Interdisciplinary Journal of E-Learning and Learning Objects **Volume 5, 2009**
IJELLO special series of Chais Conference 2009 best papers

Initial Development of a Learners' Ratified Acceptance of Multibiometrics Intentions Model (RAMIM)

Yair Levy
Nova Southeastern University, GSCIS, Ft. Lauderdale, FL, USA
levyy@nova.edu

Michelle M. Ramim
Nova Southeastern University, Huizenga School of Business, Ft. Lauderdale, FL, USA
ramim@nova.edu

Abstract

Authenticating users is a continuous tradeoff between the level of invasiveness and the degree of system security. Password protection has been the most widely authentication approach used, however, it is easily compromised. Biometric authentication devices have been implemented as a more robust approach. This paper reports on initial results of student perceptions about their acceptance of a multibiometrics authentication approach in the context of e-learning systems. Specifically, this paper reports on the initial empirical development of a learners' Ratified Acceptance of Multibiometrics Intentions Model (RAMIM). The model proposed investigates the impact of students' code of conduct awareness, perceived ease-of-use, perceived usefulness, and ethical decision making on learners' intention to use multibiometrics for authentication during e-learning exams. The study's participants included 97 non-information technology (IT) students who attended e-learning courses. Additionally, results of a path analysis using Partial Least Square (PLS) indicate that perceived usefulness has the most significant impact on learners' intention to use multibiometrics during e-learning exams. Students' ethical decision making and perceived usefulness demonstrated significant impact on their intention to use multibiometrics. Additionally, students' code of conduct awareness appears to have a positive impact on their ethical decision making. Conclusions are discussed including recommendations for future research on extending this initial research into applied experiments to address e-learning security issues.

Keywords: E-learning Security, Biometrics Systems, Multibiometrics in E-Learning, Technology Acceptance, Online Exam Security, Secured Exam Submission.

Introduction

Security concerns associated with information technology (IT) has intensified with the growth of IT enabled networks within organizations, the growing use of organizational electronic records, and organizational dependency on *information* as a key corporate asset (Gal-Or & Ghose, 2005; Gerber & von

Editor: Alex Koohang
An earlier, shorter version of this paper was presented at the Chais conference 2009, in Raanana, Israel, and included in Y. Eshet-Alkalai, A. Caspi, S. Eden, N. Geri, & Y. Yair (Eds.), *Proceedings of the Chais conference on instructional technologies research 2009: Learning in the technological era*. Raanana: The Open University of Israel. http://www.openu.ac.il/research_center_eng/conferences.html

Solms, 2008; Goodhue & Straub, 1991; Wang, Chaudhury, & Rao, 2008). In the context of higher education, e-learning has experienced a massive growth over the past decade, with reports indicating 10% increase of e-learning students in the U.S. higher education annually (Koohang, Riley, Smith, & Schreurs, 2009). According to Zhang, Zhao, Zhou, and Nunamaker (2004), "E-learning can be defined as technology-based learning in which learning materials are delivered electronically to remote learners via a computer network" (p. 76). Additionally, Koohang et al. (2009) reported a staggering number of nearly 20% of all higher education students in the U.S. attended at least one e-learning course during the fall term of 2006, while others have indicated a massive increase in use of e-learning systems to support on-campus courses, known as *hybrid courses* (Buzzetto-More, 2008). However, such astounding growth of e-learning, facilitated via e-learning systems, has also raised concerns about proper authentication of students during e-learning course activities (Kritzinger, 2006; Kritzinger & von Solms, 2006; Ramim & Levy, 2006). Valid authentication of IT users is a perpetual challenge amongst organizations (Furnell, Dowland, Illingworth, & Reynolds, 2000; Siponen & Heikka, 2008). Moreover, according to Furnell et al. (2000), use of password authentication is "easily compromised" (p. 529). Yet, Kritzinger and von Solms (2006) admitted that "one aspect that has not received much attention is the important role *Information Security* plays within the e-learning environment" (p. 319). According to Ramim and Levy, authentication of students in e-learning systems should expand beyond the superficial username/password verification upon entry to the system to a more diverse authentication approach. They also noted that such approach may help reduce academic misconduct incidents in e-learning including cheating in exams (Ramim & Levy, 2007). Furthermore, a recent U.S. Higher Education Opportunity Act (HEOA) (U.S. Department of Education, 2008) mandates all higher education accreditation bodies to require:

> an institution that offers distance education or correspondence education to have processes through which the institution establishes that the student who registers in a distance education or correspondence education course or program is the same student who participates in and completes the program and receives the academic credit. (p. 248)

In recent years, the price of commercial biometrics authentication devices has been steadily dropping (Anderson & Choobineh, 2008). The use of security related devices has sharply increased beyond highly secured environments such as financial institutions, government agencies, and military facilities (Cavusoglu, Mishra, & Raghunathan, 2005). Nowadays, biometrics authentication devices are utilized to measure employee attendance and track employee's daily activities (Yeh & Chang, 2007). Additionally, Podio and Dunn (2001) reported the use of biometrics in school lunch programs in the U.S. However, there is a growing concern about the invasiveness of such devices and effective safeguarding of biometrics information, as well as potential misuse of information captured by biometrics devices (Lin, Chuang, & Fan, 2005). Some of these concerns maybe attributed to lack of education and/or experience with biometric technologies. Thus, prior to implementation of such advanced technologies, an investigation of the factors that may impede the acceptance of such devices is warranted (James, Pirim, Boswell, Reithel, & Barkhi, 2006). Given the demonstrated staggering increase in the use of e-learning systems in higher education and the new requirements set by HEOA, such investigation is further warranted in the context of e-learning systems security.

This research proposes an investigation of a multibiometric authentication method in the context of e-learning systems. As the context of this research is in e-learning, this work reports on initial empirical results collected in the process to develop and validate a learners' Ratified Acceptance of Multibiometrics Intentions Model (RAMIM). The multibiometrics authentication approach includes two devices: fingerprint scanner and Web-camera head geometry scanner to be integrated to monitor e-learning activities (Levy, 2008). Information systems (IS) literature reports extensive evidence that users' perceived usefulness and ease-of-use are strong predictors of tech-

nology acceptance (Simon & Paper, 2007; Viswanath & Hillol, 2008). Moreover, there is compelling empirical evidence in literature that intention to use a technology is a significant contributor to actual technology acceptance and use (Bagozzi, 2007; Gefen, Karahanna, & Straub, 2003). Additionally, organizational behavior literature provides support that employees' code of conduct awareness and their ethical decision making are potential antecedent constructs to technology use (Cronan, Leonard, & Kreie, 2005; Kreie & Cronan, 1998). Following such literature and in the context of e-learning, this work was set to investigate the contribution of students' perceived usefulness and ease-of-use of e-learning systems, their university's code of conduct awareness, and their academic ethical decision making to their perceived intention to use multibiometrics during e-learning.

Information Security in E-Learning

The surge in use of e-learning systems in higher education has been documented extensively (Buzzetto-More, 2008; Eshet-Alkalai & Geri, 2007; Geri & Gefen, 2007; Koohang et al., 2009; Levy, 2006). Over the past decade and a half, considerable amount of research has been focused on developing and improving e-learning systems to offer more effective and efficient learning experience. Additionally, concerns about security of e-learning systems are not new (Littman, 1996, 1997, 1998). However, some researchers have raised a valid criticism that information security in e-learning research is scarce. For example, El-Khatib, Korba, Xu, and Yee (2003) criticized that "Most e-learning innovations have focused on course development and delivery, with little or no consideration to privacy and security as required elements" (p. 2). Kritzinger (2006) concurred by claiming that "A lot of research has been done regarding the advantages of e-learning. However, not much attention is given to the important role that information security plays within the e-learning environment" (p. 347). Clearly, there is a substantial interest for additional research on issues related to e-learning security.

