Technical Journal, University of Engineering and Technology (UET) Taxila, Pakistan Vol. 22 No. 3-2017
ISSN:1813-1786 (Print) 2313-7770 (Online)

Security Threats and Measures in E-learning in Pakistan: A Review

S. Farid[1], M. Alam[2], G. Qaiser[3], A. A. U. Haq[4], J. Itmazi[5]

[1]*Computer Science Department, Bahauddin Zakariya University, Multan, Pakistan*
[2]*Informatics Complex, ICCC, H-8/1, Islamabad, Pakistan*
[3]*Information Technology Department, Bahauddin Zakariya University, Multan, Pakistan*
[4]*National College of Business Administration, Multan, Pakistan*
[5]*IT and eLearning Centre, Palestine Ahliya University, Bethlehem, Palestine*
[1]shahidfarid@bzu.edu.pk

Abstract-Security has become one of the key research domains of Information and Communication Technology (ICT). Information security and privacy concerns in e-learning environment are crucial because multiple users are communicating via networking (Internet). On the other hand developers show negligible tilt in this regard while developing an e-learning system. Internet is the core mean of communication in e-learning which is inherently an insecure medium. Furthermore, Internet is available for all so it is also becoming the hub of various prohibited activities. Due to this interconnectivity, data or information is exposed to the large numbers of security threats and vulnerabilities. This study intends to explore the security challenges encountered by e-learning environment in Higher Education Institutions (HEIs) of Pakistan. A thorough review about security issue has been presented and concerns about local environment are emphasized. The remedies to the security threats have also been suggested to ensure the secure electronic learning environment.

Keywords-E-learning, E-security, Security Threats and Risks, Internet, Higher Education Institutions (HEIs).

I. INTRODUCTION

Advancements in Information and Communication Technology has formed e-learning in mainstream due to ease of training and learning, cost effectiveness, accessibility and flexibility of time and place[i-vi]. ICT has transformed the focus of education and training from traditional or distance education to electronic-based highly value-added and resourceful education. This new paradigm of learning has been referred in a number of ways in the literature such as Internet-based learning [v, vii], borderless learning [viii], technology-based learning, online learning, web-based learning, flexible learning, and e-learning[iv, ix-xiv]. This study has adopted "e-learning" terminology to refer the ICT-based education.

E-learning generally involves in the development of instructional/learning material [xv]. However, in Higher Education arena, it refers to the situation where learning is accomplished over Internet-based delivery of contents and programs [xvi]. Due to penetration of the Internet, the Web has been evolved into numerous applications like banking, gamming, e-commerce, e-learning etc. [xvii]. The web is an ideal platform for offering a lot of related information to the learners. As web, browsers have been adopted as a mean for the interaction with learners and other Information Systems (IS) such as e-learning. These systems facilitate learners, teachers and institutions by providing a collaborative and interactive environment to enhance learning and teaching activities[xviii].

E-learning environment (sometimes also recognized as e-learning tools) comprises of Learning Management System (LMS), Knowledge Management System (KMS), Content Management System (CMS) or contents authoring tools [xix-xxi]. E-learning environment is an Information System (IS) based on World Wide Web (WWW) [xxii]. According to IEEE Learning Technology Standard Committee, *"a learning technology system that uses Web-browsers as the primary means of interaction with learners, and the Internet or an intranet as the primary means of communication among its subsystems and with other systems"*[xxiii].

As the Internet is one of the primary means of implementing e-learning which faces numerous illegal activities and security threats. Hence, e-learning environment is unavoidably exposed to the wide variety of security threats, risks, attacks and vulnerabilities [xxiv-xxv]. E-learning is a multi user environment having shared information and most probably accessed through Internet which makes it security sensitive especially cyber security. Cyber security has become an integral part for various organizations dealing with communication systems, management systems, medical platforms, e-learning and etc.[xxvi]

Moreover, most of the state-of-the-art e-learning tools (LMS, CMS, KMS etc.) have information security mechanism up to some extent as authentication, authorization and access is granted only on the basis of users' unique login and protected password [xxvii]. Only use of login and password do not make e-learning enough secure and building confidence to the potential users of e-learning. Therefore, this study intends to elaborate the existing security issues encounter by e-learning systems in the context of HEIs. Moreover, this work also contributes in a fashion by suggesting possible remedies and measures to avoid security threats of e-learning system by ensuring the privacy, integrity and confidentiality of the learners' data.

The rest of the paper is organized as follows: the background of e-learning in the context of Pakistan has been presented in Section 2. Section 3 describes our research design. Section 4 delineates possible entry threats and their measures, whereas section 5 sums up efforts as the conclusion of this work.

II. Background

The advancement in computer technology has made it feasible to reduce the price of computers in the range of ordinary people. On the other hand, availability of the Internet has connected the people and computers anywhere in the world. Due to this reason e-learning is becoming mainstream and its market growth rate is 35.6% globally [vi, xxviii]. Therefore, HEIs round the globe are switching to this digital learning approach in order to increase their revenue by diminishing the educational cost and having good quality. It is urged byHassanzadeh, Kanaani [xviii] that 75 percent of the top 129 US universities have been switched to this learning paradigm. In addition, 1000 institutions in 50 countries are practicing e-learning[i]. This modern trend is slowly penetrating in developing countries such as Pakistan, especially since the last decade when the country started experiencing a rapid growth of ICT infrastructure [xxix]. Increasing popularity of e-learning boost the enrolment of students in this borderless paradigm due to its ease of accessibility, flexibility of time and cost [xxx, xxxi]. However, this growing adoption of e-learning has been raised security threats on the traffic produced by this paradigm i.e. educational material delivered to or from learners can be altered or controlled by “modern pirates”. So there is the need to deeply explore the security threats faced by the e-learning paradigm.

