Available online at http://www.journalcra.com

International Journal of Current Research
Vol. 8, Issue, 11, pp.41664-41673, November, 2016

INTERNATIONAL JOURNAL OF CURRENT RESEARCH

ISSN: 0975-833X

RESEARCH ARTICLE

SECURITY ENHANCEMENT USING TRI MODEL FOR USERS' ACCEPTANCE AND E-LEARNING PLATFORM SUCCESS

[1]Yassine KHLIFI and [2, *]Adel BESSADOK

[1]E-learning and Distance Learning Deanship, Umm Al-Qura University, KSA and Research Member Digital Security Lab., SupCom, Carthage University, Tunisia
[2]E-learning and Distance Learning Deanship, Umm Al-Qura University, KSA

ARTICLE INFO

Article History:
Received 18th August, 2016
Received in revised form
22nd September, 2016
Accepted 08th October, 2016
Published online 30th November, 2016

Key words:

e-learning platform,
TRI model,
User security requirements,
e-learning infrastructure success,
Information security management.

ABSTRACT

The exponential growth of Internet due to the emergence of advanced applications and services has provided significantly enhancement to the educational domain, especially e-learning. Currently, e-learning becomes an attractive educational domain in which the acceptance progress and more people are taking courses based on the use this platform. Principally, e-learning platform uses Internet infrastructure which has become a site for illegal events and actions, particularly exposed to a set of intrusions or threats. Moreover, most of e-learning platforms are made without considering specific security concerns. In this paper, we focused on e-learning environment, such characteristics, development, growth, benefits and challenges. We also argued the use of Technology Readiness Index (TRI) that is widely used for studying the behavior process behind the utilization of technological products and services. The TRI study results prove that there is a necessity for introduction of an advanced security scheme which incorporates users' behaviors and requirements for improving e-learning utilization. For this reason, we develop an innovative security scheme that associates the usae of information service management and a set of new algorithms for providing the security requirements and needs. Finally, we demonstrate that our approach can guarantee the appropriate environment which gives users' satisfaction and acceptance as well as e-leaning platform success.

Citation: Yassine KHLIFI and Adel BESSADOK, 2016. "Security Enhancement Using TRI Model for Users' Acceptance and E-learning Platform Success", *International Journal of Current Research*, 8, (11), 41664-41673.

INTRODUCTION

The growth of the Internet has delivered several innovative services, applications and technologies, principally information and communications technology, which has major effects on people in general or users in particular. Presently, these technologies usage provided the ability to reach more Internet services due to its benefits including universal, openness and easiness. Now, several advanced services have been introduced widely in the education environment that has fully detained its novel potential as learning procedures using the web applications advantages. E-learning progress has consequently induced to a new learning technique and provided equal opportunities to everyone for becoming learners. However, e-learning gave the training information transaction and built a new relationship between learners and instructors regardless of time and space (Sun *et al.,* 2008). E-learning is the delivery of learning, training based on the use of electronic resources which include computer or electronic devices, especially for offering training, education or learning material (Sung *et al.,* 2011). In recent years, e-learning increased exponentially and became a popular education manner for schools, universities and businesses (Weippl, 2005). However, e-learning clients used web applications as the standard to support the popular of online services and evolve the major goal of Internet attacks. Nevertheless, the Internet as a platform to reach all necessary information and knowledge, it also can be considered as a location for new ranges of illegitimate activities. Two questions can be considered in this work, the first one consisted how to provide a secure e-learning platform whereas the second question involved how this security can be introduced related to users' behaviors. To offer for e-learning safer users' environment and reach e-learning success, Technology Readiness Index (TRI) has been introduced for measuring tendency of the users to accept and adopt new technologies for achieving goals in home life and at work. TRI has become a widely known metric for studying the behavior process behind the usage and the acceptation of novel technologies and services (Cooper and Schindler, 2003). The study conducted using TRI can provide, as output, the metrics which can be used to evaluate the requested security level by e-learning platform users. As consequence, when trying to improve user acceptance, a typical orientation can be explored by many e-learning stakeholders, researchers and vendors, is integrating more practice alternatives and improving multimedia aptitudes of the system. Although, these technical

