SECURITY ANALYSIS OF MASSIVE OPEN ONLINE COURSE PLATFORMS

Naveen Kumar
Indira Gandhi National Open University
naveenkumar@ignou.ac.in

ABSTRACT

One of the major technological advancements in online learning is Massive Open Online Course. It is a platform for learners around the world to have access to quality education through the internet. The delivery of Massive Open Online Course raises many questions about information security, which calls for serious academic attention. These challenges include user authentication, user authorisation, data protection and privacy, confidentiality, non-repudiation, attendance tracking and electronic copyright protection. These security questions cannot be overlooked or ignored. This paper explores the analytical perspective of all the major security threats with respect to the Massive Open Online Courses while suggesting remedial mechanisms. This paper is an outcome of the research undertaken on the major providers like edX, Coursera, Udacity and Khan Academy. Possible security threats were analysed at different stages of course delivery, from course registration, access of modules, and communication between teachers and learners, to assessment, examination and certification. Further, possible solutions to these threats are discussed in this paper. It was noticed that the security issues and challenges are inconsistent and incongruent among different providers. Standardisation and designing a global policy framework for security are essential for an effective educational delivery system. Various tools and technological solutions should be integrated and implemented to address the security challenges of Massive Open Online Course.

Keywords: *Online Learning, Massive Open Online Course, Security.*

INTRODUCTION

Massive Open Online Course (MOOC) platform has proven to be a catalyst in Open and Distance Learning over the last few years. In the fall of 2011, Stanford University launched three courses, where in one course enrolment crossed 160000 students (The Massive open online course, 2016). The New York Times, has announced 2012 as "the year of the MOOC" as several well-financed providers, associated with top universities, emerged, including Coursera, Udacity, and edX. According to some leading agencies, the number of MOOCs learners exceeded 35 million worldwide in year 2015 and around 4200 MOOCs are being offered by 500 universities (ICEF Monitor, 2016).

MOOC is an online phenomenon, which is gaining momentum over the past five years. MOOC incorporates the property of social networking, the facilitation of an acknowledged expert in a field of study, and a group of freely accessible on-line resources (Malathi, 2015; McAuley, Stewart, Siemens, & Cormier, 2010). The foremost facet of a MOOC is that it builds on the dynamic engagement of a very large number of learners/students, who are self-motivated and self-organised towards learning, have prerequisite knowledge and skills,

and have customary interests (Malathi, 2015). In comparison to conventional or classroom courses, a MOOC can have a predefined timeline and weekly topics for reflection and deliberation. MOOC typically carries no fees, however; the upcoming MOOC platforms are coming up with several business models in MOOCs. As stated by Daphne Koller, Coursera Co-founder and President, “We’re confident (verified certificates) could be a significant revenue source that will make us a sustainable business while still allowing us to continue offering free education” (Shah, 2015). Similarly, specialisations, which feature a sequence of courses such as the Nanodegree by Udacity, and guaranteeing that students find a job within six months are some other business models which are being offered by major MOOC providers. MOOCs are gaining significant attention in the education world, including from open and distance learning institutes as well as conventional universities and training institutes or companies. However, there are still relevant drawbacks that impede MOOCs in realising their actual potential for education. Among these limitations are issues and problems related to information security in MOOCs, which are explored in this paper.

LITERATURE SURVEY

Security is an essential requirement of any online platform. In online learning, security means that learning resources are available and unimpaired for all authorised users when they are needed (Adams & Blandford, 2003). It becomes more important when the number of users and participants are large and covering wide geographic range. Security is essential as a means to retain users’ trust in the online learning environment because any risk can dramatically affect students’ perceptions of a system’s reliability and trustworthiness (Adams & Blandford, 2003).

