A Context-Aware Framework for Continuous Authentication in Online Examination

Hussaini Abubakar Zubairu[1*], Idris Kolo Mohammed[2], Stella Oluyemi Etuk[3], Faiza Jada Babakano[4], Anda Ilyasu[5]

[1,3,4]*Department of Information and Media Technology, Federal University of Technology, Minna, Nigeria,*
abu.zubairu, abiolastella, faiza.bkano {@futminna.edu.ng}
[2]*Department of Computer Science, Federal University of Technology, Minna, Nigeria, idris.kolo@futminna.edu.ng*
[5]*Department of Library and Information Technology, Federal University of Technology, Minna, Nigeria,*
ilyasu.anda@futminna.edu.ng

Abstract
Online examination is the technology-enabled means for student's assessment electronically. No doubt it has lots of advantages, but establishing true user authentication is very difficult. This is largely due to the virtual and anonymity nature of the online system, relative to the conventional examination. Security of the online examination system is necessary due to the increasing cases of malpractices; an imposter may take the examination on behalf of the real candidates in which the conventional username or password may not be able to detect. Therefore, for effective authentication of users during their entire session, continuous authentication is required. This paper proposes a context-aware based continuous authentication framework to address the problem of cheating in an online examination.

Keywords: Authentication, context awareness, malpractices, online examination, security

1. Introduction

Online examination is gradually gaining wider acceptability and becoming the new normal in the 21st century. Online examination is the use of Information Technology (IT) to assess students electronically either on the Internet or Intranet on Local Area Network (LAN). Technology is adding value to the learning processes and the organization and administration of learning institutions (Singh, 2015). As a result of technology evolution, especially IT, many examination bodies and learning institutions are now adopting the electronic delivery of examination, and as a result, e-assessment has increased for both formative and summative purposes (Singh, 2015).

However, authentication to prove the legitimacy of the user, and to do so securely and conveniently remain a challenge. According to (Ketab, Clarke & Dowland, 2017) an online examination system should be resistant against possible cheating and unauthorized participation or illegal assistance. Therefore, it is necessary for an effective security mechanism, to guarantee correct authentication, this can be achieved through the implementation of a strong authentication approach (Ashibani & Mahmoud, 2017). User authentication is very crucial for the online examination system, its databases and the network system security (Agashe & Nimbhorkar, 2015). User authentication approaches such as knowledge-based authentication (Password, PIN and pattern), object-based authentication (ATM Card, Smart card, Mobile phone) and biometric-based authentication (fingerprint, facial and voice), have all been explored to solve the security challenges in the online examination. However, with lots of drawbacks, weaknesses and security vulnerability (Agashe & Nimbhorkar,2015). The knowledge-based authentication approach requires owners to remember authentication credentials, which may be vulnerable to attacks. Object-based approaches demand that users must always have tokens that are likely to be loss or theft. Besides, it is unrealistic for users to always have tokens, especially those users who have many identification tokens (Li, Wang & Sun, 2017). To address these challenges, come continuous login authentication scheme like behavioural biometrics (keystroke dynamics, mouse dynamics, signature, Gait and voice), physiological biometrics (face, finger, iris, retina and ear) and multimodal biometrics (a combination of two or more biometrics features), have been explored (Ayeswarya & Norman, 2019).

Although the aforementioned continuous authentication approaches have been implemented for security purpose in the online examination system, cheating-free online examination remain elusive and not yet accomplished, it is still very difficult to completely trust e-examination system within the virtual environment (Sabbah, Saroit & Kotb, 2012). Impersonation is a major threat that threatening the security and integrity of the online assessment and requires context-awareness continuous authentication. Context-awareness in the IT context implies that a computer or any digital devices can perceive or sense its operational environment and the application can be tailored or programmed to react accordingly (Kayes, Rahayu, Dillon, Chang & Han, 2019). The need for adequate security measures in online examination demand that e-exam systems should verify and ensure that a candidate that initially login into the system is the actual person throughout an exam (Agashe, & Nimbhorkar, 2015). Contextual data in respect to the examination's resources and environment can be collected from various sources like the networking devices, system's environment and electronic resources, these information can be constructed for useful decision and authentication mechanism. The analysis of this information becomes a necessary determinant for accessing the resources, thus complementing the authentication process (Ashibani, Kauling & Mahmoud, 2019). This paper proposed a framework that contributes to resolving the issue of security challenges, especially impersonation in online examination using context-awareness for continuous authentication.

