ISSUES AND SOLUTIONS IN E-LEARNING SYSTEM

Sapan Kumar Gupta¹
Juneesh K. Kuriachan²

ABSTRACT:
One of the most effective uses of information and network technology is the advent of E-Learning. Given the importance and realizing the necessity, E-learning in recent years has experienced drastic changes in teaching methods in higher education. Certainly, the three main units in E-Learning system that can be considered are student, teacher and Administration. E-Learning system has total integrity among all units at each level. Apart from the application of the integrity, security application in the entire system is essential otherwise organizing it become difficult. Internet is the backbone of the whole system, which itself is uncertain, so transaction message in the e-learning system invites hackers attack with various gaps in technology. Safeguards are to be imposed on the various segments of the systems. In this piece of research work, emphasis is put on different risks and hazards and of course remedies called e-solutions to build trust in the minds of all participants in the e-learning system.

KEYWORDS - E-Learning, E-Learning system, E-Learning risks, E-Learning remedies, E-Learning security

¹ (Amity University, Noida, U.P., India), sapankumargupta@gmail.com, 9313604325
1. INTRODUCTION

The use of information and network technology in E-Learning environment has brought drastic changes in higher education system. In this connection, the Internet provides the platform for the growing demand of advanced study materials and research related resources. Any educational setup (school, colleges university & corporate, etc.) with some financial transactions is the case of concern. But in an era of IT revolution, students from different regions and communities can be future ready with the same degree or diploma at a distance and location is not a problem at all. Then, E-Learning is engineered in a variety of contexts, such as distance education, online learning, Web-based learning and learning to push educational interaction between learner, faculty/facilitator and administrative groups.

E-Learning means making Internet as a platform for all learning activities that to be electronically. The advancement of a number of e-learning systems is changing higher education completely, especially in terms of content, delivery and quality. There are five main participants - authors, students, leaders, teachers and Administrator (system administrators) play role in E-learning. Hackers can hack authenticated documents like training materials, e-certification, e-exam papers, reference materials, notes, etc., that transfers between student, administrator and the authors as required. As technology has evolved the current scenario of education system is changing dramatically, students (in a broad sense "students") interested in learning, not restricted to the conventional setup of education alone.

Risk is associated with different threats, and the consequent loss. E-risk becomes visible at the time of any electronic transaction, while a threat expected means danger. Most common threats are viruses in a network, penetrations, theft and unauthorized access and alterations of data, interception, and lack of personal access to servers and personal equipment. During the transaction period data/information can be changed, altered or destroyed by hackers’ attacks. Therefore, knowledge of risk is prioritized in E-Learning. In this research paper, I focus on the various risks of the participants and their mitigation to design the system reliable and efficient. The second section describes the common threats, followed by the different risks participants and the need for risk analysis in e-Learning. The third section shows how these risks can be minimized by using several security tools and techniques. The fourth section provides a brief conclusion.

2. THREATS AND RISKS

The loss of assets causes because of the threats or risks. All threats / risks are made through the medium of accessibility. The biggest threats are

Confidentiality violation: An unauthorized person can access resources in the E-Learning system.
Integrity Violation: An unauthorized access and playing with a resources used in E-Learning system.
Denial of Service: Stopping access rights to disrupt traffic during transaction between users of the e-learning system.

Illegitimate use: The process of the privileges of legitimate users.

Malicious program: Lines of program code that harms other programs.

Repudiation: People denial of participation in already executed transaction.

Masquerade: One way to do that hides the status from hackers.

Traffic analysis: Leaking information from misuse of communication channel.

Brute-force attack: A study of all possible combinations to discover the reason. As a result of these threats the risks may occur during the operation of textual and non-textual communications between the various participants in the e-learning system.

2.1. Author’s risk

Information technology has made it easier for authors to provide access to resources such as books, journal articles, etc. for a wide range of people. Authors are responsible for the design, development and implementation of resource. The reason of not sharing their resources from many authors is the lack of confidence of illegal and unauthorized use of their resources. Since only registered participants can access these teacher notes, tasks, etc. it is the duty of the author to protect against illegal and unintended use, alteration and reuse of resources in different e-learning contexts.