Online learning systems have attracted hackers and other malicious users. The risk is great; as the functionalities and features of online learning systems are becoming more complex, online learning is increasingly exposed to security threats (Alwi & Fan, 2010). Online learning are open to many security risks, such as loss of confidentiality and availability, the exposure of critical data, and vandalism of public information services (Graf, 2002). Along with these security risks, it is also suggested that online learning must consider the inherent security risks on the internet, such as identity theft, impersonation, and inadequate authentication (Ayodele, Shoniregun, & Akmayeva, 2011). Furnell, Onions, Bleimann, Gojny, Knall, Roder & Sanders (1998) looks at the different stages of the online education system and discusses security issues that must be considered at each stage. These various requirements are being addressed in practice by the security framework being developed by the SDLearn research project, a collaborative initiative between higher academic establishments in the UK and Germany (Furnell & Karweni, 2001). Furnell et al. (1998) also identifies various areas of security which demands attention like remote student authentication and accountability; access control; intrusion detection; protection of network communications; non-repudiation issues; and "housekeeping" issues.

Furnell and Karweni (2001) emphasised the need to address security issues in online distance learning. They mentioned that security was not considered as high priority in an educational environment, but evidence indicates that it is definitely a crucial need. Further, an overview of the key security requirements and the main technical elements needed to address them are discussed. Chen and Wu (2013) attempted to understand online learning providers’ awareness of potential security risks and discuss the protection measures. The survey outcomes generated by the two different methods verified that online learning providers and practitioners have not considered security as a top priority. Chen and Wu (2013) also discussed the need for next generation of online learning systems that offer safer personal learning environment. This requires a one-stop solution for authentication, assures the security of online assessments, and balances security and usability. Miguel, Caball´e, Xhafa, and Prieto (2015) proposed a model based on trustworthiness approaches.

It is claimed that such a model can overcome the security threats and support e-assessment requirements for e-Learning.

Serb, Lacob, and Petrei (2013) described that with a large number of users in any online learning environment (among them students, visitors, instructors, tutors, and administrators), both a login system and a strong delimitation marking registered users and user groups are needed to safeguard the access. The open accessibility, low cost, and internationally connected nature of MOOCs has increased the growth of MOOCs. However, Fowler (2013) revealed many challenges regarding the MOOC model. A detailed analysis of MOOCs platform and its challenges was discussed by Schulz (2014), who suggested that MOOCs offer much varied and innovative potential in their wide geographic range and their ability to reach many and diverse participants, and in their use of collaborative formats and transparent teaching. However, MOOCs are also associated with problems and risks. Some of these are open access, integration into degree courses, the legal framework and the sustainability of their business models.

SECURITY ANALYSIS OF MOOC PLATFORMS

This paper examines the potential security threats in Massive Open Online Courses (MOOC) platforms. This analysis is an outcome of the research undertaken on the major MOOC providers like edX, Coursera, Udacity and Khan Academy. This analysis adopts two approaches to carrying out the review of security risks and protection in online learning. Firstly, an online security tool “Securi” available at https://sitecheck.sucuri.net/ is used to understand the possibility of major security flaws such as malware, website blacklisting, website firewall and outdated website. However, this security test can only provide basic information of the major security threats. Secondly, to understand the possibility of security threats at different stages of courses in each platform, manual security testing was conducted on selected MOOCs platforms.

Basic Security Analysis using an Online Tool

The security check using the online software tool called Securi was conducted around August, 2016. The results may vary from time to time according to the updates made at the MOOC platforms and in the testing software. The results as shown in Figure 1, 2, 3 and 4 show some elementary details about malware, website blacklisting, website firewall and outdated website. If the severity is medium or high, website developers must review the website as the possibility of security attacks is higher. However, these results are not foolproof because they are highly dependent on the available software tool.

As shown in Figure 1, www.edx.org has no malware and has no website blacklisting. It shows that website is not updated. Outdated websites may be vulnerable to security attacks.

