Novel Solution for Addressing Identity Theft and Cheating in Electronic Examinations using Mouse Dynamics

Meshach Baba and Victor Legbo Yisa
Department of Cyber Security Science
Federal University of Technology, Minna, Nigeria
babameshach01@futminna.edu.ng, victor.yisa@futminna.edu.ng

***Abstract*—Conducting examinations electronically has gained a lot of acceptance in the educational sector especially in Nigeria tertiary institutions; the complexity of electronic examinations has made it very difficult to verify the identity of students compared to writing exams in the traditional environment. In order to get good scores, an impostor may be used to write the exam for the student. This paper proposes the application of a continuous behavior-metric user authentication in electronics examination via mouse movement dynamics that will verify the identity of a student writing an electronic examination by comparing his mouse movement against the one in his profile. The proposed system will also be able to detect the identity of the imposter.**

Keywords*—*e-examination; examinee; imposter; authentication; integrity; security; continuous mouse movement.

I. INTRODUCTION

E-exam platform is a tool that is understood to advance the quality and equity in education by offering objective evaluations of written exams and equal access to anyone [1]. The platform has been able to reduce cost and time it takes for examination results to be ready. Due to the several benefits attached to e-examination, a large number of tertiary institutions around the world are now making use of it and Nigeria institutions are not exception.

The adoption and proliferation of information technology (IT) into tertiary institutions in Nigeria in conducting e-examination has been an area of interest for researchers over some years back, especially the security(authenticity and integrity) aspect. E-examination engages several parties such as the candidates, examiners, invigilators, examination authorities, information systems, thereby making it a complex and difficult system to deal with.

Several researches have been carried out on examination data at rest and in motion [2]; login in to a system through traditional means of authentication using username and password [3]; through the use of different form of Biometric security mechanism such as physiological mechanism (for example hand geometry, face, fingerprints, and iris) [4] [5] [2] [6] and behavioral mechanism (such as voice, signature, and keystrokes) [7] [8] [9].

Although most researchers have carried out their research in the area of authentication when candidate's login into the system, little research has been carried out in the area of what happens after the candidate's login into the system and how the identity of an imposter can be known when one is detected. Therefore, the integrity and authenticity of e-examination can still be compromise by some of the parties involved with the examination process. To eliminate this loophole, a new form of authentication is required.

Despite several researchers that have been carried out on e-examination, most researches have failed to address one major area which is the identification of the person who tries to impersonate someone within the examination venue.

Also a major challenge to the integrity of the e-examination within Nigeria institutions is that students do not get to see their results immediately as their results may take days to weeks to be released [2], thereby creating room for manipulation of results.

The research work is to propose a design of e-examination platform that will make use of continuous mouse dynamics that will continuously record and compare data from the mouse movement to the one already stored in the database. Also incorporated into the design will be the ability of detecting the impersonator within the examination center. The design will also enable the students to see their results immediately at the end of the exam. The result will also be automatically encrypted and stored on the database with a copy of the result mailed to the respective email address of the respective candidate immediately.

The main purposes of this research work are:

A. To design a system that will eliminate cheating by candidates and some dubious supervisor(s) after the candidate login into the e-examination platform through the use of continuous mouse movement monitoring and few cameras in the examination hall.
B. To detect and identify the identity of anyone that is trying to impersonate another candidate by comparing and analyzing the imposter's mouse movement logs with that on the database
C. To design a system that will prevent manipulation of candidates result at the end of each examination by storing encrypted result in the database and forwarding the result to the students and the administrative email immediately signed with digital signature

This research work will be limited to processes that take place during the conduction of the e-examination, but will not be considering the security aspect of the examiners, administrative personnel and examination questions

This paper is organized as follows: Section II describes background and related work. Section III presents the design and description of the system. Section IV discusses the Discusses the system and future work.

II. USER AUTHENTICATION

Authentication is used by all secure systems to ensure the confidentiality, authenticity integrity and availability of any document within it. It is always used as the first means of defense in any environment to secure systems against unintended use [10]. Since authentication is used in verifying and validating the identity of a person that is trying to access a particular resources in a secure system, it is now been implemented as the first line of defense by most e-examination platform to secure and protect the resources meant for students, lecturers, admin against malicious use.

