Information Security Modelling In an E-Learning Environment

Ann Baby
Assistant Professor
Rajagiri Colelge of Social Sciences
Kalamassery
Kerala, India

Dr.A.Kannammal
Associate Professor
Coimbatore Institute of Technology
Coimbatore
Tamil Nadu, India

Abstract

This paper performs a research on the e-learning strategies involved in organizations, especially educational institutions. E-learning industry is poised to become one of the largest sectors in the world economy. A review into the literature is performed, looking into aspects of Information Security Modelling in the e-learning strategies and environment. A security model is suggested, after taking into account all the threats, risks and vulnerabilities of the e-learning environment.

Keywords :

I. INTRODUCTION

The growth of Information Technology and Communication has led the world to a dramatic change. People stay connected to each other and are able to access services globally. This has indeed paved way to facilitating the people to have different communities like organizational institutions, educational departments' and other government offices to convey its message to the people and communicate between them [1]. All organizations, in this context should realize that information is an extremely valuable resource and must be protected at any cost [2].

Moreover, eservices have been introduced widely; thus, the education industry has fully detained its new potential as long life learning tools from the Internet features, such as in the form of the web application, for example. Most of the organizations use internet for e-Learning. E-learning most often means an approach to facilitate and enhance learning through the use of devices based on computer and communications technology. This industry is poised to become one of the largest sectors in the world economy [3]. As the Internet is open for all users to access and share information, the security of e-learning technologies is of utmost importance.

The research paper is structured as follows: section 1 gives an introduction to the paper, section II describes about e-learning, the benefits of e-learning, the disadvantages of e-learning and the growth and development of e-learning, section III describes security issues in e-learning, section IV recommends an Information Security framework for the e-learning technologies, and section V gives a conclusion to the paper.

II. E-LEARNING

A.DESCRIPTIONS OF E-LEARNING

E-learning is inclusive of, and is broadly synonymous with multimedia learning, technology-enhanced learning (TEL), computer-based instruction (CBI), computer-based training (CBT), computer-assisted instruction or computer-aided instruction (CAI), internet-based training (IBT), web-based training (WBT), online education, virtual education, virtual learning environments (VLE) (which are also called learning platforms), m-learning, and digital educational collaboration [4].

"e" should be interpreted to mean "exciting, energetic, enthusiastic, emotional, extended, excellent, and educational" in addition to "electronic." [5]. Both educators and technology experts need to understand not just the hardware but also the "wetware" of human behavior in response to technology-supported teaching and learning. Various technologies are used to facilitate e-learning.

Most e-learning uses combinations of these techniques, including blogs, collaborative software, ePortfolios, and virtual classrooms. Technologies like audio, video, PCs, tablets, notebooks, Smartboards, webcams, screencasting etc are used for e-learning. Tools used to support e-learning cover a wide range of different applications. They include discussion forums, chat, file sharing, video conferences, shared whiteboards, e-portfolios, weblogs and wikis. Such tools can be used to support different activities involved in the learning process. E-learning finds its applications in pre –schools, K-12, graduate and postgraduate courses, and in the corporate and professional world.

ADL is a U.S. government-sponsored organization that researches and develops specifications to encourage the adoption and advancement of e-learning. The most widely accepted ADL publication is the ADL Shareable Content Object Reference Model (SCORM). SCORM defines a Web-based learning 'Content Aggregation Model' and 'Run-Time Environment' for learning objects. SCORM is a collection of specifications adapted from best practices of various existing e-learning standards to provide a comprehensive suite of e-learning capabilities that enable interoperability, accessibility and reusability of Web based learning content. [17]

B. BENEFITS OF E-LEARNING

The advantages of e-learning include improved open access to education, including access to full degree programs, better integration for non-full-time students, particularly in continuing education and improved interactions between students and instructors [6]. It also includes provision of tools to enable students to independently solve problems and acquisition of technological skills through practice with tools and computers. [7]. E-learning could be seen as a professional level of education but with the advantages of lower time and cost. Larger learner population, shortage of qualified training staff and lower cost of campus maintenance, up-to-date information and accessibility are also advantages of e-learning.