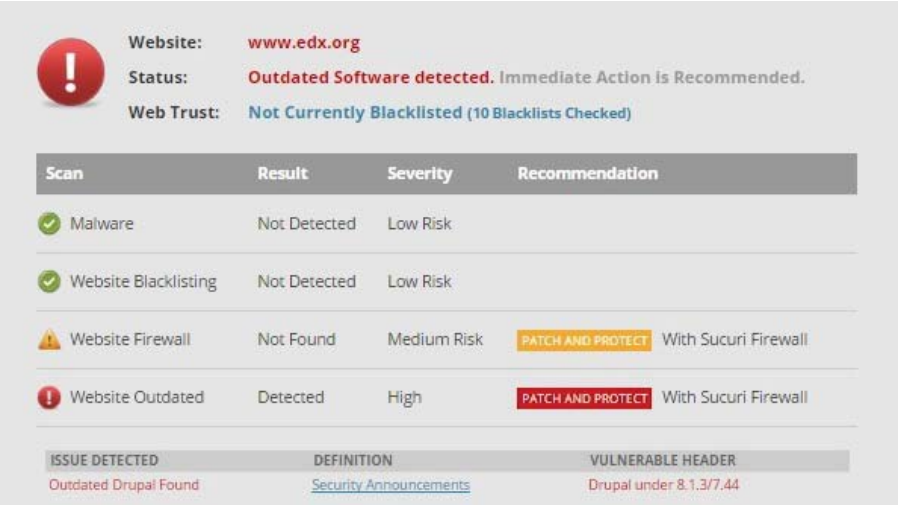

Figure 1: Security test result of www.edx.org using Securi online software tool

Figure 2 shows the output of security test conducted on www.coursera.org. The result shows that it has no major security issues.

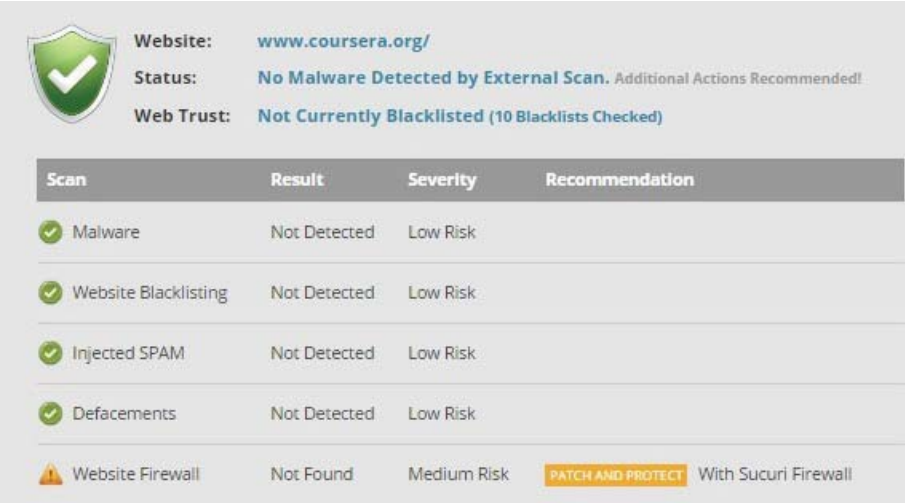

Figure 2: Security test result of www.coursera.org using Securi online software tool

As depicted in Figure 3, www.udacity.com also has no major problem with malware, website blacklisting, SPAM and defacements.

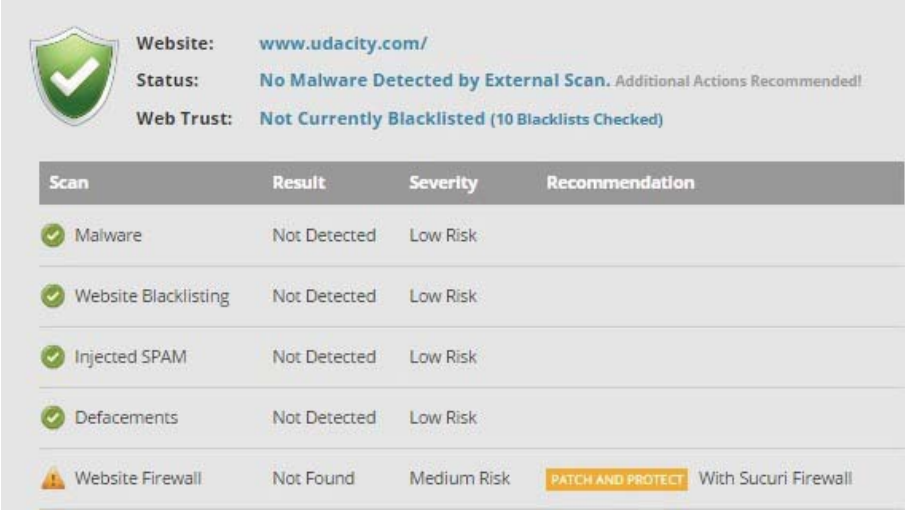

Figure 3: Security test result of www.udacity.com using Securi online software tool

Figure 4 depicts the results of the security test using the online software tool, Securi. It shows that khanacademy.org has no major problems with malware, website blacklisting, SPAM and defacements.

