International Review of Research in Open and Distributed Learning

Institutional Level Identity Control Strategies in the Distance Education Environment: A Survey of Administrative Staff

Alexander Amigud

Volume 14, numéro 5, décembre 2013

URI : https://id.erudit.org/iderudit/1066887ar
DOI : https://doi.org/10.19173/irrodl.v14i5.1541

Aller au sommaire du numéro

Éditeur(s)

Athabasca University Press (AU Press)

ISSN

1492-3831 (numérique)

Découvrir la revue

Citer cet article

Amigud, A. (2013). Institutional Level Identity Control Strategies in the Distance Education Environment: A Survey of Administrative Staff. *International Review of Research in Open and Distributed Learning*, *14*(5), 128–143. https://doi.org/10.19173/irrodl.v14i5.1541

Résumé de l'article

Physical separation of students and instructors creates the gap of anonymity and limited control over the remote learning environment. The ability of academic institutions to authenticate students and validate authorship of academic work at various points during a course is necessary for preserving not only perceived credibility but also public safety. With the growing scope of distance education programs that permeate critical areas such as healthcare, airspace, water management, and food solutions, universities have a moral obligation to employ secure measures to verify learning outcomes. This study examines the measures universities with large distance education programs employ to align identity of learners with the academic work they do, as well as the effectiveness of and challenges and barriers to their implementation. The research was undertaken using a multiple case approach and examined survey responses from five academic administrators at five officially accredited post secondary institutions in three countries. The cases examined in the study include: Athabasca University, Open University UK, Penn State University World Campus, University of Maryland University College, and eConcordia,Concordia University's distance learning facility. This study is not an exhaustive attempt to examine all aspects of academic integrity, but rather to create awareness about various learner authentication strategies. This study confirms that secure learner authentication in the distance education environment is possible. However, with greater pressure to enhance security of learner authentication, the openness of open learning is challenged and may change as we know it.

THE INTERNATIONAL REVIEW OF RESEARCH IN OPEN AND DISTANCE LEARNING

Institutional Level Identity Control Strategies in the Distance Education Environment: A Survey of Administrative Staff

Alexander Amigud
Athabasca University, Canada

Abstract

Physical separation of students and instructors creates the gap of anonymity and limited control over the remote learning environment. The ability of academic institutions to authenticate students and validate authorship of academic work at various points during a course is necessary for preserving not only perceived credibility but also public safety. With the growing scope of distance education programs that permeate critical areas such as healthcare, airspace, water management, and food solutions, universities have a moral obligation to employ secure measures to verify learning outcomes. This study examines the measures universities with large distance education programs employ to align identity of learners with the academic work they do, as well as the effectiveness of and challenges and barriers to their implementation. The research was undertaken using a multiple case approach and examined survey responses from five academic administrators at five officially accredited post secondary institutions in three countries. The cases examined in the study include: Athabasca University, Open University UK, Penn State University World Campus, University of Maryland University College, and eConcordia,Concordia University's distance learning facility. This study is not an exhaustive attempt to examine all aspects of academic integrity, but rather to create awareness about various learner authentication strategies. This study confirms that secure learner authentication in the distance education environment is possible. However, with greater pressure to enhance security of learner authentication, the openness of open learning is challenged and may change as we know it.

Keywords: Academic integrity; plagiarism detection; accessibility; identity assurance

Introduction

Technology improves learning and teaching by making it more effective and efficient, by increasing accessibility to a wider range of learning resources, and by creating authentic learner environments that address individual learning styles (Bates & Poole, 2003). And as technology becomes more embedded into the academic structure, it may generate new ethical challenges (Mitchell, 2009). One crucial ethical concern strongly influenced by the advancement of technology, coupled with the growth of popularity of online learning, is academic integrity (Chiesl, 2007; Faculty Senate Committee on Technology, 2005; Grijalva, Nowell, & Kerkvliet, 2006; Mott, 2010).