2. Problem definition and Motivation

The use of online platforms for student's assessment in both objectives and subjective examination, popularly called e-exam (online exam) is on the increase even in developing countries due to technology advancement (Singh, 2015). Along with this increase and wider adoption, various security threats are emerging. An online exam is usually a web-based system, which is technology dependent. This virtual form of an online examination system creates a major vulnerability to cyber-crimes and security risks (Sabbah, Saroit & Kotb, 2012).

Impersonation is a major threat in the online exam and the most critical security risks (cheating cases) that are common in an electronic or online examination system. Impersonation occurs when a person pose to be someone else (Apampa, Wills & Argles, 2010). Consider the cases in Figure 1.

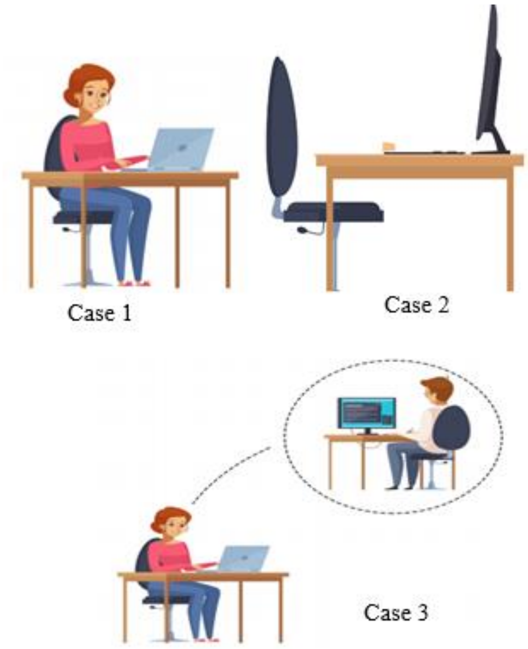

Figure 1: Malpractices scenarios

Case 1: an examinee's login detail was passed to an impostor, who uses the login credentials to impersonate and write the examination.

Case 2: an examinee log in to an online exam platform, but moves away and letting an impostor write the examination as the authentic candidate.

Case 3: The real candidate logins with valid credentials, however, the answer to the exam's question was provided by a remote assistant.

Continuous authentication approaches (behavioural biometrics, Physiological biometrics and multimodal biometrics), have been explored to address the scenarios in Figure 1. While these methods are reliable, they all have one weakness or the other when applied in real e-examination. For instance, a candidate might access local computer resources or surf the Internet for an answer after the initial authentication.
Furthermore, the case 3 scenario in Figure 1, where the candidate logins and the answers to the questions are provided remotely by an assistant has not been considered in the existing literature. Most of the proposed continuous authentication cannot detect case 3, in Figure 1. Therefore, a context-based continuous authentication is required to continuously verify the contextual environment and the authenticity of the user. By harnessing and incorporating context into the authentication and privilege access, the online examination system will be accessible with an enhanced security mechanism (Benzekki, El Fergougui & Elalaoui, 2018).

3. Literature Review

3.1 Continuous Authentication

Continuous Authentication is an advance authentication schemes that verifies the user presence throughout an active session (Brocardo, Traore & Woungang, 2014). Continuous authentication was in response to the limitations of conventional authentication approaches that only authenticate the user at the initial login of the examination, with all the privileges granted until the allotted expires or the candidate formally logs out. While the candidate or the user’s session is active, the entire resources of the system are accessible to the active session user. Therefore, sensitive data are likely to be misused when granted access to the e-exam system or services immediately after authentication is completed.

To address these drawbacks of the traditional authentication approaches, continuous authentication was envisaged to periodically validate and authenticate the user beyond the initial authentication at the initial login. Several approaches have been used in the literature to accomplish continuous user authentication (Ayeswarya & Norman, 2019). Context-awareness as one of these approaches is currently been explored for continuous authentication, especially in smartphones.

