International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 1135-1141www.ijaem.net ISSN: 2395-5252

Strategies for Establishing Identity of Examinees in a Distance Learning Environment

Dr. MaryRose NgoziUmeh[1];Obiokafor, Ifeyinwa Nkemdilim[2]& Dr. Felix. C. Aguboshim[3]

[1]*Senior Lecturer, Department of Computer Science, Nnamdi Azikiwe University, Awka.Nigeria*
[2]*PG Student, Department of Computer Science, Nnamdi Azikiwe University, Awka.Nigeria*
[3]*Chief Lecturer, Department of Computer Science, Federal Polytechnic, Oko. Nigeria.*

Submitted: 10-03-2021 Revised: 30-03-2021 Accepted: 01-04-2021

ABSTRACT: Distance learning and its related contexts such as distributed learning, blended learning, and online learning have become ubiquitous and significant in realizing sustainable online teaching and learning. Learners and teachers, in a distance learning environment, seek for more convenient and new strategies for establishing the identity of examinees. Despite these global impacts of technological interconnections that have significantly increased the productivity and efficiency of learning and teaching roles in a distance learning environment, numerous investigations have shown that poor identification and authentication of examinees poses serious and high stake security challenges, especially in Nigeria. These security challenges resulted majorly from the high rate of identity theft among examinees. Effective strategies to determine the identity of examinees, and secure the confidentiality, integrity, and availability of examines' data, which is the pivot for sustainable online teaching and learning, have remained relatively nonexistent or unattended to. Online platform software developers in Nigeria lack strategies to determine the identity of examinees and minimize the high rate of identity theft among examinees. In this study, the authors explored a narrative review of vast works of literature that revealed significant information on the conceptual framework, existing systems that revealed the effective methods for establishing the identity of examinees. Using some keywords "Establishing of the identity of examinees", "identity theft", "identity security threats", "distance learning environment", etc., an electronic database search extracted peer-reviewed articles from the last five years. Results revealed that keystroke dynamics, voice biometric recognition can be adapted as a way of establishing the identity of examinees. The result from this study may minimize identity theft, and positively impact effective teaching and learning in a distance learning environment

Keyword: Identity theft, Voice recognition, biometric recognition, identity security, distance learning environment.

I. INTRODUCTION

Historically, validating the identity of students in a distance learning environment has not been without controversy. One of the challenges of distance online education was the establishment of convenient and effective strategies for identification and authentication of examinees in a distance learning environment that ensures that the student who registers in a distance learning environmentor program is the same student who participates and completes the program, and receives the academic credit. Choosing convenient and effective strategies:biometrics and Web Video Recording, standardized databases, face-to-face proctored Examinations, or Video Conference Proctor for establishing identity of examinees in a distance learning environment by software developers and education stakeholders are major important factors that affect identification and authentication of examinees in a distance learning environment (Bailie & Jortberg, 2019). The increased and ubiquitous nature of online learning has further led to an increased concern about security threats accompanying distance learning environment and examinations (Ramu & Arivoli, 2013). Our purpose in this study is to identify strategies to create convenient and effective identification and authentication of examinees in a distance learning environmentthat prevents identity theft and ensures credibility of their certificates

A provision of documental proofs of how distance learning institutions verify student identities to ensure academic integrity and credibility has become the topmost concern of

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 1135-1141www.ijaem.net ISSN: 2395-5252

educational accrediting bodies.In this paper, the authors reviewed some relevant professional and academic literature on strategies to create identification and authentication characteristics for examinees in a distance learning environment, and their implementation and strengths to mitigate security attacks, threats, and identity theft. The authors reviewed existing authentication features, and their benefits and constraints. Findings from this study may cause a tremendous technological impact because more distance educational institutions will embrace effective and convenient strategies for identification and authentication of examinees in a distance learning environment that ensure academic integrity and credibility. This may also bring about better communication of technological ideas among developers and educational stakeholders that will establish best practices and inculcate effective and convenient strategies for identification and authentication of examinees in a distance learning environmentin Nigeria.The findings from this study may encourage social change as more software developers and distance education stakeholders in Nigeria will learn and appreciate effective and convenient strategies for identification and authentication of examinees in a distance learning environment.A successful result of this study mayalso bring social change by advancing the use of other technology outlets that require effective and convenient strategies for identification and authentication that ensures credible identification.Furthermore, more distance learning institution will be accredited as proofs of students' identification and authentication becomes more visible to online institutional accreditation bodies.

