

## Proposal: A Design of E-learning User Authentication System

Byeong Ho Kang<sup>1</sup> and Hyejin Kim<sup>2</sup>

<sup>1</sup>*School of Engineering and ICT, University of Tasmania, Sandy bay, TAS,  
Australia*

<sup>2</sup>*(Corresponding Author) Institute of School Safety Research, Sungshin Women's  
University, Seoul, Republic of Korea  
bhokang@gmail.com, hyejinaa@hanmail.net*

### Abstract

*The user authentication is very crucial in developing an e-learning system. Emerging standards for distance learning and education influence in a major way the development of e-learning systems. E-learning system must be secured against manipulation from the side of the students and also it protects user's privacy. This paper examines privacy and security issues associated with e-learning. It presents the basic principles behind privacy practices and legislation. Concrete solutions for improving the degree of security achievable are shown. A design of an e-learning user authentication system is introduced. This framework prevents manipulation from the side of the students during learning, thus allowing a reliable control of learning success.*

**Keywords:** *E-learning Privacy, Security Requirements, e-learning security*

### 1. Introduction

The growth of Information and Communication Technology has significant effects on all people around the world. These days, the Internet itself is drastically varying the provisions of services and goods, simply because of its features: immediacy, openness, ubiquity, and global reach. With this growth, people are able to connect with each other, especially through the Internet. The approach of e-Learning has become a powerful way to deliver knowledge considering the increase in on-line users. E-learning systems are considered an essential application in educational institutions today. The use of these systems is not limited to universities but extends to include schools, government departments and private enterprises [3].

The security is very crucial in developing an e-learning system. Emerging standards for distance learning and education influence in a major way the development of e-learning systems. E-Learning system must be secured against manipulation from the side of the students and also it protects user's privacy. This paper examines privacy and security issues associated with e-learning. It presents the basic principles behind privacy practices and legislation. It investigates the more popular e-learning standards to determine their provisions and limitations for privacy and security. Privacy requirements for e-learning systems are explored with respect to the "Privacy Principles". The capabilities of a number of existing privacy enhancing technologies, including methods for network privacy, policy-based privacy/security management, and trust systems, are reviewed and assessed. E-learning can be defined as technology-based learning in which learning material is delivered electronically to remote learners via a computer network. E-learning could be seen as a professional level of education but with the advantages of lower time and cost. Some other advantages of e-learning include larger learner population, shortage of qualified training staff and lower cost of campus maintenance, up-to-date information and accessibility. In a typical e-learning environment the lecturers, students and information are in different geographical locations and are connected via the Internet. The e-learning promotes the construction of life-long learning opinions and learning society. e-

Learning is a broad concept and it consists with different types, namely Synchronous and Asynchronous e- Learning. Both methods have different characteristics and they use different methods to broadcast the learning materials. Asynchronous e-Learning occurs when students begin and complete their training courses at different times according to their own schedule. Synchronous e-Learning allows real-time interaction and raises a sense of community among learners. The security is very crucial in developing an e-learning system. Emerging standards for distance learning and education influence in a major way the development of e-learning systems. E-Learning system must be secured against manipulation from the side of the students and also it protects user's privacy. This paper examines privacy and security issues associated with e-learning. It presents the basic principles behind privacy practices and legislation. Security is an important issue in the actual educational context where e-learning increases in popularity and more and more people are taking online courses. The e-learning platforms are today production systems that need to be secured. To achieve a good level of security, there are many important elements that must be taken into account: authentication, access control and data integrity.

## 2. Background

This section discuss about the brief background of e-learning. E-learning refers to the use of electronic media and information and communication technologies in education. E-learning is broadly inclusive of all forms of educational technology in learning and teaching. E-learning is inclusive of, and is broadly synonymous with multimedia learning, technology-enhanced learning, computer-based instruction, computer-based training, computer-assisted instruction or computer-aided instruction, internet-based training, web-based training, online education, virtual education, virtual learning environments which are also called learning platforms, m-learning, and digital educational collaboration. These alternative names emphasize a particular aspect, component or delivery method.