Some scholars note that assessment of remote learners and the identity validation aspect of it in particular has historically been a challenging issue often cited by critics of distance education (Bailie & Jortberg, 2008; Moore & Kearsley, 1996). There are many benefits of using online assessments not only in distance courses but in traditional courses as well. These may include cost savings and greater accessibility. But the very same technology that makes education more accessible presents a cornucopia of cheating methods (Mott, 2010). For example, mobile devices play a pivotal role in enabling mobile learning. However, electronic communication and computing devices capable of transmitting, capturing, storing, retrieving, and processing information also pose a challenge for the exam integrity (Faculty Senate Committee on Technology, 2005). These devices may not only simplify finding solutions to a variety of test problems, but also streamline capture and distribution of digitized exam documentation. They are compact and easy to conceal, and they provide high processing power. Another important concern is the increasing availability of over-the-counter essays (Sheridan, Alany, & Brake, 2005).

In a traditional school setting, many of the examinations are taken in a proctored environment. Identity documents are verified by proctors, thus to spoof an identity, a proxy test taker must forge the identity documents or work in collusion with proctors. In distance environments, proctored examinations through examination invigilation networks remain a popular choice of secure assessment. However, institutions of distance education tend to shift away from secure testing towards project-based or authentic assessment strategies such as written assignments, projects, and portfolios (Bailie & Jortberg, 2008, p. 65). Instructional design strategies that minimize pressure to engage in unethical behavior have also been adopted as an alternative to traditional testing and examination (Chiesl, 2007).

As a result, courses that do not follow a proctored exam route may require students to submit a number of written assignments. In an online environment where username and password are often the only credentials used for identity verification, there is no need to forge documents. Changing identity is as easy as typing two strings of text on a login screen. Thus, without a secure process that aligns student virtual identities with the academic work they do, the identify validation by legitimate universities offering

distance courses and programs may not be perceived as credible as that provided by traditional institutions.

Much literature on academic misconduct in distance education is concerned with prevention of plagiarism, with wrongful appropriation of intellectual property, and with the technological means of prevention. There is little research done on the institutional level identity control measures or their effectiveness. Data on the incidence rates of student academic dishonesty show a wide variance. One of the challenges with academic integrity research is that it often relies on self-reporting (Scanlon & Neumann, 2002). A study conducted by McCabe and Trevino (1996) examines the magnitude of academic dishonesty and historical trends of student behavior in traditional universities by comparing data from two research projects conducted almost 30 years apart involving multiple campuses and large samples. The patterns observed in these two studies are relatively consistent and at the same time raise serious concerns about academic integrity. The findings suggest that over 80% of students cheated at least once on a major written assignment. Although, this research was aimed at analyzing data from traditional college settings where testing and examinations are proctored, one may argue that the trends identified in the study are transferable to the distance education environment, where project based assessment may replace secure examination and where proctoring is not always an option. Some scholars argue that students who admit engaging in cheating behavior may not limit its scope to only one medium, but rather employ both conventional and internet plagiarism (Scanlon & Neumann, 2002). The internet may simplify access to a wider source of information, but whether or not it influences one's preference for cheating is still unknown. Data from studies on academic integrity in a distance environment suggest that student and faculty perceptions of cheating in distance courses are similar and that it is easier to cheat in the distance environment (Kennedy, Nowak, Raghuraman, Thomas, & Davis, 2000).

Some scholars consider academic integrity a policy issue (Isa, Samah, & Jusoff, 2008; Sheridan et al., 2005) while others argue for a technology-based solution (Mott, 2010; Kennedy et al., 2000). There is a variety of technology available to institutions ranging from plagiarism detection tools (Sheridan et al., 2005) and remote proctoring services to biometric authentication systems designed to secure the process of remote learner authentication. These technologies have been pilot tested at several universities (Case & Cabalka, 2009; McNabb & Maynard, 2010). The pilot project results suggest that biometric and remote monitoring technologies hold great promise in providing learner identity assurance.

Method

This study was designed to examine measures universities with large distance education programs employ to align identity of learners with the academic work they do, as well as examine the effectiveness of and challenges and barriers to their implementation. The research was undertaken using a multiple case approach and examines survey responses from five academic administrators at five officially accredited post secondary institutions in three countries. The data collection was carried out from June to October, 2012.