1.1 Problem Statement

Establishment of convenient and effective strategies for identification and authentication of examinees in a distance learning environment,coupled with the assurance that the student who registers in a program is the same student who participates and completes the program, are crippled by inappropriate, non-sustainable, or virtually non-existent practices, awareness, and literacy campaign systems in Nigeria. The security threats to distance learning examinations pose some detrimental impacts and damages on the credibility of distance learning courses that make extensive use of online examinations. The general IT problem is the lack of convenient and effective strategies for identification and authentication of examinees in a distance learning environmentconvenient and effective strategies for identification and authentication of examinees in a distance learning environment. The specific IT problem is that some software developers and education stakeholders of distance learning systems in Nigeria lack strategies to create convenient and effective identification and authentication of examinees in a distance learning environmentthat ensures the credibility of their certificates.

1.2 Research Question

What are identification and authentication of examinees practices and strategies used by stakeholders to effectivelyensure the credibility of their certificatesof examinees in a distance learning environment in Nigeria?

II. LITERATURE REVIEW

The reputation of distant learning, especially in Nigeria has been questioned following the fact that cheating and student impersonation have posed serious gaps in the credibility of distance education, which need to be closed. In a distant learning environment, students are meant to submit their work remotely. This process normally passes through some identity verification challengesin order to be sure that the identity of a person taking online examination is same as the person who registered and completed the course work. Distance learning Education stakeholders are confronted with a crucial issue of efficient and convenient strategies for determining studentidentity that will ensure academic integrity and credibility to all, especially to educational accrediting bodies. Distance learning Education stakeholders are driven to adopt best technological identification innovationsthat are credible and free from security threats.

2.2 Existing Authentication Method

Sufficient evidences have shown that online examinations have better results than traditional exams (Paullet, et al., 2014; Ramu & Arivoli, 2013). However, following the track record of high identity theft involved in distance learning examinations, it is become extremely relevant to employ reliable,efficient and convenient student authentication system in an online examination(Goel, 2019; Li, et al., 2019).Reliable, efficient and convenient student authentication is one that attempts to verify students as who they claim to be. A reliable,efficient and convenient student authentication in a distance learning environment is one that verifies true students' identify and plays a key role in identify theft mitigation and security measures. In the face-to-face (traditional) examinations, authentication

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 1135-1141www.ijaem.net ISSN: 2395-5252

appears to be better supervised were verifying of students'identity could be through: a secure login and pass code, proctored examinations, or other identity theft security policies and practices that are effective in verifying student identification. Methods of authentication may include: knowledge based authentication, object based authentication, and profile based authentication, or biometrics based authentication such as face authentication, voice Authentication, and signature authentication. These methods of identification may not guarantee creditability for a distance learning environment. It is the credibility of authentication in a distance learning environment that guarantees its credibility among the students, and before the teachers, stakeholders, and online institutional accreditation bodies. Reliable,efficient and convenient student authentication is seen as the currency of any distance learning institution, and the legitimate proof for authentic academic results and certifications.

In this section, the authors aimed at identifying efficient and convenient strategies for determining studentidentity that will ensure academic integrity and credibility to all. Sufficient evidences have shown thatthe mainstream authentication strategies for determining studentidentity are based on user's knowledge, objects possession and biometric features (Griffiths, 2013; Monaco, et al., 2013; Paullet, et al., 2014). This authentication strategies perspective is supported by Verhoeven, et al. (2019) who claimed that identity authentication in a distance learning environment comprised sociocultural perspectives, psychosocial perspectives, social psychological perspectives, and sociological perspectives. These perspectives suggest that identity authentication is complex and all-encompassing with some security measures undertone. Therefore students' identityverification strategies must integrate all perspectives with some security control automation potentials. There are existing evidences that demonstrate keystroke rhythm identity verification as a method that can reliably, creditably, and accurately determine user identity in a distance learning environment (Paullet,et al.,2014).Keystroke rhythm or keystroke dynamics or biometric keyboard identity verification method adopts a technique that scrutinizes user's typing style at their terminal keyboard by monitoring their keyboard inputs thousands of times per second (typing biometrics) in an attempt to identify their habitual typing rhythm patterns.

