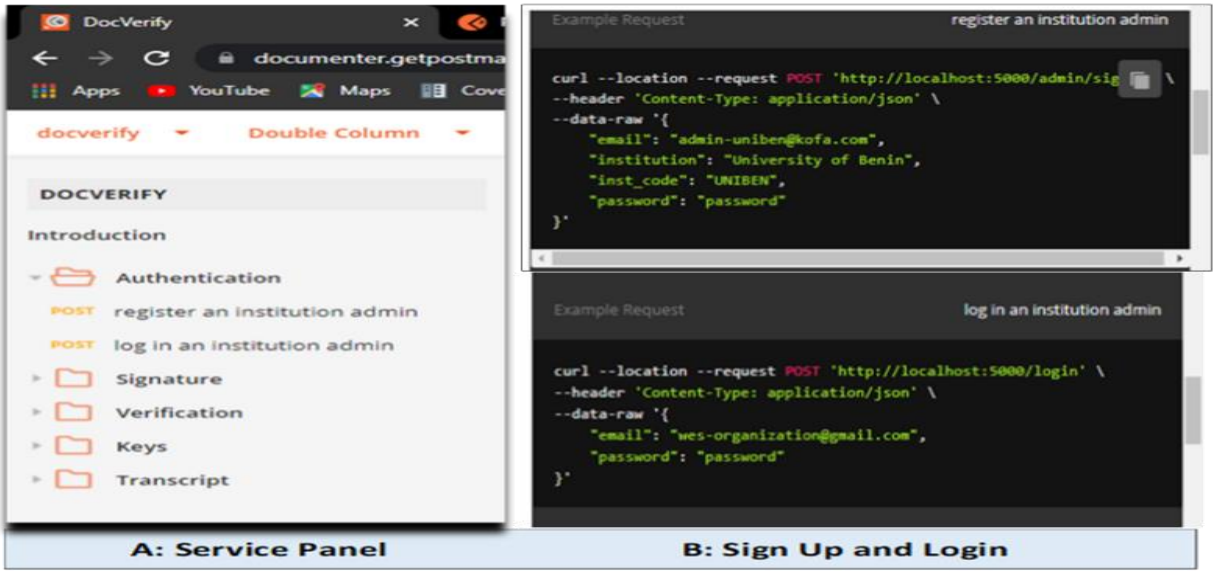


Figure 3: *Authentication Service for Sign-up and Login Endpoints.*

Figure 4. captures the Signature and Verification service endpoint orchestrations. Technically, to sign a document, DocVerify deploys a workflow that initially permits the creation of a document from an upload of a student's academic details: scores, grades, level, year of entry, graduation year, full name, matriculation number, course, etc., and then creates an identification number (doc_id) for the document with the aligning parameters. The signing process uses a Rivest-Shamir-Adleman (RSA) algorithm with the concept of asymmetric cryptography (Mohamad et al., 2021) to sign and return the status of the document with the unique ID assigned to it as shown in the signature service panel in Figure 4. It then digitally generates the key for verification from the Sign endpoint.