A. Authentication Methods

There are several authentication methods in use today, but they can all be categorized into three factors (1) Knowledge Factors (2) Ownership Factors and (3) Inherence Factors [10] [11].

i. **Knowledge Factors:** This authentication factor has to do with something the user of any particular system knows. Examples of such type authentication are: password, pass phrase, challenge response (the user answer some predefine question) or personal identification number (PIN).

ii. **Ownership Factors:** this is a piece of device that the user of a system **has** such as cell phone, security token, wrist band, software token, phone, or ID card.

iii. **Inherence Factors:** this authentication factor is divided into something the user **is** or **does.** Examples of something the user **is** are DNA sequence signature, fingerprint, voice, retinal pattern, face, unique bio-electric signals while examples of something the user does are mouse movement mechanism and keystroke.

B. Advantages and disadvantages of each authentication method

Some of The weaknesses in each of the authentication method are discussed in Table 1 below.

***Table 1** Advantages and disadvantages of each authentication method.*

Factors	*Strength*	*Weakness*
Knowledge Factors	• Very low cost • Portability • familiar to users • No special equipment	• susceptible to sniffing • susceptible to brute force attack • can be guessed • User memory burden • Easily phishable • Cannot be use for continuous user authentication
Ownership Factors	• good usability • better security than knowledge factor • resistant to phishing and credential theft	• Can be stolen • More expensive than knowledge factor due device cost • More expensive to implement • Limited capabilities against advanced threats • Limited capabilities against advanced threats • Cannot be use for continuous user authentication
Inherence Factors	• better general security • No user memory burden • resistant to phishing and credential theft	• Low level of Acceptance due to privacy issues • High cost • Difficult to implement. • Enrollment process

Although most of the weaknesses highlighted in each of the authentication method in Table 1 can be eliminated by combining two more factors of authentication. Although, most combinations cannot be use for continuous authentication of examinee, some few of them can be use for it. Therefore, most authentication types will create loopholes that can compromise the integrity and authenticity of the e-examination as another examinee may help another person within the examination hall.

C. Mouse Biometric Authentication

Mouse biometric authentication makes use of the behavioral attributes of subject, when he/she is making use of the mouse. Since the way each person makes use of the

mouse while using the system is unique to each an individual. Therefore, attributes on how each person makes use of the mouse can be use in identifying the person. All biometric authentication system always involve two phases; the enrollment phase where the attributes of the subject mouse movement are collected and stored; and the verification phase which involves the identification of the subject by comparing the present attributes with the attributes stored in the database as enrollment signature [12].

1) Acquisition and Extraction Feature

Low level mouse events such as button up and button down, raw movement events generated by the mouse are intercepted and captured through the use of a software program. Several attributes such as event type, mouse action type, timestamp and cursor coordinates may be associated with each of the event. These low level mouse events are first aggregated and converted into high level abstraction (e.g. drag-and-drops, point-and-clicks, Common Movement, Silence, single click, double click etc.) in other to detect meaningful behavioral patterns that can be use in identifying a person [9] [12]. These features are extracted from each student during their first semester registration in the school.

III. RELATED WORK

[2] proposed the use of encryption for the exchange of examination questions and e-examination center when either internet or intranet is used. They went further to propose the use of fingerprint authentication biometric scheme to authenticate all the stakeholders involved with the examination.

[10] proposed the use of two authentication scheme, username/password with palm-based biometric authentication scheme to authenticate examinee, in both online-based and computer-based. They went further to incorporate the use of video capturing technique to improve the authenticity and integrity of the e-examination process.

[13] Designed a profile based authentication framework (PBAF) for secure online examination that comprises of two layer authentication. The first layer consists of the username and password and the second being the challenge questions. The username and password is used to login in into the online environment, and challenge questions are asked based on the students profile to ascertain the user, a user is not authenticated if answers to the challenge questions is in conflict with that in the students profile.