C. DISAVANTAGES OF E-LEARNING

Disadvantages of e-learning include potential distractions that hinder true learning, ease of cheating and bias towards tech-savvy students over non-technical students. It would also include teachers' lack of knowledge and experience to manage virtual teacher-student interaction.[8]. It is also suggested in literature that the disadvantages also include lack of social interaction between teacher and students; lack of direct and immediate feedback from teachers, asynchronic communication hinders fast exchange of question and danger of procrastination. [9]. Though e-learning activities and initiatives are not achieving great expectations, the market demand is of an increasing nature.

D. GROWTH AND DEVELOPMENT OF E-LEARNING

The traditional learning environment consists of physical entities like teachers, students and a physical database where all the teaching/learning material is stored. [2]. The data stored could be either public data or private data.

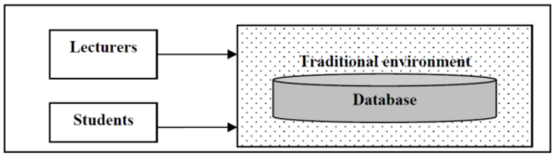


Figure 1: The Traditional Teaching Environment.

In the traditional environment, Information Security is addressed well as they are normally restricted a physical location. Teachers, students and the information database are very location-wise physically close to each other. Teachers are very sure about who writes exams as students carry with them their hall-tickets and id-cards to the physical examination hall. This eliminates the possibility of an outsider impersonating a student.

In the E-learning environment, the learning material is delivered electronically to learners who may or may-be remote through a computer network [10]. In a e-learning environment the lecturers, students and information are in completely different geographical locations and are connected via the Internet.

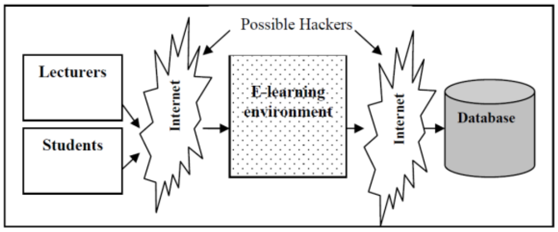
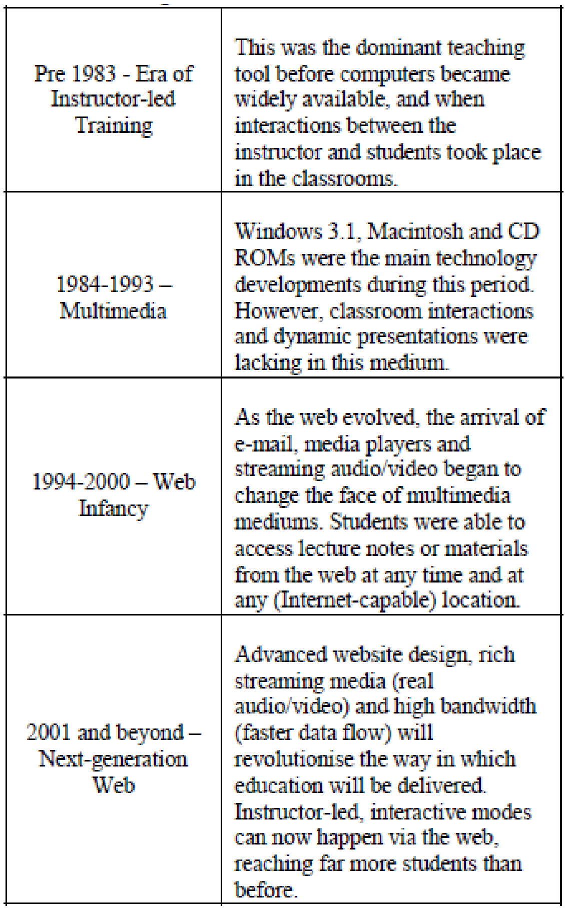


Figure 2: E-learning environment.

The 1980s saw a trend of technology used to support the process of teaching and learning. It was during this period that Personal Computers (PCs) started to become widely used by people at homes and in organizations. In fact, higher learning institutions have also dramatically changed over the last thirty years in consideration of policy drivers, such as widening participation, long life learning, and quality assurance [11].



Pre 1983 - Era of Instructor-led Training	This was the dominant teaching tool before computers became widely available, and when interactions between the instructor and students took place in the classrooms.
1984-1993 – Multimedia	Windows 3.1, Macintosh and CD ROMs were the main technology developments during this period. However, classroom interactions and dynamic presentations were lacking in this medium.
1994-2000 – Web Infancy	As the web evolved, the arrival of e-mail, media players and streaming audio/video began to change the face of multimedia mediums. Students were able to access lecture notes or materials from the web at any time and at any (Internet-capable) location.
2001 and beyond – Next-generation Web	Advanced website design, rich streaming media (real audio/video) and high bandwidth (faster data flow) will revolutionise the way in which education will be delivered. Instructor-led, interactive modes can now happen via the web, reaching far more students than before.