3.2 Context Awareness

Context-awareness within the context of the computer domain implies that computer or digital devices can perceive their immediate operational environment (Murugesan & Gangadharan, 2012). It is the harnessing of contextual information to generate data and services for both the user and the object in the immediate operational environment (Habib & Leister, 2015). An object is assumed to exhibit contextual awareness if it uses contextual data to generate information and services related to users, where relevancy is a factor of user's activities (Dey, 2000). Context-awareness as a concept was proposed for the first time by (Schilit, Adams & Want, 1994), within the context of mobile computing. Accordingly, the context implies the location of an object of interest, the users of the objects, other objects within the proximity, and the changes related to the objects over time (Prakash, 2014). Any available data that could be relevant to provide a situational status of an entity is referred to as context. The entity can be anything related to user interaction with the system or an application (Habib & Leister, 2015). Context is a structured integration of data, physical or conceptual resources about an entity or the state of digital resources (Kirsh, 2001). Context-awareness system life cycle to deliver contextual information is as shown in Figure 2.

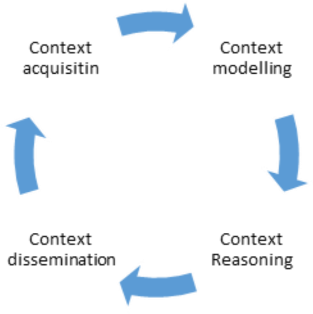

Figure 2: Context-awareness system process

Contextual awareness is becoming very crucial in information systems of dynamic environs, where users are expected to remotely access resources in a distributed manner. Therefore, access and privilege in such remote and unstable environments need to take the contextual information into cognizance. Through harnessing the non-static context information, a context-specific control over access to digital information resources and services that suit the security requirement of online examination can be achieved.

3.3 Context-Aware Authentication

Most of the existing security mechanisms in an e-exam system have well complied with a grant-and-deny based access control framework (Habib & Leister, 2015). In these cases, the user's authentication credentials are pre-registered and stored in the system. Access privileges are grant or deny depending on whether the user's credential matches or not with already stored information. This form of authentication is considered static since it does not take into cognizance the contextual information of the user or the device's immediate environment while taking granting or denying decision. Nevertheless, an online examination system's environment is dynamic, where incorporating contextual information into the authentication process can significantly enhance the effectiveness of security policies.

Context-aware authentication refers to the consideration of the contextual information while deploying a new authentication policy due to the changes that could occur in an entity's environment. An authentication policy is about the rules that govern or decided on who or what has the privileges to certain digital resources. The weakness of the existing authentication approaches requires improvement through context-awareness for continuous authentication in an online examination system.

3.4 Related studies

A secure touch-based behavioural biometrics for continuous authentication was proposed in the work of (Bours & Mondal, 2015; Shaji, Das & Kizhakkethottam, 2015; Wu et al., 2018; Watanabe & Houryu, 2013). Aside from the use of keystrokes, their approaches acquire single-touch motion detection characteristics for the entire user's interaction with the device. The limitation of this approach is that it is not enough to identify a user with a single touch. To enhance the device's security flaw and to address the limitations inherent in the behavioural biometrics adoption in continuous authentication, (Deutschmann, Nordstrom & Nilsson, 2013) adopt the use of multimodal behavioural biometrics. This was the premise on the fact that; it is very difficult to spoof multiple behavioural models concurrently.

Similarly, (Alshehri, Coenen & Bollegala, 2016a) proposed a keyboard usage authentication using time series analysis, but consider the only static text. This research was further enhanced to be applicable in the context of continuous text by (Alshehri, Coenen, & Bollegala, 2016b), but considered only hold time. This approach might be applicable in a certain context of static authentication under a controlled setting. However, its feasibility in the context of continuous authentication in an online examination remains an open challenge; online examination can take place without the user typing from the key, an online assistant remotely was not considered. Therefore, remote cheating can take place.

Flior and Kowalski (2010) developed a continuous authentication system for electronic examination platforms. A Steinhaus approach using cosine correlation was adopted to carry out authentication through keystroke patterns. In the proposed system, 500 characters are required to be collected in a restricted setting, with neither backspace nor deletion. Though this approach might work for limited cases, the fixed text nature of these approaches might be a serious drawback in a real-world implementation. This drawback was addressed in the research by (Feng, Zhao, Carbunar & Shi, 2013) through the production of different signatures from a collection of text and using the similarity average value of the text.