The author’s paper, conferences summary, lectures, class tests, homework, etc. can be changed / ruined by hackers through various attacks. It is therefore in the author's role and responsibility to make sure that users receive the content unchanged and users can check the integrity of the text. Timely backup and an action plan in case of failure of some components (e.g. storage device, network connections) are essential components of a risk/threat analysis. The economic interests also play an important part in all cases. Authors only know how long it takes to write each chapter and therefore all books / materials. Therefore, it is the task of the group of writers who contribute their opinions to risk analysis.

2.2 Instructor’s risk

Instructors are responsible for facilitating every possible support and guidance to related student academic issues. Teachers can have their resource or buy the outsourced course content, presentations.

All E-Learning related problems could not be limited to the technical system. It is necessary to cover the teaching methodology throughout the study process, evaluation and qualification. Teaching methods can differ from one teacher to another, but there are common events such as risk in conference delivery, sending notes and tasks, accept, and mark the answer sheets, preparation and distribution of e-books etc.

The discussions are an important part of teaching any course. One way of discussion may be through the online chat forum. An advantage of online discussion forums on oral discussions is that all written resources are stored electronically on a server system, but digital storage includes high risk of privacy for students and teachers. Teaching with any method can help students and the teachers for clear understanding. Only secure and effective security mechanism can lead to this type of prolonged interaction.
There is a risk, which includes the standard format of test questions and a list of questions. It may be restrict teacher’s academic freedom. Depending on the contract of employment, a teacher plays an important role in the academic center. There must be a team to take solve all these issues.

Risk related to the study is directly related to traps. Beside from cheating, teachers are also concerned about the availability and non-repudiation of evaluations. Also in tests Students are more willing to pick up materials compared with the study content. All teachers must be aware of the risk that the student receives the document unchanged questions before start of the test and all answers are stored in an unchanged form, too. Although the conference is simple and natural way to communicate there is always a risk of class conference (expression) when it comes to students.

2.3. Administrator’s risk

In any e-learning system, the appointed Board or the authority is responsible to grant a diploma or master certificate to a student at the end of the course. It’s like any government body, which is responsible to give its approval to any normal high school full-time academic in India. But board always formulates some rules and regulations for the establishment and operation of the e-Learning Institute. It is risky at the time of the inspection, if there is any ambiguity found in following these rules.

Major risks in E-Learning involve students pose and write tests on behalf of other students enrolled and the unauthorized assistance during the drafting of the online survey, All faculty members and students generally neglect the legal aspect, because they are usually more intended towards academic field. Legal issues such as copyright, online test, sending official documents, etc., can be a big risk to participants. Administrators should be careful in admission to a course and debarring when the need arises. The inclusion of students enrolling in more than one course carries the risk to a larger organization. There should be backup ready for recovery and test. Else providing updated data at the time requirement will be difficult.

It is also a risk for the management to distribute responsibility on sensitive issues such as maintaining password for all servers and routers, recording network traffic daily, see for the uninterruptible power supply to the server and other network devices.

It is the duty of the administrator to manage the authorization procedures, i.e. access strategies (reading, writing and run) for students and other participants in the efficient operation of the system. Otherwise it can be difficult to maintain privacy. So Manager designs system to assign people (DBA) and allow the e-learning system uses (Developer) to perform the search as an index, allowing the creation and deletion of indices, the resources that allows the creation of new tables, add or delete. Alteration allows attributes in a ratio, i.e. group provides suppression of the compounds. Also authorized to read, insert, update, and delete parts of multimedia databases of e-learning materials. But the student who has a consent form can not afford to grant this permission to other students and the system administrator who has a permit may be allowed to withdraw (revoke) a prior authorization has been given.

Besides all this, there are several other risks that must be addressed by the Administrator. These are as follows
1. The server and the workstation can be affected by internet virus, at the time, receive e-mail or by running different applications on your computer.
2. The physical security of the building.
3. Remote access, LAN, WAN damage.
4. Education, production and access problem.
5. LMS (Learning Management System) or CMS (content management system) damage
Also development costs may exceed original estimates, unless production goals are clear and implementation and will be a challenge, if not well planned in advance; development process will not cover all content suitable for delivery through E-Learning