Researches by various authors under various contexts have confirmed that verifying students' identity in a distance learning environment by conventional user-id and password authentication is not sufficient (Abrar, et al., 2012;Alwi & Fan, 2010; Ramu & Arivoli,2013). Alwi and Fan (2010) opined that security threats resulting in cheating and student impersonation have been serious problems to the reputation and success of distant online learning in spite of its anticipated benefits.A more authentic way to identify and validate student identities, known as keystroke dynamics are beginning to be used (Paullet,et al., 2014). Keystroke dynamics major more on how one types rather than what one types. Existing significant evidence demonstratesthe reliability and accuracy of keystroke rhythm to accurately determine user identity (Paullet,et al., 2014). Keystroke recognition is an authentication method or behavioural biometric that utilizes the unique or the rhythm of a person's keystroke dynamics on the computer keyboards, mobile phones, and touch screen panels derived mainly from the two events that make up a keystroke: the Key-Down and Key-Up. Keystroke dynamics refers a detailed recording of the exact time when each key was pressed on a keyboard or digital device and when it was released as a one types. Keystroke dynamicsis based on the simple principles of what is referred to as typing biometrics analyses measured by keystroke patterns of users expressed by the duration of pressing a key by user (press time) and the time it takes the user to find the next key (flight time). In determining the typing patterns of user, analyses of keystroke dynamics of the 44 keys used most of the time is used. Other parameters of measurement include the pattern of individual interacts with the device while typing. Typing biometrics is frictionless and does not compromise the user experience when compared to other more intrusive biometrics such as facial identification or retina scan that may hinder the authentication process. With keystroke dynamics, authentication can go further than just checking what you know (your password), what you have (your PIN), or moving towards what you are (biometric solutions such as the phone's TouchID).

Also, numerous support services are being developed to support audio-based learning in a distance learning environment that can also encourage the establishment of convenient, effective and efficient identification and authentication of examinees in a distance learning environment. Applications such as Google Listen22, can allow users to do voice searches for audio files and to subscribe, download, and stream these files onto Android-

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 1135-1141www.ijaem.net ISSN: 2395-5252

enabled cell phones to create personalized audio magazines or audio PowerPoint presentations (Watson & Sottile, 2010). With the use of microphone, voice comments, type comments, or phone in comments can be recorded, while, teachers can post still and moving images, view and comment on videos asynchronously or in real time and in a collaborative multimedia space (Black, et al., 2008). This can be a good strategy for establishing convenient and effective strategies in identifying and authenticating examinees in a distance learning environment to ensure that the student who registers in a distance learning environment or program is that the same student who participates and completes the program, and receives the tutorial. Voice Thread can be used extensively to help examiners ensure examinees authentication based on online voice identification embedded in an assignment, and observed physically at one time or the order in the course of the students' program. Also with the use of Voice over Internet Protocol (VoIP), teachers can engage in reflective, analytic learning activities and discussions around specific teaching attributes and practices which can serve or provide synchronous feedback and guidance that creates automatic archived body of knowledge that may be accessed to check for any identity theft. Also, Webinars are known to facilitate interaction between instructors and students via voice and chat especially with the use of commercially based software that has more features. This also allows students to ask questions (via text or audio), provide quick formative assessments (via an electronic "show of hands"), and enable document exchanges, Like webcasts, webinars bring a flexible mode of distance-based professional development, because they are available on demand or prepackaged and may stream live or be archived for later viewing (Watson & Sottile, 2010).