A general framework towards enhancing security in digital devices was proposed by (Prakash, 2014; Bhandwalkar & .Hanwate, 2014) using a combination of hard and soft biometrics; the hard biometric was adopted for initial validation and soft biometric for subsequent validation of the user. However, this framework did not take cognizance of colour variation, especially variation in light with low accuracy. The drawback in research by

Prakash, 2014) was addressed by (Samangouei, Patel & Chellappa, 2015), using a face-based authentication technique for enhancing the accuracy of recognition. Nevertheless, the method is not feasible for dynamic attributes such as the colour of the hair and changing in the skin due to advancing in age. This limitation was addressed by (Bhandwalkar & .Hanwate, 2014), where the proposed system depends on hard and soft biometric traits using the Independent Components Analysis dimension for video frames. The system captures and enrols soft biometric features whenever the user logins and combines soft biometric matching with the traditional authentication approaches. However, a soft biometric mechanism is used to know whether the current user of the system is the same as the user who initially logged in, however, it cannot establish the authenticity of the subject because soft biometrics lack distinctiveness and permanence (Samangouei, Patel & Chellappa, 2015). Also, it suffers the same limitations with hard biometrics authentication, when online cheating is involved.

Samangouei, Patel and Chellappa (2017) developed an attribute-based authentication system using a facial biometric feature for seamless identification of the user. However, lighting variation is a major problem with this approach. Asep-Hadian and Bandung (2019) address the challenge of lighting variations in the work of (Samangouei, Patel & Chellappa, 2017), by proposing an approach to enhance lighting variations through the use of an increment training by adopting the training data set from mobile learning online lecture sessions. Nevertheless, these approaches are not enough to mitigate cheating in online examination especially when accessing the system resource or seeking online help.

Ehatisham-ul-haq et al. (2018) proposed a novel approach using weighted generalized Weber face (WGWF) for facial recognition, biometric fingerprint recognition using minutiae-based geometric hashing and images classification using rough set fuzzy k-means and Hidden Markov Model that does not need a large storage bank. This method was reported to be secure, accurate and not vulnerable to physical attacks or malpractice. But remote cheating was not considered. To improve this system, (Alshehri, Coenen & Bollegala, 2018) proposed a real-time continuous keystroke authentication using Spectral Analysis, where validation of user's typing samples is controlled by recording keystroke patterns in spectral format. It encompasses the use of vectors for continuous keyboard pressing patterns authentication, but the size of the feature vectors and their generation, make this approach not good for real-time authentication as required in the electronic examination. This limitation was addressed in the work of (Alshehri, Coenen & Bollegala, 2018b) where an iterative real-time keystroke continuous authentication was proposed to avoid an inherent problem with the feature vector approach. The report of the evaluation reveals an improved performance relative to the feature vector based technique. However, these approaches are not adequate to address security in term of online examination that takes place in a virtual world. Despite these measures, cheating can occur in an online examination without the movement of the face or typing from the keyboard especially when accessing the system resource or seeking online help.

None of the previous studies on continuous authentication addresses remote cheating in e-examination as demonstrated in case 3, in Figure 1. Therefore, the case remains an open challenge for online examination. This is the gap that this research is intended to fill using a context-awareness framework for continuous authentication.

4. Proposed Context Awareness Continuous Authentication Framework

Our proposed framework for context-aware continuous authentication allows for the collection and integration of contextual information for the continuous authentication of the examinee (candidates or students) to access online examination platforms beyond the conventional authentication schemes. This section presents the contextual frame architecture and the flow chart. The contextual information to be collected by the system from the environment is given in Table 1.

Table 1: Contextual Information

Context type	Characteristics
User context	GPS Time zone Connection type Log profile
Device context	Operating system Browser Access point MAC address Installed App Device features
Network context	IP address Connection type Ping
Environmental context	Lighting Noise Loudness

The contextual information shown in Table 1, would be invoked whenever the user attempts to access the online examination system remotely. This information would be collected by the virtual sensor and processed by the context management module as shown in the architecture in Figure 3. As shown in Table 1; the Geographical position system (GPS), gives details as per the user's location. The Time-Zone information assists in verifying the user's Time Zone. Installed or resident applications give information relative to the operation and the environmental context. The device features describe the operating systems and their version, among others.

