Towards a Framework of Biometric Exam Authentication in E-Learning Environments

Michelle M. Ramim, Nova Southeastern University, USA, 3301 College Avenue, Fort Lauderdale, FL 33314, USA; E-mail: ramim@nova.edu
Yair Levy, Nova Southeastern University, USA, 3301 College Avenue, Fort Lauderdale, FL 33314, USA; E-mail: levyy@nova.edu

ABSTRACT
In the past fifteen years the use of Internet technologies has been substantially growing for delivery of educational content. E-learning environments have been incorporated in many universities for the delivery of e-learning courses. However, opponents of e-learning claim that a central disadvantage of such teaching medium is the growing unethical conduct in such environments. In particular, opponents of e-learning argue that the inability to authenticate exam takers is a major challenge of e-learning environments. As a result, some institutions proposed to take extreme measures including asking students to take exams in proctor centers or even abandon completely the offering of e-learning courses in their institutions. This paper attempts to address this important problem by proposing a theoretical framework that incorporates available fingerprint biometric authentication technologies in conjunction with e-learning environments to curb unethical conduct during e-learning exam taking. The proposed framework suggests practical solutions that can incorporate a random fingerprint biometric user authentication during exam taking in e-learning courses. Doing so is hypothesized to curb exam cheating in e-learning environments. Discussions on future research and possible implications of the proposed theoretical framework for practice are provided.

Keywords: E-learning Environments, Biometric Systems, Unethical Conduct, Academic Misconduct, Online Exam Security, Secured Exam Submission.

1. INTRODUCTION
This paper proposed a theoretical framework for fingerprint biometrics authentication of exam takers in e-learning environments. The following section provides literature review on the increase use of e-learning environments in higher educational institutions. Additionally, the subsequent section provides a review of literature on issues related to unethical conduct in educational settings and in e-learning environments. The subsequent section provides a review of literature related to security issues in e-learning environments, biometric solutions and fingerprints biometric solutions. Subsequent section suggests the theoretical framework combining existing technologies into electronic exams (e-exams). The final section addresses the conclusions with expected contribution of the proposed framework, review of some observed limitations of the proposed theoretical framework, and proposed future research.

2. THEORETICAL BACKGROUND
2.1 E-Learning and E-Learning Environments
Teaching via the Internet has become a popular choice for academic institutions as well as business organizations (Hiltz & Turoff, 2005). Advances in information systems have enabled educational institutions to implement electronic learning (e-learning) systems as a teaching environment (Alavi & Leidner, 2001). Furthermore, e-learning has become a powerful medium for academic institutions and corporate training due to the incorporation of cutting edge technologies. Hiltz and Turoff (2005) have commented that e-learning is “the latest of social technologies that ... has improved distance learning” (p. 59).

The spectacular growth in e-learning in the past decade has been documented in numerous studies. The U.S. National Center for Education Statistics (NCES) reported that “56 percent of all 2-year and 4-year degree-granting institutions offered distance education courses ... during 2000–2001 academic year” (US NCES, 2005, p. 3). The dramatic growth in distance and e-learning is evident in the number of institutions that offer e-learning. US NCES reported that “undergraduate level online courses were offered at 48 percent of all institutions while graduate level online courses were at 22 percent of all institutions” (p. 3). Among these institutions, e-learning courses and video technology were the most common kinds of instruction delivery systems. NCES reported that 90% of institutions employed e-learning courses using asynchronous communication systems. While, only 43% of institutions employed synchronous communication systems for the delivery of e-learning courses (US NCES, 2005).