[14]also designed a system a system that continuously verify the authenticity of a candidate by comparing captured images with already stored images in the encrypted image bank collected during the registration period. If image captured during examinations do not match that in the image database captured for the user, a mismatch is declared and the candidate is not authenticated. Also to curb cheating in the examination hall, the system will warn the candidate if he is found not to be focused on the examination and is looking sideward's.

[8] Designed a Continuous Biometric User Authentication in Online Examinations. The system will continuously monitor the activities of the student by monitoring of the key stroke dynamics of the student. For the purpose of continuous monitoring, they considered some important metrics which can be recorded and used for user verification e.g. Typing speed; Keystroke seek-time; Flight-time; Characteristic sequences of keystrokes; and Examination of characteristic errors. The student keystrokes are identified based on these metrics at the point of registration and is stored in a database, these metrics are then compared with a new signature generated by the student during the examination.

IV. E-EXAMINATION SCHEME SECURITY REQUIREMENTS.

In other to have a successful e-examination, each stage of the examination must be secure. The various stages in e-examination are 1) preparation phase 2) examination enrolment and admission 3) examination conduction and 4) result announcement. The success of each examination starts from when students register for the courses (which proves whether an examinee will be eligible to write the exam), to when the results are announced. The security requirement for an examination schemes are confidentiality, authenticity, integrity and non-repudiation.

Confidentiality: only eligible exam participant should be allowed to see the questions and the result. And it should also be at the specified period of time. This means examinee should not be allowed to view examinations questions until it is time to write such examination paper and the examinee has been properly authenticated. The only examination participant that should be allowed access to the questions apart from the authenticated examinee should the lecturer (the examination participant that sets the questions) except in the case of external examination moderator been involved.

Integrity: The originality of the questions and results is of paramount importance whenever the issue of e-examination is raised. How do we know the questions are sent from course lecturer? Or was the question altered on transit? Or can someone change the result of a student? For an examination to be called a success, integrity of both the examination questions and students results must be maintained.

Non-Repudiation: for e-examination to be a success, the system should be able to hold each participating member accountable for their actions. This will prevent the examinee from denying not to have performed some certain actions (claiming not to be the person that wrote the exam). The e-examination system should also have the capability of preventing the examiner of denying the original questions sent by him to the e-examination system.

Authenticity: this should ensure that the identities of all participants of the examination are properly verified and

that they are granted access to only information that they are authorized to access and at the appropriate time.

V. PROPOSED E-EXAMINATION SYSTEM

The proposed system, shown in Figure 1, will make use of continuous mouse monitoring system with username and password to authenticate the examinee. The system will work in conjunction with few CCTV cameras placed at strategic location within the examination hall.

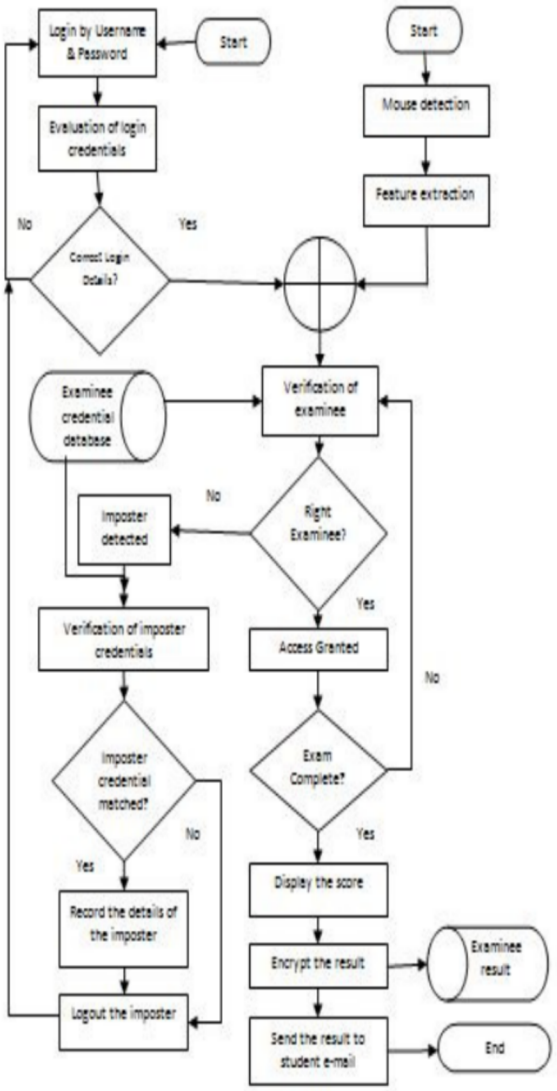

Fig. 1: Proposed e-examination system with continuous authentication scheme.