Figure 4: Security test result of khanacademy.org using Securi online software tool

Further, to identify any spam activity on these domains, blacklist checking was also done on these domains. It was found that all these four domains are free of any spam activity. These websites were declared clean by Google Safe Browsing, Norton Safe Web, Phish tank, Opera browser, SiteAdvisor, etc. using the online software tool of Securi.

Observatory Survey of MOOCs Platforms

To understand the parameters that may affect the security of these online platforms, an observatory survey analysis was conducted. In this process, each stage starting from registration to assessment of each platform was checked manually. These stages are checked according to common security requirements of an online learning system suggested by a number of studies (Adams & Blandford, 2003; Ayodele et al., 2011; Furnell et al. 1998;

Chen and Wu 2013). During this analysis, arbitrary parameters were identified and an observatory survey of four MOOC platforms was carried out.

EdX

EdX is one of the popular MOOCs providers, which came into existence in 2012 with the collaboration of MIT and Harvard University. It has several million registered students (Malathi, 2015). EdX has an extensive range of higher education courses. One important feature of EdX is its self-paced and timed-based classes (McAuley, 2010; McGuire, 2014). As mentioned on Edx website, EdX platform is open source, which provides a feature through which developers can easily create and share modules.

During our analysis, we observed that there is no mechanism to verify a dummy user or a fake user. Anyone who has an email address can register with Edx. In the process of user registration, it requires either an email account or a Facebook or Google+ or Microsoft account. The password is not highly secure as it can accept passwords of fewer than seven alphanumeric characters. This platform can accept a password which is exactly the same as the username. Overall, it was found that standards for password policy were not followed, which can easily lead to hacking of any user account. It has some provisions through which a learner can opt for a free or verified certificate course, where the verified certificate is a paid option. Anyone can register for any course or any number of courses; there is no restriction. It has no provision for checking or verifying the prerequisites of a course. It is purely dependent on the declaration of an individual. After registration, a user can easily see any communication available in the discussion forum of that course. Without registration, the user has no privilege to access the other modules or course. Communication options are provided in the discussion forums. It is observed that sometimes, peer group members can give close hints or answers to the assignments or quizzes, which can lead to easy completion of the course. Assessment of courses is mostly done through question bank and users are given limited attempts, and hence, the possibility of question repetition in exams is quite high. There is also another possibility of the user having multiple accounts and obtaining the list of questions by multiple attempts through different accounts.

Coursera

Coursera has the largest variety of courses. It provides free and low-cost options as well as financial aid. There are self-paced courses, courses on-demand, and timed classes. The classes usually range between four and twelve weeks (Schulz, 2014; McGuire, 2014). Most courses on Coursera are free, and a few require a small fee to participate in certificate programmes and specialisations, or a sequence of classes that include a capstone project. These certificates can also be shared on LinkedIn. One of Coursera's unique offerings is peer assessments (McGuire, 2014; About coursera.org).

Anyone can register in this platform using Facebook account or any email address. It is observed that like other platforms, this platform also has weak password policy and has no mechanism for identifying fake or dummy users. The password strength check is also weak; for example, there are no conditions to have numbers or special characters as part of the password. It also accepts passwords of six characters and the username as the password too. Like other portals, email verification is sent; however, users are generally allowed to do any activity in the platform without such confirmation. During the test, discussion forums were not found in the course. It was observed that detailed subtitles and transcripts of the videos are available in the course for each video. Attention toward copyright needs to be enforced to protect peer-generated content. It was also observed that in many courses where prerequisites are essential but there is no provision or proper mechanism to verify the credentials of the registering students. There is a possibility for someone else to appear for certification on behalf of others. Thus, it is very difficult to maintain the trust in large

communities. Verification is based on an online account, such as LinkedIn; where there is the possibility of breaches.