The e-learning development focuses more on instructional design, development of learning objects, delivery of learning material and ignoring or giving confined attention to privacy and security issues of e-learning systems [xiii, xxxii-xxxiv]. Nevertheless, security is vital for the both development and execution of an e-learning system since it manages delivery of data among learners, instructors and administrators when accessed at the same time [xxxv]. Therefore, e-learning systems must be secured not at the administration end but also protects user's privacy at the learner's end [xiv]. In the case of e learning environment, administrator may require strong security measures like strong authentication for user's privacy [xxxi]. Therefore, the existing escalation in e-learning adoption round the globe demands for higher magnitude of confidentiality and privacy in e-learning environment. It is hard to secure and protect the contents and personal data among learners and systems. It is therefore crucial to take the advantage of ICT for learning and training practices in a secure manner. Due to advancement of ICT and Internet technology, security threats, attacks and other illegal activities like hacking, session hijacking are also getting common to the web based application systems like e-learning.

The significance of security for the integrated platform, which is a shared environment, is vital since it manages sensitive data that is accessed simultaneously by a variety of users. Users as a stakeholder have different roles and responsibilities according to their position and skills. The heterogeneity that characterizes those users raises the necessity of utilizing a Role Based Access Control (RBAC) mechanism to regulate user actions within the system [xxxvi]. These roles can guarantee that no user can perform ineligible acts. Keep in mind that e-learning systems are web-based applications, so that these inherit all vulnerabilities of web-based applications but still e-learning have some domain specific issues like teaching and learning activities and collaboration between students and teachers. Therefore, e-learning systems have various challenges other than traditional/conventional web based application systems.

A. E-Learning in Pakistan

With the prompt boost in the utilization of ICT, enormous universities around the world are shifting to this mode of learning by integrating ICT in education to enhance learning experience of learners [xxxvii]. This drift can easily be comprehended in Pakistan, as the country started experiencing a swift evolution of ICT Infrastructure since the last decade. Higher education facilities are progressively expanding for elevating the socio-economic condition of the people. The Government of Pakistan (GoP) has been profound in establishing IT infrastructure and enhancing digital learning in the country. For this purpose, in 2002, a university has been established with the name of the Virtual University (VU). Later in 2007, the National ICT R & D Fund for ICT-based learning and training has been established [xxxviii, xxxix]. Moreover, the HEC administers all the HEIs in the country to gauge, enhance and encourage not only research activities but also higher education in the country as well. In the steady evolution of the adoption of e-learning, security issue has become vital for the HEIs offering e-learning. Several questions has been raised about the security of the e-learning systems e.g. how to secure the e-learning system? What measures should enforced for keeping system secure from unauthorized access? Answer to such questions can enhance the acceptability of e-learning in Pakistan among all communities.

Various studies as illustrated in Table I regarding adoption, promotion and implementation of e-learning systems have been conducted in Pakistan. However, these identified studies have confined to emphasize diverse issues like technological, infrastructural, user satisfaction, bandwidth etc. None of the identified study has addressed the security and privacy challenges encountered by e-learning systems and stakeholders. However, [xlv] addressed the security issues with other various challenges, no further work has been done by the authors. Therefore, an in-depth review has been conducted in this work regarding security threats and their remedies to the e-learning systems, which consequently lead the HEIs to take precautionary measures in order to facilitate learners with the secure learning environment.

TABLE I
IDENTIFIED STUDIES ADDRESSING VARIOUS ISSUES IN THE CONTEXT OF PAKISTAN

Identified Issues	Citation
Technological and institutional infrastructure, Computer literacy, English competency, lack of awareness, Teacher training and interaction between students and teachers	[xl]
Teacher training, Electric power, ICT infrastructure, Student assessment and insufficient funding	[xli]
User satisfaction, Lack of user training, Underestimation, Lack of awareness, Lack of technical and administrative end-user support and Resistance to change	[xlii]
Inertia of behavior of people, Like their resistance to changes, etc., Underestimation, Lack of awareness and Negative attitudes towards ICTs., Lack of systemic approach to implementation and lack of follow-up, High rates of system non-completion, Lack of user-training, Lack of administrative and technical end-user support, User dissatisfaction with new systems, Mismatches between technologies and the context, Culture and work practices.	[xliii]
User satisfaction	[xliv]
Computer literacy, Computer access, Security and privacy, Face-to-face interaction, English competency and Students' resistance to change	[xlv]
Lack of user perception, Ineffective user training, Borrowed e-learning models, Digital divide and lack of technical support	[xlvi]
Lack of knowledge about technology, Usage problems and Accessibility to e-learning tools	[xlvii]
Cost of mobile Internet, Practical arrangements for practical oriented courses, Literacy rate	[vi]
Lack of instructional designers, Lack of instructional design processes, Lack of software quality assurance processes, Bandwidth, Lack of formal implementation processes, Lack of faculty interest, Lack of ICT enabled teachers, Lack of ICT enabled students, Power failure, Lack of LOs in the local language, Socio-cultural norms, Lack of resources, Accessibility to Internet broadband, Access to the latest computers, Borrowed e-learning models, Lack of leadership, Change in university structure, E-learning environment, Software interface design, Support for students, Support for teachers, Role of teachers and students, Learning style, Cost of mobile Internet, Practical arrangements for practical oriented courses, Literacy rate	[xxix]