Figure 3 : The growth of e-learning

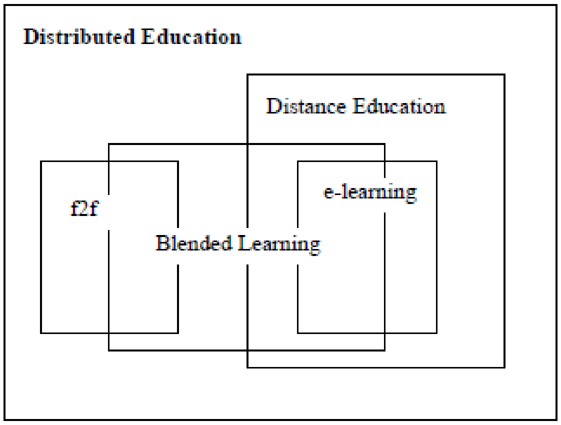


Figure 4: The Relationship of E-learning to Distribution Learning (Mason & Rennie, 2006)

Distance education is more of self-learning by the students. Here, the learning materials are either posted through the physical mail or can be accessed online through the internet. Correspondence sessions, if any are conducted a few times in each semester/year/course. The combination of face-to-face (f2f) and online learning sessions are referred to blended learning. Blended learning utilizes technology combined with traditional learning or training. Strategic learning delivery channels are used, such as physical classrooms, virtual classrooms, print, email and message boards, mentoring systems, software simulations, online collaboration, and mobile and wireless channels [12].

E-learning systems can be accessed by both students and teachers who are located remote. The databases which contain all the required information are stored in servers at any location, as per the requirement, by the educators. Once the student gives a request to access the required information, the databases in the servers are accessed through the web server. The students have facilities to access documents/files uploaded by the educator, provided the student has sufficient authentication privileges.

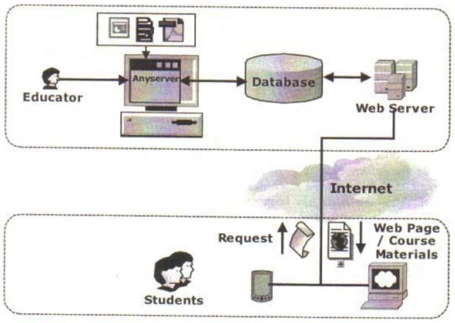


Figure 5: E-Learning Systems Components Diagram (Au *et al*., 2003)

III. SECURITY ISSUES IN E-LEARNING

The e-learning technologies have several security threats to both the user and the provider. Students can copy another student's work and claim it to be his own. A student can also gain unauthorized access to the databases which store mars/questions etc and do manipulations in it so that he can gain and other students lose. A student can also login from a remote place for an examination and use fraudulent measures to pass the examination, as physical examination supervision does not happen in e-learning technologies. These actions could occur due to malicious intent or by plain ignorance on the part of the user on how to properly secure the information they work with. Other security issues include loss of confidentiality of information like financial records, data and other plans. Loss of emails is also a concerning issue. Sharing of data to adversaries can pose a threat to your competitive data and thus pose a threat to the institution's competitive advantage.

Vandalism of public information services, such as Web sites is also a security issue in e-learning.

According to Rosenberg [13], e-learning is based on three fundamental criteria, which are: 1) network-capable updating, storage/retrieval, distribution and sharing of information; 2) delivery to the end of user via computer using standard Internet technology; and 3) focus on the broadest view of e-learning. The first two criterions depicts the e-learning institutions to the threats, as the use of ICT could ultimately lead to many possible information security risks which might negotiate data, such as loss of confidentiality, availability, exposure of critical data, and vandalism of public information services [14]. Undesirably, hardly any efforts have been done to address these alarming issues in e-learning technologies. Among the various security problems in e-learning are safeguarding against exploitation (students, insider), user authentication, and confidentiality [14].