Levy (2008) developed a list of 36 e-learning activities students value most during their e-learning experience, and a majority of these are subject to security threats. Kritzinger (2006) indicated that e-learning activities open doors to a considerable amount of compromises to an e-learning system. Kritzinger and von Solms (2006) identified 11 information security risks students and course instructors may anticipate when using e-learning systems. Such security risks include: unauthorized alteration to course material, fake course material posted to students, unauthorized copying of submitted assignments, unauthorized changes or removal of submitted assignments, unauthorized changes or removal of course grades, unauthorized access to e-learning exams, unauthorized changes or removal of e-learning exams, receiving unauthorized assistance during e-learning exams, destruction of e-learning course and/or database, denial of service attack to the e-learning server, as well as interception and misuse of students' and course instructors' e-learning system authentication information. Furnell (2008) also provided a similar argument and outlined five information security threats that students might face when taking e-learning courses, including spam, phishing, spyware, malware, and hackers. Additionally, he outlined three key information security threats educational institutions might face when running e-learning systems, including data theft, malicious alteration to e-learning content, and denial of service attacks. He then indicated that as e-learning students have been reported in literature to be more active online than other Internet users, such threats appear more prominent for them than for other Internet users.

Recently, Bailie and Jortberg (2009) as well as Bedford, Gregg, and Clinton (2009) conducted research on two different authentication approaches during e-learning exams. Bailie and Jortberg (2009) discussed the collaboration between Acxiom® Corporation and Blackboard™ Inc on the incorporation of challenge questions into e-learning exams. This technique enables the course instructor to set an e-learning exam whereby challenge questions are required prior to entry to the

e-learning exam questions. Their pilot study was conducted during 2008 and early 2009. Although the number of participating students was not reported, Bailie and Jortberg (2009) provided data of 183 identity verifications instances used, where an average of 8% either failed the verification process or the process was incomplete (i.e. student aborted the verification process). The key thrust behind their research was that adding the challenge questions can assist in the authentication of e-learning students by preventing imposters from logging in. Bedford et al. (2009) discussed a case study of implementing Remote Proctor™ system by Software Secure®. Remote Proctor™ system is a device combining a single sign-on authentication using a swipe fingerprint biometric reader, voice recorder, and a camera set in a cone/sphere shaped cover. This system is combined with Software Secure®'s browser and desktop lockdown application called SecureExam™, while recording of the students' environment is being done and transmitted to Software Secure®'s servers. Bedford et al. (2009) used a sample of 31 students who experienced the system during e-learning exams and 20 faculty members, who were asked to review the recorded videos of students taking the e-learning exams. Their study queried students on their acceptance of such technology using perceived usefulness and perceived ease-of-use. They concluded that a majority of students find Remote Proctor™ system to be easy to use and useful in deterring cheating in e-learning exams and are willing to accept such technology. They also found that a majority of instructors supported the adoption of this technology. Unfortunately, these current commercially available techniques discussed by Bailie and Jortberg (2009) as well as Bedford et al. (2009) are dependent upon the use of a third party provider (Acxiom®, Software Secure®, etc.). While these can be a viable starting point in ensuring tighter security during e-learning exams, the use of third party provider at any part of the student's authentication, rather than the educational institution, may raise concerns about student privacy among school administrators. Additionally, there are other e-learning activities beyond e-learning exams that provide significant credit for students towards their final course grade, such as discussion forums and assignment submissions. Concentrating significant research efforts on approaches that can only secure e-learning exams may open the doors for students to engage in academic misconduct in other e-learning activities. Therefore, secured student authentication that can go beyond a single sign-on is needed, while extension of such work should expand even beyond securing a single e-learning activity (i.e. e-learning exam) into multiple e-learning activities. However, prior to implementing such technique, an investigation of the acceptance of secured student authentication is necessary.

Biometrics and Authentication

A vital aspect of security is authentication whereby the system verifies the user's identity as declared (Liebl, 1993). Authentication includes two principal elements, namely, identification and verification. During the identification stage, the user declares his or her identity followed by the verification stage in which the identity is validated. Consequently, IT enabled authentication protocols establish the identification processes between the host and the user. Examples of IT enabled authentication protocols include password authentication protocol (Simon & Paper, 2007), encryption, and Kerberos. The standardization of authentication protocols for authentication systems is critical to establishing a secured environment (Liebl, 1993; Oorschot & Thorpe, 2008).

According to Furnell et al. (2000), "There are three main approaches to user authentication: something the user knows (e.g. password or personal identification number (PIN)), something the user has (e.g. a card or other token) and something the user is (e.g. a biometric characteristic)" (p. 529). Funnel et al. (2000) and Oorschot and Thorpe (2008), as well as Rodwell, Furnell, and Reynolds (2007), suggested that, while passwords are the most common authentication methods, passwords tend to be undermined by users. Though users perceive passwords to be the preferred method, there is a need to promote additional authentication methods including physiological and behavioral biometrics. As a result, researchers recommend enhancing authentication methods by

utilizing multiple means of authentication to provide for better authentication verification (Mizuno, Yamada, & Takahashi, 2005; Tsalakanidou, Malassiotis, & Strintzis, 2007).

Research efforts in the area of biometrics have been driven partly as a result of the increase in identity fraud crimes and the compromising of existing identification methodologies (James et al., 2006). Moreover, the U.S. Federal Trade Commission (U.S. Federal trade commission, 2008) has reported that financial loss resulting from such crimes has been mounting and exceeds $1.2 billion annually. As a result, business organizations and government agencies have been motivated to identify and adopt advanced identification technologies (James et al., 2006; Wang et al., 2008). While prices of biometric solutions have been declining, ongoing research about biometrics has focused on three main themes. These three themes include: a) adoption and utility (James et al., 2006; Woodward, 1997), b) methods including biological and behavioral (Clarke & Furnell, 2007; James et al., 2006; Pusara & Brodley, 2004), and c) evaluation of back-end technologies (Abate, Nappi, Riccio, & Sabatino, 2007; Rodwell et al., 2007).

James et al. (2006) defined biometrics as "biological features, especially with regard to the study of unique biological characteristics of humans" (p. 3). Such unique biological characteristics refer to individual human identities such as DNA, voice, retinal and iris, fingerprints, facial images, hand prints, or other unique biological characteristics. James et al. (2006) noted that biometric is "a method of identification that has been growing in popularity" (p. 2). Moreover, Pons (2006), as well as Jain, Hong, and Pankanti (2000), noted that biometric devices are technological devices that utilize an individual's unique physical or behavioral characteristic to authenticate (identify and verify) an individual almost precisely given very low error rate. Essentially, biometric technologies operate by scanning a biological characteristic and matching it with stored data. The U.S. Federal Bureau of Investigation (FBI) (U.S. Federal Bureau of Investigation, n.d.) has been using fingerprint identification system and claims to have "the largest biometric database in the world", while Disney™ has started using fingerprint scanning as added security to their theme parks following 9/11 (Ramim & Levy, 2007).