A. Design consideration

In designing the e-examination system, cost implication, confidentiality, authenticity, integrity and non-repudiation were considered and some assumptions were made.
The following assumptions were made.

Assumption 1: It was assumed that during the registration of the student, information's such as the courses qualified and registered for; name, student identification number and the department are stored on the database, which is important for authentication and detecting the identity of the imposter.

Assumption 2: It was also assumed that the mouse biometrics features for each student have been extracted and stored in the database before the day of the examination. Also, that the student has created username and password alongside their profile during this process.

Assumption 3: it was assumed that all connections between the database and any connecting device is using HTTPS as the connecting protocol

B. Authentication

Authenticating an examinee during an examination should not just end after he/she has been logged in into the system but ensuring the right examinee is taking the examination throughout the duration of the examination is necessary to avoid cheating. The propose system is shown the figure 1.0 above. The propose system will make use of two multimodal authentication method to log in examinee into the system. The authentication methods to be use are username and password in combination with continuous mouse movement monitoring.

When the examinee runs the application for the e-examination platform, he/she will be asked to enter a username and password to be authenticated first, but will be forced to use the mouse as the mouse cursor will be placed at the extreme end. Also after the user have authenticated, he/she will be ask to perform some few task with the mouse like selecting his/her faculty and department before been authorize to access the examination questions. These steps will allow necessary mouse movement features of the examinee to be collected and compared with the one on the database, before granting the candidate the authorization to write the examination. To achieve this, the username and the password of the authenticated examinee are compared with features extracted from the mouse movement with what is stored on the database to find a match. If the examinee is found to be a legitimate person for the credentials verified, he/she is authorized to write the examination, otherwise the system logouts the person. The MAC address of the system been use by the examinee with date and time the exam begins are stored in the database, when the exam ends, the time will also be recorded by the system

Throughout the duration of the examination of the examinee, the mouse movement software keeps running behind the scene to verify if the authorized examinee is still the person taking examination. If the answer is yes, the software checks if the examination time has expired or the examinee has ended the examination and if yes, the software stops extracting and comparing the features of the examinee.

.

C. *Imposter Identification*

If at some point during the examination, the features extracted from the authenticated examinee do not match with what is stored on the database, the system will flag the examinee as an imposter.

Since the system as discovered the presence of an imposter writing the examination, the features extracted from the imposter is compared with what is stored on the database to discover the identity of the imposter.

After the identity of the imposter has been discovered, the names, student identification number and the student department of both the imposter and the examinee are stored in the database labeled as cheat. The system will allow the imposter to continue with the exam for a short period of time as the system alerts the appropriate authority immediately. Though, if the short period of time frame given expires, the system automatically logs out the imposter and prevents him/her from login into the system with the same login credentials.

We propose the use of a mobile device by the proctors. This device will receive an alert indicating the presence of an imposter with all the information regarding the imposter and the system been used by the person. The device will only receive alert but will not be able to perform any other action. This will help the authority in catching the imposter during the act.

The presence of CCTV cameras will also help in validating the alert from the propose system, as the imposter cannot later deny not to have used that system at that particular period of time.

D. *Result integrity*

Immediately the examinee clicks the submit button on his/her examination platform, the results are encrypted and sent to the database through a secure channel of https using secure socket layer (SSL). The result is then displayed on the screen for the student to see but subject to final validation from the examination management.

The system will make use of public key cryptographic encryption scheme. The public key will take action when the student click submit button. The result can only be decrypted by the person authorized to use the private key.