The differences in typing time may be largely imperceptible with the human eye, but with a computer, different typists or different typing times may be differentiated by monitoring how one types. For instance, how long one takes between each keypress, the length of time one takes pressing each key, how long it may take one to type a particular string of characters, and so forth. Keystroke dynamics uses a singular biometric template to spot individuals supported typing pattern, rhythm and speed. The raw measurements used for keystroke dynamics are referred to as "dwell time: and "flight time". Dwell time represents the duration that a key is pressed, while flight time represents the duration between keystrokes. Keystroke dynamics therefore, is a software-based algorithm that measures both dwell and flight time to authenticate examinees identity.

III. METHODOLOGY

In this study, the authors adopted Narrative Review Methodology. Narrative review methodology is usually recommended and adopted, where analysis and synthesis of different and related research findings are required to draw holistic interpretations or conclusions based on the reviewers' own experience (Hill & Burrows, 2017). A narrative study approach is best suited for qualitative, descriptive or explanatory studies (Happel-Parkins & Azim, 2017). Narrative studies exhibit substantial strengths, acceptability, and ability that provide platforms for comprehension of diverse and numerous understanding around scholarly research findings. Narrative studies are also most suited for studies thatopportunity to make reflective practice and acknowledgment of researchers' views and knowledge (Scarnato, 2017). In this study, the authors reviewed, analyzed, and synthesized prior research findings. These reviews are done comparatively and extensively using various sources in order to gain multiple perspectives, maximize reliability and validation of data, and to build coherent justification for interpretation and conclusion that relates to the study. This approach ensures reliability and validity of data, and justification of interpretations from the reviews.

IV. DATA COLLECTION

Data collection came from reviewed vast professional and academic research findings that are relevant and concerned with establishment of convenient and effective strategies for identification and authentication of examinees in a distance learning environment. Our sources came majorly from research findings extracted from the Google Scholar and ScienceDirect databases and peer-reviewed journals, and other related texts. Intelligent phrases such as "Identity theft", "Voice recognition", "biometric recognition", "identity security", "distance learning environment", etc., were used as key search words in the databases for related literature. Our reviews incorporated relevant peer-reviewed journals that are within the last five (5) years.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 3 Mar. 2021, pp: 1135-1141www.ijaem.net ISSN: 2395-5252

V. ANALYSIS AND SYNTHESIS OF PRIOR RESEARCH

Not all researchers agreed with the accuracy of Keystroke dynamics as a unique biometric template, to identify individuals. There are contrasting or opposing researches on Keystroke dynamics. Some researchers believe that the overall accuracy of Keystroke biometrics is still lower than other biometric authentication systems, such as iris (Ali, et al., 2017; Thakur, et al., 2015). Some proposed that for a language course, students can only get enough scheduled time to practice conversation at different levels of comfort via voice recognition. This is achieved through posting of a sound file by lecturers, subsequently starting a debate or conversation about a relevant topic, while the students first reply to the lecturer and then to each other, and then post these files in either a discussion board or in a 'voice board' using either free recording software and microphones or with voice-recording software now found in many universities such as Walden University WIMBA Voice Tools (a sort of online language lab).

Others propose that despite its shortcomings in terms of overall accuracy, keystroke dynamics is more accessible and unobtrusive and requires fewer hardware besides a keyboard, thereby making it easily deployable for use in a distance learning environment when compared to workstation log-ins and other access security points (Alsultan & Warwick, 2013; Balagani, et al., 2011). Alsultan and Warwick (2013) argued that keystroke is captured entirely by key pressed and press time, adding that data can be transmitted over low bandwidth connections. Other benefits of keystroke biometrics as noted by other research studies included its ability to seamlessly integrate with existing work environments and security systems with minimal alterations with no additional hardware, along with its non-invasive nature and scalability (Alsultan & Warwick, 2013; Darabseh & Siami_Namin, 2015). Moreover, keystroke dynamics, having the keyboard is the only necessary hardware that is used, is inexpensive when compared to other biometric systems. Several researchers believe that one major drawback of keystroke biometrics is the assumption that keystroke biometrics may be involve erratic and inconsistent keystrokes resulting from muscle malfunctions like cramped muscles and sweaty hands that could significantly change users typing patterns (Deutschmann, et al., 2013; Rybnik, et al., 2013). Also, some researchers claimed that typing patterns may vary significantly depending on keyboard type used, especially when user changes systems often. The contrasting views of these researchers on keystroke biometrics notwithstanding, keystroke biometrics authentication is practically and theoretically justified based on these properties: keyboard biometrics involves multi-factor authentication, has high awareness levels that will benefit the continued growth of keystroke dynamics market, its low price attributes are expected to drive the use of the technology in a range of end-use applications. These properties of keystroke dynamics authentication make it generally acceptable authentication strategy for identifying students in a distance learning environment.