Sasamoto, Christin, and Hayashi (2008), as well as Pusara and Brodley (2004), referred to keystrokes dynamics and mouse clicks as examples of behavioral characteristics. Though behavioral-characteristic-based biometrics has been associated with a low error rate in lab settings, further work is needed to commercialize such methods to large scale systems. Additionally, there is a recent trend in biometric practice to integrate more than a single biometric method of authentication in order to increase its accuracy, transparency, and reliability beyond the initial point of entry while monitoring real-time users' activity in a non intrusive manner (Clarke & Furnell, 2005, 2007; Jain & Ross, 2004; Ross, Nandakumar, & Jain, 2006).

Following the literature reviewed above, this paper proposes a theoretical model on the integration of multibiometrics and e-learning systems. Multibiometrics, also known as 'multimodal biometrics' or 'multiple biometric modalities', is defined as a multilateral model scheme that utilizes a combination of two or more different biometric features, biological and/or physiological characteristics (Ross et al., 2006; Snelick, Uludag, Mink, Indovina, & Jain, 2005). Examples of multibiometrics include combinations of face geometry, facial thermogram, fingerprint, hand geometry, ear, palmprint, voice, lip movement, retina, hand vein, iris, signature, and voice-print (Ross et al., 2006). According to Jain and Ross (2004), "multibiometric systems provide anti-spoofing measures by making it difficult for an intruder to simultaneously spoof the multiple biometric traits of a legitimate user" (p. 38). Multibiometrics aids to authenticate and verify users in a secured environment (Ross et al., 2006). Additionally, multibiometrics can enable ongoing non-intrusive verification not only at the point of entry but also throughout a logged-in session and ongoing activities. Thus, multibiometrics can further support the attempt to achieve a near foolproof protection against unauthorized access by overcoming the limitation of a single biometrics method (Tsalakanidou et al., 2007). Therefore, such a multi-faceted authentication approach us-

ing multibiometrics has a promising potential in e-learning systems. This important integration appears very valuable for universities that offer e-learning programs, especially those that are accredited and will be required to comply with the requirements set by the HEOA.

In the context of higher education, Ramim and Levy (2007) indicated that there is a very limited amount of research conducted about the incorporation of biometrics into educational settings, let alone into the authentication of students when using e-learning systems. Major inhibitors of such research maybe attributed to the funding needed to purchase biometrics, integrate it into e-learning systems, and train students on using such technologies. As these are fruitful extensions of this work, this study was focused only on the assessment of students' perceptions about their acceptance of a 'multibiometric' authentication method during e-learning exams. The multibiometric authentication method proposed includes two devices: fingerprint scanner and Web-camera head geometry scanner. This study outlines the initial development and validation of the learners' Ratified Acceptance of Multibiometrics Intentions Model (RAMIM). Figure 1 demonstrates examples of latest devices for integration into the multibiometrics method to authenticate students during e-learning activities, including the (a) DigitalPersona®'s U.are.U 4500 Fingerprint Reader (DigitalPersona, nd) and the (b) Logitech® Portable Webcam C905 (Logitech, nd), which fits laptops and mobile computers.

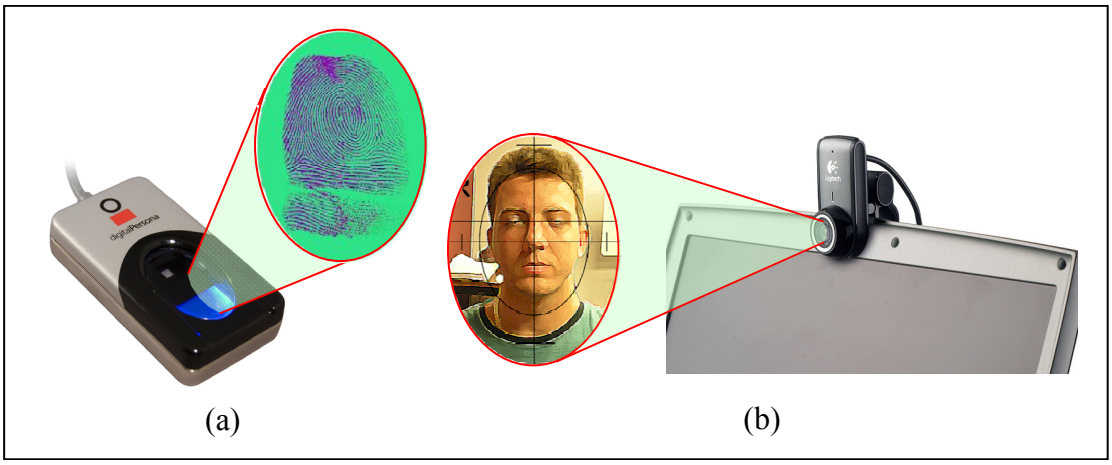

Figure 1. Examples of Devices as Part of the Multibiometric Method to Authenticate Students during E-learning Activities

E-Learning Acceptance

One of the most prominent studies about users' acceptance of information technologies is the Technology Acceptance Model (TAM) by Davis (1986, 1989) and its successors technology acceptance models (Venkatesh & Bala, 2008; Venkatesh, Morris, Davis, & Davis, 2003). Technology acceptance models are based on the Theory of Reasoned Action (TRA) proposed by Ajzen and Fishbein (1980). Accordingly, such models of technology acceptance propose two central constructs, perceived usefulness and ease of use, which were found to be strong predictors of intentions to use a technology and ultimately impact actual technology usage (Davis, Bagozzi, & Warshaw, 1989). Davis (1989) defined perceived usefulness as "the degree to which a person believes that using a technology would enhance [his/her] job performance" (p. 320). He defined perceived ease of use as "the degree to which a person believes that using a particular system would be free of effort" (p. 320). He indicated that users are more likely to adopt a technology that is perceived to be useful and easier to use than others. Davis et al. (1989) provided empirical evidence to support the constructs of usefulness and perceive ease of use as the key predictors of

intentions to use and actual use. Following that seminal work, hundreds of studies have further validated these results in various types of technologies (Legris, Ingham, & Collerette, 2003; Thompson, Compeau, & Higgins, 2006). Additionally, hundreds of studies have documented the validity of using the construct of intentions to use as an appropriate predictor of actual usage, particularly when a system is not yet deployed for users to experience.

The steady growth in the use of e-learning in academic institutions has led researchers to explore technology acceptance theories in research areas also (Selim, 2003, 2007). Ngai, Poon, and Chan (2007) examined the association between technology acceptance constructs, technical support, and its impact on intentions to use e-learning systems in higher education. Their results also indicated that perceived usefulness and ease of use impact intentions to use e-learning systems and, ultimately, the actual use of such systems. Saade and Bahli (2005) investigated the effect of cognitive absorption factors, such as temporal dissociation, focused immersion, and heightened enjoyment, on the acceptance of e-learning systems. Their results also indicated that perceived usefulness and ease of use had a significance effect on intention to use e-learning systems. However, their results indicated that perceived usefulness was three times stronger compared with ease of use in its impact on intentions to use e-learning systems. These results suggest that learners may be more focused on the usefulness of the system rather than the ease of use of the technology. Given such findings, this study investigated if indeed students' perceived usefulness and ease of use are the two key constructs in predicting intentions to use multibiometrics in e-learning exam. Moreover, the main thrust behind this work is a pre-implementation investigation. Thus, the focus of this work is on intentions to use emerging technology, such as multibiometrics, rather than actual usage.