Gunasekaran, McNeil, and Shaul (2002) described the growth in e-learning as the “new dynamic learning models ... and is leading the [academic] market to a significant paradigm and cultural change” (p. 45). Courses and entire degree programs are delivered via the Web anywhere at anytime. In addition, e-learning courses are offered by private, public as well as corporate universities. As a result, new resources such as e-books, books on CD-ROMs and e-exams have been adapted to e-learning courses. Students’ enrollment in e-learning courses has proliferated reaching more than three million students in the U.S. in 2005 (US NCES, 2005). About 82% of those online students were enrolled in undergraduate level courses during the year 2000-2001 (US NCES, 2005). As a result numerous academic institutions are planning to increase the number of e-learning courses to meet the growth in this demand. However, security issues related to e-learning systems have been raised by several scholars (Ramim & Levy, 2006). Moreover, opponents of e-learning argue that the inability to authenticate exam takers is one of the major challenges of e-learning medium. Although there is a major growth in e-learning programs, some institutions proposed to take extreme measures including asking e-learning students to take exams in proctor centers (Gunasekaran et al., 2002). However, this requirement may not be feasible for e-learning programs with students in remote locations or under various circumstances such as students who are in military service in remote or combat areas, students with severe disabilities, and working professionals. In order to protect the integrity of exams in e-learning environments, solutions for such a significant problem are warranted.

2.2 Unethical Conduct in E-Learning
Given the development of technologies and the demonstrated growth of e-learning usage in academia, students’ unethical conduct in e-learning has become a major concern (Kennedy Nowak, Raghubaram, Thomas, & Dacis, 2000). Pillsbury (2004) argues that students’ unethical conduct has intensified as a result of the use of technology and the Internet. Most administrators and instructors focus on one type of unethical conduct, namely plagiarism (Naude & Hörne, 2006). However, students’ unethical conduct encompasses a wide array of behaviors including technology enabled behaviors such as cheating during an exam by using technology devices (i.e. PDA, calculator, and cellular phone), engaging in online collaboration when it’s forbidden (i.e. groupware like Instant Messenger services, chats, forums, and newsgroups), and deceiving (i.e. logging with another student’s username/password). These unethical technology enabled conduits are often undetected by instructors in e-learning courses. Moreover, numerous researchers admit that most e-learning programs adopt policies and practices from traditional learning programs and ignore the technology related issues (Kennedy et al., 2000;
McCabe, 2003; Gunasekaran et al., 2002), Pillsbury (2004) noted a number of Web enabled detection mechanisms such as turnitin.com™ that are available to curb plagiarism. Though, extensive body of knowledge is available on plagiarism detections (Decoo, 2002; Hamilton, 2003; Hannabuss, 2001; McLafferty & Foust, 2004), very little attention has been given to providing solutions to other students' unethical conduct such as cheating on exams in e-learning courses. Pillsbury (2004) noted that detection mechanisms for unethical conduct are necessary not only in the initial portal access. Moreover, additional mechanisms are necessary to authenticate users' access in various e-learning course activities (Newton, 2003). For example, instructors attempt to verify that e-exam submission is truly performed by a given student rather than another one.

According to the Center for Academic Integrity (2005), cheating on exams has been reported at an alarming rate of 74%. McCabe and Trevino (1996) reported that 70% of students in their study confessed to cheating on multiple exams. A study by Pincus and Schmellink (2003) compared faculty members' perceptions on various students' unethical conducts seriously. They concluded that students' unethical conduct related to exam taking perceived by faculty to be one of the most serious unethical behaviors (Pincus & Schmellink, 2003). Similarly, Dick et al. (2002) also noted that 24% their study participants believed that “advances on technology have lead ... to increase cheating” (p. 173). The perceived seriousness of cheating on exams has led numerous academic institutions to reduce their e-learning course offering and in other instances, cease e-learning altogether. In fact, Gunasekaran et al. (2002) admitted that the inadequate technology has led some academic institutions to cease offering e-learning courses due to concerns over the quality of students' assessment and standards. Thus, the central aim of this paper is to propose a conceptual level security solution for this out-braking phenomenon by suggesting a theoretical framework of biometrics authentication to secure e-exams.