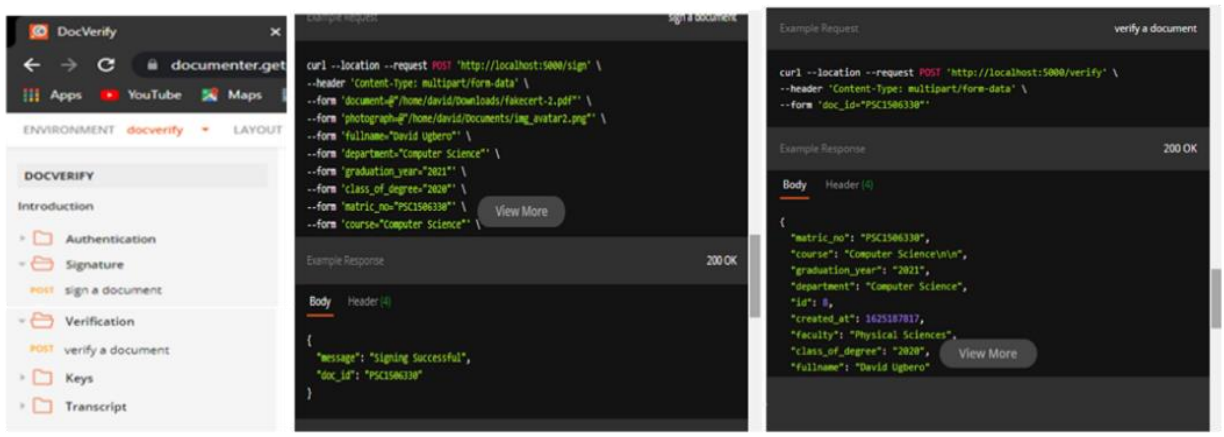


Figure 4: *Service Endpoints for Certificate Signature and Verification*

The panel for verification as depicted in Figure 4., requires the cryptographic component of the digitally signed document by which a QR code has been generated to indicate the digitally signed document as shown in Figure 7. The signature and verification cryptographic services adopt the key mechanism depicted in Figure 5. denoting that after signing, two keys are generated by the key service endpoint for private and public handshakes. The private key is generated when there is a request for verification and a public key is generated and returned upon the reception of the private key.

The orchestration for the transcript services integrated two endpoints for both the upload and request actions. To begin with, a transcript is only generated for a student who has completed or graduated from the institution according to policy. DocVerify generates transcripts in two ways: either by direct entry or by extracting from a .csv file from any storage location.

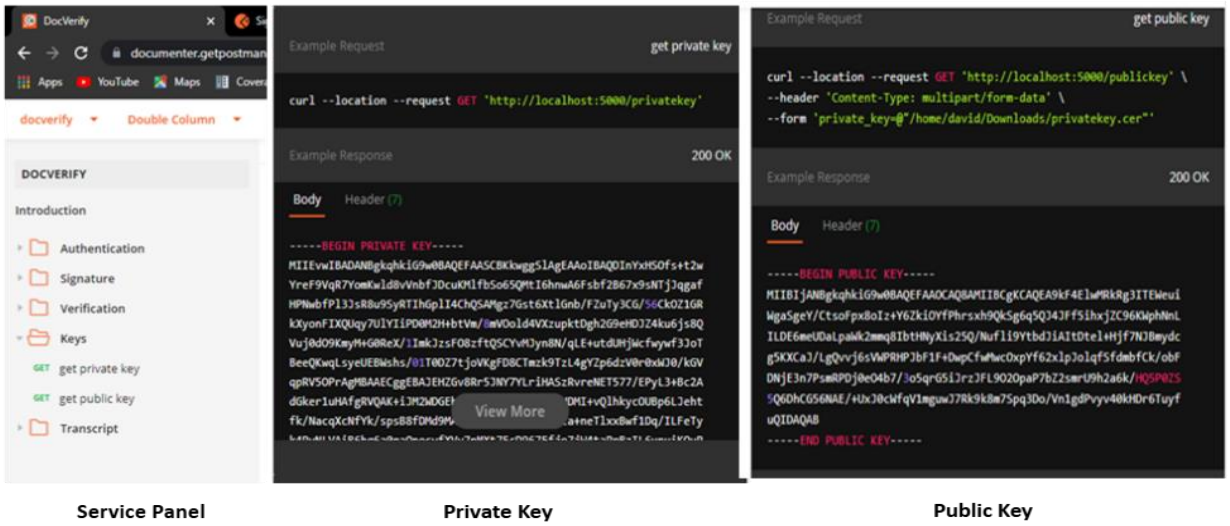


Figure 5: *Key Services for Document Signature and Verification*

Figure 6. depicts the upload and request service implementation for DocVerify; indicating that once a transcript is generated, it is added to the repository with a unique identifier for possible request consumption by third-party clients.