The five leading universities, in three countries, were selected for this study. This multiple case study examines the cases of Athabasca University, Open University UK, Penn State University World Campus, University of Maryland University College, and eConcordia,Concordia University's distance learning facility. These institutions fit the criterion of officially accredited universities that offer distance education courses and programs. Each institution has already implemented or evaluated an identity control strategy. A strategic convenience sample of university administrative staff involved in development, administration, or enforcement of an academic integrity policy was selected.

Publicly available information from university websites was used to generate a preliminary participant list of V.P. Academic and Registrar office staff involved in academic integrity matters. Introductory emails were then sent out to the preliminary list of participants in order to introduce the study and identify the key experts on the academic integrity and in particular identity control issues at each institution. Additional referrals were received, and the final participant list was created. The data from one participant from each university to the total of five participants for the entire study was collected and analyzed. Participants were selected on the basis of involvement in development, administration, or enforcement of an academic integrity policy and expressed interest in participating in this research project.

The rationale for choosing to survey administrative staff as opposed to faculty or academic leaders was that the administrators tend to have broader knowledge of academic integrity issues and are responsible for overseeing the entire academic integrity process from policy making to financing to enforcement, whereas other groups tend to have limited involvement and are delegated specialized tasks within the process. Although faculty and staff share a common understanding of the academic integrity process, the survey results should be interpreted as the opinions of the stakeholder group that is likely to be most informed on the subject of academic integrity. However, a note of caution on this interpretation is appropriate since administrators' opinions may not be widely, and are certainly not unanimously, endorsed by all university faculty and staff.

Data Collection Strategies

The data collection process was divided into four phases. First, each university's website was examined for general academic integrity guidelines as well as admission requirements and examination instructions for students. In the second phase of the data collection, strategic convenience sampling was used to select an administrative office staff member from each university and these were invited to answer a brief questionnaire and participate in a follow up interview. A personal introductory email was sent to prospective participants by the researcher to introduce the study and identify the key experts responsible for the development, administration, or enforcement of the academic integrity policy. During the third phase of the data collection process and once a final list of participants had been established, an introductory letter containing a brief description of the study and the questionnaire was distributed via email. In the final phase of the data collection process, follow up questions were asked through email and via telephone to clarify the questionnaire responses. As well, the participants were provided an opportunity to review, validate, and provide additional comments on the summary of the research findings.

Survey Instruments

A survey instrument was developed for this study and consisted of seven Likert-like scale questions (with a 5 point range from *strongly agree* to *strongly disagree*) and one multiple choice question. The questionnaire also allowed for qualitative information and extra details to be recorded if the participant wished to provide them. A follow up to clarify the answers was conducted by email or telephone. The data collection was performed using LimeSurvey, web-based survey software hosted by Athabasca University and via email. Some participants considered it easier to complete the survey via email. Each participant was assigned a unique participant identification number.

Questionnaire

1. Identity fraud has emerged as an issue at my institution. (SA/A/N/D/SD)

2. My institution tracks and trends academic misconduct data. (SA/A/N/D/SD)

3. My institution has an adequate system of identifying online students before each project or paper submission. (SA/A/N/D/SD)

4. My institution has an adequate system of identifying online students before each final and/or midterm exam. (SA/A/N/D/SD)

5. My institution has encountered barriers to implementation of identity control measures. (SA/A/N/D/SD)

6. The identity control measures my institution employs to authenticate the identities of online students are effective. (SA/A/N/D/SD)

7. The system my institution employs to conduct remote identification of test takers has challenges. (SA/A/N/D/SD)

8. The best practice for authenticating the work of remote learners is:

    a. Remote Proctoring using web cams

    b. Biometric Authentication asserting the identity of the student by fingerprints, keyboard activities etc.

    c. Traditional Proctoring

    d. Policy Enforcement

    e. Other

Data Analysis Procedures

Upon collecting the necessary data from documents, surveys, and follow up emails or phone interviews, the collected information was organized into categories and cross-compared. Data analysis was concluded using the analytic comparison framework (Neuman, 2006).

Results

The survey results are summarized from questions as depicted in Table 1 and 2.