Ethical Decision Making in E-Learning

Ethical issues with the use of e-learning systems have also been a growing concern for higher educational institutions as well as for researchers (Kennedy, Nowak, Raghuraman, Thomas, & Dacis, 2000; McCabe, 2003; Ramim, 2007; Rogers, 2006). Examples of some unethical behaviors that have been documented in literature include cheating during e-learning exams using devices such as personal digital assistants (PDAs), calculators, and cellular phones; engagement in unauthorized e-collaborations by using instant messaging, chat, and forums; and deception by logging on with another student's username and/or password (Johnson, 2001; Nitterhouse, 2003; Popyack, Herrmann, Zoski, Char, Cera, & Lass, 2003; Tavani, 2004). Low, Ferrell, and Mansfield (2000) have demonstrated that ethical decision making is a key driver behind ethical behavior. Ethical decision making is defined as an individual's ability to make a decision based on what is a morally correct action when facing an ethical challenge (Dorantes, Hewitt, & Goles, 2006). Thus, ethical decision involves the cognitive process of seeking an ethical course of action when facing an ethical challenge (Dufrene & Harriet, 2004). Therefore, it appears that students' acceptance and intentions to use multibiometrics may be driven by their ethical decisions. Additionally, Chonko, Wotruba, and Loe (2003), Coughlan (2005), and Wotruba, Chonko, and Loe (2001) conducted research on the impact of a code of conduct on ethical decision making in various organizations. A code of conduct is defined as a set of guidelines for ethical decision making created by an organization (Chonko et al., 2003). However, Wotruba et al. (2001) concluded that the existence of a code of conduct, in most organizations, does not have a direct impact on individuals' ethical decision making; rather, individuals' code of conduct awareness appeared to be stronger factor in such decisions. Code of conduct awareness is defined as an individual's acknowledgement that the code of conduct exists and is aware of its content (Wotruba et al., 2001).

As a consequence of these concerns, researchers emphasized the need to conduct studies that investigate students' ethical decisions making (McCabe& Pavela, 2004; Pincus & Schmelkin, 2003; Rawwas, Al-Khatib, & Vitell, 2004). Additionally, organizational behavior literature provides

support that employees' code of conduct awareness and their ethical decision making are potential contributing constructs to their use of IS (Cronan et al., 2005; Kreie & Cronan, 1998). Despite these findings, research related to the role of code of conduct awareness in ethical decision making appears warranted (Chonko et al., 2003). With the documented growth of e-learning and the unethical conducted indicated, it appears that issues of code of conduct and ethical decision making in e-learning remain unresolved.

Methodology

This study used a quantitative survey-based instrument employing validated measures from prior literature. This was done following the recommendation of Boudreau, Gefen, and Straub (2001) who noted, "Researchers should use previously validated instruments wherever possible, being careful not to make significant alterations" (p. 11). As such, the items to measure the constructs of perceived ease-of-use, perceived usefulness, and intention to use were adopted from Gefen et al. (2003) as well as James et al. (2006) to the context of a multibiometric system during e-learning activities. Additionally, the items to measure code of conduct awareness and ethical decision making were adopted from Ramim (2007). The items for perceived ease-of-use, perceived usefulness, code of conduct awareness, and intention to use, used a 5-scale Likert-type scale ranging from 'strongly disagree' [1] to 'strongly agree' [5], while the items for ethical decision making used a 5-scale Likert-type scale ranging from 'not at all unethical' [1] to 'very unethical' [5].

Population and Sample

The sample included 100 non-IT students who attended e-learning courses in a major university in the southeastern U.S. Students received a consent e-mail indicating the intentions of the study and a short explanation about the integrated system of multibiometric authentication devices and e-learning (see Figure 1). Following Mahalanobis distance analysis and response set review, three cases were removed due to multivariate outliers and two due to response set. This resulted in data set of 97 participants used in this analysis.

Hypotheses

H1: Learners' perceived ease-of-use will have a significant positive impact on their intention to use multibiometrics for authentication during e-learning exams.

H2: Learners' perceived usefulness will have a significant positive impact on their intention to use multibiometrics for authentication during e-learning exams.

H3: Learners' ethical decision making will have a significant positive impact on their intention to use multibiometrics for authentication during e-learning exams.

H4: Learners' code of conduct awareness will have a significant positive impact on their ethical decision making during e-learning exams.

Figure 2 depicts the conceptual model for the learners' Ratified Acceptance of Multibiometrics Intentions Model (RAMIM).

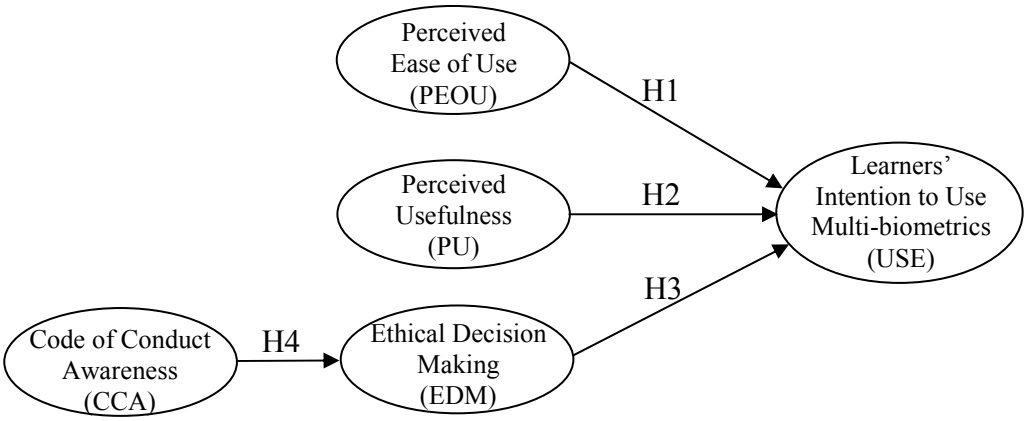

Figure 2. Ratified Acceptance of Multibiometrics Intentions Model (RAMIM)

Results

Descriptive Statistics

Table 1 depicts the demographics of the sample collected. The sample includes about 40% females and 60% males. Additionally, the initial sample includes a bi-polar distribution on ages with about 60% between the ages of 19 to 34, and about 30% between the ages of 40 to 54. A majority of the learners have experience with e-learning courses and more than half of the learners are working full time.