VI. CONCLUSION

There are no likely single strategy that can guarantee full efficient and convenient system for determining student identity that will ensure academic integrity and credibility to all. A combination of different tools or strategies may be required. Sufficient evidences have shown that the mainstream authentication strategies for determining student identity in a distance learning environment are based on a combination of user's knowledge, objects possession and biometric features. Identity theft resulting from poor security technical control on identification and authentication of examinees, especially in Nigeria, is a knowledgebase affair. The analysis and synthesis of prior research have revealed and identified identity theft and poor identification and authentication of examinees resulted majorly from poor implementation or inappropriate application or combinations of convenient and effective identification and authentication of examinees in a distance learning environmentthat ensures the credibility of their certificates.Security strategies used by stakeholders to effectively identify and authenticate examinees practices to minimize identity theft and ensure the credibility of their certificates in a distance learning environment in Nigeria may become complex due to incomplete state of knowledge about a process or the inherent randomness in a process. These complexities may be minimized if stakeholders ensure continuous information gathering on better evidences from various identity authentication methods that will increase the systems knowledgebase for more appropriate strategies that ensure convenient and effective identification and authentication of examinees in a distance learning environment. This will also enhance the various facets of security platforms to minimize identity theft.

The main objective of this study was to inform stakeholders of distance learning environment, the strategies to create convenient

and effective identification and authentication of examinees in a distance learning environmentthat ensures the credibility of their certificates, and to minimize security threats, vulnerabilities, and risks of identity theft especially among examinees. From our narrative study, keystroke biometrics appears to have outstanding benefits: its ability to seamlessly integrate with existing work environments, ability to successfully integrate with security systems with minimal alterations with no additional hardware, has a unique property of having non-invasive nature and scalability, dynamics and mare require just the keyboard as the only necessary hardware, and is inexpensive when compared to other biometric systems. However, there is one major drawback of keystroke biometrics, and that is the assumption that keystroke biometrics may be involve erratic and inconsistent keystrokes resulting from muscle malfunctions like cramped muscles and sweaty hands that could significantly change users typing patterns, or affected by the type of keyboard used, especially when user changes systems often. These shortcomings on keystroke biometrics notwithstanding, keystroke dynamics authentication has excellent properties that make it generally acceptable as authentication strategy for identifying students in a distance learning environment. These properties include, among others: keyboard biometrics has a multi-factor authentication attribute, has high levels awareness resulting in continued growth in the keystroke dynamics market, and low prices expected to drive the keystroke biometrics technology into higher innovations.

REFERENCES

[1]. Abrar, U., Hannan, X., Mariana, L., & Trevor, B. (2012). Using Challenge Questions for Student Authentication in Online Examination. International Journal for Infonomics (IJI), 5(3/4), 631-639

[2]. Ali, M. L., Monaco, J. V., Tappert, C. C., & Qiu, M. (2017). Keystroke Biometric Systems for User Authentication. Journal of Signal Processing Systems, 86(1), 175-190. https://doi.org/10.1007/s11265-016-1114-9

[3]. Alsultan, A., & Warwick, K. (2013). Keystroke dynamics authentication: a survey of free-text methods. International Journal of Computer Science Issues, 10(4), 1-10.

[4]. Alwi, N. H. M., & Fan, I. S. (2010). Threats analysis for eLearning. International Journal of Technology Enhanced Learning, 2(4), 358-71.

