Chapter 43
Applications of Keystroke Dynamics Biometrics in Online Learning Environments:
A Selective Study

Anandhavalli Muniasamy

iD https://orcid.org/0000-0001-8940-3954

King Khalid University, Saudi Arabia

ABSTRACT

The biometric authentication in the online learning environment (OLE) is still exploratory and, despite an increase in keystroke dynamics biometrics research, many challenges remain in designing this authentication system due to the fact that it is economical and easily integrated with existing computer security system in OLE. Existing research in keystroke dynamics tends to focus on finding how keystroke dynamics of users can support non-intrusive authentications of users in OLEs. However, there is little evidence that researchers have approached the issue of unauthenticated users to take the role of authenticated users and perform tasks in the OLE with the intent of building models based on the keystroke dynamics of users. In a nutshell, the aim of this chapter is to provide an overview of the existing applications of keystroke dynamics as biometric authentication in the OLE, keystroke dynamics framework being designed for the OLE, advantages and disadvantages of a keystroke dynamics biometrics approach, as well as offering suggestions and possible future research directions.

INTRODUCTION

The prevalence of online education has increased dramatically in the past decade as it offers several significant benefits. (U.S. Higher Education System, 2016; Freidman, 2016; Newton, 2015). Among those benefits are availability, accessibility, affordability, updatability, and economical (Li & Irby, 2008; Ruiz, 2017). However, along with the benefits of online learning come several challenges, one of which is academic dishonesty among students (Grijalva, Nowell, & Kerkvliet, 2006; King, Guyette,

& Piotrowski, 2009). Unethical behavior in schools is rampant (King, Guyette, & Piotrowski, 2009). While cheating in school is not new, it has taken on new forms and is becoming easier to undertake due to increased use of technology to facilitate OLEs (King, Guyette, & Piotrowski, 2009; Sewell, Frith, & Colvin, 2010). The main challenge that the providers of online education facing is to assure a student who wants to take an exam is really the individual who is expected to attend to that test. Cyber cheating is far more widespread than originally believed because it is nearly impossible to verify the identity of an individual being assessed online (Moini & Madni, 2009).

To solve this cyber cheating issue, US government passed the Higher Education Opportunity Act (HEOA 2008) which requires that institutions offering online education have to make greater access control efforts for the purposes of assuring that students of record are those actually accessing the systems and taking online exams by adopting identification technologies as they become more ubiquitous (Monaco, Stewart, Cha, & Tappert, 2013). To comply with the requirements of this law, institutes of higher education who provide online courses have begun exploring the use of biometrics to authenticate students.

Biometric methods verify and authenticate the identity of a user based on a physiological or behavioral characteristic (Miller, 1994). One frequently used authentication mechanism is using usernames and passwords (Bours, 2012); thus "once only" authentication. However, in the case of online assessments and exams, there is a requirement to monitor the identity of users throughout the course of an entire assessment, thus continuous authentication. This includes how science and technology can be utilized to identify physiological or behavioral attributes that are unique to individual students (Karnan, Akila & Krishnaraj, 2011).

Commonly used biometric indicators (e.g., finger or palm prints, iris scans, facial and voice recognition) are effective because technology can accurately authenticate a user's identity by comparing samples of unique physiological characteristics (Karnan, Akila & Krishnaraj, 2011). The main concern with using biometrics in the authentication process is systems needed to capture and compare these metrics can be prohibitively expensive to implement (Panchumarthy, Subramanian, & Sarkar, 2012). They can also be somewhat intrusive (e.g., taking facial recognition videos while working on a course). These biometrics are good gatekeeper measures; however, they do not serve well as in-system verification tools. It promotes high recognition accuracy due to its permanence and high uniqueness. However, it possibly suffers from low public acceptance due to invasiveness (iris scanning) and high implementation cost (DNA analysis) in large-scale deployment.

Behavioral traits such as handwriting, signatures, keystroke dynamics, and mouse dynamics can be used like physiological characteristics to identify individuals (Karnan, Akila & Krishnaraj, 2011). Metrics using keystroke and mouse dynamics can examine the behavior of those admitted into the learning system to verify the person completing the coursework is the person signed up to take the course. These metrics can be somewhat less accurate than physiological characteristics as they often change slightly depending on circumstances, but they are less obtrusive and obtained during the process of an individual completing work in the course rather than merely at the beginning of a work session (Marsters, 2009).

Keystroke dynamics is a behavioral biometric characteristic based on the assumption that different people type in a unique manner on digital devices. (Joyce & Gupta, 1990) portrayed that keystroke dynamics in online assessment could lead to increased security when a learner is completing a test unsupervised at a distance using technology. Keystroke dynamics record and analyze the way a user types, based on habitual typing patterns (Monrose & Rubin, 2000). Like a fingerprint or a signature, the users can be identified using keystroke dynamics to create what is called a keyprint that represents the user's typing behavior. (Monrose & Rubin,1997) suggest that the use of keystroke dynamics to create

Related Content

A Process-Oriented and Technology-Based Model of Virtual Communities of Practices: Evidence from a Case Study in Higher Education
Giustina Secundo, Gianluca Eliaand Cesare Taurino (2010). *Web-Based Learning Solutions for Communities of Practice: Developing Virtual Environments for Social and Pedagogical Advancement (pp. 249-262).*
www.irma-international.org/chapter/process-oriented-technology-based-model/36367

Reusing Alignments for Discovering Instances Correspondences
Wafa Ghemmaz, Fouzia Benchikhaand Maroua Bouzid (2021). *International Journal of Web-Based Learning and Teaching Technologies (pp. 60-95).*
www.irma-international.org/article/reusing-alignments-for-discovering-instances-correspondences/279575

An Examination of High School Students' Online Engagement in Mathematics Problems
Woong Lim, Ji-Won Son, Susan Gregsonand Jihye Kim (2018). *International Journal of Web-Based Learning and Teaching Technologies (pp. 1-15).*
www.irma-international.org/article/an-examination-of-high-school-students-online-engagement-in-mathematics-problems/198373

Building Quality Online Courses: Online Course Development Partnership and Model
Veronica Outlaw, Margaret L. Riceand Vivian H. Wright (2017). *Handbook of Research on Building, Growing, and Sustaining Quality E-Learning Programs (pp. 301-323).*
www.irma-international.org/chapter/building-quality-online-courses/165788

The Nuts and Bolts of Online Course Planning
Ron Lombard (2010). *Technology Leadership in Teacher Education: Integrated Solutions and Experiences (pp. 14-29).*
www.irma-international.org/chapter/nuts-bolts-online-course-planning/44352