Table 1. Descriptive Statistics and Demographics of Learners (N=97)

Item	Frequency	Percentage (%)
Gender		
Male	59	60.8%
Female	38	39.2%
Age		
18 or under	1	1.0%
19-24	17	17.5%
25-29	25	25.8%
30-34	17	17.5%
35-39	5	5.2%
40-44	16	16.5%
45-54	14	14.4%
55-59	1	1.0%
60 or older	1	1.0%

Number of previous e-learning courses taken		
None, this was my first	10	10.3%
1	8	8.2%
2	11	11.3%
3	3	3.1%
4	7	7.2%
5 to 9	22	22.7%
10 or more	36	37.1%
Weekly hours for work/job		
No, I'm not working	16	16.5%
Less than 20	4	4.1%
20 to 29	10	10.3%
30 to 39	5	5.2%
40 to 49	45	46.4%
50 to 59	13	13.4%
60 or more	4	4.1%

Validity and Reliability

The overall validity of the instrument was twofold. First, in order to maintain construct validity, the instrument was set to use existing validated measures for the constructs under study. However, the instrument included several minor adjustments of the item text and name of the systems in order to better target the survey instrument to the precise technology under investigation. Second, in order to protect the internal validity of the instrument, a small group of five subject matter experts were asked to review the initial draft of the instrument and provide their comments. Minor textual adjustments were resulted from the subject matter experts group. The reliability of the measures was investigated using Cronbach's Alpha measure. According to Mertler and Vannatta (2001), measures that demonstrate reliability score using Cronbach's Alpha of over 0.70 are considered reliable. The initial results of this study indicate very strong reliability for each of the constructs as measured, with a Cronbach's Alpha of 0.848, 0.916, 0.922, 0.946, and 0.892 for usefulness, ease-of-use, code of conduct awareness, ethical decision making, and intention to use correspondingly (see Table 2).

Table 2. Summary of Construct Reliability Analysis using Cronbach's Alpha (N= 97)

Construct	No. of Items	Cronbach's Alpha
Code of Conduct Awareness (CCA)	4	0.922
Perceived Ease of Use (PEOU)	6	0.916
Perceived Usefulness (PU)	6	0.848
Ethical Decision Making (EDM)	21	0.946
Intention to Use (USE)	8	0.892

Partial Least Square (PLS)

Data was analyzed using Partial Least Square (PLS) (Chin, 1998; Chin, Marcolin, & Newsted, 2003) with SmartPLS 2.0 (beta) (Ringle, Wende, & Will, 2005). As a sub-type method of structured equation modeling (SEM), PLS is widely used in IS research (Gefen & Straub, 2005). With the demonstration of the good reliability results indicated above, the constructs under investigation appear to provide adequate convergent and discriminant validity. Results of the standardized PLS path coefficients model for the proposed RAMIM are presented in Figure 3. The numbers noted above the arrows in the model represent the path coefficient, where results indicated that all path coefficients were significant at least at the .05 level. Results of the R-squared (R^2) values are indicated in the lower right corner below the given constructs where R^2 is applicable. Wetzels, Odekerken-Schröder, and Van-Oppen (2009) suggested a global fit measure (GoF) for PLS path modeling as a geometric mean of the average communality and average R^2. They also indicated three cut-off points for GoF GoF_{small}=0.1, GoF_{medium}=0.25, and GoF_{large}=0.36. Following such global PLS fit measure, the calculated GoF for this model, based on $\overline{Ave} = .693$ and $\overline{R^2} = .374$ (Figure 2) is 0.509 that well exceeds the 0.36 cut-off point value of the large, indicating that the overall proposed RAMIM (Figure 2) is valid.

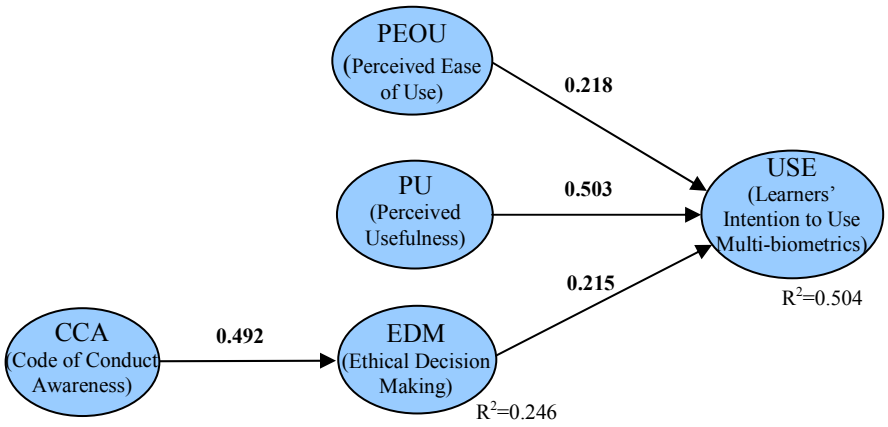

Figure 3. Results of the PLS Analysis (N=97)

Results of the PLS analysis demonstrated that PU had the strongest significant impact on USE ($\beta_{PU \rightarrow USE} = 0.503$, $p < .001$), PEOU and EDM had also significant impact on USE ($\beta_{PEOU \rightarrow USE} = 0.218$, $p < .05$; $\beta_{EDM \rightarrow USE} = 0.215$, $p < .05$), and CCA had a strong significant impact on USE ($\beta_{CCA \rightarrow USE} = 0.492$, $p < .001$). Such results indicated that all four hypotheses (H1, H2, H3, and H4) are supported.

Table 3. Summary of Hypotheses Results

Hypothesis	Relations:	Sig. Impact
H1:	PEOU → USE	Yes
H2:	PU → USE	Yes
H3:	EDM → USE	Yes
H4:	CCA → EDM	Yes

Conclusions and Discussions

Summary of Results

The central aim of this study was to investigate students' acceptance of multibiometrics for authentication during e-learning exams. A quantitative survey investigation was conducted following measures adopted and validated from prior technology acceptance and computer ethics literature. The following is a summary of the results found in this research following the sequences of the hypotheses presented previously.

First, results demonstrated that students' perceived ease-of-use (PEOU) is the second most significant predictor of students' intention to use multibiometrics (USE) during e-learning exams, which supports H1. Students intent to use multibiometrics in e-learning exams increases when their perceived ease-of-use of such technology increases. This finding is significant to higher education institutions that contemplate employing multibiometrics to authenticate exam takers, especially in response to the U.S. Higher Education Opportunity Act (H.R. 4137) (U.S. Department of Education, 2008). Concerns that students may decline to enroll in e-learning programs that employ multibiometrics may require further investigation. Conversely, the use of multibiometrics can offer additional flexibility to students who are unable to reach a testing center due to mobility issues, availability of services in remote areas, and the high fees associated with such services, when their institution or program mandates stronger authentication of e-learning exam takers than the current practiced approach of username/password.

Second, perceived usefulness (PU) demonstrates the strongest significant impact on students' intention to use multibiometrics (USE) during e-learning exams, which supports H2. These results support the notion that usefulness of multibiometrics in e-learning exams is of utmost importance for students' intentions to use multibiometrics. This is significant as e-learning instructors should advocate such technologies to ensure that their learners perceive this technology to be useful for ensuring the integrity of e-learning exams and e-learning courses in general. The majority of the participants in this study (60.8%) were between the ages of 19 to 34 years old. Thus, it appears that they may appreciate and accept the incorporation of advanced authenticating methods more than older students. Furthermore, the majority of students in this age group recognize that multibiometrics is useful and may already utilize biometrics in their workplace.

Third, results of this study demonstrate that students' ethical decision making (EDM) has a significant positive impact on USE, which supports H3. This finding confirms the positive connection between ethical decisions and intention to use multibiometrics in e-learning exams. As such, the findings indicate that individuals who state they are more ethical in their decisions are more likely to use multibiometrics during e-learning exams. This is consistent with the notion that ethical individuals are more open to accountability in their actions, therefore, appear keener to use multibiometrics.