Table 1

Likert-Like Scale Survey Responses

Case 1	Case 2	Case 3	Case 4	Case 5
1. Identity fraud has emerged as an issue at my institution.				
Strongly agree	Strongly agree	Strongly agree	Neither agree nor disagree	Agree
2. My institution tracks and trends academic misconduct data.				
Strongly agree	Agree	Strongly agree	Agree	Strongly agree
3. My institution has an adequate system of identifying online students before each project or paper submission.				
Agree	Agree	Strongly disagree	Neither agree nor disagree	Disagree

Case 1	Case 2	Case 3	Case 4	Case 5
4. My institution has an adequate system of identifying online students before each final and/or midterm exams.				
Strongly agree	Agree	Agree	Agree	Disagree
5. My institution has encountered barriers to implementation of identity control measures.				
Agree	Disagree	Strongly agree	Agree	Neither agree nor disagree
6. The identity control measures my institution employs to authenticate the identities of online students are effective.				
Neither agree nor disagree	Neither agree nor disagree	Strongly disagree	Neither agree nor disagree	Neither agree nor disagree
7. The system my institution employs to conduct remote identification of test takers has challenges.				
Disagree	Disagree	Agree	Agree	Agree
8. The best practice for authenticating the work of remote learners is:				
Traditional proctoring / Invigilator network	Traditional proctoring / Invigilator network	Traditional proctoring / Invigilator network	Each system has advantages and disadvantages. What is best depends on circumstance, cost and context	Remote proctoring / Biometric/ policy enforcement

Table 2

Authentication Summary

Case #	Case 1	Case 2	Case 3	Case 4	Case 5
Authentication methods	Password, traditional proctoring	Password, traditional proctoring	Password, traditional proctoring	Password, traditional proctoring	Password, remote proctoring, traditional proctoring
Plagiarism detection tools	Turnitin, Google	Turnitin, Google	Turnitin	Turnitin, Copycatch	Turnitin
Challenges	Provision of examination facilities	No challenges cited	Provision of examination facilities	Technical issues, provision of examination facilities	Technical issues
Barriers	No barriers reported	No barriers reported	Cost	Cost, complexity	No barriers reported

Discussion

Academic Integrity

Identity fraud is an issue that affects all academic institutions and is particularly a concern for those who provide service to remote learners. One administrator indicated reported cases of students sharing login credentials and hiring others to complete online assignments. Since physical separation creates the gap of anonymity, authentication protocols need to be implemented to close the gap and align virtual identities with the work that students do. Access to academic resources and learning management systems is often protected by a username and password authentication. This method is not designed to validate one's identity or authorship of submitted materials, but rather act as a gatekeeper granting access to anyone with the correct user name and password combination. Like a door lock, it prevents unauthorized access, but does very little to examine the identities of people inserting the key. The problem is serious enough to have drawn the attention of the United States Department of Education. In 2008, U.S. Congress enacted the Higher Education Opportunity Act. Section 602.17 of the act requires institutions to develop and employ measures that validate identities of distance learners (Higher Education Opportunity Act, 2008).

Policy and Enforcement

All of the surveyed institutions have designated staff to deal with reported incidents of academic misconduct. This process often involves multiple stakeholders. While some cases are handled by instructors, other cases may be escalated and reviewed by designated committees. The reported data are tracked and trended by all five institutions; however, the criteria for tracking incidents and methodology of data collection may vary. A disciplinary action is generally the last resort. Education and communication are the preferred methods of managing academic misconduct cases. Students are provided with academic integrity tutorials and resources, and they may be required to sign a statement of academic integrity or complete a quiz. In serious cases, penalties are assigned by designated committees on a case by case basis as the magnitude of an offence may hinge on a number of factors. It often takes a retributive justice approach. Since copying and pasting of a website article is different from uploading a digital image of a final exam taken with a smart phone to a file sharing website, the penalty needs to be proportional to the damages caused. Tracking incident data is a vital part of risk management and is a process that is worth examining in itself.