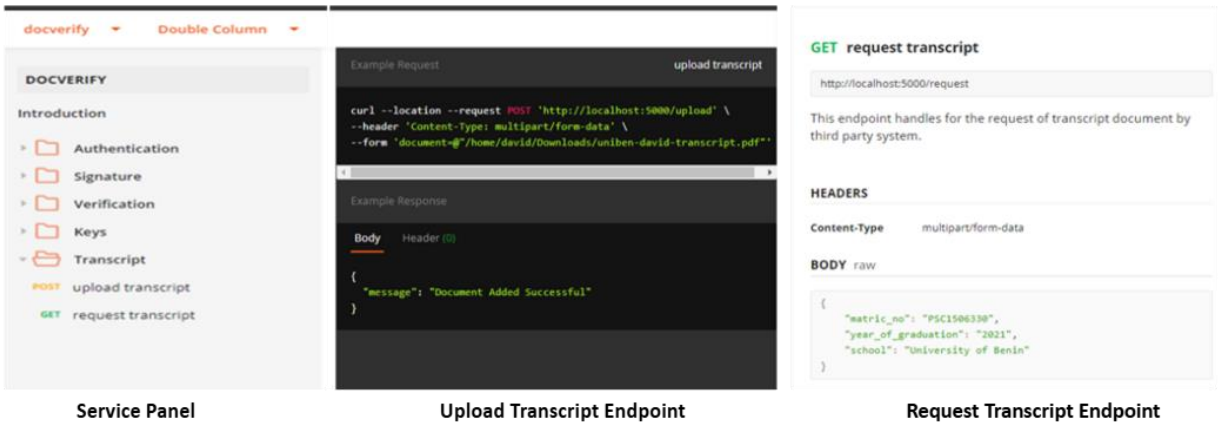


Figure 6: *Transcript Service Endpoints.*

3. RESULT AND DISCUSSION

A dataset of the case study alumni was utilized for evaluation of the service endpoints to ascertain its efficiency. However, all information pertaining to the student is solely for the purpose of evaluation. Thus, two scenarios were tested: the certificate verification and transcript services. These test cases showcased the performability of the service system in accordance with the design specifications.

3.1. Testcase One: Certificate verification.

Reiterating the concept of verification from Figure 7., every signed academic credential is assigned a unique identifier for the purpose of authenticity and verification. With this unique identifier, a query can be made on the DocVerify interface. The query string requires only the document ID. For example, the ID: 0000001', references a certificate with details of a student shown in Figure 7.