2.4. System Developer’s risk

In an existing system, there is some limiting factors. At some point, to improvise entire system
These factors should be changed. But is extensive and too expensive. In an E-Learning system, courses are classified into different modules. Due to the requirement of market demand
a model (for example, all the changed module MCA MTech [Computer Science]) can be changed to another model. New development team will face different problem of maintaining and implementing new unless all modules are designed previously.
Design, development and distribution of e-learning requires quality hardware components such as high-end web server and database server, Internet broadband leased and an LMS line quality, together with a robust infrastructure can support multiple users and web-based applications. System equipment must propose solutions to those risks properly
otherwise the total project cost will almost double.
Another risk that developers must deal with storing passwords in clear text in the application
code as an intelligent student may be able to get access to the source code of the script to access password databases. Also a password system on risks or damaged when
User passwords can be stolen, altered by attackers. Today attacker uses many tools to guess the user's password (Ref 2nd type (i)). System Developer or DBA should be familiar with SQL injection, Cross-site scripting (XSS) attacks to keep the multimedia database

2.4. System Developer’s risk

In an existing system, there are some limiting factors. At one point, improvising the whole system means these factors must be changed. But it is complex and expensive. In an E-Learning system, courses are classified into different modules. Because of the requirements for the demand a model (for example, all the MCA module changed to MTech [Computer Science]) can be changed to another model. New development team will face different problem with maintaining and using new system unless all modules are designed before. Design, development and delivery of e-learning products requires
quality hardware components such as high-end web server and database server, broadband leased, LMS line and quality, along with a robust infrastructure that can support multiple users and web-based applications. Computer system must propose solutions these risks properly otherwise the total project cost will almost double. Another risk that developers must deal with storing passwords in clear text in the application code as an intelligent student may be able to gain access to the source code for the script to access password databases. Also a password system can be in danger or damaged when user password can be stolen, altered by attackers. Today attacker uses many tools to guess the user's password. Systems or SQL DBA should know injection, Cross-site scripting (XSS) attacks to keep the media database safe.

2.5. Student’s risk

The maximum number of users on the E-Learning system is students who earn and share their knowledge with others in the system. Student group can be divided into different levels like secondary level, diploma, undergraduate, graduate to doctorate level. However, each user should be aware of all materials received from the department, teachers or other students. Otherwise, if intruders have edited the question papers and other important documents, students have to deal with problems at the time of the study. Ability to store the login information (username and password). All students should be aware of abuse of login information, or attack can try to prevent unauthorized students to access the e-learning server with previous attacks. Teachers are not always available to help students, so they must be disciplined to work independently without the help of the teacher. Students must also have written and communication skills. When teachers and other students do not meet face to face is the time when it may misinterpret what they meant. As a mechanism for student feedback, it always enriches teachers; there is a risk to the student page to send the same feedback managing E-Learning Institute. Finally, all students should be aware of phishing, where the attacker creates fake websites that seem like a real website in E-Learning as well. Human eye will not be able to distinguish between a real and hacker site. Here students are asked to enter sensitive information

2.6. Others threats and risks in E-Learning

Besides the above risks and threats there are several other risk and threats present in the system.

2.6.1. Natural Act

Natural threats may be caused by natural calamities like fire, storm, volcanic eruption, earthquake, floods etc. E-Learning system can be affected highly by these threats.

2.6.2. Deliberative Act

Threats may come from fraud, blackmail, theft etc. caused by deliberate practices

2.6.3. Unintended Act
There may be some unavoidable threats like Computer bug, power outage, handling error etc.
So all participants in E-Learning system must plan for a risk analysis where external IT and security experts could be included. Structuring of ideas and plans related to risks may be represented by different mechanisms.

3. SOLUTIONS OF RISKS

Participants of E-Learning system face above mentioned risks. Following tools or techniques may be used to stop or minimize these risks.

3.1 Authorized Access through Firewall

A firewall is hardware or software or combination of both through which security is in place to prevent unauthorized access to a corporate network from outside the organization. Technically, a firewall is a specialized version of a router. Besides the basic functions and routing rules, The router can be configured to perform firewall functionality, with the help of additional software resources. Fundamental principles based on the rule that all traffic from the inside to the outside and vice versa must pass through the firewall. To do this, all access to the local network only physically blocked and only accessible through the firewall should be allowed. Only traffic approved under local security policy should be allowed to pass through. The firewall itself must be strong enough to handle attack. In practical implementations, a firewall is usually a combination of packet filtering and applications (or circuit) gateways. Such firewall is shown in Figure-1. So sophisticated firewalls can block a portion of the incoming traffic, but permit users E-Learning (can be students, teachers, etc.) to communicate freely inside out.

![Figure 1. Structure of Firewall in E-Learning System.](image-url)
Therefore, it is the duty of all system administrators to gain knowledge and skills to implement firewall,
To configure the firewall and monitor and troubleshoot firewalls.