III. RESEARCH METHOD

Exploratory research model has been adopted to explore state of the art literature intensively. Exploratory method is useful where either the targeted issue has never been addressed or inadequate information is obtainable and researcher intends to probe the research area [xlviii, xlix]. Furthermore, an exploratory research begins constructing observations and penetrating for a pattern. The researcher puts forward idea about why this pattern occurs. This approach is sometimes known as the inductive method. Therefore, this mode of research provides an appropriate way to facilitate researcher with the basic work for later studies[xlviii, l].

IV. E-LEARNING SECURITY ISSUES

Security is one of the serious concerns in education sector where ICT is the way of transferring knowledge, which is known as e-learning. Primarily, there are four main stakeholders of the e-learning system as illustrated in e-learning access model Fig. 1. These include developers, instructors, administrator and learners /students [xxix]. The developers design the instructions, also called Learning Objects (LOs), and upload on the servers in the form of web utilities. Learning Object can be defined as an entity in electronic form. It may be a text, an audio, a video, a power point presentation for online courses which may also be recognized as an e-learning product or a pedagogical entity [xxix, li]. Administrator maintains the material on server and controls the services. Learner access the LOs through network (Internet). Observing the e-learning access model one can say that two major security dimensions are network security and web security.

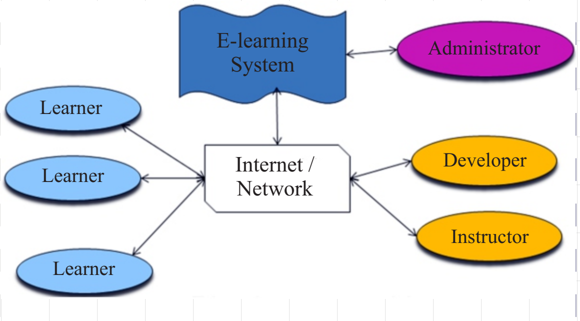


Fig. 1. E-learning access model

E-learning systems have multiple users and hence work in distributed environment connecting web and network resources. The distributed systems are more sensitive to security comparatively because of multiple users accessing from different locations. The primary security feature of e-learning paradigm is to facilitate the user with a secure transmission of information between learners and e-learning system [xxxiii]. Hence, security and privacy is one of the crucial concerns in educational context where e-learning enhancing the learning experience consequently enrolment of learners in online courses progressing rapidly [xxv]. Existing e-learning environments are production systems that demand to be secured [xiv]. Whereas, most of the e-learning systems are deficient to cope with the essential security requirements [lii]. Therefore, major issues of network security and web security like availability, confidentiality, integrity should be concentrated to achieve the effective level of e-security. Beside these there are some other factors, given below those contribute towards secure e-learning.

A. *Privacy*

Privacy also refers as confidentiality. It is prime concern of learners to feel the sense of privacy while working in an e-learning environment i.e. the transferring of information between learner and the e-system is secure and in the actual format in which it has been transferred. As learners send their data or assignment to the instructors/e-system over the Internet which expose to various threats and vulnerabilities of Internet [xxv, xxxiii]. This threat is concerned with the e-learning environment. Users will hesitate to adopt this new environment of learning until privacy is not ensured.

B. *Authentication*

It means who has created or sent the data. In other words, it is necessary to confirm the source of information for secure communication. Each user has unique identity that should be protected and checked before access and transmission of data. Protecting the identities of learners is crucial in cyberspace [xxxiii]. Rapid development in Internet technology makes it easy for the criminal to hack the users' identity. Hence, reliable identification of the learner is one of the essential factors of e-learning environment as it is the basis for access control[xiv]. Once the user is identified then it is required to verify that the learner is the same as the person is claiming to be[liii]. The learner's identity is in digital format in an online environment. Each identity in e-learning environment is unique due to specific characteristics and preferences. These characteristics may include login information, password, courses taken etc.

C. *Authorization*

Authorization states that legal users can access the information as per defined privileges. E-learning system lies under distributed system and multiple users are accessing it from scattered locations. It needs to identify the user with its identity. Therefore, there is a need of a secure authentication mechanism not only to recognize the user but also determines the users' access privileges on the e-learning system. Authorization services validates that whether the authenticated entity has privilege to access the demanded contents of e-system or not [liii, liv]. Only registered users are authorized with defined and limited facilities or level of learning content [xiv, lv]. All stakeholders like students, instructors, developers etc., are accessing e-learning system according to their responsibilities. Especially students, known as learners, are using e-learning environment from dispersed learning centres and require concrete assurance regarding identification of learners. Normally administrator of the system registers the users and assigns their access rights.