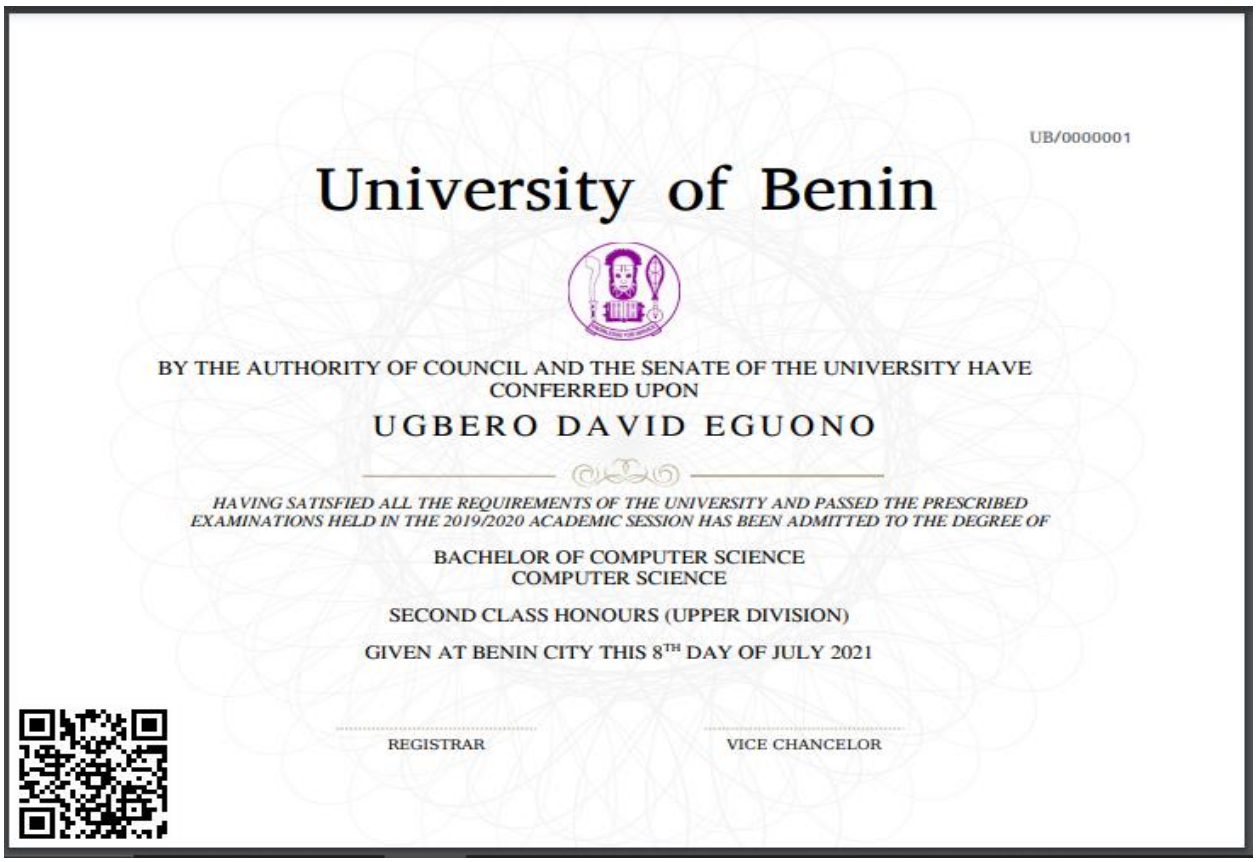
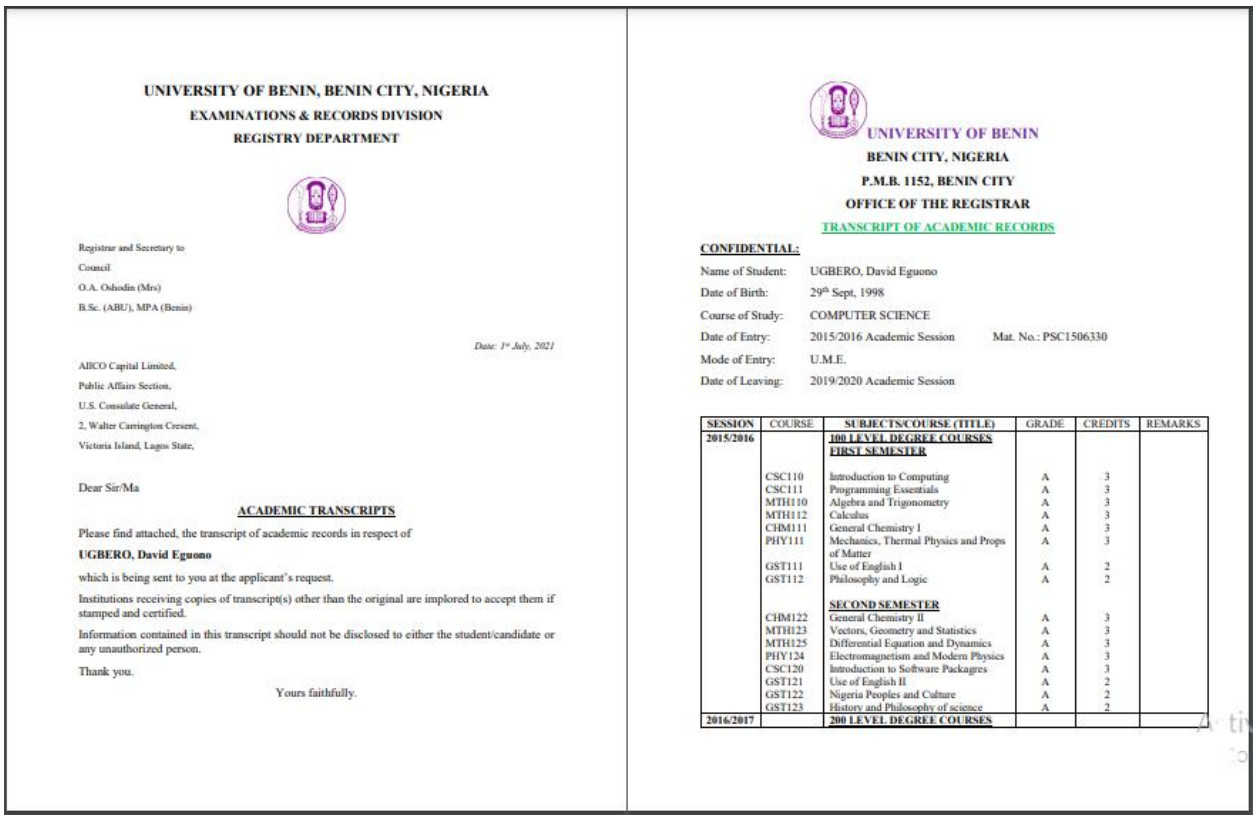