Finally, results of this study demonstrate that students' code of conduct awareness (CCA) has a significant positive impact on the EDM during e-learning exams and supports H4. CCA is positively related to EDM, which is consistent with prior ethics literature. The more aware students are about their university's code of conduct, the more their overall decision making appears to be ethically driven (Ramim, 2007). This finding supports prior studies in which organizational factors, such as a code of conduct, are directly related to the decision making process and employees that support the code of conduct are more likely to engage in ethical decisions (Fang, 2006; VanSandt, Shepard, & Zappe, 2006). Additionally, results of this study demonstrate that CCA makes students more likely to accept multibiometric authentication during e-learning exams.

This work was an initial step in an investigation on the factors that may influence students' use of multibiometric authentication during e-learning exams. The essence of this work was to better understand what factors may help increase the acceptance of a multibiometric authentication approach when students take e-learning exams. Although this work will seek additional data to better validate the initial model and results, these initial findings are substantial for higher educational institutions especially in the context of the recent U.S. Higher Education Opportunity Act (H.R. 4137) (U.S. Department of Education, 2008) that mandates stronger authentication of students that attend e-learning programs. First, higher educational institutions must fully understand the centrality of their students' perceived usefulness and ease-of-use related to multibiometrics authentication when implementing such technology in order to increase its acceptance. Second, it appears that ethical decision making may have some contribution to students' acceptance of multibiometric authentication; however, such contribution is also derived by students' code of conduct awareness. This study highlights the need to incorporate multibiometrics approach as no single biometric device appears to be wholly appropriate to fit successfully a wide range of authentication needs of e-learning systems.

Implications for Practice

This study has several implications for practitioners including e-learning administrators and biometric vendors. E-learning administrators may consider initiating the deployment of multibiometrics in their institutions as a mechanism to address the authentication requirements set by the recent U.S. Higher Education Opportunity Act (H.R. 4137) (U.S. Department of Education, 2008). Additionally, e-learning administrators should ensure a proper advocating of multibiometric authentication technologies and highlight its usefulness both for e-learning instructors and learners. Biometric vendors should ensure that the interface developed for using multibiometric technologies for higher education is easy to use (i.e. user friendly) both for students and instructor. Additionally, biometric vendors should ensure a seamless integration of multibiometric authentication with e-learning systems.

Limitations of the Study

The limitations of this study are threefold. First, the sample utilized in this study was gathered in one higher educational institution; therefore, additional research should validate the results in other institutions. Second, participants of this study attended courses by one instructor and were self selected into e-learning courses. Third, although there is a substantial evidence in IS literature that intention to use a technology is a significant contributor to actual use (Levy & Green, 2009), this study only measured intention to use multibiometric authentication. Additional research should also investigate measures of actual use of such technology as well.

Future Research

Future research may include several new avenues. Future studies may attempt to examine the use of multibiometrics in e-learning exams in an experimental setting and compare results with a control group. Second, another set of studies should attempt to investigate the use of traditional authentication methods combined with biometric methods to develop new multi-authentication approaches.

Acknowledgments

The authors would like to thank all the anonymous employees that participated in this study. The authors would like to thank the editor-in-chief Dr. Alex Koohang, Dr. Nitza Geri, as well as the anonymous referees, for their careful review and valuable suggestions. Additionally, the authors

wish to acknowledge the input of participants at the Chais 2009 conference on Learning Technologies Research, February 2009, where an earlier version of part of this article was presented.

References

Abate, A. F., Nappi, M., Riccio, D., & Sabatino, G. (2007). 2D and 3D face recognition: A survey. *Pattern Recognition Letters, 28*(14), 1885-1906.

Ajzen, I., & Fishbein, M. (1980). *Understanding attitudes and predicting social behaviors*. Engelwood Cliffs, NJ: Prentice Hall.

Anderson, E. E., & Choobineh, J. (2008). Enterprise information security strategies. *Computers & Security, 27*(1-2), 22-29.

Bagozzi, R. P. (2007). The legacy of the technology acceptance model and a proposal for a paradigm shift. *Journal of the Association for Information Systems, 8*(4), 243-256.

Bailie, J. L., & Jortberg, M. A. (2009). Online learner authentication: Verifying the identity of online users. *MERLOT Journal of Online Learning and Teaching, 5*(2), 197-207.

Bedford, W., Gregg, J., & Clinton, S. (2009). Implementing technology to prevent online cheating: A case study at a small southern regional university (ssru). *MERLOT Journal of Online Learning and Teaching, 5*(2), 230-238.

Boudreau, M.-C., Gefen, D., & Straub, D. W. (2001). Validation in information systems research: A state-of-the-art assessment. *MIS Quarterly, 25*(1), 1-16.

Buzzetto-More, N. A. (2008). Student perceptions of various e-learning components. *Interdisciplinary Journal of E-Learning and Learning Objects, 4*, 113-135.

Cavusoglu, H., Mishra, B., & Raghunathan, S. (2005). The value of intrusion detection systems in information technology security architecture. *Information Systems Research, 16*(1), 28–46.

Chin, W. W. (1998). Issues and opinions on structural equation modeling. *MIS Quarterly, 22*(1), 7–16.

Chin, W. W., Marcolin, B. L., & Newsted, P. R. (2003). A partial least squares latent variable modeling approach for measuring interaction effects: Results from a monte carlo simulation study and an electronic mail adoption study. *Information Systems Research, 14*(2), 189–217.

Chonko, L. B., Wotruba, T. R., & Loe, T. W. (2003). Ethics code familiarity and usefulness: Views on idealist and relativist managers. *Journal of Business Ethics, 42*(3), 237-252.

Clarke, N. L., & Furnell, S. M. (2005). Authentication of users on mobile telephones - a survey of attitudes and practices. *Computers & Security, 24*(7), 519-527.

Clarke, N. L., & Furnell, S. M. (2007). Advanced user authentication for mobile devices. *Computers & Security, 26*(2), 109-119.

Coughlan, R. (2005). Codes, values, and justifications in the ethical decision-making process. *Journal of Business Ethics, 59*(1), 45-53.

Cronan, T. P., Leonard, L. N. K., & Kreie, J. (2005). An empirical validation of perceived importance and behavior intention in IT ethics. *Journal of Business Ethics, 56*(3), 231-240.

Davis, F. D. (1986). Technology acceptance model for empirically testing new end-user information systems: Theory and results. Dissertation abstracts international. (umi no. Aat 0374529). MA, USA: Massachusetts Institute of Technology.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), 319-339.

Davis, F. D., Bagozzi, R. P., & Warshaw, P. R. (1989). User acceptance of computer technology: A comparison of two theoretical models. *Management Science, 35*(8), 982-1004.

DigitalPersona. (nd). U.Are.U 4500 fingerprint reader. Retrieved July 13, 2009, from http://www.digitalpersona.com/index.php?id=dev_hdw_uareu_reader

Dorantes, C. A., Hewitt, B., & Goles, T. (2006). Ethical decision-making in an IT context: The roles of personal moral philosophies and moral intensity. *Proceeding of the Hawaii International Conference on System Sciences,* Big Island, HI, pp. 1-10.

Dufrene, R. L., & Harriet, L. G. (2004). The ethical decision-making scale-revised. *Measurement and Evaluation in Counseling and Development, 37*(1), 2-14.

El-Khatib, K., Korba, L., Xu, Y., & Yee, G. (2003). Privacy and security in e-learning. *Journal of Distance Education Technologies, 1*(4), 1-19.