D. *Diverse Location Access*

There is the special characteristic of e-learning system that multiple users can access it simultaneously from diverse locations. Beside this, different users belong to diverse fields as well as background. These factors make the security of e-learning system more complex. An e-system can have enormous users includes instructors, learners, administrators or managers, these might access e-learning systems [xxv] in order to perform their educational activities like downloading, uploading or to exchange distributed information over the network. Hence, there are multiple places for interaction inside e-learning system that may provide multiple opportunities to intruders as numerous users can access e-learning system simultaneously from disperse locations [lv]. This has increased the security risk to the e-learning data. The security risks can be reduced by limiting the entry point to the e-learning systems. On the other hand, implementation of e-learning systems loses its unique feature of access to large number of users from various geographical locations round the globe by reducing the entry point.

E. Confidentiality

The protection of the assets of e-system from unauthorized access is termed as confidentiality. Research indicates that privacy is the state of being secluded and confidentiality is the state of keeping data secure from unauthorized access and modification. Numerous security risks can arise in e learning that disrupt privacy and confidentiality of learners[lvi]. The learners need assurance that the data and information in e-system remain secure and private and never expose to unauthorized entities, devices or systems [xiv, xxxiii]. The access control to resources can helps to achieve the confidentiality of an e-system, that can enable secure contents delivery over the network and the storage of data [xxv]. The confidentiality is one of the prime concerns of the registered learners which means that their submitted assignments, papers, information will only be accessible by the relevant examiner or personal. The user should prevail access only to authorized contents and those persons who are not the legitimate users must not be able to gain access to the e-system.

F. Integrity

In network security, integrity means that data has not been altered. Data integrity defines the accessibility, reliability, correctness and high quality of stored data [lvii]. Integrity is the assurance that only authorized users or programs has right to modify data or executable programs. Hence, ensuring the integrity of the data and information is one of the major goals in relation to the security of an e-system [xxv]. Integrity depends on access control and requires to recognize all the users who try to access e-system[xxxiv]. Moreover, learners of e-system are required to assure that the intended personal (examiner, instructor, administrator etc.) will receive their submitted contents/material (assignments, papers etc.) in its original and unedited state[xxxiii].

G. Availability

Availability can be explained as the degree to which a system is available and operational for use to the learners when it should be [xxxiv, lviii]. Moreover, availability of the system is also refers as the extent to which the system is available for learners whenever it is required[lix]. In addition, it refers to permanence, non-erasure and deals with Denial of Service (DoS) attacks and viruses that delete files. There are two main facets of availability includes Distributed Denial of Service (DDoS) and loss of data processing capabilities [lv], where DDoS attack is the root attack for data unavailability [lvii]. Hence, it is vital to confirm that information and communication resources are always available when demand is raised so that the authorize learners may submit their assignments, comments, notes or papers within the specified time. If the user is not able to access the required material or e-contents on time they may frustrate or lose their interest or even may fail at most to use e-learning system[lv, lx].

H. Non-Repudiation

Non-repudiation enforce legal users to not refuse the accomplished operation that they have done [xxv]. For example, if a learner submits his or her assignment he/she must not deny from submitting his material. Hence a systematic and formal mechanism is needed in order to enforce the registered users from denying the work or modifications that they have performed in the system[xxvii].

V. SECURITY MEASURES FOR E-LEARNING

E-learning users encounter various risks, attacks or threats while working in an e-learning environment as mentioned in previous section. As instructors, learners, administrator and data reside at various disperse physical and logical locations and the Internet is the only mean of their connectivity which makes difficult to implement the information security mechanism [xxv]. Therefore, there must be the mechanism to protect information to achieve the confidentiality, integrity and availability to attract the users to utilize the e-learning system. As an e-learning is open to many fold to multiple threats so it is required to consider and apply various measures especially to Pakistani universities in order to secure the e-system from prospective risks, attack or threats. These measures may include access control mechanism using firewall, digital signature and biometrics authentication. Cryptography and session authentication are also major network security methodologies and have lot of applications for online communication and transmission of data. Beside these, using alert SMS (Short Message Service) of mobile devices can provide secure authentication and authorization to ensure the integrity and confidentiality of the e-system. The objective of this study is to focus that how mechanisms of security, mentioned above, can be applied to an e-learning system efficiently.

A. Access Control (Firewalls)

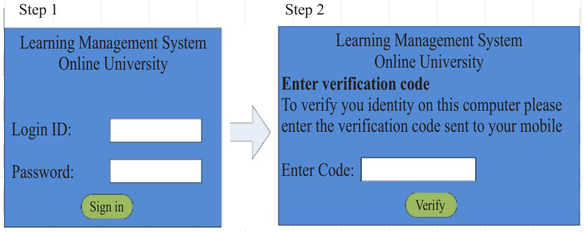
The simplest way to ensure access control is using firewalls. One of the possible techniques for improving security of the web applications is a firewall [lxi]. Firewall is firmware developed to secure the e-system from unauthorized access whether from outside or within the institution [lxii]. To enforce security, all traffic from inside to outside or vice versa must pass through it for screening, it acts as a protective layer. Therefore, all access to the system must be physically blocked and the authorize traffic should only allow to pass through it to make the e-learning system secure. A firewall creates a barrier between a trusted secure inside the network and the outside network, like the Internet, because it is supposed not to be protected or trusted. The goal of firewall is to protect the networks from threats and attacks. Firewalls can strengthen the network systems and protect systems from intruders. [lxiii]. Firewall blocks the unwanted and vulnerable communication between the networks. It is based on security policies that are predefined to secure the network from the threats [lxiv]. Firewalls are already available in the market and in use for communication over network (Internet). Therefore, it is proposed to incorporate firewalls to improve the security level of e-learning systems.