4.1 Proposed system architecture

The goal of this work is to design and implement a dynamic authentication model for mobile clients (users) for accessing online examination platforms using traditional credentials along with context-aware information to checkmate the issue of remote cheating in the online examination. Figure 3, demonstrates the proposed system architecture framework, separating the user from the context-aware e-exam system with the context management component mediating all communication for authentication or authorization.

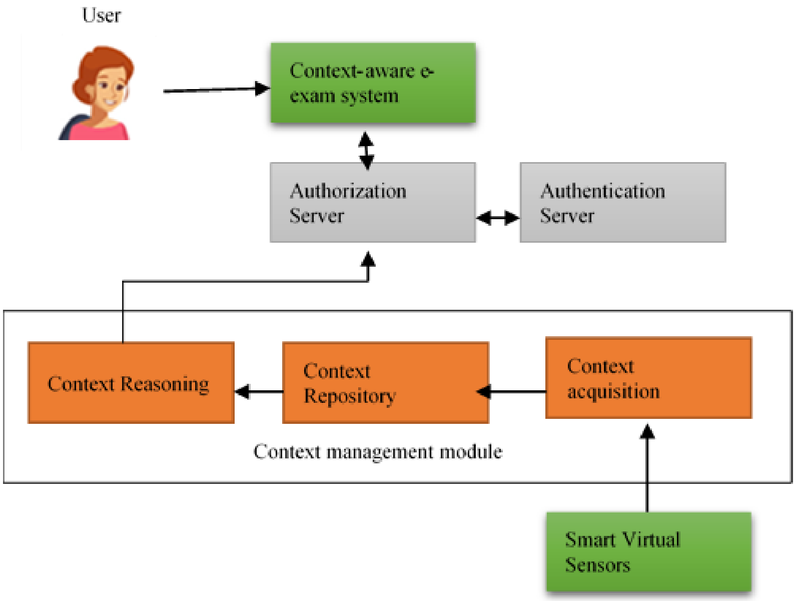

Figure 3: Context-aware E-exam Architecture

As shown in the architecture (Figure 3), the contextual information will be acquired by virtual sensors using appropriate virtual sensor technology for context information acquisition. These data will be processed and made available in a machine-processable format to the authorization server.

The context management module should contain a set of if-then clauses that control the behaviour of a context-aware e-exam system based on the sensed context. The context repository parses the received context information through the contextual rules to make appropriate decisions by the context reasoning. The decisions are then communicated to the authorization server in an appropriate technique to achieve desired agent behaviour (grant or deny access). The flow chart for the system is shown in Figure 4.

