MULTIFACTOR AUTHENTICATION REQUIREMENTS FOR ACADEMIC CREDENTIAL

Ben Calvins Odhiambo[1*], Charles Ochieng' Oguk[2]

[1]Rongo University – Kenya, bodhiambo@rongovarsity.ac.ke*
[2]Rongo University – Kenya, coguk@rongovarsity.ac.ke

Corresponding Author:
**Email ID: bodhiambo@rongovarsity.ac.ke*

Abstract:

This paper investigates the current practices for academic credential authentication in Kenyan universities and establishes the functional requirements for a robust multifactor authentication (MFA) system to combat widespread document fraud. Drawing on a mixed-methods research design, primarily descriptive, data was collected through questionnaires, interviews, and observations from selected public and private universities and recruitment agencies. Findings reveal a high prevalence of fake academic credentials (80% of respondent universities experienced cases), highlighting the insufficiency of existing manual and single-factor authentication methods. The study details the observed manual verification processes and, critically, identifies the specific functional requirements necessary for modeling an effective MFA system, providing a scientific answer to a pressing practical issue. This research offers both practical and theoretical significance by enhancing security and integrity in academic credential verification and addressing a clear knowledge gap in this context.

1. Introduction

Background Context: Academic credentials are crucial for educational and professional progression, but their integrity is increasingly challenged by sophisticated fraudulent practices globally and locally. The absence of reliable verification practices creates significant gaps in trust and negatively impacts recruitment and public safety.

Problem Statement: Existing manual and single-factor authentication methods in many institutions, particularly in Kenya, are insufficient against the rising menace of falsified academic credentials. This leads to unqualified individuals holding critical roles and diminished institutional credibility.

Research Objectives:
This study aimed to:

i. Examine the current authentication practices being used to verify academic credentials in Universities in Kenya.
ii. Establish suitable functional requirements needed to develop a multifactor authentication model for academic credentials.

Significance of the Study: This research holds significant practical and theoretical implications by providing a blueprint for robust MFA systems to combat degree fraud, restore public trust, and contribute to positive societal change. Theoretically, it addresses a critical knowledge gap concerning specific MFA requirements and a suitable model within the Kenyan university context.

2. Literature Review

A comprehensive literature review is a cornerstone of a robust academic work, providing a thorough understanding of existing research and identifying crucial knowledge gaps that the current study aims to address (Marais, 2012; San Jose State University Writing Center, 2019). This section synthesizes extant literature on current academic credential authentication practices, critically reviews various document verification systems and multifactor authentication (MFA) approaches, and clearly articulates the identified knowledge gaps.

Current Authentication Practices

Historically, the verification of academic credentials in many institutions, including those in Kenya, has heavily relied on traditional, manual processes and paper-based methods (Namukose, 2018). These conventional approaches typically involve physical checks of documents, direct contact with issuing institutions, or the engagement of third-party agencies. Common manual practices observed include communicating directly with the issuing university, physically examining parameters on the certificate (such as the student's name, institutional details, certificate structure, wording, signature ink, and watermarks), and verifying institutional logos.

However, these traditional methods are increasingly inadequate and highly vulnerable to sophisticated forgery and fraud (Shende, Mullapudi, & Challa, 2024). The prevalence of fake and unmerited certificates has become a significant global challenge, profoundly undermining the integrity of higher education (Mulenga, Robert, & Shilongo, 2024). Advanced scanning and printing technologies allow criminals to easily produce counterfeit documents at low cost with high efficiency and quality, making them difficult to differentiate from authentic ones (Warasart & Kuacharoen, 2012). In Kenya, a substantial percentage of organizations, specifically 80% of those surveyed in one study, have reported encountering cases of fake and unmerited degrees, highlighting a rising global trend in academic fraud (KNQA, 2021). The ease of creating such fake certificates is partly attributed to insufficient transparency and verifiability in some issuing processes, leading to fraudulent documents being mistakenly accepted as genuine (Mulenga, et al., 2024).
Manual verification processes are time-consuming, tedious, repetitive, and labor-intensive (Namukose, 2018;). They can prolong the verification duration from minutes to weeks, depending on the availability of responsible officers and the patience of the requesting party. Human reliance in verification can lead to errors due to fatigue, unlike computerized systems that consistently detect discrepancies (Mulenga, et al., 2024). Employers and other organizations often experience difficulties authenticating documents instantly, frequently requiring physical visits or emails, which are costly and time-wasting. Furthermore, the current certificate verification process typically only verifies the document's details and validity but often fails to authenticate the certificate holder. This means the information provided might not be 100% authentic due to potential manipulation and falsification, and there is a significant lack of collective integration among institutions, making it difficult to provide firsthand information. Issues concerning privacy and confidentiality of student data also arise when third-party agencies are involved, as academic details are considered private data.