3.2. E-Learning-Digital Right Management (DRM)

One of the main strategies to be implemented to reduce the risks associated with the assets of e-learning is Digital Rights Management. Assets divided in the simple device such as a static HTML page or PDF document, or a collection of files, such as images and stylesheets. On the other hand active e-learning system can be defined as the content of E-Learning (exam, notes, Degree), content encryption key, user data, personal data messages between users, another group member information, bandwidth, the integrity of the message and availability of messages. E-Learning authors define active as the services provided by the E-Learning system, as learning resources, study or assessment questions, student performance, user profile, forum content, and communication student Award in the e-learning system. Digital Right Management (DRM) makes the system more secure for their content. E-Learning System work, either in a distributed network or the Internet, where more rights regarding students, teachers, content providers, administrators etc play in which content and services created, distributed, aggregated, stored unbundled, find and use. It is therefore digitization is necessary. In a general sense, the DRM used for licenses and copyright protection or prevent copying.

3.3. Cryptography

Confidentiality is intended to ensure that information and data is not disclosed to any unauthorized person or entity. Moreover, readers should be able to trust the accuracy of the subject. One of the techniques of this aspect is cryptography. Various cryptographic tools and techniques are necessary for the implementation of security in Internet-based transactions. There are two types of cryptography algorithms

3.3.1. Private-key algorithms

In private-key algorithms, the encryption key and decryption are the same, requires that the sender and receiver agree on the key before communicating, the main characteristic of this algorithm is data encryption. Examples of such algorithms are the Data Encryption Standard (DES), Encryption algorithms international data (IDEA), and the Advanced Encryption Standard (AES). So just for encryption techniques to e-learning content, we can use these techniques.

3.3.2. Public-key algorithms

Public systems of encryption key, on the other hand, use a key (the public key) to encrypt messages or data, and a second key (the private key) to decrypt these messages or data. Here three Mathematical models are used primarily-integer factorization, discrete
logarithms and elliptic curve. Different public key algorithms are RSA, El-Gamal, and Diffie-Hellman. Approved participants can use the following technologies using the public key algorithm
• Digital Signature
• Digital Certificate

3.4. Neural Cryptography

This is a new approach based on artificial neural networks (ANN) for data security in electronic message. Again, it is a cryptosystem based on the biological, particularly network architecture and operations biological learning process. Therefore the complexity of generating the secure channel is linear with the size of the network. This biological mechanism can be used to construct an efficient coding system that modifies key permanently. It is very simple and easy to implement in the context of possible attacks, at the same time the service of e-Learning remains uninterrupted.

3.5. Elliptic Curve Cryptography (ECC)

As large amount of textual and non-textual messages to be transferred between the participants and ECC solution is stronger than any other cryptographic techniques. It proved a popular key size required for 2048-bit RSA where ECC requires 224 bits for the same security. Confidentiality and authentication can be preserved in case of transfer of documents in E-Learning.

3.6. Biometric Authentication

Among all authentication techniques, such as passwords, smart cards, digital signatures and digital certificate, there is no guarantee that the dishonest students keep their passwords secret. The password can be abused at the time of submission of the assignment, receiving the questionnaires, downloading course materials, etc., where the biometric authentication provide greater security. But this requires a little more capital.

3.7. Digital Watermarking

This technique allows an individual to add hidden copyright to audio, video, images signals, server databases and multimedia. E-learning system can be protected by unauthorized use of using digital watermarking.

4. CONCLUSIONS

We discussed risks that can occur by several participants in the e-learning and its counterpart by measurement tools / techniques to minimize these risks. Even in E-Learning only the student unlock your private data, rest all challenges on how to implement and maintain a high privacy levels to set the learning process. IT department always strives to ensure the availability of services using redundant hardware as a server,
One more thing which is important is that minimizes the risk registers. Records are distributed by virtue of the fact which can be stored in different applications running on different computers. The details of transaction, including the time of occurrence would "sign", and the record secured by cryptographic techniques. We can also improve the security of e-learning using several other techniques to minimize the risk if the system is not absolutely assured. Readers should be able to trust the accuracy of the content otherwise by reading the wrong competent readers or lack of content to lose confidence in the texts or reject to read next time onward. In the future, the concept of m-learning is presented in new electronic learning functions; however, there are also new risks with M-Learning

REFERENCES