[5]. Bailie, J. L., & Jortberg, M. A. (2019). Online Learner Authentication: Verifying the Identity of Online Users. MERLOT Journal of Online Learning and Teaching, 5(2), 1-9. https://jolt.merlot.org/vol5no2/bailie_0609.htm

[6]. Balagani, K. S., Phoha, V. V., Ray, A., & Phoha, S. (2011). On the discriminability of keystroke feature vectors used in fixed text keystroke authentication. Pattern Recognition Letters, 32(7), 1070-1080.

[7]. Black, E., Greasers, J., & Dawson, K. (2008). Academic honesty in traditional and online classrooms: Does the "media equation" hold true Journal of Asynchronous Learning Networks, 12(3-4), 23-30

[8]. Darabseh, A., & Siami_Namin, A. (2015). Keystroke active authentications based on most frequently used words. In Proceedings of the 2015 ACM international workshop on international workshop on security and privacy analytics (pp. 49-54). ACM.

[9]. Deutschmann, I., Nordstrom, P., & Nilsson, L. (2013). Continuous authentication using behavioral biometrics. IT Professional, 15(4), 12-15.

[10]. Goel, R. K. (2019). Identity theft in the internet age: Evidence from the U.S. states. Managerial and Decision Economics, 40(2), 169-175 https://doi.org/10.1002/mde.2991

[11]. Griffiths, M. (2013). 'Establishing Your True Identity': Immigration Detention and Contemporary Identification Debates. In: About I., Brown J., Lonergan G. (eds) Identification and Registration Practices in Transnational Perspective. St Antony's Series. Palgrave Macmillan, London. https://doi.org/10.1057/9781137367310_

[12]. Happel-Parkins, A., & Azim, K. A. (2017). She Said, She Said: Interruptive Narratives of Pregnancy and Childbirth. Forum: Qualitative Social Research, 18(2), 16-21.

[13]. Hill, C., & Burrows, G. (2017). New voices: The usefulness of a narrative approach to social work research. Qualitative Social Work: Research and Practice, 16(2), 273-288. https://doi.org/10.1177/1473325017689966

[14]. Li, Y., Yazdanmehr, A., Wang, J., &Rao, H. R. (2019). Responding to identity theft: A victimization perspective. Decision Support Systems, 121(1), 13-24. https://doi.org/10.1016/j.dss.2019.04.002

[15]. Monaco, J. V., Stewart, J. C., Cha, H., & Tappert, C. C. (2013). Behavioral biometric verification of studentidentity in online

course assessment and authentication of authors in literary works. IEEE 6th InternationalConference of Biometrics, BTAS 2013.

[16]. Paullet, K., Douglas, D. M., &Chawdhry, A. (2014). Verifying User Identities In Distance Learning Courses: Do WeKnow Who Is Sitting And Submitting Behind The Screen?Issues in Information Systems, 15(1), 370-379.

[17]. Ramu, T., &Arivoli, T. (2013). A framework Of Secure Biometric Based Online Exam Authentication: An Alternative To Traditional Exam. International Journal of Scientific & Engineering Research, 4(11), 1-9.

[18]. Rybnik, M., Tabedzki, M., Adamski, M., & Saeed, K. (2013). An exploration of keystroke dynamics authentication using non-fixed text of various length. In 2013 international conference on biometrics and Kansei engineering (ICBAKE) (pp. 245-250). IEEE.

[19]. Scarnato, J. M. (2017). The value of digital video data for qualitative social work research: A narrative review. Qualitative Social Work: Research and Practice,https://doi.org/10.1177/1473325017735885

[20]. Thakur, K., Ali, M. L., & Tappert, C. (2015). User authentication and identification using neural network. i-manager's Journal on Pattern Recognition, 2(2), 28-39.

[21]. Verhoeven, M., Poorthuis, A. M. G., & Volman, M. (2019). The Role of School in Adolescents' Identity Development. A Literature Review. Educational Psychology Review, 31(1), 35–63. https://doi.org/10.1007/s10648-018-9457-3

[22]. Watson, G., & Sottile, J. (2010). Do students cheat more in online courses? Online Journal of Distance Learning, 13(1). 1-12