SQL Injection attacks are also common in e-learning technologies. It takes advantage of the Web application to obtain and manipulate information from the database. Hackers can enter SQL queries or characters into the Web application so that they can perform an unforeseen exploit that is capable of taking action in a malevolent manner. Such queries can result in access to unauthorized data, bypassing of authentication or the explicit closing of a database even though the database happens to be on the either the Web Server or a standalone physical server [1].

Buffer overflows are a common security risk in web applications. Applications like e-learning technologies could be susceptible to buffer overflows, which could take place at what time a program tries to accumulate additional data in a static buffer than it is designed to manage. The supplementary data would overwrite the memory, thus corrupting it. It thus allows an intruder to interleave random commands on the Web server, thus crashing the server. Applications might not sufficiently avoid the beginning of arbitrary code into the system that might be run with the administrator rights of the operating system. [1].

Cross Site Scripting (XSS) flaws can happen if hackers create websites through which they can use browsers of other users who are using the e-learning technology user could unknowingly visit the hackers website through hoax links received in his email and thus malicious code from the hacker would be run on the user’s machine. A victorious assault can reveal the end user's session token; attack the machine, server and even spoof the content. Denial of Service (DoS) attacks is also largely seen in e-learning technologies.

Other possible attacks to the e-learning technology would include deliberate software attacks through viruses, worms and macros. Technical software failures like those of bugs, or coding problems can happen in the e-learning technologies. Events like “Acts of God” in the form of earthquakes; famines etc are a threat to security. Human prone errors like accidents or employee mistakes and deliberate acts of spying or intrusion can happen. Premeditated acts of damage or destruction, technological hardware failures or errors like equipment malfunction, illegitimate taking away of hardware, software and information are also increasing risks that could arise in the various e-learning technologies. Infringements on IPR (Intellectual Property Rights), piracy, service quality problems from service providers, outdated technologies and extortion are also highly rising today. [3].

IV. E-LEARNING INFORMATION SECURITY MODELLING

E-learning technologies security should address the problems of login security, assessment, web applications, delivery of learning materials, searching, etc. As e-learning technologies are triggered and functioned over the Internet through the web, it is necessary that security is to be provided primarily to the web communication.

The SKiP (Security Knowledge in Practice) method developed by The Carnegie- Mellon University is widely used to secure the web applications in e-learning technologies. In the SKiP method, the network software is secured, and the hardware is hardened so that none can break into the hardware. Detection and Responsiveness to network intrusions is also taken care by the SKIP method. Event logs are maintained, in case of intrusions [15]. In SKiP, customized system software is purchased from the vendor. The known vulnerabilities are listed and the system is secured from them.

In case anomalies are detected, the system is analyzed, for potential problems. Whenever any intrusion occurs, the system is made to respond to it. Periodically, the system should be made to be updates on the practices and procedures. The SKiP process is repeated as long as the organization requires protection. This technology can be used for the e-learning technologies in organizations.

Insecure services need to be eliminated from the system. Files and directories which are vulnerable need to be restricted access. It needs to be looked into the fact that the vulnerabilities should be reduced to maintain a low-profile. Proper firewalls are to be installed all over the network to restrict access only to authenticated and authorized users. Secure Socket Layer (SSL) should be used to transfer sensitive data such as login name and password over the Internet via HTTPS. Unencrypted passwords should not be stored in the database. The passwords are to be encrypted before storage into the database or server. During retrieval, a comparison should happen for the user authentication.

The Information Security measures to be maintained in an e-learning technology environment comprises of Identification and Authentication, Authorization, Confidentiality, Integrity, Non-repudiation and Availability. [2]

Procedural Counter measures necessarily need to be given importance. Controls like ensuring Information Security Governance, implementing an E-learning Information Security Policy, establishing an E-learning Security Risk Management Plan and proper Monitoring of Information Security measures - Information security periodically I n a timely manner adds to the security modeling of e-learning technologies. [2]

The RIPEMD-160 hash function is nowadays widely used for authentication. It has been researched that RIPEMD-160 provides the maximum authentication than any other hash function. [16] The use of RIPEMD-160 is for the prevention of impersonation and violation of data, this authentication is the assurance that the communicating entity is the one that it claims to be. Different algorithms are used for the authentication of legal users. [1] Other hash functions which can be used are MD4, MD5 and RIPEMD with different key length. The weaknesses of MD4 are replaced by the MD5, while currently MD5 is becoming insecure one and under attacks. The other versions of RIPMD are 128,256,320. But the strengthened version of RIPEMD-160 and expected to be secure for the next ten years. [16]