2.3 Security in E-Learning

Given the importance of e-learning environments for academic institutions, security related challenges of e-learning environments are capturing the attention of program administrators. Ramim and Levy (2006) discussed a case study of an academic institution that faced a tragic cyber attack to their e-learning environment by an insider intruder. Other scholars have documented related security problems in academic institutions. Yu and Tao (2003) discussed security challenges of e-learning environments. However, their exploration focused on shielding the technology infrastructure against unauthorized users. Current security practices in e-learning systems relay principally on the utilization of passwords authentication mechanisms. Similarly, Huang, Yen, Lin, and Huang (2004) discussed aspects of security in e-learning systems and suggested attention to two layers when securing e-learning systems. The first layer addresses security of the technology infrastructure used to facilitate e-learning (i.e. hardware, networks, etc.) and the second layer addresses the various applications employed in enabling e-learning (i.e. learning management systems, rich media communication tools, etc.). Huang et al. (2004) criticized existing proprietary e-learning systems for not paying enough attention to the issue of properly authenticating students, in particular during quizzes and exams. Hugl (2005) noted numerous security related technologies that are not currently employed in e-learning. One such solution can include biometric technologies that may potentially become an integral part of e-learning systems.

2.4 Biometric Solutions

According to Tabitha, Pirin, Boswell, Reithel, and Barkhi (2006) biometric is defined as “the application of computational methods to biological features, especially with regard to the study of unique biological characteristics of humans” (p. 3). Such unique biological characteristics relies on individual humane identities such as DNA, voice, retinal and iris, fingerprints, facial images, hand prints, or other unique biological characteristics. Tabitha et al. (2006) note that biometric is “a method of identification that has been growing in popularity” (p. 2). Moreover, Pons (2006) notes that biometric devices are technological devices that utilize an individual’s unique physical or behavioral characteristics to identify and authenticate the individual precisely. Essentially, biometric technologies operate by scanning a biological characteristic and matching it with the stored data. Jain, Hong, and Pankanti (2000) note that a biometric system is “essentially a pattern recognition system that makes a personal identification by establishing the authenticity of a specific physiological or behavioral characteristic possessed by the user” (p. 92).

Copyright © 2007, Idea Group Inc. Copying or distributing in print or electronic forms without written permission of Idea Group Inc. is prohibited.
size as standard mouse, however, it also has an integrated fingerprint scanner that is managed by client side software and controlled by server side software centralized on an authentication server. Figure 2 provides an image of Authenteon™, a biometrics authentication server. JayPeetek Inc. claims that their patented Scan.U.Match™ biometrics mouse solution is unique as it “does not capture the finger image and scrambles the algorithm at the point of scan”, rather it “creates a 500 byte secure template that cannot be replicated into a user fingerprint” (JayPeetek Inc.). As such, the Scan.U.Match™ is claimed to be highly reliable with “false rejection rate” that is only 0.01%, or 1 out of 100,000 cases.

There are numerous other vendors that offer similar solutions in attractive prices. Examples of some of the other vendors include SecuGen® Biometrics Solutions (2005) with their OptiMouse III™, onClick® Corp. (2005) with their VIA™ solution, to name a few.

Aside from the biometrics fingerprint mouse solutions, there are other biometrics fingerprint solutions including keyboard with fingerprint pad scanner (See Figure 3), PCMCIA fingerprint scanner (See Figure 4), and USB fingerprint token scanners (See Figure 5).

3. PROPOSED METHODOLOGY AND DATA COLLECTION

The proposed theoretical framework that this work focuses on is to incorporate biometric fingerprint solutions for user authentication during e-exams. Figure 6 demonstrate the proposed conceptual solution. In standard e-exam, the learner’s access is authenticated once by the e-learning server at login for the entire duration of the activity session, while the repeated authentication performed is based on the password cached in the browser. As such, students are able to login to the e-learning server and have someone else take the e-exam on their behalf. The proposed solution will enhance the current authentication process by adding the fingerprint biometrics solution. For example, in WebCT, during e-exam a random fingerprint authentication can occur to validate the e-exam taker. Although not a foolproof approach, requiring the fingerprint authentication of the learner randomly during
e-exam with required very short fingerprint scanning response time should provide additional added security. It may discourage learners from having someone else take the e-exam for them. Therefore, the central claim of this proposed approach is that the incorporation of fingerprint biometrics solution in conjunction with e-learning environments will enable a reduction in exam cheating.