Document Verification Systems and Multifactor Authentication (MFA)

Document verification is defined as the process of establishing the authenticity, validity, and accuracy of a document, ensuring it is genuine and issued by an established body (Namukose, 2018). In today's digitized world, the need for secure and verifiable academic credentials is paramount for various professional and personal needs, ranging from job applications to validating competencies or pursuing further education (Zircon Tech, 2024). This critical need necessitates the exploration and adoption of more robust authentication models to safeguard integrity (Mulenga, et al., 2024).

Multifactor Authentication (MFA) is a security measure that requires multiple forms of authentication to confirm identity (Computer Security Resource Center, 2021; Lewis, 2024& Shacklett, 2021). It requires a user to provide two or more verification factors from independent categories (McKeown, 2020;). These factors typically include "something they know" (e.g., a PIN), "something they have" (e.g., a smart card or the physical certificate itself with unique features), and "something they are" (e.g., biometrics like facial recognition or fingerprint scanning) (Whitley, 2018). This approach aims to provide higher assurance of identity and significantly enhance security compared to single-factor authentication (SFA) (McKeown, 2020; Mulenga, et al., 2024;). The theoretical basis of MFA emphasizes the conceptual need for multiple, independent pieces of evidence to confidently confirm identity and document authenticity.

Several electronic verification methods have been proposed and implemented:

Online Academic Document Verification Systems: The case study by Namukose (2018) at Nkumba University designed an online system to computerize the verification of academic documents, allowing easy retrieval of accurate and timely information based on a unique serial number on transcripts. This web-based system made verification accessible 24/7 from anywhere. However, while digitizing the process, this system primarily verifies certificate details and validity but *does not explicitly authenticate the certificate holder.* It also highlights a lack of collective integration among institutions, making it difficult to provide firsthand information on qualifications.

QR Code-Based Systems: Studies have proposed using Quick Response (QR) codes for paper-based document authentication (Maysaa, Jasim, & Al-Mashhadi, 2020; Singhal & Pavithr, 2015). QR codes can hold extensive information to authenticate official documents and can be decoded by smart-phones. Some approaches involve encoding and printing unique QR codes on paper to prove validity, using hash algorithms to encrypt data for confidentiality before conversion to a QR code (Warasart & Kuacharoen, 2012). The verification process can be automatic or semi-automatic. However, critiques suggest limitations such as the absence of a trusted certification authority (Singhal & Pavithr, 2015) and the failure to authenticate the document holder.

Cloud Computing-Based Systems: Some academic certification verification systems have been developed using cloud computing environments (Musee, 2015). These systems, such as the one proposed by Osman (2016), aim to enhance verification, reduce forgeries, and improve security, validity, and confidentiality by utilizing a cloud-based model (Osman, 2016). Boukar, Yusuf, and Muslu (2017) also designed a web-based approach using JDBC and MySQL to replace traditional manual verification, retrieving certificate data from institutions and archiving it in a database to eliminate security threats and human error (Boukar, Yusuf, & Muslu, 2017). However, these systems often rely on Relational Database Management Systems (RDBMS) for data storage, which may struggle with horizontal scaling and managing huge amounts of data as data grows, becoming complex (Musee, 2015; Nwachukwu & Igbajar, 2015; Sumathi & Esakkirajan, 2008). MySQL, specifically, may not support very large database sizes efficiently, leading to system slowdowns (Boukar, Yusuf, & Muslu, 2017; Rohan, 2013).