The handbook of Information Security Modelling lists out access controls; communication system; risk management and business continuity planning; policy, standards and organization; computer architecture and system security; law, investigation and ethics; application program security; cryptography, operation security and physical security as the main control mechanisms. The same can be employed for e-learning technologies. The major areas of computer management comprise guaranteeing confidentiality, integrity, and availability of all assets. [18]

The British standard BS ISO/IEC 17799:2005 Information Security Management System (ISMS) can be adopted for e-learning technologies. Kritzinger and Von Solm [19] recommend four most important fundamentals of information security within e-learning environments, together with ensuring e-learning information security governance, creating e-learning information security policy and procedures, implementing e-learning information security countermeasures, and monitoring the e-learning information security countermeasures.

There have been more than a few research studies which propose that e-learning ISM frameworks be supposed to unavoidably take account of a variety of particulars on policies, process, procedures, organizational structures, and software and hardware functions so as to augment security implementation.

V. CONCLUSION

E-learning technologies are not a novel application but relatively a new advance to the employment of innovative technologies for learning. E-learning can provide a more holistic learning environment by bringing together sources and contexts for learning Ensuring the availability and integrity of information and other content within the e-learning environments require that countermeasures, like security in the technology, hardware and software, need to be implemented. In today's increasing level of e-learning's presence in organizations and institutions, there remain many issues to be resolved. As the Internet is not a secure source of transmitting information, when online methods are used, information security management in e-learning is of increasing importance. A combination of the security measures discussed in the paper can be to an extent used to overcome the security issues in e-learning technologies.

REFERENCES

1."Security Enhancement for E-Learning Portal", A. Jalal, Mian Ahmad Zeb, Department of Computer Science City University, Peshawar, Pakistan, IJCSNS International Journal of Computer Science and Network Security, VOL.8 No.3, March 2008
2. "Information Security in an E-learning Environment", E. Kritzinger
School of Computing, University of South Africa,

PO Box 392, UNISA, 003, South Africa.

3. "E-Learning and Information Security Management", Najwa Hayaati Mohd Alwi, Ip-Shing Fan Cranfield University, International Journal of Digital Society (IJDS), Volume 1, Issue 2, June 2010

4. http://en.wikipedia.org/wiki/E-learning

5. "Think "Exciting": E-Learning and the Big "E"", Bernard Luskin Published on Wednesday, March 3, 2010

6. "Virtual Education System (Current Myth & Future Reality in Pakistan)", Zameer Ahmad, Virtual University of Pakistan, November 16, 2010

7. "Social software: E-learning beyond learning management systems", Christian Dalsgaard, Institute of Information and Media Studies University of Aarhus, Denmark

8.http://www.ion.uillinois.edu/resources/tutorials/overview/

9.http://www.elearningcompanion.com/disadvantages-of-online-learning.html

10. "Can e-learning replace classroom learning?" Zhang, J., Zhao, L. & Nunamaker, J. F. (2004). Communications of the ACM, 47(5): 75-79.

11. "A critique of the impact of policy and funding", Conole, G., Smith, J. and White, S. (2007), Contemporary perspectives in
E-learning Reserach themes, methods and impact on practice, Routledge, London; New York, pp.38-54.

12. Morrison, D. (2003), E-learning strategies, Wiley Chichester.

13. "E-learning strategies for delivering knowledge in the digital age", Rosenberg, M. J. (2001), McGraw-Hill, New York.

14. "Providing security for eLearning", Graf, F. (2002), Computers & Graphics, vol. 26, no. 2, pp.355-365.

15. "Five common Web application vulnerabilities", Sumit Siddharth, Pratiksha Doshi, April 2006.

16. "Security and QoS Optimization for Distributed Real time Environment", A. Jalal, Mian Ahmad Zeb, Proc. of IEEE 7th International Conference on Computer and Information Technology (CIT2007), Japan, 16-19 Oct, 2007.

17. "Security modelling for e-Learning", Jianming Yong

18. Whitson, G. (2003), 'Computer security: theory, process and management', J. Comput. Small Coll, vol. 18, no. 6, pp.57-66.

19. Kritzinger, E. and von Solms, S. H. (2006), 'Elearning: Incorporating Information Security Governance', Issues in Informing Science and Information Technology, vol. 3.