Standardization and compatibility are vital for both e-learning vendors and end users to be able to sell or purchase portable content and inter-changeable components on the market. They are also very important where different e-learning systems must interact with one another.

Figure 1 shows the typical overview of e-learning system. The learner accesses the learning resources and does the activities as instructed. The Moderator acts as a teacher me evaluate and act as moderator of the learners. In the end, there is an evaluation process. Basically, this illustration contains the processes and the databases.

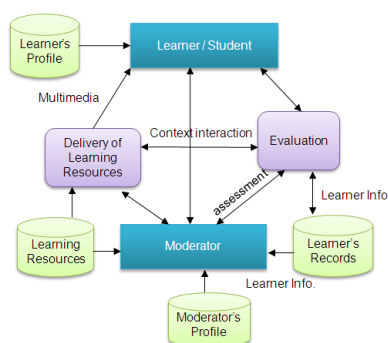


Figure 1. Overview of Typical e-learning System

## 3. E-learning Elements

Various technologies are used to facilitate e-learning. Most e-learning uses combinations of these techniques, including blogs, collaborative software, and virtual classrooms.

**Audio:** The radio has been around for a long time and has been used in educational purposes. Recent technologies have allowed classroom teachers to stream audio over the internet. There are also webcasts and podcasts available over the internet for students and teachers to download. For example, iTunes has various podcasts available on a variety of subjects that can be downloaded for free.

**Video:** Teachers can access video clips through the internet instead of relying on DVDs or VHS tapes. Videos allow teachers to reach students who are visual learners and tend to learn best by seeing the material rather than hearing or reading about it. Websites like YouTube are used by many teachers. Teachers can use messaging programs such as Skype, Adobe Connect, or webcams, to interact with guest speakers and other experts. Research on the use of video in lessons is preliminary, but early results show an increased retention and better results when video is used in a lesson. Creating a systematic video development method holds promise for creating video models that positively impact student learning.

**Blogging:** Blogging allows students and instructors to share their thoughts and comments on the thoughts of others which could create an interactive learning environment. Blogs allow students and teachers to post their thoughts, ideas, and comments on a website.

**Whiteboards:** Interactive whiteboards or smartboards allow teachers and students to write on the touch screen, so learning becomes interactive and engaging.

**Screencasting:** Screencasting is a recent trend in e-learning. There are many screencasting tools available that allow users to share their screens directly from their browser and make the video available online so that the viewers can stream the video directly. The advantage of such tools is that it gives the presenter the ability to show his ideas and flow of thoughts rather than simply explain them, which may be more confusing when delivered via simple text instructions. With the combination of video and audio, the expert can mimic the one-on-one experience of the classroom and deliver clear, complete instructions. From the learner's point of view this provides the ability to pause and rewind and gives the learners the advantage of moving at their own pace, something a classroom cannot always offer.

**Virtual Learning Environment:** Virtual Learning Environments (VLE), also known as learning platforms, utilizes virtual classrooms and meetings which often use a mix of communication technologies. One example of web conferencing software that enables students and instructors to communicate with each other via webcam, microphone, and real-time chatting in a group setting, are GoToTraining, WebEx Training or Adobe Connect, which are sometimes used for meetings and presentations. Participants in a virtual classroom can raise hands, answer polls or take tests.

## 4. Security Consideration

The roles of security include the following: user authentication /authorization, protection of private information from unintended access, and protection of data integrity guarding against data corruption by attackers. We have examined the security requirements and investigated current e-learning standards for their privacy and security provisions. Authentication is very crucial in e-learning because user's information is needed to be secured. Security is an important issue in the actual educational context where e-learning increases in popularity and more and more people are taking online courses. The e-learning platforms are today production systems that need to be secured. To achieve a good level of security, there are many important elements that must be taken into account: authentication, access control and data integrity.

### 4.1. Database Security

Database security concerns the use of a broad range of information security controls to protect databases, potentially including the data, the database applications or stored

functions, the database systems, the database servers and the associated network links against compromises of their confidentiality, integrity and availability.