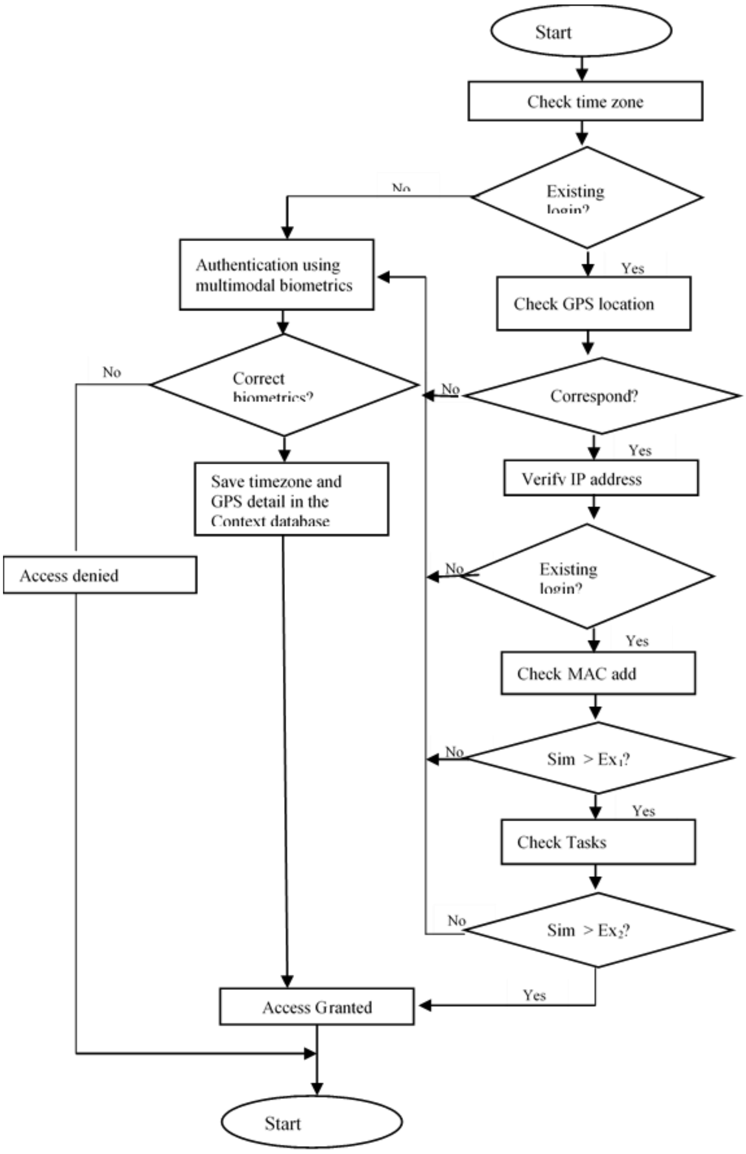

Figure 4: The system flow chart

As shown in Figure 4, when the user makes an access request to the e-exam system that employs the proposed approach, the Time Zone for the device will be verified first. If the time Zone corresponds, then, the global positioning system (GPS) information is required for verification about the region covered by the Time Zone and the relative GPS of the system. Then, every user is asked to authenticate using multimodal biometrics already pre-registered in the system. The user is granted access to the e-exam system once a successful authentication is achieved. The Time Zone in which the system is verified will be recorded for subsequent use. The system characteristics such as MAC address, IP address, operating system version information are verified using the object connect from. In the last stage, a similarity method will be applied to the last two criteria to arrive at the decision to either grant or deny an access request made by the user. A measure of similarity is evaluated for every saved pair list against the two new lists associated with the authentication request (MAC address and tasks). If the similarity values obtained falls below already established thresholds Ex1 and Ex2 respectively for the MAC address and processes tasks list, the user will be requested to perform an authentication process via a multimodal authentication system (using biometrics and keystroke dynamics). This will certainly address the remote cheating in an online exam, as it strengthens the multimodal authentication scheme.

5. Conclusion and future work

Security in the online system continues to be challenging issues. Many existing authentication approaches apply conventional authentications mechanisms that do not lend themselves well to the network-dependent and virtual nature of the online exam. This is particularly true for authentication; as conventional authentication mechanisms rely on physical presence to authenticate every access request by a user. This approach is not adequate in the online exam system where remote access is possible.

This paper is proposing a context-aware framework for continuous authentication in an online examination system that considers environmental information relating to user's geographical location and digital device information (MAC and IP address among others), as requisite information necessary to either grant or denies access during decision making regarding access request. The proposed system will address the remote cheating scenario case 3, in Figure 1, because the user's location relative to the Time Zone that covers a particular region and the GPS for the exact location will be verified. The verifications are necessary to ensure that the user is genuine and that, user's account is accessed from the expected user device and location. All this information will be fused to make a correct prediction as per the legitimacy of the access request by the user. The context-aware continuous authentication as proposed in this paper is envisaged to strengthen existing continuous authentication and provide extra security measure for online examination systems.

As a work in progress, its prototype implementation is the expected future work, where its usability and effectiveness will be evaluated against remote cheating, instant messages and local resources access.

References

Agashe, N. M. & Nimbhorkar, S. (2015). A Survey Paper on Continuous Authentication by Multimodal Biometric. *International Journal of Advanced Research in Computer Engineering & Technology (IJARCET)*, 4(11), 4247 -4253

Alshehri, A., Coenen, F., & Bollegala, D. (2016a). Keyboard usage authentication using time series analysis. *International Conference on Big Data Analytics and Knowledge Discovery*, 239–252.

Alshehri, A., Coenen, F., & Bollegala, D. (2016b). Towards keystroke continuous authentication using time series analytics. *In Proceeding of AI 2016, Research and Development in Intelligent Systems XXXIII*, Springer, 275-287.

Alshehri, A., Coenen, F. & Bollegala, D. (2018). Spectral Analysis of Keystroke Streams: Towards Effective Real-time Continuous User Authentication. *Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018)*, 62-73

Alshehri, A., Coenen, F. & Bollegala, D. (2018b). Iterative Keystroke Continuous Authentication: A Time Series Based Approach, *KI - Künstliche Intelligenz*, 32(1), 231–243

Ashibani, Y., Kauling, D. & Mahmoud, Q. H. (2019). Design and Implementation of a Contextual-Based Continuous Authentication Framework for Smart Homes. *Applied systems innovation*, 2(4), 2- 20.