Udacity

Udacity has a wide range of courses mostly in computer science and vocational training. Their paid courses also include personal training, feedback, and verified certificates (McGuire, 2014). Udacity associates with academic institutes to create courses and has a special feature called nano-degrees. As per official website of Udacity, the course content in Udacity courses are available free of cost but verified certificates are paid. Compared to other MOOCs, it is found that Udacity has a smaller catalogue of courses.

The signup process on the platform is simple and is based on any email, Facebook or Google account. This platform also has a weak password policy as there is no condition of having numbers or special character. It also accepts passwords containing the username. However, it forces users to create passwords of more than seven characters. Like other portals, email verification is sent; however, users can be allowed to do any activity in the platform prior to the confirmation. Discussion forums are open to every user and discussions take place in any group on any topic. This may lead to some social engineering attacks. Also, such forums can be used for bullying and negative or fake publicity. It was found that the examinations do not have many safeguards in place to prevent cheating. Also, it is easy to deceive the examination process and get certification on behalf of others, and thereby affecting the trust in a large community.

Khan Academy

Khan Academy is an educational non-profit organisation founded in September 2008 by Salman A. Khan. According to its website, its mission is to “change education for the better by providing a free world-class education for anyone anywhere”. It started as a small initiative of its founder and has since grown to contain over 3,300 videos, most of which were made by Khan himself. There are over 47 courses, receiving over six million unique users each month, with around 380,000 YouTube subscribers. The organisation is supported by donors such as Google Inc. and the Bill and Melinda Gates Foundation (Faviero, 2012).

The registration process is quite simple and can be done through Google, Facebook, or any email address. Age is one of the parameters used here to identify the user. It has a weak password policy as it can easily accept password containing the username. Also, it has no restriction of using a number or special characters in the password and passwords with less than eight characters are also accepted. It is evident that such a weak password policy is susceptible to dictionary attacks and brute force attacks (Kumar & Doja, 2007). This platform has one important feature to safeguard the privacy of online students, which is the student privacy pledge. However, this pledge should also be supported with other security requirements and provisions. It is also observed that in many courses, prerequisites are essential but there is no provision or proper mechanism to verify the credentials of registering students or to verify the prerequisites. After registering for a course, a user can easily view and participate in the discussion forums and old threads of the discussions. In different places, it is observed that students may get direct help in assignments/test easily through these discussion forums. Also, the possibility of cheating in the examinations is high.

SECURITY THREATS AND SOLUTIONS IN MOOCS PLATFORMS

Based on our security analysis and observations we have listed some of the key issues or problems in MOOC platforms at different stages. The solution for these security threats are also listed briefly in Table 1 based on our literature survey and academic knowledge. Most of

these solutions are being implemented in the industry and by many online portals for better security. Implementation of these security solutions may lead to better MOOC services and will ensure the trust of the public and industry.