Figure 7: *Signed and Verified Certificate*

Figure 7 is the prototype of a digitally signed degree certificate for the student who graduated with a class of degree denoting the upper division from the Department of Computer Science, awarded in 2021. This prototype is adaptable for enhancement and hence, the printout copy is signed manually by authorized stakeholders (registrar and vice chancellor) to solidify the automation phase in essence. This is one of the objectives of the study to curb fraudulent practices associated with certificate fraud.

3.2. Testcase Two: Transcript Request and Generation

In this scenario, the transcript request and generation illustrate an instance of a transcript request service with parameters an interface of DocVerify. The outcome of this service results in a fully generated transcript depicted in Figure 8. with details of the requester's designated and recipient addresses from the institutional transcript service. A separate service endpoint is responsible for the makeup design. The transcript generated is poised of details including the courses and the grades from the year of entry to graduation for a particular request – only the sections depicting the recipient and detail page were captured for this study. This outcome justifies the efficiency of the DocVerify service solution.



UNIVERSITY OF BENIN, BENIN CITY, NIGERIA
EXAMINATIONS & RECORDS DIVISION
REGISTRY DEPARTMENT

Registrar and Secretary to
Council
O.A. Oshodin (Mrs)
B.Sc. (ABU), MPA (Benin)

Date: 1st July, 2021

AIICO Capital Limited,
Public Affairs Section,
U.S. Consulate General,
2, Walter Carrington Cresent,
Victoria Island, Lagos State,

Dear Sir/Ma

ACADEMIC TRANSCRIPTS

Please find attached, the transcript of academic records in respect of
UGBERO, David Eguono
which is being sent to you at the applicant's request.
Institutions receiving copies of transcript(s) other than the original are implored to accept them if stamped and certified.
Information contained in this transcript should not be disclosed to either the student/candidate or any unauthorized person.
Thank you.

Yours faithfully.

UNIVERSITY OF BENIN
BENIN CITY, NIGERIA
P.M.B. 1152, BENIN CITY
OFFICE OF THE REGISTRAR
TRANSCRIPT OF ACADEMIC RECORDS

CONFIDENTIAL:

Name of Student: UGBERO, David Eguono
Date of Birth: 29th Sept, 1998
Course of Study: COMPUTER SCIENCE
Date of Entry: 2015/2016 Academic Session Mat. No.: PSC1506330
Mode of Entry: U.M.E.
Date of Leaving: 2019/2020 Academic Session

SESSION	COURSE	SUBJECTS/COURSE (TITLE)	GRADE	CREDITS	REMARKS
2015/2016		100 LEVEL DEGREE COURSES FIRST SEMESTER			
	CSC110	Introduction to Computing	A	3	
	CSC111	Programming Essentials	A	3	
	MTH110	Algebra and Trigonometry	A	3	
	MTH112	Calculus	A	3	
	CHM111	General Chemistry I	A	3	
	PHY111	Mechanics, Thermal Physics and Props of Matter	A	3	
	GST111	Use of English I	A	2	
	GST112	Philosophy and Logic	A	2	
		SECOND SEMESTER			
	CHM122	General Chemistry II	A	3	
	MTH123	Vectors, Geometry and Statistics	A	3	
	MTH125	Differential Equation and Dynamics	A	3	
	PHY124	Electromagnetism and Modern Physics	A	3	
	CSC120	Introduction to Software Packages	A	3	
	GST121	Use of English II	A	2	
	GST122	Nigeria Peoples and Culture	A	2	
	GST123	History and Philosophy of science	A	2	
2016/2017		200 LEVEL DEGREE COURSES			