5. CONCLUSION AND RECOMMENDATIONS FOR FUTURE RESEARCH
Unethical conduct, in particular cheating in e-exams was documented in literature as a growing concern by many higher educational institutions. The proposed theoretical framework suggested above is unique as it proposed a biometric solution for exam taking in e-learning environments. This theoretical framework may add to the general knowledge of e-learning environments by addressing a major issue of e-exam cheating. Future work in this line of research should incorporate this theoretical approach and conduct a study on the incorporation of biometric solutions in e-exams. One example of a study may include comparison of the same instructor teaching two e-learning sections of the same course, where one section will use regular e-exams and the other section will use the fingerprint biometric approach proposed. The study can propose that:

Proposition 1: Students taking e-exams using the fingerprints biometric solution will have lower grades on the e-exam than their counterparts.

Proposition 2: Students taking e-exams using the fingerprints biometric solution will take longer time to complete their e-exam than their counterparts.

Results of such study can provide initial investigation in an attempt to address the outweighing phenomena of unethical conduct in e-learning exam taking. If results of this propose study will show that the group of learners who took the exams using the fingerprints biometric solution will have lower grades and take longer time to complete their exam, thus, have a lower cheating rate. Having such results will allow suggesting the proposed framework for higher educational institutions to incorporate it in order to reduce cheating in online exam taking.

Future investigation should be performed by implementing the proposed framework and conducting the experiment proposed above. Additional research can be conducted on the incorporation of biometric solutions to address other academic misconduct behaviors in e-learning environments. However, researchers must be aware of the limitations associated with the theoretical framework proposed here. The first observed limitation deals with the fact that in a remote setting, students may ask to have a subject matter expert seat next to them while they take the exam. The current proposed framework is overlooking this possibility and additional work to address such unethical behavior is warranted. The second observed limitation of the proposed framework is the funding the costs associated with implementing such study in an experimental basis, let alone in a large scale e-learning program. Additional work is needed in exploring the costs and funding sources needed to provide the technological and implementation aspect of this framework. A third observed limitation is related to individual perceptions on the use of biometric systems. For example, Alterman (2003) note several perceived ethical issue with biometric systems, while Tabitha et al. (2006) document a study on the acceptance of such system by individuals. Future research is warranted to further explore issues related to the ethical and acceptance of biometric systems in the context of e-learning.

REFERENCES


ENDNOTE

1 Source: http://www.jaypeetex.com/products/Biometrics/Fingerprints/Scanunmatch.htm
2 Source: http://www.jaypeetex.com/products/Biometrics/Fingerprints/Authentcon.htm
3 Source: http://www.secugen.com/products/pk.htm
5 Source: http://bssc.sel.sony.com/Professional/puppy/products.html
Related Content

An Approach to Distinguish Between the Severity of Bullying in Messages in Social Media

A Framework for Exploring IT-Led Change in Morphing Organizations
[www.irma-international.org/chapter/a-framework-for-exploring-it-led-change-in-morphing-organizations/183782/](www.irma-international.org/chapter/a-framework-for-exploring-it-led-change-in-morphing-organizations/183782/)

Road Safety 2.0: A Case of Transforming Government’s Approach to Road Safety by Engaging Citizens through Web 2.0
Dieter Fink (2013). *Cases on Emerging Information Technology Research and Applications* (pp. 216-238).
[www.irma-international.org/chapter/road-safety-case-transforming-government/75862/](www.irma-international.org/chapter/road-safety-case-transforming-government/75862/)

Incremental Learning Researches on Rough Set Theory: Status and Future
[www.irma-international.org/article/incremental-learning-researches-on-rough-set-theory/111315/](www.irma-international.org/article/incremental-learning-researches-on-rough-set-theory/111315/)

Exploring Drivers of Closed Loop Supply Chain in Malaysian Automotive Industry
[www.irma-international.org/chapter/exploring-drivers-of-closed-loop-supply-chain-in-malaysian-automotive-industry/184241/](www.irma-international.org/chapter/exploring-drivers-of-closed-loop-supply-chain-in-malaysian-automotive-industry/184241/)