**E-Learning resources:** Database should be secured from data loss, file corruption and authorized access. Learning resources should be secured from any cyber attacks, virus, malware and etc. It should only be accessible by the authentic user who are intitled to participate or access the learning resources.

**Secured Access:** This means the e-learning system should have a strong authentication mechanism. It has a log-in system where only the true user are only allowed to use the system or only the person who are enrolled are permitted. With the requirements, the e-learning system should have a strong authentication, an example of the effective authentication mechanism is by using the biometric authenticator or any authentication that can prove the identity of the user and that impersonation or fake user can be avoided. This is very important requirement in e-learning system.

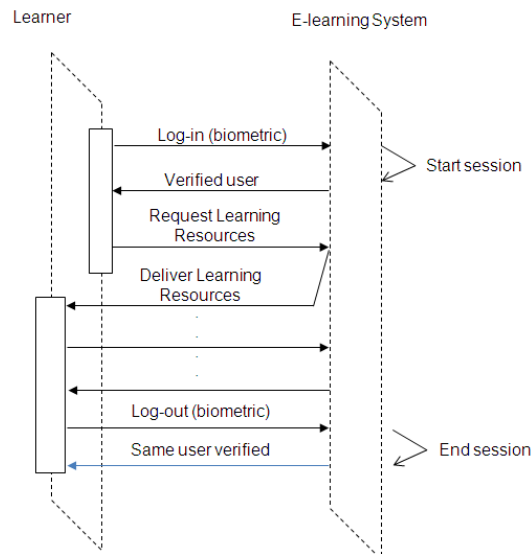
**Evaluation Results Integrity, Authenticity and Confidentiality:** The evaluation must have integrity and that the Learners Record must be authentic because the Evaluation Records (Exam, Activities, Quizzes). Since Evaluation Results are important, it should be confidential only to the true learner and cannot be viewed by others.

#### 4.2. User Information Security

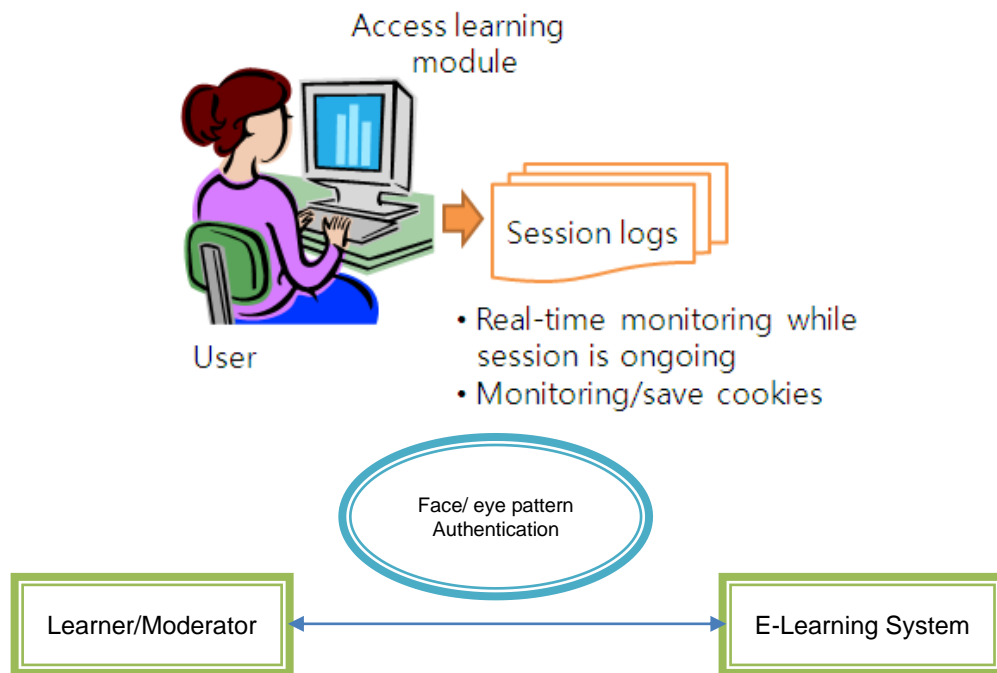
Learners and Moderators Profile should be secured also. Secured access is required to verify the user. This is to prove the identity of the user against impersonation or pretention. In this way, only the true user can participate. The most effective method is by using the biometric authentication, for example, it could be in form of iris scanning or finger print. In the recent technology like for example in smartphones, there is an eye detection, which detects a person's eyes while looking on the device's screen. This authenticator must be running while learner has an ongoing session.