Eshet-Alkalai, Y., & Geri, N. (2007). Does the medium affect the message? The influence of text representation format on critical thinking. *Human Systems Management, 26*(4), 269-279.

Fang, M. L. (2006). Evaluating ethical decision-making of individual employees in organizations-an integration network. *Journal of American Academy of Business, 8*(2), 105-112.

Furnell, S. (2008). Cybercrime in society. In S. Wheeler (Ed.), *Connected minds, emerging cultures: Cybercultures in online learning*. Charlotte, NC: Information Age Publishing.

Furnell, S. M., Dowland, P. S., Illingworth, H. M., & Reynolds, P. L. (2000). Authentication and supervision: A survey of user attitudes. *Computers & Security, 19*(6), 529-539.

Gal-Or, E., & Ghose, A. (2005). The economic incentives for sharing security information. *Information Systems Research, 16*(2), 186–208.

Gefen, D., Karahanna, E., & Straub, D. W. (2003). Trust and TAM in online shopping: An integrated model. *MIS Quarterly, 27*(1), 51-90.

Gefen, D., & Straub, D. (2005). A practical guide to factorial validity using PLS-graph: Tutorial and annotated example. *Communications of the Association for Information Systems, 16*(5), 91-109.

Gerber, M., & von Solms, R. (2008). Information security requirements - interpreting the legal aspects. *Computers & Security, 27*(5-6), 124-135.

Geri, N., & Gefen, D. (2007). Is there a value paradox of e-learning in MBA programs? *Issues in Informing Science and Information Technology, 4*, 163-174.

Goodhue, D. L., & Straub, D. W. (1991). Security concerns of system users : A study of perceptions of the adequacy of security. *Information & Management, 20*(1), 13-27.

Jain, A., Hong, L., & Pankanti, S. (2000). Biometric identification. *Communications of the ACM, 43*(2), 91–98.

Jain, A. K., & Ross, A. (2004). Multibiometric systems. *Communications of the ACM, 47*(1), 34-40.

James, T., Pirim, T., Boswell, K., Reithel, B., & Barkhi, R. (2006). Determining the intention to use biometric devices: An application and extension of the technology acceptance model. *Journal of Organizational and End User Computing, 18*(3), 1-25.

Johnson, D. G. (2001). *Computer ethics*. Upper Saddle River, NJ: Prentice Hall.

Kennedy, K., Nowak, S., Raghuraman, R., Thomas, J., & Dacis, S. (2000). Academic dishonesty and distance learning: Student and faculty views. *College Student Journal, 34*(2), 309-315.

Koohang, A., Riley, L., Smith, T., & Schreurs, J. (2009). E-learning and constructivism: From theory to application. *Interdisciplinary Journal of E-Learning and Learning Objects, 5*, 91-109.

Kreie, J., & Cronan, T. P. (1998). How men and women view ethics. *Association for Computing Machinery. Communications of the ACM, 41*(9), 70-78.

Kritzinger, E. (2006). Information security in an e-learning environment. In D. K. J. Turner (Ed.), *International federation for information processing, education for the 21st century — impact of ict and digital resources* (Vol. 210, pp. 345-349). Boston: Springer.

Kritzinger, E., & von Solms, S. H. (2006). E-learning: Incorporating information security governance. *Issues in Informing Science and Information Technology, 3*, 319-325.

Legris, P., Ingham, J., & Collerette, P. (2003). Why do people use information technology? A critical review of the technology acceptance model. *Information & Management, 40*, 191–204.

Levy, Y. (2006). *Assessing the value of e-learning systems*. Hershey, PA: Information Science Publishing.

Levy, Y. (2008). An empirical development of critical value factors (cvf) of online learning activities: An application of activity theory and cognitive value theory. *Computers & Education, 51*(4), 1664–1675.

Levy, Y., & Green, B. D. (2009). An empirical study of computer self-efficacy and the technology acceptance model in the military: A case of a U.S. Navy combat information system. *Journal of Organizational and End User Computing, 21*(3), 1-23.

Liebl, A. (1993). Authentication in distributed systems: A bibliography. *ACM Operating Systems Review, 27*(4), 31-41.

Lin, C.-L., Chuang, T. C., & Fan, K.-C. (2005). Palmprint verification using hierarchical decomposition. *Pattern Recognition, 38*(12), 2639-2652.

Littman, M. K. (1996). Guidelines for network security in the learning environment. *Journal of Instruction Delivery Systems, 10*(1), 35–40.

Littman, M. K. (1997). Security in the telelearning environment. Cyberinvasions and countermeasures. *HyperNexus: Journal of Hypermedia and Multimedia Studies, 8*(1), 12–18.

Littman, M. K. (1998). Security in the telelearning environment. Cyberproblems and cyberpolitics. *HyperNexus: Journal of Hypermedia and Multimedia Studies, 8*(2), 11–18.

Logitech. (nd). Portable webcam c905. Retrieved July 13, 2009, from http://www.logitech.com/index.cfm/webcam_communications/webcams/devices/5868&cl=us,en#

Low, T. W., Ferrell, L., & Mansfield, P. (2000). A review of empirical studies assessing ethical decision making in business. *Journal of Business Ethics, 25*(3), 185-204.

McCabe, D. L. (2003, Sep 10). Caught copying: Electronic plagiarism is a new addition to the IT lexicon. *Businessline,* 1-3.

McCabe, D. L., & Pavela, G. . (2004). Ten updated principles of integrity. *Change, 36*(3), 10-17.

Mertler, C. A., & Vannatta, R. A. (2001). *Advanced and multivariate statistical methods: Practical application and interpretation*. Los Angeles, CA: Pyrczak Publishing.

Mizuno, S., Yamada, K., & Takahashi, K. (2005). Authentication using multiple communication channels. *Proceeding of the 2005 workshop on Digital identity management,* Fairfax, Virginia, USA, pp. 54-62.

Ngai, E. W. T., Poon, J. K. L., & Chan, Y. H. C. (2007). Empirical examination of the adoption of webct using TAM. *Computers & Education, 48*(2), 250-267.

Nitterhouse, D. (2003). Plagiarism - not just an academic problem. *Teaching Business Ethics, 7*(3), 215-227.

Oorschot, P. C., & Thorpe, J. (2008). On predictive models and user-drawn graphical passwords. *ACM Transactions on Information and System Security, 10*(4), 17-33.

Pincus, H. S., & Schmelkin, L. P. (2003). Faculty perceptions of academic dishonesty: A multidimensional scaling analysis. *Journal of Higher Education, 74*(2), 196-209.

Podio, F. L., & Dunn, J. S. (2001). *Biometric authentication technology: From the movies to your desktop*. Retrieved. from http://www.itl.nist.gov/div893/biometrics/Biometricsfromthemovies.pdf.

Pons, A. P. (2006). Biometric marketing: Targeting the online consumer. *Communications of the ACM, 49*(8), 60-66.

Popyack, J. L., Herrmann, N., Zoski, P., Char, B., Cera, C., & Lass, R. N. (2003). Academic dishonesty in a high-tech environment. *Proceeding of the the Technical Symposium on Computer Science Education,* Reno, Nevada, pp. 357-358.

Pusara, M., & Brodley, C. E. (2004). User re-authentication via mouse movements. *Proceeding of the 2004 ACM workshop on Visualization and data mining,* Washington, DC, USA, pp. 1-8.