Figure 8: *Generated Transcript.*

3.3 Discussion

A service-based system was deployed with abstraction from a service architecture (Figure 1.) that modelled core features of a verification system to battle the prevalence of certificate forgery as highlighted in the recent and relevant literature (Gujar, 2023; Noorhizam et al., 2023; Sultana et al., 2023). To model such a system, the service interfaces and their interactions were modelled using SoaML designs as shown in Figure 2., illustrating a service-based DocVerify platform where multiple participants are involved in the process of signing, verifying, and requesting documents (such as transcripts). The institution (presumably a university) acts as the central provider of document services, while third-party systems and API services interact with it to manage requests. Each service interface represented different functionalities for document processing ensuring a separation of concerns by defining clear service endpoints and roles to also enable interoperability between various actors in the system. This makes the system more modular, scalable, and easier to maintain; a notion well-emphasized in the works of literature (Madana, 2016; Rai and Gangadharan, 2021).

The DocVerify Architecture demonstrates the interaction of various participants (like the institution and third party) with an API Code which serves as the central service provider that responds to requests from both the institution and third-party actors. This structure, as established by related literary works (Noorhizam et al., 2023; Al Ahmed et al., 2024; Gairola et al., 2024; Sy et al., 2024), is suitable for

service-oriented applications where service consumers (like institutions and third-party services) interact with a centralized API to perform document-related processes – a notable service functionality substantiated in related efforts such as SuperCred, CredChain, and EduCredPH.

Evaluating the resultant service integration while leveraging service-based architecture, service-oriented computing, and web services, the resultant verification outcomes demonstrate that the service-oriented model effectively addresses the credential integrity challenges faced by Nigerian academic institutions. This is an indication that the DocVerify system significantly improves the veracity of certificate verification processes for Nigerian universities and third-party employers like WES. This finding is akin to the outcome of Noorhizam et al. (2023) on the enhancement of the certificate verification process in academic institutions.

Several implications are drawn from the study outcome. First, the system's measure to reduce certificate verification times has significant implications for Nigerian academic institutions. This impact on the academic setting is attributed to the authentication and verification mechanism ensuring that once a certificate is issued and verified, it cannot be altered or forged. This greatly reduces the incidence of fraudulent certificates in circulation and restores trust in the academic qualifications issued by Nigerian universities. Also, with faster verification processes, universities can enhance their credibility both locally and internationally. Another significant implication lies in the critical outcome of the system's integration which plays a vital role in the reduction of administrative burden: that is, university staff who previously managed manual verification processes can now allocate their time to other important tasks, improving overall institutional efficiency. This aligns with global trends toward the automation of administrative processes in education (Sozon et al., 2024).

Although the system shows significant promise and allows for gradual integration, some factors might limit the adoptability of the proposed DocVerify. For example, resistance to change is a common barrier when implementing new technologies; thus, addressing this will require ongoing training and support for university staff to ensure that they can fully utilize the system's capabilities. For future direction, expanding the system's use across many institutions would further validate its scalability and effectiveness in diverse academic settings. While the DocVerify solution has been tested with two instances for a single university, potential research could focus on scaling the system to other academic institutions, regions and countries facing similar verification gaps in academic credential integrity.

4. CONCLUSION

The service-oriented model for academic credential verification has proven to be a promising panacea with a prototype solution for addressing the challenges faced by academic institutions in the Nigerian context. By reducing verification times, and improving the veracity of academic document verification services, the system offers a promising approach to improving the credibility and integrity of academic credentials in Nigeria. Significantly, the ability to quickly verify academic credentials ensures that employers and other educational institutions can trust the authenticity of Nigerian graduates' qualifications. This, in turn, improves the global employability of graduates and enhances the reputation of Nigerian institutions. However, challenges such as data migration and technology adoption must be addressed to ensure broader adoption and long-term success.

CONFLICT OF INTEREST

No conflict of interest was declared by the author.