The system will attach the MAC address of the system used by the examinee with the time and date he/she took examination. These values can letter be compared with what was recorded when the examinee was authenticated and authorized to write the examination. This feature will allow the detection of any manipulation of the results by third party as the timestamp will change and the mac address may also change if different system was used.

VI. CONCLUSION

In this paper, we have proposed a secure e-examination system that can be use in ensuring the authenticity, non-repudiation and integrity of the exam. The paper proposes the use of username and password with continuous mouse movement to authenticate and continuously ensure that the authenticated examinee remain the person writing the examination throughout the duration of the exam. The system uses the features of the continuous mouse movement to detect the identity of the imposter, thereby ensuring the integrity of the examination throughout. The system also uses some few CCTV cameras to monitor the activities of all the parties involved, therefore ensuring non-repudiation by the parties involved. We also propose the use of public key cryptographic algorithm to ensure that the integrity of the result is not compromised. Some features such as the time of login and logout; MAC address of the system are added to the result before encryption, which can be compare with similar feature stored in the database when the examinee logs into the system

REFERENCES

[1] R. Giustolisi, G. Lenzini, and G. Bella, "What Security for Electronic Exams? (Extended Abstract)," in *International Conference on Risks and Security of Internet and Systems (CRiSIS)*, 2013.

[2] O. Adebayo and S M Abdulhamid, "E- Exams System for Nigerian Universities with Emphasis on Security and Result Integrity," *International Journal of the Computer, the Internet and Management (IJCIM)*, vol. 18, no. 2, pp. 47.1-47.12, 2014.

[3] X. Ren and X. Wu, "A Novel Dynamic User Authentication Scheme," in *International Symposium on Communications and Information Technologies (ISCIT)*, 2012, pp. 713-717.

[4] M. M. Ramim and Y. Levy, "Towards a Framework of Biometric Exam Authentication in E-Learning Environments," in *Managing Worldwide Operations & Communications with Information Technology*, 2007, pp. 539-542.

[5] T. Ramu and T. Arivoli, "A Framework of Secure Biometric Based Online Exam Authentication: An Alternative to Traditional Exam," *International Journal of Scientific & Engineering Research*, vol. 4, no. 11, pp. 52-60, 2013.

[6] S. M. Al-Saleem and H Ullah, "Security Considerations and Recommendations in Computer-Based Testing," *The Scientific World Journal*, pp. 1-7, 2014.

[7] P. Bours and C. J. Fullu, "A Login System Using Mouse Dynamics," *Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, pp. 1072-1077, 2009.

[8] E. Flior and K. Kowalski, "Continuous Biometric User Authentication in Online Examinations," in *Seventh International Conference on Information Technology*, 2010, pp. 488-492.

[9] C Shen, Z Cai, and X Guan, "Continuous

Authentication for Mouse Dynamics: A Pattern-Growth Approach," in *Dependable Systems and Networks (DSN), 2012 42nd Annual IEEE/IFIP International Conference on*, Boston, MA, 2012, pp. 1 - 12.

[10] Y. Sabbah, I. Saroit, and A. Kotb, "An Interactive and Secure E-Examination Unit (ISEEU): A Proposed Model for Proctoring Online Exams," in *10th Roedunet International Conference (RoEduNet)*, 2011, pp. 1-5.

[11] A E Monge, "Matching Algorithms within a Duplicate Detection System," in *blletin of the IEEE Computer Society Technical Committee on Data Engineering.*, 2000.

[12] Z. Jorgensen and T. Yu, "On Mouse Dynamics as a Behavioral Biometric for Authentication," in *ASIACCS*, Hong Kong, China, 2011, pp. 476-482.

[13] Abrar Ullah, Hannan Xiao, Mariana Lilley, and Trevor Barker , "Using Challenge Questions for Student Authentication in online Exainations," *International Journal for Infonomics*, vol. 5, no. 3/4, pp. 631-639, 2012.

[14] Ayham Fayyoumi and Anis Zarrad, "Novel Solution Based on Face Recognition to Address Identity Theft and Cheating in Online Examination Systems," *Advances in Internet of Things*, vol. 4, pp. 5-12, 2014.