

Security of Internet–, Intranet–, and Computer–Based Examinations in Terms of Technical, Authentication, and Environmental, Where Are We?

Babak Sokouti

Tabriz University of Medical Sciences, Iran

Massoud Sokouti

Mashhad University of Medical Sciences, Iran

INTRODUCTION

Over the past decades, the use of Internet and its various applications in several environments such as academic communities and industries has been dramatically increased. Fundamental aspects of these applications are commonly related to sending and receiving small or large amounts of data through the local or global network communications. Transferring data over the insecure tunnel of Internet requires applying security services when especially the sensitive data are involved. The main security services are confidentiality, integrity, and availability namely called the CIA triad. The recent advancements in computer networking lead many technologies to be solely or partly upgraded their traditional environments into e-environments and hence, dependent on electronic-based objects such as e-mail and digitalized records and images. The security of shared or archived data or information personally or in organizations are vital and important due to the development of information science in modern society with everyday dramatically increase. Because of its rapid changing nature driven mostly by technology such as smart phones and development of new virtual communities, there are several demands for generating information systems in which security properties play vital roles. By considering these developments, the

e-learning parts of academic communities (i.e., online education) at universities have been affected in order to keep up with the knowledge innovation and they also provide some of their degrees and courses in a distance-based structure by taking the advantage of web-based infrastructures such as LMS (Learning Management System) and MOODLE (Modular Object- Oriented Dynamic Learning Environment). And, this makes the research areas open for modern education era to conduct paperless examinations by providing more security and efficiency. Although, this technological transition in the educational section is to some extent valuable and time effective, however, in most cases the evaluations and examinations of examinee are carried out and monitored in a supervised manner. Precisely speaking, for taking an exam in a traditional examination environment generally examinees, proctors, professors, pen and exam papers and a secure or isolated examining hall are included. For implementing such exams in a distance- or electronic-based model, many security issues whether they are technical or environmental are raised and essential to be resolved. In this regard, an examinee may take the exam alone at home; the professor makes the exam questions and sends them to a web server; the proctors' role can be performed supervised or unsupervised;

the sufficient security measurements should be in place of e-exam's environments.

As of now, providing the most of security services for unsupervised e-exams is still in its infancy and needs much of attention to be taken in to consideration, however, most of technical and communication-based security issues have been addressed in abundance.

In this chapter, the literature researches carried out on potential security aspects of conducting a robust secure e-exam are discussed, then their pros and cons with respect to their provided security services are evaluated and reviewed, and finally a hybrid security model for satisfying most of security properties will be proposed as a secure e-exam model for all conditions along with negotiating future directions.

BACKGROUND

For managing and conducting any types of e-exam systems, literature researchers have performed diverse studies considering special security aspects of them whether they are supervised or unsupervised including technical (e.g., networking, question generation, servers, clients), examinee authentication and identification (e.g., passwords, tokens, and biometrics), environmental monitoring (e.g., webcams, microphones) for preventing possible cheatings during the examination period. Nowadays, for universities providing distance learning courses and degrees are getting epidemically widespread and educationally of much of interest over the world. To survey the current position of state of art related to online exams considering the security aspects, the SCOPUS database is searched and reviewed with the keywords "online" AND "exam" AND "security" in which 19 out of 49 were filtered out based on their relevant contents (i.e., by using title and abstract) for this study. However, one out of 19 was proposed as a web tool for teachers and did not discuss the security aspects of the online examinations (Castillo-Ramoran, 2008).

In order to prevent various types of cheatings, some of the supervised approaches are carried out by employing video and audio devices such as webcams and microphones, biometric recognition tools, manually controlling the port and IP of the connected network devices most of which are relevant case studies for their classrooms in the local area networks (LANs) (Bari, Sullivan, & Blair, 2004; Jung & Yeom, 2009; Savulescu, Polkowski, & Alexandru, 2015). However, these environments are monitored manually via instructor-student networking communications.

From technical point of view and assuming that the only security problems can be carried out by outside attackers, Ming-Ming and Yan have proposed a simple security environment by considering only the data encryption by using triple DES algorithm and secure communication channel (i.e., virtual private network (VPN)) for secure connection of students and stopping the outside attackers (Ming-Ming & Yan, 2013). Also recently, a simple secure computer based examination was also carried out using the B/S structure (Singh & Tiwari, 2016). Another two approaches were conducted as frameworks in which the security countermeasures and the access control to the database servers (e.g., SQL server) were considered (Darong & Huimin, 2010; Haiyan, GHong, Lijun, & Jie, 2014).

For physically distance monitoring of a classroom or a room in which online exams were conducted, an environmental based secure framework was proposed by Stocco and colleagues by incorporating sets of logical and physical sensors (Stocco, Otsuka, & Beder, 2012). Employing the logical architecture of object oriented business application which has five layers including interface layer, interface control business layer, data access, and data storage and management will also bring some advantages (Basar & Haji-zada, 2014). These pros are summarized in scalability, flexibility, and security (Basar & Haji-zada, 2014). So, only the network access manages to stop all types of attacks applied on local and global networks. In other study, the authors have considered four

6 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

www.igi-global.com/chapter/security-of-internet--intranet--and-computer-based-examinations-in-terms-of-technical-authentication-and-environmental-where-are-we/183883

Related Content

Architecture of an Open-Source Real-Time Distributed Cyber Physical System

Stefano Scanzio (2018). *Encyclopedia of Information Science and Technology, Fourth Edition* (pp. 1227-1237).

www.irma-international.org/chapter/architecture-of-an-open-source-real-time-distributed-cyber-physical-system/183836

Sleptsov Net Computing

Dmitry A. Zaitsev (2018). *Encyclopedia of Information Science and Technology, Fourth Edition* (pp. 7731-7743).

www.irma-international.org/chapter/sleptsov-net-computing/184468

Detecting the Causal Structure of Risk in Industrial Systems by Using Dynamic Bayesian Networks

Sylvia Andriamaharosa, Stéphane Gagnon and Raul Valverde (2022). *International Journal of Information Technologies and Systems Approach* (pp. 1-22).

www.irma-international.org/article/detecting-the-causal-structure-of-risk-in-industrial-systems-by-using-dynamic-bayesian-networks/290003

Machine Learning-Assisted Diagnosis Model for Chronic Obstructive Pulmonary Disease

Yongfu Yu, Nannan Du, Zhongteng Zhang, Weihong Huang and Min Li (2023). *International Journal of Information Technologies and Systems Approach* (pp. 1-22).

www.irma-international.org/article/machine-learning-assisted-diagnosis-model-for-chronic-obstructive-pulmonary-disease/324760

Cyber Profiling in Criminal Investigation

Szde Yu (2021). *Encyclopedia of Information Science and Technology, Fifth Edition* (pp. 333-343).

www.irma-international.org/chapter/cyber-profiling-in-criminal-investigation/260196