***Blockchain Technology*:** This emerging technology is seen as a promising alternative to resolve issues of academic record forgery, record misuse, data tampering, time-consuming verification, and issues related to ownership and control, by increasing trust among entities (Kaneriya & Patel, 2023; Kumutha & Jayalakshmi, 2022; Mulenga, et al., 2024;). Blockchain-based solutions offer decentralization, immutability, integrity, privacy through selective disclosure, and enhanced security for educational digital credential issuance and verification (Alnafrah & Mouselli, 2021; Kaneriya & Patel, 2023; Saleh, Ghazali, & Rana, 2020). Proposed models utilize Ethereum Blockchain and smart contracts to automate data handling (Kaneriya & Patel, 2023). The application of blockchain features in multifactor authentication models can protect employers, employees, and the public from degree fraud (LifeHash, 2021). However, the application of blockchain technology in the education domain is still in an exploratory phase, requiring further research, standardization, and regulation to expand its use.

A robust verification system should ensure confidentiality, data integrity, non-repudiation, and authentication (Kuacharoen, 2012). Confidentiality means only intended people can access information, data integrity ensures information hasn't been illegally altered; non-repudiation means neither sender nor receiver can deny creation/transmission, and authentication verifies all parts of the document (Kuacharoen, 2012). The system should allow universities to upload and authenticate academic credentials, generating a unique verification key for the end-user (verifier) to access certificate holder details.

Furthermore, the advancement of predictive maintenance using machine learning highlights the suitability of multi-linear and non-linear models for solving real-time problems, even amidst ongoing discussions in the scientific community about their respective advantages in accuracy versus interpretability (Buhari & Sahu, 2022). New models that combine non-linear and multi-linear techniques are considered critical for developing more easily understandable solutions than those currently available (Buhari & Sahu, 2022). This aligns with the broader methodological perspective that quantitative and qualitative research approaches can be mutually complementary, offering a more nuanced approximation of the truth (Marais, 2012).

Knowledge Gap

Despite the existence of various authentication methods and systems, a critical gap remains: current methods, particularly manual and single-factor authentication (SFA), have proven insufficient against increasingly sophisticated fraudulent practices (Mulenga, et al., 2024;). While some digital solutions exist, they often fail to provide a comprehensive approach that authenticates both the document and the identity of the person presenting it (Namukose, 2018; ; Shende, Mullapudi, & Challa, 2024). The current certificate verification process primarily shows certificate validity but does not link the certificate holder to the certificate, leaving room for manipulation and falsification.

Many existing systems also lack robust implementation of critical security principles such as authorization, confidentiality, privacy, and ownership (Saleh, Ghazali, & Rana, 2020). Previous modeling approaches, relying on RDBMS, exhibit scalability limitations when dealing with massive datasets common in academic institutions (Hampo, 2012; Musee, 2015; Nwachukwu & Igbajar, 2015). Furthermore, while digital signature and QR code systems improve convenience, they often face security vulnerabilities, such as the absence of a trusted certification authority, or fail to explicitly authenticate the document holder (Maysaa, Jasim, & Al-Mashhadi, 2020; Singhal & Pavithr, 2015; Warasart & Kuacharoen, 2012).

Moreover, there is a lack of concrete, detailed MFA designs in existing literature that explicitly incorporate multiple distinct authentication factors (knowledge, possession, inherence) specifically for authenticating the verifier during the credential verification process (Kaneriya & Patel, 2023; Saleh, Ghazali, & Rana, 2020). While blockchain technology shows significant promise for secure credential verification, its application in the education domain is still in an exploratory phase, requiring further research, standardization, and regulation to expand its use and fully leverage its features like immutability and selective disclosure (Kaneriya & Patel, 2023).

This identified gap highlights the urgent need for a more precise, secure, and efficient system for authenticating academic documents and verifying the identity of credential holders against sophisticated fraudulent practices (Mulenga, et al., 2024). Therefore, this study aimed to address this critical gap by systematically establishing the specific requirements for and designing a robust multifactor authentication model, specifically tailored to the context of Kenyan universities, to provide a scientific answer to this pressing practical issue.

3. Research Design and Methodology

To achieve Objectives 1 ("Examine the current authentication practices for academic credentials in universities in Kenya") and 2 ("Establish suitable requirements for modeling a multifactor authentication system for academic credentials"), the methodology primarily leveraged a descriptive research design within a broader mixed-methods approach.