Table 1: Possible Security Threats and Solutions in MOOC Platforms

Stage	Possible Threats	Possible Solutions
Course Registration	Fake user or dummy user	Biometric authentication. Multiple user authentication schemes (Kumar & Doja, 2007).
	Verification of prerequisites	Collaboration with local centres /agencies. Uploading of earlier certification/degrees for verification.
	Online payment security issues	Secure payment/protection of users details. Multi-factor authentication. End-to-end encryption (Makrushin, 2013; Elefant)
	Weak password policy	Standard password policy should be followed (SANS Password Protection Policy, 2014).
Course Delivery	Fake attendance	Time Monitoring and Attendance Tracking software
	Electronic copyright protection	Content filtering, protocol blocking, blocking access to infringing online location. Digital Rights management
	Secure submission of work	Encryption, separate and secure channel for such submissions, end-to-end encryption (Miguel, et. al., 2015; Elefant)
	Confidentiality and non-repudiation	Hash Function, Digital Signature, Policy framework (Ayodele, et al. 2011; Furnell & Karweni, 2001).
Communication between Teachers and Learners	Data privacy	Encryption, Anti-virus, Firewall, Intrusion detection system (Furnell et al., 1998; Furnell & Karweni, 2001).
	Social engineering attacks	User Awareness, Policy framework, Training to technical and web support (Chen and Wu, 2013)
	Copyright protection of digital content	Policy for ownership of user-generated content, Need a policy framework for digital content rights.
	Negative publicity or Wrong reviews	Regular monitoring, Answering appropriately. Deleting fake users or warning users from time to time. User awareness. Policy framing.
Examinations and Continuous Assessments	Confidentiality of student grades	Safe storage and retrieval of information, firewall, Intrusion detection system (Furnell et al., 1998; Furnell & Karweni, 2001).
	Verification of identity in exams/tests	Video recording of exams, verification of photography, collaboration with local centres for physical examinations and secure learning assessment, live proctoring.
	Plagiarism or cheating in assessments	Anti-plagiarism software, additional audio or video recording of solutions.
	Repeating assessment (Retrieving Questions)	Location and IP based monitoring, firewall and Intrusion detection system (Furnell et al., 1998; Furnell & Karweni, 2001).
Certifications	Verification of certificate integrity	Requirement of photography at the time of registration and examination, Digital Signature, collaboration with local centres (Furnell & Karweni, 2001; Chen and Wu, 2013)

CONCLUSION

The mounting accessibility of the web and easy availability of computing devices have facilitated the growth of Open and Distance learning. The rise of MOOCs has started a brand new era in Open and distance learning in particular, and education at large. However, the information security threats inherent to the utilisation of the web are also of concern to the MOOCs platforms. Online learning platforms have not taken information security threats seriously. Our study of the MOOC platforms has also proved the same. It is evident that these platforms have weak password policies, which would compromise the security of users' accounts and consequently the trust of larger communities may be at stake. In this paper, two primary approaches were used to understand the security issues of MOOC platforms (edX, Coursera, Udacity and Khan Academy). First, an online security testing tool was used to understand basic security threats and problems in these platforms. Second, an observatory survey analysis was conducted to understand security issues. In this process, each stage, starting from registration to assessment of each platform was checked manually. These stages were checked according to common security requirements of an online learning system. The possible security threats and solutions at different stages of MOOC platforms were listed and presented. Future studies are required to understand the security issues of paid services offered by these MOOC platforms, such as nano-degree and verified certificates. Also, large-scale user studies on 'security and usability' of these platforms would be highly useful. Considering the weak password policies of these platforms, it is speculated that these platforms may have a large number of fake/dummy learners. Hence, it would be appropriate to refer to active learners of these platforms in order to understand the actual growth of MOOC learners. MOOCs providers have to play an important role as there is a significant demand for MOOCs and the inherent challenges of the internet must be addressed to provide quality education.

REFERENCES

About Coursera. Retrieved from https://about.coursera.org/

About Khan Academy. Retrieved from https://www.khanacademy.org/about

About Open edX. Retrieved from https://open.edx.org/about-open-edx

About Us. Retrieved from https://www.udacity.com/us

Adams, A., & Blandford, A. (2003). Security and online learning: To protect or prohibit. *Usability Evaluation of Online Learning Programs*, 331-359.

Alwi, N. H. M., & Fan, I. S. (2010). E-learning and information security management. *International Journal of Digital Society (IJDS), 1(2),* 148-156.

Ayodele, T., Shoniregun, C. A., & Akmayeva, G. (2011). *Towards e-learning security: A machine learning approach*. Paper presented at IEEE International Conference on information Society (i-Society), London, United Kingdom. pp. 490-492.