Authentication Strategies

There are several authentication strategies available to universities, aimed at enhancing authentication of student work. These are depicted in Table 3. They also provide different levels of assurance. A course or program may employ any combination of these strategies to manage academic integrity and maximize identity assurance. Some strategies provide a greater degree of confidence in the identification of students than others; therefore, they are classified into two categories. Courses that do not follow the exam route often employ low level authentication measures for validation of student identity before submission of projects, assignments, and papers as well as participation in online discussion groups or completion of an online quiz. They often rely on the username and password authentication for access to learning management systems. In order to compensate for limitations of the traditional authentication methods, additional validation measures such as login pattern analysis, instructor validation, and plagiarism detection tools are often employed. Although the latter is not an identity control strategy, but rather a method of disproving authorship of any written work, assignments that are submitted electronically are often screened by instructors for plagiarism, using plagiarism detection tools. Turnitin was cited in all five cases, and Copycatch was used by one institution. Google search engine was also occasionally used by some instructors as a first line of defense against plagiarism.

Table 3

Authentication Strategies

Low level authentication	High level authentication
Password authentication	Biometric authentication
Instructor validation (large groups)	Instructor validation (supervised study)
IP monitoring/login pattern analysis	Proctoring (traditional)
Plagiarism detection (similar content)	Proctoring (remote)

Instructors play an important role in student work authentication and contribute to identity assurance. Learners demonstrate academic skills throughout the course allowing an instructor to track student progress and flag any suspicious activities or question the source of the submitted content. It may serve as an effective identity authentication and authorship validation mechanism when students' activities are closely supervised and continuously evaluated; such may be the case with supervised research projects where intermediate snapshots of work in-progress are examined and discussed through telecommunication technologies that replicate face to face communication. Furthermore, a login data analysis may not be effective in aligning student identities with the academic work they do. It is not safe to assume that the variance in login patterns is indicative of a problem, whereas a correctly entered username and password is not.

However, the second list of strategies shares much of the same validation protocols as that employed by the traditional institutions. This usually involves interaction with instructors or support staff, validation of officially issued identification documents, and participation in proctored exams at designated examination facilities. Technologies that enable synchronous communication such as video conferencing substitute for physical meetings. Even in project route courses, instructors may include interactive participation components through the web or telephone conference systems, allowing students to present and discuss their ideas, research, and assignments and to conduct thesis defense and oral examination.

Unlike electronic paper and project submissions, exams emphasize higher security measures. Facilitation of exams requires traditional methods of authentication such as verification of officially issued identification. The remote proctoring process follows a similar pattern. When remote proctoring is used outside of the designated test centers, students are required to create an identity profile often comprised of a keystroke signature and a photograph before access to the exam is allowed.

The survey results show that perceived adequacy of identifying students before final and/or midterm exams was reported to be higher than that of a project or paper submission. Furthermore, four out of five administrators consider proctoring as the best

practice for remote learner authentication. Three administrators selected traditional proctoring, and one selected remote proctoring. Although proctoring is perceived favourably and offered by all universities examined in this study, it is not the primary learner authentication strategy that is consistently applied across all courses, likely due to costs and management challenges. Only one institution reported proctoring all of the final exams.

Challenges

In the distance education environment, academic integrity and technology are interconnected and continuously evolving. New methods of student authentication emerge, as do technologies that facilitate cheating. For some institutions, technology was not able to provide the desired level of performance. For others, the high cost of technology created a barrier to implementation. In addition to the cost of technology selection and initial deployment, maintenance, support, and administration may exert a significant impact on the budget. This in turn may affect student tuition rates and consequently accessibility.

High level authentication strategies add logistical burden on instructors and administrators. Provision of examination facilities, time zone differences, and technical issues are some of the challenges that administrators reported when dealing with exam invigilation both traditional and remote. Examination facilities are managed differently based on location and, therefore, there is a variance in level of service and support quality. Facilitation of standardized exams in examination centers dispersed over multiple time zones is also a challenge, as it creates a potential for sharing exam information between learners in different time zones.

Technical issues were also reported emerging outside of examination facilities. Remote monitoring of students' computers that use different operating systems may be affected by compatibility issues. Technical glitches resulting from software or hardware failure or loss of connectivity during examination may undermine reliability and efficient operation of the remote proctoring. Nevertheless, the future outlook for secure and reliable remotely managed examination is optimistic.