Methodology for Objectives 1 & 2

The research to examine current authentication practices and establish requirements (Objectives 1 and 2) predominantly employed a descriptive research design. This design was instrumental in systematically studying characteristics of the target population at a specific point in time, enabling the collection of data on existing practices and the elicitation of functional and non-functional requirements.

The target population for these objectives included all universities in Kenya (both public and private) and relevant recruitment agencies. A multiple sampling technique was applied, combining stratified, simple random, and purposive sampling. Stratified sampling categorized universities into public and private sectors, from which a simple random sample of seven universities (four public, three private) was selected using a 10% condition rule for representativeness. For in-depth insights crucial for establishing requirements, purposive sampling was used to select key informants, including System Administrators, Database Administrators, Academic Registrars (one from each sampled university), and two representatives from recruitment agencies, chosen for their expertise and information-rich perspectives.

Data collection relied on a robust combination of primary and secondary sources. Semi-structured questionnaires were the primary instrument for gathering quantitative and initial qualitative data on current practices from a broader range of respondents. Key Informant Interviews (KIIs) were conducted to obtain rich, in-depth qualitative data from experts on current practices and detailed requirements. Focus Group Discussions (FGDs) were particularly valuable for uncovering collective ideas and specific functional and non-functional requirements for the proposed model, covering aspects like data type, source, presentation, access, storage, and verification processes.

Observation provided first-hand information by critically examining current manual verification systems at sampled universities, validating insights from interviews. For secondary data, a comprehensive document review (journals, papers, textbooks) identified strengths, weaknesses, and missing links in existing systems, informing the conceptualization of the new model. All data collection adhered strictly to ethical considerations, including securing necessary permits from NACOSTI and Rongo University, obtaining informed consent, and ensuring confidentiality, anonymity, and protection of sensitive data.

Finally, the collected data underwent a tailored analysis. For Objective 1, qualitative data from interviews, FGDs, and observation was systematically interpreted into thematic areas and presented narratively, while quantitative questionnaire data was processed using descriptive statistics (frequencies, percentages) and presented in tables, graphs, and charts. For Objective 2, qualitative findings, especially from FGDs, were subjected to a rigorous requirements analysis process to generate the ultimate functional and non-functional requirements, presented in both narrative and tabular formats. This entire process ensured comprehensive understanding and concrete specifications for the subsequent design phase.

Findings and Discussion

Objective 1: To examine the current authentication practices being used to verify academic credentials in Kenyan Universities. The study found that existing methods for verifying academic credentials in selected institutions are predominantly manual and vary slightly from one institution to another. The process typically involves candidates submitting original or copy certificates, followed by the organization contacting the issuing university for a confirmation letter. Data revealed that 25% of respondents directly contact universities, while 60% scrutinize parameters like student names, logos, and document structure on certificates and transcripts.

A significant finding was the high prevalence of fraudulent documents, with 86.7% of surveyed organizations reporting cases of fake and unmerited degrees. This highlights a critical and globally reported issue. When fraud is detected, feedback is only communicated to the party that requested the verification in 71.0% of cases, with 29.0% revoking the credential but not communicating the outcome. This limited communication suggests a gap in public disclosure regarding academic fraud. Furthermore, the current manual verification process is inefficient, taking more than two days for certificate verification. These findings underscore the urgent need for a more secure, efficient, and transparent authentication method.

Objective 2: To establish requirements for modeling multifactor authentication systems for verifying academic credentials. Based on current practices and discussions with system and database administrators, suitable functional requirements for the MFA model were gathered through Focus Group Discussions (FGDs). Key data fields recommended for capture include full names, ID Number, KRA PIN, Huduma Number, registration number, university name, date of graduation, course, certificate, transcripts, and passport photos. Academic institutions are expected to provide this data.