Ashibani, Y. & Mahmoud, Q.H. (2017*). An Efficient and Secure Scheme for Smart Some communication Using Identity-Based Signcryption.* Proceedings of the IEEE 36th International Performance Computing and Communications Conference, IPCCC, San Diego, CA, USA, 10–12, 1–7.

Asep Hadian S. G & Bandung, Y. (2019). A Design of Continuous User Verification for Online Exam Proctoring on M-Learning. *International Conference on Electrical Engineering and Informatics (ICEEI)*, Bandung, Indonesia, 284 – 289

Apampa, K. M., Wills, G. & Argles, D. (2010). User security issues in summative e-assessment security. *IJDS*, 1(2), 12-16

Ayeswarya, S. & Norman, J. (2019). A survey of different continuous authentication systems. *International Journal of Biometrics*, 11(1), 67–99.

Benzekki, K., El Fergougui, A. & Elalaoui, A.E.B. (2018). A Context-Aware Authentication System for Mobile Cloud Computing. *Procedia Comput. Sci.* 12(7), 379–387.

Bours, P. & Mondal, S. (2015). Continuous Authentication with Keystroke Dynamics, *Inf. Secur. Tech. Rep*. 2(3), 41–58.

Bhandwalkar, K. T. &.Hanwate, P.S. (2014). Continuous User Authentication Using Soft Biometric Traits for E-Learning. *International Journal of Innovative Research in Science, Engineering and Technology*, 3(4), 231- 235

Brocardo, M..L., Traore, I. & Woungang, I. (2014) 'Toward a framework for continuous authentication using stylometry', Proc. – *Int. Conf. Adv. Inf. Netw. Appl. AINA*, pp.106–115

Dey, A. K. (2000). "Providing Architectural Support for Building Context-Aware Applications," PhD thesis, Computer Science, Georgia Institute of Technology, Atlanta.

Deutschmann, I., Nordstrom, P. & Nilsson, L. (2013). 'Continuous authentication using behavioural biometrics, *IT Prof.*, 15(4), 12–15.

Ehatisham-ul-haq, M., Azam, M.A., Naeem, U. & Loo, J. (2018). 'Continuous authentication of smartphone users based on activity pattern recognition using passive mobile sensing. *J. Netw. Comput. Appl.*, 109(13), 24–35.

Feng, T., Zhao, X., Carbunar, B. & Shi, W. (2013). Continuous mobile authentication using virtual key typing biometrics. *Proc. – 12th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. Trust*, 1547–1552.

Flior, E. & Kowalski, K. (2010). Continuous Biometric User Authentication in Online Examinations, *2010 Seventh International Conference on Information Technology, IEEE*.

Habib, K., & Leister, W. (2015). Context-Aware Authentication for the Internet of Things. *The Eleventh International Conference on Autonomic and Autonomous Systems (ICAS 2015)*

Kayes, A., Rahayu, W., Dillon, T., Chang, E. & Han, J. (2019) .Context-aware access control with imprecise context characterization for cloud-based data resources. *Future Gener. Comput. Syst*., 93, 237–255

Kirsh, D. (2001). The Context of Work. *Human-Computer Interaction*, 16(1), 305 – 322.

Li, Y., Wang, H., & Sun, K. (2017). Personal Information in Passwords and Its Security Implications. *IEEE Trans. Inf. Forensics Secur*. 12, 2320–2333.

Murugesan, S. & Gangadharan, G.R. (2012). *Harnessing green its principles and practices*, A John Wiley & Sons, Ltd., Publication, first edition

Prakash, A. (2014) 'A biometric approach for continuous user authentication by fusing hard and soft traits. *Int. J. Netw. Secur*., 16(4), 65–70.

Sabbah, Y., Saroit, I. & Kotb, A. (2012). Synchronous Authentication with Bimodal Biometrics for e-Assessment A Theoretical Model. *6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT*), 139 – 145

Ketab, S.S., Clarke, N.L., & Dowland, P. S. (2017). A Robust e-Invigilation System Employing Multimodal Biometric Authentication. *International Journal of Information and Education Technology*, 7(11), 796-802

Samangouei, P., Patel, V.M. & Chellappa, R. (2017). Facial attributes for active authentication on mobile. *IMAVIS*, 58 (12). 181–192.