Bad publicity: how to limit damage to your reputation. Retrieved from http://www.marketingdonut.co.uk/pr/handling-bad-publicity/bad-publicity-how-to-limit-damage-to-your-reputationwww.marketingdonut.co.uk/node/3155

Bruno B. F. Faviero. (2012). *Major players in online education market*. Retrieved from http://tech.mit.edu/V132/N34/education.html

Copyright Solutions for the Digital Age. Retrieved from https://www.sla.org/learn/certificate-programs/cert-copyright-mgmt/ccm400-digital-content-and-social-media-copyright-issues/

Elefant, S. M. *Secure online payment system requires end-to-end encryption.* Retrieved from http://searchsecurity.techtarget.com/magazineContent/Secure-online-payment-system-requires-end-to-end-encryption

Fowler, J. (2013). An early report card on massive open online courses. *The Wall Street Journal*. , Retrieved from http://www.wsj.com/articles/SB10001424052702303759604579093400834738972 wsj.com/articles/SB10001424052702303759604579093400834738972.

Free Website Malware and Security Scanner. Retrieved from https://sitecheck.sucuri.net/ (last seen at 15th August 2016)

Furnell, S.M., & Karweni, T. (2001). Security issues in Online Distance Learning. *Vine*, 123 28-35.

Furnell, S.M., Onions, P. D., Bleimann, U., Gojny, U., Knahl, M., Roder, H.F., & Sanders, P.W. (1998). A security framework for online distance learning and training. *Internet Research: Electronic Networking Applications and Policy, Vol. 8 No. 3*, pp. 236-42.

Graf, F. (2002). Providing security for eLearning. *Computer & Graphics, 26(2)*, 355-365.

ICEF Monitor, *MOOC enrolment surpassed 35 million in 2015*. (2016). Retrieved from http://monitor.icef.com/2016/01/mooc-enrolment-surpassed-35-million-in-2015/

IFPI ISP - Technical options for addressing online copyright infringement. Retrieved from https://www.eff.org/sites/all/libraries/pdf.js/web/viewer.html?file=https%3A%2F%2Fwww.eff.org%2Ffiles%2Ffilenode%2Feffeurope%2Fifpi_filtering_memo.pdf

Kumar, N. & Doja, M. N. (2007). *Comparative Analysis on Alternative Schemes of User Authentication*. Paper presented at the 2nd international Conference on Embedded System, Mobile Communication and Computing, Bangalore, India, pp. 168-179.

Makrushin, D. (2013). *Money Online: Threats and Electronic Payment Protection*. Retrieved from https://blog.kaspersky.com/money-online-threats-and-electronic-payment-protection/2810/

Malathi, S. (2015, December). *Comparative Analysis of Massive Open Online Course (MOOC) Platforms*. Paper presented at the 4th International Conference on Global Business, Economics, Finance and Social Sciences, Kolkata, India.

McAuley, A., Stewart, B., Siemens, G., & Cormier, D. (2010). *The MOOC Model for Digital Practice*. Canada: University of Prince Edward, Island

McGuire, R. (2014). *The Best MOOC Provider: A Review of Coursera, Udacity and Edx.* Retrieved from http://www.skilledup.com/articles/the-best-mooc-provider-a-review-of-coursera-udacity-and-edx

Miguel, J., Caball´e, S., Xhafa, F. & Prieto, J. (2015). Security in Online WebLearning Assessment: Providing an Effective Trustworthiness Approach to Support e-Learning Teams. *World Wide Web Journal (WWWJ)*

SANS Password Protection Policy. (2014). Retrieved from https://www.sans.org/security-resources/policies/general/pdf/password-protection-policy

Schulz, E. (Ed.). (2014).The potential and problems of MOOCs: MOOCs in the context of digital teaching. Beiträge zur Hochschulpolitik 2/2014 paper presented at German Rectors' Conference, June 2014. Retrieved from http://www.hrk.de/uploads/media/MOOCs_EN_01.pdf

Serb, A., Defta, C., Lacob, N. M., & Apetrei, M. C. (2013). Information security management in e-learning. *Knowledge Horizons*, *5*(2), 55-59.

Shah, D., (2015). *MOOC Trends in 2015: Big MOOC Providers Find their Business Models.* Retrieved from https://www.class-central.com/report/mooc-business-model/

The Massive open online course. In *Wikipedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=Massive_open_online_course&action=edit

Yong Chen & Wu He (2013). Security Risks and Protection in Online Learning: A Survey. *International Review of Research in Open and Distributed Learning, Vol 14*, No 5 (2013).