B. Biometrics Authentication

Various authentication techniques like passwords, smart card, digital certificate and digital signature are in practice. E learners can use smart cards for their authentication process because smartcard stores different parameters during registration phase and proves the authenticity of the user [lxv]. Moreover, apart from smart cards learners can use digital signatures and certificates for authentication process. Digital signatures are encrypted electronic stamp and to create a digital signature, signing certificates are needed that proves the identity [lxvi]. Even then no body cannot guarantee that the users will not provide their password [lxii] at the time of downloading, uploading of e-contents, submission of assignment, receiving/attempting the question papers and etc. Using password is an old and widely used mechanism and has good results in many cases incurring minimum cost. Still there is a chance of stealing or forging the password. Attacker can forcefully get the sensitive data like passwords through pre-functioned software[lxvii]. Biometrics authentication is a best choice to replace password matching. Therefore, biometric authentication mechanism can provide a comparatively better and secure environment as user can never misplace their biometrics and the biometric signal is difficult to steal or forge [lv]. HEIs of Pakistani can restrict the enrolled students to provide their one or more biological characteristics like face, handwriting, fingerprints, blinking of eyes or voice, which is stored in the database in order to authenticate the respective user. Keep in mind that this technique requires biometric device that incurs some cost. Recently these devices, like fingertips recognition device, are easily available in the market within affordable price. These facts prove that biometrics authentication is a feasible solution for e-learning system in Pakistan.

C. SMS Authentication

In Pakistan like other countries, use of mobile phone is increasing day by day as a mean of communication regardless of the age and educational level. Increase of cellular phone subscribers as compared to the computer users is very rapid. With such growth of telecom and mobile industry these mobiles phones are more than a simple phone. These have now become smart phone[vi]. These smart phones have potential advantage to the HEIs offering e-learning system and can be used for authentication purposes. It is proposed to use SMS for secure access of e-learning system. Possible procedure may be divided into two steps. In first step, a student submits the user ID and password through his/her cellular phone. In response to this e-learning system generates a special code and sends it to the registered phone of the user by SMS, which is actually the key for the current session. In second step, student enters this code in order to authenticate his identity and access the e-learning system safely. The complete possible login scenario with two steps login and verification is shown in Fig. 2. Such mechanism is already used for web accessing by some applications but not for e-learning systems. It is proposed to HEIs of Pakistan for adopting this two steps login and verification scheme. This simply can be done by adding a cryptographic algorithm that takes username and password as input and provide output in the form of random/unique pass code. This code is sent to user's registered mobile phone not only to identify but also to authenticate and authorize the all kinds of users with pre-granted privileges.



Enter verification code

To verify you identity on this computer please enter the verification code sent to your mobile

Fig. 2. Login scenario for two step verification

D. Cryptography

Cryptography is one of the essentially recommended techniques implemented to enforce the security in Internet based transmission of information. It has two parts encryptions, hide the data at sender end, and decryption or retrieve original data from hidden form. Cryptography is useful for protecting data from theft or alteration during transmission as well as in storage and can perform the user authentication too. According to [lxviii] cryptographic algorithms can be categorized into three major types: secret-key (symmetric) algorithm, public-key (asymmetric) algorithm and hash functions. Public-key crypto-systems use two keys. The purpose of first key is to encrypt the information on sender end while role of second key is in the decryption process of the delivered data or message. In contrast to public key, secret-key cryptography uses a single key for both encryption and decryption [lxii]. Where as in hash algorithms, hash value is appended to the data/message at the source at a time when the message is assumed or known to be correct. Then encrypt the appended message and send to the destination. The receiver authenticates that message by re-computing the hash value. Hash algorithms are used to provide a digital fingerprint of a file's contents for confirmation that an intruder has not modified data. Many operating systems utilize the hash functions to encrypt passwords [lxviii]. If any intruder, make system compromised then hashing algorithms [lxix] and cryptographic techniques [lxx] can keep the information safe.

E. Session Authentication

Session hijacking or cookie hijacking is the way to misuse the legal computer session. Attacker can hijack the session to have unauthorized access in your computer system. [lxxi]. Authentication methods are not reliable and secure; the challenge is to design such an e-system which authenticate a true user during the class session or at specified time intervals [xiv, xxv]. Two-step authentication method is more secure than the single authentication method [lxxii]. First it is required to login using ID and passwords and after that it is required to authenticate sending an email or by short message using hand held device[lxxiii]. This type of re-authentication have successfully been implemented by various secure web application systems like e-banking etc.