ACKNOWLEDGEMENT

All names and information used for evaluation in this study were fictitious and solely for the purpose of research.

REFERENCES

[1] Al Ahmed, S., Mamun Rudro, R. A., Prity, A. J., Saha, S., Mansoor, N. and Nur, K. (2024). CredChain: Academic and professional certificate verification system using blockchain. *International Conference on Advances in Computing, Communication, Electrical, and Smart Systems (iCACCESS)*, Dhaka, Bangladesh, 1-6. https://doi.org/10.1109/iCACCESS61735.2024.10499520

[2] Andrade, H. and Crnkovic, I. (2018) A review on software architectures for heterogeneous platforms. *25th Asia-Pacific Software Engineering Conference (APSEC),* Nara, Japan, 209-218. https://doi.org/10.1109/APSEC.2018.00035

[3] Delport, P. M. J., Solms, R. V. and Gerber, M. (2024). Methodological guidelines for design science research. *Procedia Computer Science*, 237, 195-203. https://doi.org/10.1016/j.procs.2024.05.096

[4] Effiong, M., Norta, A., Udokwu, C., and Hattingh, M. (2022). Adoption of blockchain technology in academic certificate-verification systems. *IEEE 1st Global Emerging Technology Blockchain Forum: Blockchain & Beyond (iGETblockchain),* Irvine, CA, USA, 1-6. http://doi.org/10.1109/iGETblockchain56591.2022.10087108.

[5] Elvesæter, B., Berre, A., and Sadovykh, A. (2018). Specifying services using the service oriented architecture modeling language (SoaML) - A baseline for specification of cloud-based services. *Proceedings of the 1st International Conference on Cloud Computing and Services Science*, 276-285. https://doi.org/10.5220/0003393202760285

[6] Fortune, A. C., Garba, E. J., Usman, M., and Adaiti, A. K. (2024). Blockchain-enabled conceptual framework for enhancing academic transcript issuance and authentication in the Nigerian educational system. *International Journal of Development Mathematics (IJDM)*, 1(2), 227-236. https://doi.org/10.62054/ijdm/0102.19

[7] Gairola, A., Shaikh, A., Salian, S., Malve, S. and Jangid, P. (2024). SuperCert - An anti-fraud identity intelligence blockchain solution for educational certificates. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*, 10(2), 541-550. https://doi.org/10.32628/CSEIT2410266

[8] Gemlau, K. B., Köhler, L. and Ernst, R. (2021). A platform programming paradigm for heterogeneous systems integration. *Proceedings of the IEEE*, 109(4), 582-603. https://doi.org/10.1109/JPROC.2020.3035874

[9] Gledson, B., Rogage, K., Thompson, A. and Ponton, H. (2024). Reporting on the development of a web-based prototype dashboard for construction design managers, achieved through design science research methodology (DSRM). *Architecture, Building and Construction*, 14, 335-340. https://doi.org/10.20944/preprints202312.1555.v1

[10] Gujar, V. (2023). Enhancing verification & authenticity through digital certificate generation with facial recognition for educational institutions: A case study of IndoAI app. *International Journal for Research in Applied Science & Engineering Technology*, 11(12), 2173-2179. https://doi.org/10.22214/ijraset.2023.57818

[11] Kareem, A., and Shakir, A. C. (2023). Review: verification process of academic certificates using blockchain technology. *Kirkuk Journal of Science*, 18(1), 62-75. https://doi.org/10.32894/kujss.2023.135876.1072

[12] Kumutha, K., and Jayalakshmi, S. (2022). Blockchain technology and academic certificate authenticity – A review. Expert Clouds and Applications. *Lecture Notes in Networks and Systems,* 209. Springer, Singapore. https://doi.org/10.1007/978-981-16-2126-0_28

[13] Madana K. R. C. (2016). Reliability and scalability of service-oriented architecture in web services: signature verification. In G. Sreedhar (Ed.),

Design Solutions for Improving Website Quality and Effectiveness, 342-356. IGI Global. https://doi.org/10.4018/978-1-4666-9764-5.ch015

[14] Mohamad, M. S. A., Din, R. and Ahmad, J. I. (2021). Research trends review on RSA scheme of asymmetric cryptography techniques. *Bulletin of Electrical Engineering and Informatics*, 10(1), 487-492. https://www.doi.org/10.11591/eei.v10i1.2493

[15] Noorhizam, N. K., Abdullah, Z., Kasim, S., Rahmi, I., Hamid, A. and Isa, M. A. M. (2023). Verification of Ph.D. certificate using QR code on blockchain ethereum. *International Journal on Informatics Visualization*, 7(3), 716-725.