Ramim, M. M. (2007). An examination of factors associated with students' ethical decision making in post-secondary e-learning programs. *Dissertation Abstracts International, 68*(12), 1-123. (UMI No. AAT 3290937).

Ramim, M. M., & Levy, Y. (2006). Securing e-learning systems: A case of insider cyber attacks and novice IT management in a small university. *Journal of Cases on Information Technology, 8*(4), 24-35.

Ramim, M. M., & Levy, Y. (2007). Towards a framework of biometrics exam authentication in e-learning environments. *Proceedings of the Information Resources Management Association International Conference (IRMA) 2007,* Vancouver, Canada, pp. 539-543.

Rawwas, M. Y. A., Al-Khatib, J. A., & Vitell, S. J. (2004). Academic dishonesty: A cross-cultural comparison of U.S. And chinese marketing students. *Journal of Marketing Education, 26*(1), 89-100.

Ringle, C. M., Wende, S., & Will, A. (2005). *SmartPLS 2.0 (beta)* Retrieved March 11, 2009, from http://www.smartpls.de/.

Rodwell, P. M., Furnell, S. M., & Reynolds, P. L. (2007). A non-intrusive biometric authentication mechanism utilising physiological characteristics of the human head. *Computers and Security, 26*(7), 468-478.

Rogers, F. C. (2006). Faculty perceptions about e-cheating during online testing. *Journal of Computing Sciences in Colleges, 22*(2), 206-213.

Ross, A., Nandakumar, K., & Jain, A. K. (2006). *Handbook of multibiometrics*. London, UK: Springer.

Saade, R., & Bahli, B. (2005). The impact of cognitive absorption on perceived usefulness and perceived ease of use in on-line learning: An extension of the technology acceptance model. *Information & Management, 42*, 317–327.

Sasamoto, H., Christin, N., & Hayashi, E. (2008). Undercover: Authentication usable in front of prying eyes. *Proceeding of the 26 annual ACM SIGCHI conference on Human factors in computing systems,* Pittsburgh, PA, pp. 35-45.

Selim, H. M. (2003). An empirical investigation of student acceptance of course websites. *Computers & Education, 40*(4), 343-360.

Selim, H. M. (2007). Critical success factors for e-learning acceptance: Confirmatory factor models. *Computers & Education, 49*(2), 396-413.

Simon, S. J., & Paper, D. (2007). User acceptance of voice recognition technology: An empirical extension of the technology acceptance model. *Journal of Organizational and End User Computing, 19*(1), 24-50.

Siponen, M., & Heikka, J. (2008). Do secure information system design methods provide adequate modeling support? *Information and Software Technology, 50*(9-10), 1035-1053.

Snelick, R., Uludag, U., Mink, A., Indovina, M., & Jain, A. (2005). Large scale evaluation of multimodal biometric authentication using state-of-the-art systems. *IEEE Transactions on Pattern Analysis and Machine Intelligence, 27*(3), 450-455.

Tavani, H. T. (2004). *Ethics and technology: Ethical issues in an age of information and communication technology*. New Jersey, NJ: John Wiley and Sons.

Thompson, R., Compeau, D., & Higgins, C. (2006). Intentions to use information technologies: An integrative model. *Journal of Organizational and End User Computing, 18*(3), 25-46.

Tsalakanidou, F., Malassiotis, S., & Strintzis, M. G. (2007). A 3D face and hand biometric system for robust user-friendly authentication. *Pattern Recognition Letters, 28*(16), 2238-2249.

U.S. Department of Education. (2008). *Higher education opportunity act of 2008*. *HR4137*(sec 496.B.ii). Retrieved March 13, 2009, from http://www.ed.gov/policy/highered/leg/hea08/index.html

U.S. Federal Bureau of Investigation. (n.d.). *Integrated automated fingerprint identification system.* Retrieved July 15, 2009, from http://www.fbi.gov/hq/cjisd/iafis.htm

U.S. Federal Trade Commission. (2008). *Consumer fraud and identity theft complaint data: January – December 2007*. Retrieved September 14, 2008, from http://www.ftc.gov/opa/2008/02/fraud.pdf

VanSandt, C. V., Shepard, J. M., & Zappe, S. M. (2006). An examination of the relationship between ethical work climate and moral awareness. *Journal of Business Ethics, 68*, 409-432.

Venkatesh, V., & Bala, H. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences, 39*(2), 273-315.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425-478.

Viswanath, V., & Hillol, B. (2008). Technology acceptance model 3 and a research agenda on interventions. *Decision Sciences, 39*(2), 273.

Wang, J., Chaudhury, A., & Rao, H. R. (2008). A value-at-risk approach to information security investment. *Information Systems Research, 19*(1), 106-120.

Wetzels, M., Odekerken-Schröder, G., & Van-Oppen, C. (2009). Using PLS path modeling for assessing hierarchical construct models: Guidelines and empirical illustration. *MIS Quarterly, 33*(1), 177-195.

Woodward, J. (1997). Biometrics: Privacy's foe or privacy's friend? *Proceeding of the IEEE,* Arlington, VA, USA, pp. 1480–1492.

Wotruba, T. R., Chonko, L. B., & Loe, T. W. (2001). The impact of ethics code familiarity on manager behavior. *Journal of Business Ethics, 33*(1), 59-69.

Yeh, Q.-J., & Chang, A. J.-T. (2007). Threats and countermeasures for information system security: A cross-industry study. *Information & Management, 44*(5), 480-491.

Zhang, D., Zhao, J. L., Zhou, L., & Nunamaker, J. F. (2004). Can e-learning replace classroom learning? *Communications of the ACM, 47*(5), 75-81.

Biographies

Dr. Yair Levy is an associate professor at the Graduate School of Computer and Information Sciences at Nova Southeastern University. He serves as the director of the Center for e-Learning Security Research (http://CeLSR.nova.edu/). During the mid to late 1990s, he helped NASA develop e-learning platforms and manage Web infrastructures. He earned his Bachelor's degree in Aerospace Engineering from the Technion, Israel Institute of Technology. He received his MBA with MIS concentration and Ph.D. in MIS from Florida International University. His current research interests include e-learning security and users perceptions of IT. He authored a book and numerous research publications that appear in peer-reviewed journals, conference proceedings, invited book chapters, and encyclopedias. He is the editor-in-chief for the International Journal of Doctoral Studies (IJDS) and serves on editorial board of other recognized scholarly journals. To find out more about him, please visit his Website: http://scis.nova.edu/~levyy/

Dr. Michelle Ramim is a part-time professor at the Huizenga School of Business and Entrepreneurship at Nova Southeastern University. She has extensive experience in information technology (IT) consulting. Dr. Ramim directed the development and implementations of several IT projects including promotional and interactive websites for major enterprises such as Debeer (Diamond Trading Company). Her current research interests include ethical issues with IT, information security and crisis management, legal aspects of computing, as well as ethical decision making. She has published articles in peer-reviewed outlets including journals, conference proceedings, encyclopedias, and an invited chapter. Moreover, she has been serving as a referee research reviewer for national and international scientific journals, conference proceedings, as well as MIS textbooks. She earned her Bachelor's degree from Barry University in Miami Florida. Dr. Ramim has received her Executive MBA from Florida International University. She completed her Ph.D. in Information Systems at the Graduate School of Computer and Information Sciences, Nova Southeastern University in the area of ethical decision making. You can find her Website via: http://www.nova.edu/~ramim/