### 5. Proposed design of E-learning User Authentication System

Nowadays, the authentication method is not reliable; the challenge is to design a system where it can authenticate a true user while the class session is ongoing. One of the considerations in developing an e-learning system is the security. The challenge is to make sure that the learner and moderators are authentic. To prove that the participant is the true registered learner is quite difficult because anybody can act on behalf of the true user. In this paper, the biometric authentication is proposed, particularly the face recognition and eye pattern recognition. With the advancement in technology, this is possible. Nowadays, smartphones have eye recognition where it detects blinking eyes. With this, we can go further with the thorough research to put software and hardware altogether. What good in this authentication mechanism is that while the learner or moderator has an ongoing class session, face or eye can be detected and continuously running and making a records. This technology can be implemented in other computer devices. Camera, video device, sensors and image scanning capability are the needed hardware and also the software to make it works.



**Figure 2. Learner's Sequence Diagram**



**Figure 3. Proposed Design of E-learning User Authentication System**

## 7. Conclusion and Future Works

This paper presents a review of E-learning privacy and security requirements. It investigates the more popular e-learning standards to determine their provisions and limitations for privacy and security. The authentication has been the major consideration in developing an e-learning system. This paper introduced the concept of better authentication mechanism. Our future works includes implementation of the design and the further study of hardware and software for e-learning system implementation.

## References

- [1] F. Graf, "Providing security for eLearning", Computers & Graphics, vol. 26, no. 2, (2002) April, pp. 355–365, [http://dx.doi.org/10.1016/S0097-8493\(02\)00062-6](http://dx.doi.org/10.1016/S0097-8493(02)00062-6)
- [2] A. Ortigosa, "Sentiment analysis in Facebook and its application to e-learning", Computers in Human Behavior (2013), <http://dx.doi.org/10.1016/j.chb.2013.05.024>
- [3] A. Younis Alsabawya, A. Cater-Steel and J. Soar, "IT infrastructure services as a requirement for e-learning system success", Computers & Education, vol. 69, (2013) November, pp. 431-451.
- [4] A. D. Dharmawansa, K. T. Nakahira and Y. Fukumura, "Detecting eye blinking of a real-world student and introducing to the virtual e-Learning environment", Procedia Computer Science, vol. 22, (2013), pp. 717-726.
- [5] V. I. Zuev, "E-Learning Security Models", Management Information Systems, vol. 7, no. 2, (2012), pp. 024-028.
- [6] K. El-Khatib, L. Korba, Y. Xu and G. Yee, "Privacy and Security in E-Learning", National Research Council of Canada, <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.90.7927&rep=rep1&type=pdf>
- [7] F. Graf, "Providing security for eLearning", Computers & Graphics, vol. 26, no. 2, (2002) April, pp. 355–365, [http://dx.doi.org/10.1016/S0097-8493\(02\)00062-6](http://dx.doi.org/10.1016/S0097-8493(02)00062-6)
- [8] A. Younis Alsabawya, A. Cater-Steel and J. Soar, "IT infrastructure services as a requirement for e-learning system success", Computers & Education, vol. 69, (2013) November, pp. 431-451.
- [9] A. D. Dharmawansa, K. T. Nakahira and Y. Fukumura, "Detecting eye blinking of a real-world student and introducing to the virtual e-Learning environment", Procedia Computer Science, vol. 22, (2013), pp. 717-726.