[16] Nwaocha, V. O. and Oloyede, A. (2022). Towards the development of an enhanced certificate verification system for west african institutions. *Journal of Behavioural Informatics, Digital Humanities and Development Research.* 8(3), 79-85. https://doi.org/10.22624/AIMS/BHI/V8N3P7

[17] Oliha, F. O. and Usiobaifo, A. R. (2024). Building academic integrity and scholarly reputation: an emphasis on institutional repositories. *Benin Journal of Physical Sciences*, 1(1), 148-165.

[18] Oliha, F. O. (2022). Assessing the performability of a fault tolerant architecture for web services solution using software fault injection. *International Journal of Computing and Digital Systems*. University of Bahrain, 12(1), 1243-1256. https://dx.doi.org/10.12785/ijcds/120199

[19] Oliha, F. O. (2022). Guaranteeing performance in a fault-tolerant service-oriented architecture. *Journal of Information and Communication Technology*, Universiti Utara Malaysia. 21 (4), 595-625, https://doi.org/10.32890/jict2022.21.4.6

[20] Omogbhemhea, M. and Akpojarob, J. (2018). Development of centralized transcript processing system. *American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)*, 39(1), 235-243.

[21] Pratik, P. K., Mayuresh, J. L., Madhusudan, T. S. and Snehal, J. (2022). API testing using postman tool. *International Journal for Research in Applied Science & Engineering Technology*, 10(12), 841-843. https://www.doi.org/10.22214/ijraset.2022.48030

[22] Rai, G. N. and Gangadharan, G. R. (2021). Model checking based web service verification: A systematic literature review. *IEEE Transactions on Services Computing*, 14(3), 747-764, May-June 2021, https://doi.org/10.1109/TSC.2018.2845401

[23] Sozon, M., Sia, B. C., Pok, W. F. and Alkharabsheh, O. H. M. (2024). Academic integrity violations in higher education: a systematic literature

review from 2013–2023. *Journal of Applied Research in Higher Education*, https://doi.org/10.1108/JARHE-12-2023-0559

[24] Sultana, S. A., Rupa, C., Malleswari, R. P., and Gadekallu, T. R. (2023). IPFS-blockchain smart contracts based conceptual framework to reduce certificate frauds in the academic field. *Information*, 14(8), 446. https://doi.org/10.3390/info14080446

[25] Sy, M. P. M., Marasigan, R. I. and Festijo, E. D. (2024). EduCredPH: Towards a permissioned blockchain network for educational credentials verification system. *12th International Conference on Information and Education Technology (ICIET)*, Yamaguchi, Japan, 2024, 434-439. https://doi.org/10.1109/ICIET60671.2024.10542756

[26] Ugochukwu O., Sanjo F., and Eweje O. W. (2013). Creating pathway for enhancing student collection of academic records in Nigeria - A new direction. *Computer Science and Information Technology*, 1(1), 65 - 71. https://doi.org/10.13189/csit.2013.010108.

[27] Umar, A. B., Mohammed, M. M., Ahmad, Z. J., and Khalid, H. (2023). Design and implementation of a software result processing and transcript generation. *International Journal for Multidisciplinary Research*, 5(6), 67-75. https://doi.org/10.36948/ijfmr.2023.v05i06.10361

[28] Yustianto, P., Doss, R., Suhardi, I. and Kurniawan, N. B. (2018). Consolidating service engineering ontologies: Building service ontology from SOA modeling language (SoaML). 2018 *International Conference on Information Technology Systems and Innovation (ICITSI),* Bandung, Indonesia, 555-561. https://doi.org/10.1109/ICITSI.2018.8695936