Samangouei, P., Patel, V.M. & Chellappa, R. (2015). Attribute-based continuous user authentication on mobile devices. *IEEE Int. Conf on Biometrics Theory, Applications and Systems (BTAS)*, 3–7.

Schilit, B., Adams, N. & Want, R. (1994). Context-aware computing applications. *IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'94)*, Santa Cruz, 89–101 (http://sandbox.parc.com/want/papers/parctab-wmc-dec94.pdf

Shaji, S., Das, S. & Kizhakkethottam, J.J. (2015). Review of continuous touch-based user authentication. Proc. *IEEE Int. Conf. Soft-Computing Netw. Secur. ICSNS* 2015.

Singh, U. G. (2015). Solving the 'Riddel' of e-Assessment: Student perceptions. *The International Journal of E-learning and Educational Technologies in the Digital Media (IJEETDM)*, 1(3), 142-153.

Watanabe, Y. & Houryu, T.F. (2013). Toward introduction of an immunity-based model to continuous behaviour-based user authentication on a smartphone. *Procedia Comput. Sci.*, 22(1), 1319–1327

Wu, C., Ding, W., Liu, R., Wang, J., Wang, A.C., Wang, J., Li, S., Zi, Y. & Wang, Z.L. (2018). Keystroke dynamics enabled authentication and identification using a triboelectric nanogenerator array. *Mater. Today*, 29(3), 1-7

Authors Biography

Hussaini Abubakar Zubairu is a Lecturer in the Department of Information and Media Technology, School of Information and Communication Technology, Federal University of Technology, Minna, Niger State, Nigeria. He had his B.Sc and M.Sc in Computer Science from Ahmadu Bello University, Zaria, Kaduna State, Nigeria. He teaches web design and development, Java programming language, computer architecture and e-commerce. His research interests are knowledge management, machine learning and ICT4D. He has published several articles in both local and international journals and also attended conferences. He can be contacted at abu.zubairu@futminna.ed.ng

Idris Mohammed Kolo is a Lecturer in the Department of Computer Science, School of Information and Communication Technology, Federal University of Technology, Minna, Niger State, Nigeria. He had his B.Tech and M.Tech in Computer Science from The Federal University of Technology, Minna- a Technology-based University in Nigeria. He teaches Java Programming Language, Computer Architecture, Algorithms and Programming Languages. His research interests are Data Mining, Intrusion Detection and Evolutionary Algorithms. He has published several articles in both local and international reputable journals and also attended conferences. He can be contacted at idris.kolo@futminna.edu.ng

Stella Oluyemi Etuk is currently working as a Lecturer in the Department of Information and Media Technology at the School of Information and Communication Technology, Federal University of Technology, Minna, Niger State, Nigeria. Her first degree (B.Tech) was in Mathematics and Computer Science in 2008 and her Master’s degree (M.Tech) was in Applied Mathematics (Numerical Analysis) in 2014 from the same University. Her future research interests are in soft computing and Data Science. Her administrative responsibilities include student advising and membership of committee at faculty level in the University. She can be contacted at the following email address: abiolastella@futminna.edu.ng

Faiza Babakano Jada is an Assistant Lecturer in the Department of Information and Media Technology, School of Information and Communication Technology, Federal University of Technology, Minna, Niger State, Nigeria. She obtained her Bsc (Computer Science) from the prestigious American University of Nigeria (2009) on full-tuition scholarships and MTech (Image processing/data mining) from the Federal University of Technology, Minna in 2015. Her research interest includes Data mining, Community and Developmental Informatics. She has published in both national and international journals and conferences. faiza.bkano@futminna.edu.ng

Ilyasu Anda is a Lecturer II in the Department of Library and Information Technology at the Federal University of Technology, Minna, Nigeria. He obtained B.Tech in Library and Information Technology from the same University in 2008, he was also awarded a Master of Science Degree in Information Technology from the University of York, the United Kingdom in 2015. His research interests are in Big Data Analytics. Anda Ilyasu is a Professional Member of the Cyber Security Experts, an association of Nigeria.