Effectiveness

An effective authentication system enables aligning student work with their identities with a reasonable degree of certainty at various stages in a course. The survey results show that the effectiveness of the identity control measures employed by the surveyed institutions is not well known. Many courses are designed for authentic assessments and project-based learning and do not always provide an opportunity for identity validation. While administrators were satisfied with select components of their existing system of authentication, pilot projects or various initiatives to further strengthen authentication measures were underway. Institutions are striving for continuous

improvement and examining methods that promote academic integrity and higher identity assurance.

Organizational Issues

Logistical and administrative issues were reported among the challenges facing administrators for the provision of examination facilities. Technical issues were also reported when technology based authentication was employed. As new technologies emerge, institutions should not only examine the benefits, but also implications for the organizational structure (Bates, 2005). Implementation of new technology is often a challenging task in itself, especially when it requires organizational changes and involves a large number of stakeholders who depend on reliable and secure technology systems.

Accessibility

An open learning approach accommodates students who are unable to attend traditional universities. It is imperative that technologies that mediate open learning are accessible and available to all learners (Bates, 2005). With greater pressure to enhance security of learner authentication, the openness of distance learning is challenged and may change. One may argue that the very process that promises secure authentication of distance learners is also a barrier to accessibility. Regardless of technology employed, an identity profile needs to be accurately created prior to the authentication stage. The quality of authentication depends not only on the type of technology used, but also on the quality of initial identity enrollment. In order for a student to enroll and create a student profile, the university must provide a designated facility to do just that, either internally or through external service providers. It may work well for local institutions, but in the case of international students enrolling in a single distance course in another country or in a city that is not within driving distance, the logistics of student registration and identity validation pose a serious challenge.

Future Research

As previously noted, institutions put onus on instructors to conduct authentication tasks such as monitoring students' progress and flagging irregularities in their work. A future study may examine the process of validation of students' identities from instructors' perspectives and analyze the effectiveness of both the non technical means and technology tools instructors employ. Furthermore, studies on academic misconduct usually report data collected from student surveys. Since institutions track and trend academic misconduct data, future research may focus on an institutional level academic integrity incident reporting and not only compare institutional data collection and analysis procedures, but also examine the magnitude of academic dishonesty and identity fraud in particular.

The impact of secure authentication measures on accessibility is another question that has arisen as a result of discussion about various levels of authentication. Future

research may examine accessibility levels of several authentication technologies and evaluate their influence on instructional design considerations and distance education in general. There is a discrepancy between what administrators consider effective measures of authentication and what measures they employ. Future research may examine this gap. And to conclude with a more fundamental question, a future study may examine different perspectives on what is a reasonable degree of certainty for authentication of student work. Should distance education schools follow the footsteps of traditional institutions and conduct at least one proctored exam in every course or continue relying on username and password authentication? Finally, the use of high stakes examinations as a corner stone for academic integrity is itself under challenge. Is performance on a time stressed, high stakes examination a valid assessment of a students' knowledge, skills, or potential to perform effectively in any but this very peculiar and foreign environment?

Recommendations

This study was undertaken using a pragmatic paradigm with an aim to implement findings and conclusions into policies and practices that may help university administrators deal with academic integrity issues. A complete avoidance of secure testing is not reasonable. Identity and authorship validation can and should be conducted at various points during a distance course. Administrators and instructional designers need to start taking academic integrity issues into consideration at the course/program design stage and consistently embed high level authentication strategies into the course activities.

Conclusion

This research was conducted with the intention to examine learner authentication measures and find examples that refute the "not possible" claim made by Moore and Kearsley almost twenty years ago. When the literature review was conducted to explore the relevant research regarding the issue of remote authentication of learners, several promising developments that indeed challenge the claim Moore and Kearsley made in 1996 stood out as a potential solution to this issue. These include biometric technologies and remote proctoring systems. This study confirms that secure learner authentication in the distance education environment is possible not only through the use of technology, but also through application of policy that requires adequate identity assurance measures to be embedded into course design.

The findings from this study tend to reinforce the idea that the values and standards of academic integrity remain the same regardless of the medium of instruction. One may argue that a project paper or assignment collected by a teaching assistant in a large auditorium of a traditional school provides the same level of identity assurance as the one submitted electronically. Neither identity of students nor authorship of manuscripts

is validated at the time of collection. Students are expected to be honest across all academic activities they participate in whether in class or online. The issue of trust is key, however one may not merely rely on an assumption that the virtue of integrity is maintained by all students. Authentication measures are important not only for preserving the perceived credibility of the institution, but also for public safety as may be the case with critical areas such as aviation training or health care studies. Therefore, secure authentication is justified and ought to provide a system of checks and balances that ensures that the relationship of trust is intact.