For unique identification, the ID number was highly recommended as the primary key, with Huduma Number and KRA PIN also suggested for future system enhancements. To maintain privacy and confidentiality, it was advised that end-users/verifiers should only access limited details, such as candidate names, university name, date of graduation, class of degree, certificate, and transcripts. Random/direct data access using the primary key was recommended for efficient data retrieval. The study also specified that only academic institutions should have the authority to update candidate data, such as creating new profiles or revoking credentials. The model design identified three key actors: global administrator, institutional administrator, and the end user/verifier, with their respective responsibilities outlined. The Django web application framework was used to model the application.

Conclusion and Recommendations

The study concluded that there is a *definite need for a robust system to verify academic certificates and the identity of their holders.* The developed multifactor authentication model's prototype was tested and found to be effective not only for verifying academic certificates but also transcripts and the certificate holder's authenticity. This demonstrates the potential of the MFA model to significantly contribute to controlling academic document fraud.

Recommendations

Based on the findings from examining current authentication practices for academic credentials (Objective 1) and the established requirements for a multifactor authentication system (Objective 2), the following recommendations are made for the subsequent phases of this research and broader implementation efforts:

i. **Prioritize Prototype Development:** A prototype or mini-system should be developed based on the comprehensively established functional and non-functional requirements to validate the conceptual framework and gather initial user feedback.

ii. **Inform Policy Development:** The detailed insights into current practices and identified gaps should inform and facilitate the enhancement of existing policies and procedures governing academic credential verification in Kenya.

iii. **Focus on Foundational Integration:** Future efforts, building on the established requirements, should explore the feasibility and specific architectural considerations for integrating any developed model with national identity management systems, such as the Huduma number system, to enhance biometric identification and verification.

iv. **Continuous Technological Review:** Ongoing research into diverse security and cryptography technologies, identified as key requirements, is crucial to ensure the developed solution is comprehensive, resilient, and adaptable for various institutional verification processes.

References

1. Abraham, N. (2015). Designing an Automatic Web-Based Certificate Verification System For Institutions (Case Study: Michael Okpara University of Agriculture, Umudike). *Journal of Multidisciplinary Engineering Science and Technology*.
2. American Council on Education. (2016). *Quality Dimensions for Connected Credentials*.
3. Fairhurst, M. C. (2005). Document Identity, Authentication and Ownership: The Future of Biometric Verification. *Department of Electronics, University of Kent*.
4. Kuacharoen, M. W. (2012). Paper-based Document Authentication using Digital Signature and QR Code. *International Conference on Computer Engineering and Technology*.
5. KNQA. (2021, February 16). Tackling the menace of Fake Certificates in Kenya. Nairobi, Kenya.
6. Lampson, B., Abadi, M., Burrows, M., & Wobber, E. (1992). Authentication in Distributed Systems: Theory and Practice. *Digital Equipment Corporation*.
7. Loucopoulos, P. (2005). *Requirements Engineering: From System Goals to UML Models*.
8. Meyers, B., Segreto, J., Lawrence, M., Hegen, D., Cleene, L., & Jakubowski, J. (2012). E-Verify.
9. Mitchell, O. (2015). Experimental Research Design. *Wiley Online Library*.
10. Musee, M. (2015). An academic certification verification system based on cloud computing environment.
11. NIST. (n.d.). *Multi-Factor Authentication*. Retrieved from https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication.
12. O, M., & A, M. (2009). *Research Methods: Quantitative and Qualitative Approaches*.
13. Odhiambo, B. C. (2023). MULTIFACTOR AUTHENTICATION MODEL FOR ACADEMIC CREDENTIALS: A CASE STUDY OF UNIVERSITIES IN KENYA. *Rongo University*.
14. Shende, A., Mullapudi, M., & Challa, N. (2024). Enhancing Document Verification Systems: A Review of Techniques, Challenges, and Practical Implementations. *International Journal of Computer Engineering and Technology*, 15(1), 16–25.
15. Singh, A., Divya, & Jolanda, R. (2024). A Secure and Privacy-Preserving Student Credential Verification System Using Blockchain Technology. *Journal of Information Security Research*, 1(1), 1–10.
16. Trochim, W. (2006). *Research Methods Knowledge Base*.
17. Warasart, M., & Kuacharoen, P. (2012). Paper-based Document Authentication using Digital Signature and QR Code. *2012 4th International Conference on Computer Engineering and Technology (ICCET 2012)*.