F. Secure Socket Layer (SSL)

Secure Sockets Layer is a standard protocol used for secure information on Internet. In e system SSL is used between the server and the user [lxxiv]. The (HTTPS) secure hypertext transfers protocol is designed to transfer encrypted information on Internet. HTTPS is simple http that uses the SSL. A SSL is encryption protocol that uses HTTPS invoked on a Web server[lxxv].

G. Physical Security Device

Learners can register a security key to their account so that next time they login after enabling approvals with that USB security device. Security can be tackled with the help of their USB device. With this physical security device phishing can be handled as user do not required to enter a code by themselves. If user uses a security key with their computer for logging in, it will be as simple as a tap on the key after your insert your password.

VI. Conclusion

Various security threats, risks and attacks have been explored encountered by e-learning environment of HEIs within Pakistan. Privacy of the user and his personal identity is most crucial issue in a shared e-system. Moreover, the methods of authentication, authorization and delivery of e-content to the users require secure mechanism. Beside authentication and authorization, non-availability of the system or e-contents to the learner at the required span of time is one of the major threats to the e-system. If the e-system is not available, it is totally useless for the learners and also cause the frustration and demoralization from the e-learning. Moreover, various methods of authentication like login, password etc. are discussed and are not found to be secure and reliable. Authentication of the learner is quiet difficult as anyone can get access on behalf of the registered user. Hence, in order to cope with such authentication concerns, biometric authentication using finger impression, eye or face recognition can be implemented. Hence, the e-system is required to deploy security services such as access control, encryption, authentication, managing users and their privileges. Few remedies such as pass code login scenario or biometric based authentication have been suggested in this study. It is recommended that existing e-learning environments adopted by HEIs of Pakistan should embed the security measures described in above section to enhance the security. Moreover, the data transfer between the system and administrators or content operators or learners should employ the encryption. A secure learning platform should not only incorporate all the aspects of security but also make most of the processes transparent and easier to the teacher and the student so that it becomes attractive for all stakeholders.

References

[i] W. Bhuasiri, O. Xaymoungkhoun, H. Zo, J. J. Rho and A. P. Ciganek,"*Critical success factors for e-learning in developing countries: A comparative analysis between ICT experts and faculty.*"Computers & Education, 2012. 58(2): p. 843-855.

[ii] M. Abdellatief, A. B. M. Sultan, M. A. Jabar and R. Abdullah,"*A technique for quality evaluation of e-learning from developers perspective*." American Journal of Economics and Business Administration, 2011. 3(1): p. 157-164.

[iii] B. Collis and J. Moonen, "*Flexible learning in a digital world: Experiences and expectations*." 2012: Routledge.

[iv] P. Sajja, "*Enhancing quality in e-Learning by knowledge-based IT support*." International Journal of Education and Development using ICT, 2008. 4(1).

[v] P. Gerbic, "*What about flexible learning and ICT?-A review of technology based flexible learning in tertiary education*." Third Pan-Commonwealth Forum Conference, 4-8 July 2004. 2004.

[vi] S. Farid, R. Ahmad, I. A. Niaz, M. Arif, S. Shamsherband and M. D. Khattak, "*Identification and prioritization of critical issues for the promotion of e-learning in Pakistan*."Computers in Human Behavior 2015. 51: p. 161-171.

[vii] D. French, "*Internet based learning: An introduction and framework for higher education and business*."1999: Stylus Pub Llc.

[viii] C. Latchem, "*Towards borderless virtual learning in higher education*. Global perspectives on e-learning: rhetoric and reality", 2005: p. 179-198.

[ix] B. H. Khan, "*The global e-learning framework*." STRIDE, 2003: p. 42.

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

[xi] G. Puri, "*Critical success Factors in e-Learning–An empirical study*." International Journal of Multidisciplinary Research, 2012. **2**(1): p. 149-161.

[xii] D. Forman, L. Nyatanga, and T. Rich, "*E-learning and educational diversity*." Nurse Education Today, 2002. 22(1): p. 76-82.

[xiii] C. D. C. Luminiţa and C.I. N. Magdalena, "*E-learning security vulnerabilities*." Procedia-Social and Behavioral Sciences, 2012. 46: p. 2297-2301.

[xiv] H. Kim, "*E-learning Privacy and Security Requirements: Review*." Journal of Security Engineering, 2013. 10(5): p. 591-600.

[xv] K. Hyder, A. Kwinn, R. Miazga and M. Murray, "*Synchronous e-learning*."The eLearning Guild, 2007.

[xvi] P. Nicholson, "*A history of e-learning*." Computers and education. 2007, Springer. p. 1-11.

[xvii] R. G. Netemeyer, W.O. Bearden, and S. Sharma, "*Scaling procedures: Issues and applications*." 2003: Sage Publications.

[xviii] A. Hassanzadeh, F. Kanaani, and S. Elahi, "*A model for measuring e-learning systems success in universities*." Expert Systems with Applications, 2012. 39(12): p. 10959-10966.

[xix] N. S. C. Babu, "*Quality Assurance Framework for e-Learning*."ELEL Tech, India, 2005.

[xx] J. L. Moore, C. D. Deane, and K. Galyen, "*e-Learning, online learning, and distance learning environments: Are they the same?*."The Internet and Higher Education, 2011. 14(2): p. 129-135.

[xxi] T. W. Daugenti, "*edu: Technology and learning environments*."Higher Education. 2009: Peter Lang.