The underlying issue when dealing with remote learner authentication is finding not only the right technology, but also a healthy compromise between the credibility and accessibility of distance learning. Low level authentication methods make academic resources more accessible, as access is open to anyone with a computer and internet access. In contrast, high level authentication methods often require additional technical or administrative resources and add logistical challenges. A system of checks and balances is what defines credibility, and credibility of distance education entails greater responsibilities for all the stakeholders. Therefore, putting greater emphasis on high level authentication strategies may require greater involvement of students, administrative, and teaching staff in the evaluation process. By minimizing over-reliance on measures that do not provide authorship and identity validation, the convenience and accessibility levels of distance courses may be affected. This may consequently change the face of distance education once again.

References

Bailie, J., & Jortberg, M. (2008). A collection of papers on self-study and institutional improvement: Vol 3. Distance learning student authentication: Verifying the identity of online students. Retrieved from http://www.franciscan.edu/home2/Content/dean/PAPERS/Inovation%20and%20change/3065.pdf

Bates, T. (2005). *Technology, e-learning and distance education* (2nd ed.). London: Routledge.

Bates, T., & Poole, G. (2003). *Effective teaching with technology in higher education: Foundations for success.* San Francisco, CA: Jossey-Bass.

Case, R., & Cabalka, P. (2009). Remote proctoring: Results of a pilot program at Western Governors University. *Proceedings of the 25th Annual Conference on Distance Teaching and Learning*. Madison, WI. Retrieved from http://www.uwex.edu/disted/conference/Resource_library/proceedings/09_19933.pdf

Chiesl, N. (2007). Pragmatic methods to reduce dishonesty in web-based courses. *Quarterly Review Of Distance Education, 8*(3), 203-211.

Faculty Senate Committee on Technology (2005). Kansas State University. Retrieved from http://www.k-state.edu/facsen/policies/archives/ElectronicDevices1_05_000.pdf

Grijalva, T. C., Nowell, C., & Kerkvliet, J. (2006). Academic honesty and online courses. *College Student Journal, 40*(1), 180-185.

Higher Education Opportunity Act (2008). U.S. Department of Education. Retrieved from http://www2.ed.gov/policy/highered/leg/hea08/index.html

Isa, P., Samah, S., & Jusoff, K. (2008). Inculcating values and ethics in higher education e-learning drive: UiTM i-Learn user policy. *Proceedings of World Academy of Science: Engineering & Technology, 40*, pp. 452-456. Retrieved from the Academic Search Complete database.

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

McCabe, D. L., & Trevino, L. K. (1996). What we know about cheating in college: Longitudinal trends and recent developments. *Change, 28*(1), 28-33. (EJ 520 088)

McNabb, L., & Maynard, A. (2010). Software only biometrics to authenticate student ID report of pilot with the University of Texas System TeleCampus. Retrieved from http://www.biosig-id.com/wp-content/uploads/2011/07/Biometric-Signature-ID-and-UT-Systems-pilot-results.pdf

Mitchell, R. (2009). Ethics in an online environment. *New Directions for Community Colleges, 148*, 63-70.

Moore, M. G., & Kearsley, G. (1996). *Distance education: A systems view*. Belmont: Wadsworth Pub. Co.

Mott, J. H. (2010). The detection and minimization of cheating during concurrent online assessments using statistical methods. *Collegiate Aviation Review, 28*(2), 32-46.

Neuman, W. L. (2006). *Social research methods: Qualitative and quantitative approaches* (6th ed.). Boston: Pearson.

Scanlon, P. M., & Neumann, D. R. (2002) Internet plagiarism among college students. *Journal of College Student Development, 43*(3), 347-385.

Sheridan, J., Alany, R., & Brake, D. (2005). Pharmacy students' views and experiences of Turnitin—an online tool for detecting academic dishonesty. *Pharmacy Education, 5*(3/4), 241-250.

Athabasca University