[xxii] J. K. Lee, and W.K. Lee, "*The relationship of e-Learner's self-regulatory efficacy and perception of e-Learning environmental quality*." Computers in Human Behavior, 2008. 24(1): p. 32-47.

[xxiii] E. W. Ngai, J. Poon, and Y. Chan, "*Empirical examination of the adoption of WebCT using TAM*." Computers & Education, 2007. 48(2): p. 250-267.

[xxiv] Y. Chen, and W. He, "*Security risks and protection in online learning: A survey*." The International Review of Research in Open and Distributed Learning, 2013. 14(5).

[xxv] D. C. C. Luminita, "*Security issues in e-learning platforms*." World Journal on Educational Technology, 2011. **3**(3): p. 153-167.

[xxvi] N. Rjaibi, L. B. A. Rabai and A. B. Aissa, "*Cyber security measurement in depth for e-learning systems*." International Journal of Advanced Research in Computer Science and Software Engineering (IJARCSSE), 2012. 2(11): p. 107-120.

[xxvii]S. Assefa, "*An information security reference framework for e-learning management systems*." 2011.

[xxviii]P. C. Sun, R. J. Tsai, G. Finger, Y. Y. Chen and D. Yeh, "*What drives a successful e-Learning? An empirical investigation of the critical factors influencing learner satisfaction*." Computers & Education, 2008. 50(4): p. 1183-1202.

[xxix] S. Farid, R. Ahmad, and M. Alam, "*A Hierarchical Model for E-Learning Implementation Challenges using AHP*." Malaysian Journal of Computer Science, 2015. 28(3).

[xxx] N. H. P. Dai, D. V. Thinh, and R. Zolt, "*Learning attitude in XXI century*."IEEE 14th International Symposium on Applied Machine Intelligence and Informatics (SAMI). 2016. IEEE.

[xxxi] A. M. Gabor, M. C. Popescu, and A. Naaji, "*Security Issues Related To E-Learning Education*." International Journal of Computer Science and Network Security (IJCSNS), 2017.

17(1): p. 60.

[xxxii]K. E. Khatib, L. Korba, Y. Xu and G. Yee, "*Privacy and Security in E-Learning.*"2006.

[xxxiii]R. Raitman, L. Ngo, N. Augar and W. Zhou, "*Security in the online e-learning environment.*" Advanced Learning Technologies, 2005. ICALT 2005. Fifth IEEE International Conference on. 2005. IEEE.

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

[xxxv]C. H. Thermolia, E. S. Bei, E. G. M. Petrakis, V. Kritsotakis and V. Sakkalis,"*An ontological-based monitoring system for patients with bipolar I disorder.*"Biomedical Engineering and Computational Technologies (SIBIRCON), 2015 International Conference on. 2015. IEEE.

[xxxvi]J. B. Joshi, W. G. Aref, A. Ghafoor and E. H. Spafford, "*Security models for web-based applications.*" Communications of the ACM, 2001. 44(2): p. 38-44.

[xxxvii]P. Pagram, and J. Pagram, "*Issues in e-learning: A Thai case study.*" The Electronic Journal of Information Systems in Developing Countries, 2006. 26.

[xxxviii]S. Farid, "*A model for e-learning systems quality assessment with emphasis in Pakistan.*" 2016, University of Malaya.

[xxxix]F. Kanwal, and M. Rehman, "*E-learning Adoption Model: A case study of Pakistan.*"Life Science Journal, 2014. 11(4s).

[xl] Z. H. Siddiqui, "*Promoting E-Learning in Pakistan: Strategies and Challenges.*" e-Asia Conference and Exhibition Putrajaya Malaysia. 2007.

[xli] M. J. Iqbal, and M. Ahmed, "*Enhancing quality of education through e-learning: the case study of Allama Iqbal Open University.*" The Turkish Online Journal of Distance Education, 2010. 11(1).

[xlii] G. M. Kundi, A. Nawaz, and S. Khan, "*The predictors of success for e-learning in higher education institutions (HEIs) in NWFP, Pakistan.*" JISTEM-Journal of Information Systems and Technology Management, 2010. **7**(3): p. 545-578.

[xliii] A. Nawaz, and G. M. Kundi, "*Predictor of e-learning development and use practices in higher education institutions (HEIs) of NWFP, Pakistan.*" Journal of Science and Technology Education Research, 2010. 1(3): p. 44-54.

[xliv] Q. A. Qureshi, A. Nawaz, and N. Khan, "*Prediction of the problems, user-satisfaction and prospects of e-learning in HEIs of KPK,*" *Pakistan.*" International Journal of Science and Technology Education Research, 2011. 2(2): p. 13-21.

[xlv] I. A. Qureshi, K. Ilyas, R. Yasmin and M. Whitty, "*Challenges of implementing e-learning in a Pakistani university.*" Knowledge Management & E-Learning: An International Journal (KM&EL), 2012. 4(3): p. 310-324.

[xlvi] A. Nawaz, "*E-Learning experiences of HEIs in advanced states, developing countries and Pakistan.*" Universal Journal of Education and General Studies, 2012. 1(3): p. 72-83.

[xlvii] S. Farid, R. Ahmad, J. Itmazi and K. Asghar, "*Identifying Perceived Challenges of E-Learning Implementation.*" First International Conference on Modern Communication & Computing Technologies (MCCT'14). 2014: Nawabshah, Pakistan.

[xlviii]W. G. Zikmund, B. J. Babin, J. C. Carr and M. Graffin, "*Business research methods.*" 2013: Cengage Learning.

[xlix] M. J. Polonsky, and D.S. Waller, "*Designing and managing a research project: A business student's guide.*"2014: Sage publications.

[l] D. Davis, and R.M. Cosenza, B*usiness Research for Decision Making.*'Cosenza. 2005.

[li] D. Khattak, "*Development of Multimedia Instruction Objects for Delivery in a Localized E-Learning Environment.*" Computer Science Department. 2010, Allama Iqbal Open University, Islamabad: Pakistan.

[lii] I. Bandara, F. Ioras, and K. MaherI. "*Cyber Security Concerns in E-Learning Education.*" Proceedings of ICERI2014 Conference, 17th-19th November. 2014.

[liii] S. Assefa, and V. Solms, "*An Information Security Reference Framework for e-Learning Management Systems.*"(ISRFe-LMS). Proceedings of 9th WCCE, 2009.

[liv] E. Kritzinger, and S. V. Solms, "*Incorporating Information Security Governance.*" Issues in Informing Science and Information Technology, 2006. 3.

[lv] S. Ahmed, K. Buragga, and A.K. Ramani,"*Security issues concern for E-Learning by Saudi universities.*" 13th International Conference onAdvanced Communication Technology (ICACT), 2011. 2011. IEEE.

[lvi] A. Majeed, S. Baadel, and A. U. Haq, "*Global Triumph or Exploitation of Security and Privacy Concerns in E-Learning Systems.*"International Conference on Global Security, Safety, and Sustainability. 2017. Springer.

[lvii] M. Durairaj, and A. Manimaran, "*A study on security issues in cloud based e-learning.*"Indian Journal of Science and Technology, 2015. 8(8): p. 757-765.

[lviii] S. K. Dubey, S. Ghosh and A. Rana, "*Comparison of Software Quality Models: An Analytical Approach.*" International journal of

Emerging Technology and Advanced Engineering, 2012. 2(2): p. 111-119.

[lix] B. Behkamal, M. Kahani, and M.K. Akbari, "*Customizing ISO 9126 quality model for evaluation of B2B applications*."Information and software technology, 2009. 51(3): p. 599-609.

[lx] E. R. Weippl, "*Security in e-learning*." Vol. 16. 2006: Springer Science & Business Media.

[lxi] T. Krueger, C. Gehl, K. Rieck and P. Laskov,"*TokDoc: A self-healing web application firewall*." Proceedings of the 2010 ACM Symposium on Applied Computing. 2010. ACM.

[lxii] N. Barik, and S. Karforma, "*Risks and remedies in e-learning system*." arXiv preprint arXiv:1205.2711, 2012.

[lxiii] S. Aslam, S. Ullah, M. A. Siddiqui and A. Sattar, "*Active Attacks Detection Mechanism using 3-Phase Strategy*." International Journal of Computer Science and Network Security (IJCSNS), 2017. 17(1): p. 130.

[lxiv] R. Oppliger, "*Internet security: firewalls and beyond*." Communications of the ACM, 1997. 40(5): p. 92-102.

[lxv] T. Limbasiya, and N. Doshi, "*An analytical study of biometric based remote user authentication schemes using smart cards*." Computers & Electrical Engineering, 2017.

[lxvi] E. Aïmeur, H. Hage, and F.S.M. Onana,"*Anonymous credentials for privacy-preserving e-learning*. in *E-Technologies,*"2008 International MCETECH Conference on. 2008. IEEE.

[lxvii] R. Kaur, A. Kaur, and E. Gurjot, "*An Approach to Detect Vulnerabilities in Web-based Applications*."International Journal of Advanced Research in Computer Science, 2017. **7**(1).

[lxviii]G. C. Kessler, "*An overview of cryptography*." 2003, Gary C. Kessler.

[lxix] J. Wang, et al., "*A survey on learning to hash*." arXiv preprint arXiv:1606.00185, 2016.

[lxx] A. Verma, P. Guha, and S. Mishra, "*Comparative Study of Different Cryptographic Algorithms*." International Journal of Emerging Trends & Technology in Computer Science (IJETTCS) Volume, 2016. 5.

[lxxi] P. Kamal, "*State of the Art Survey on Session Hijacking*."Global Journal of Computer Science and Technology, 2016. 16(1).

[lxxii]F. Bergadano, D. Gunetti, and C. Picardi, "*User authentication through keystroke dynamics*." ACM Transactions on Information and System Security (TISSEC), 2002. 5(4): p. 367-397.

[lxxiii]F. Aloul, S. Zahidi, and W. E. Hajj, "*Multi factor authentication using mobile phones*." International Journal of Mathematics and Computer Science, 2009. 4(2): p. 65-80.

[lxxiv]W. Chou, "*Inside SSL: the secure sockets layer protocol*."IT professional, 2002. 4(4): p. 47-52.

[lxxv] M. S. Bhiogade, "*Secure socket layer*."Computer Science and Information Technology Education Conference. 2002.