***Corresponding author: Adel BESSADOK,**
E-learning and distance learning Deanship, Umm Al-Qura University, KSA.

enhancements can add achievement to e-learning platform, but in presence of insecurity, as the significant and vital services, comes to reduce user acceptance and employment. The motivation behind the introduction of security is to enable technology in this environment because users often do not approve using insecure platforms or infrastructures. For this reason, security is a critical issue that needs to be addressed for guaranteeing a safe e-learning environment with the respect of users' requirements and providing e-learning infrastructure success. To answer the aforementioned questions, a study of the current works will be conducted in order to identify the different set of security challenges in e-learning including the requirements of faculty staff members as well as students' behaviors and needs. In the existing works, the authors have proposed new approaches in which they introduced a model for assessing e-learning readiness in the different universities and discussed the different parameters of security services that can be introduced for providing an appropriate e-learning environment (Darab and Montazer, 2011). Others works have introduced some approaches which tried to manage information security based on the identification of the existing security risks and trigger the protection technique for guaranteeing better resources utilization of the e-learning platform (Yong Chen and Wu He, 2013). In other works authors have tried to provide new methodologies for identifying risks and enabling remedies in working e-learning infrastructure or system. In addition, other recent works have proposed certain techniques which attempt to model information security in an e-learning environment for activating or supporting the requested mechanisms of security (Bariket and Karforma, 2012; Baby and Kannammal, 2014). Even though, these works present significant contributions in the development of e-learning platform, these works have not considered several issues, principally the innovative security service utilization based on users' behavior and applications requirements which may have an important effect on user acceptance and platform success. Moreover, the tradeoff of information related to computer and networks security, especially the synchronization of information user's deployment and platform requirements were little addressed. Thus, a more complete study needs to be established for integrating the supervision of security requirements in e-learning infrastructure that can implement the needed mechanisms for information management.

To resolve these problems, we focus on this work to introduce e-learning environment such as the features, development and progress as well as the different advantages that can be considered with security field as a new challenge in e-learning infrastructure implementation and utilization. Then, we explore the information security problems and threats, and the potential of information security management for decreasing them and increasing user acceptance as well as guarantee e-learning success. In addition, we will extend the previous work (Yassine KHLIFI and Adel BESSADOK, 2015) that is related to students' needs and requirements for e-learning success. However, many e-learning organizations are adopting information and communication technologies without integrating the design requirements and the existing security concerns. Concerns such as legitimate users, integrity, confidentiality and availability of information, course components reliability, and the guarantee of accessibility as well as other parameters, all need to be carefully addressed for guaranteeing suitable e-learning platform utilization. The remaining part of this paper is organized as follows. Section 2 briefly describes the basic concepts of e-learning features and development. It also discusses e-learning advantages and limits. Then, section 3 details the security services and requirements. Section 4 presents TRI technology which handles the collected data for studying and classifying orientations and behaviors of faculty staff member for suitable e-learning platform utilization. Section 5 discusses the implemented information security scheme proposed for providing a secured e-learning environment. It also details our proposal and describes its associated algorithm as well as its fundamental functionality. Finally, section 6 concludes the paper.

E-learning Technology

This section gives a briefly presentation of the basic concepts of e-learning including characteristics, progress and development. It also discusses e-learning advantages and challenges.

A. E-learning characteristics and development

E-learning consists of the technology usage to support learning process in which information achieved and interchanged using the communication technology. Certainly, e-learning can be presented as the utilization of a set of tools and technologies such as web applications and Internet infrastructure in order to improve the teaching, and learning techniques and methods (Sun *et al.,* 2008). It has similar structures of many other e-services, especially e-commerce, e-banking and e-government. E-learning platform is assumed as a set of applications and processes including web-based learning, computer-based learning, virtual classrooms, and digitals collaboration (Sung *et al.,* 2011; Alwi and Fan, 2010). E-learning users, especially faculty staff members and students, focus on how to benefit from e-learning concerning teaching and learning purposes. However, the behaviors of e-services users are diverse based on their roles and needs as well as requirements. In addition, the e-learning users spend a period of time when accepting e-learning technique compared to traditional learning and other several e-services. In this case, numerous e-learning platforms attempt to integrate various advanced functions such as interactivity, flexibility and multimedia capabilities for providing user satisfaction and acceptance. Whereas, these benefits can add several improvements that can offer user satisfaction and acceptance but security provision has considered as the fundamental part for e-learning system success. The reason why security can be seen as a support of e-learning technology is that users often abstain from using systems that cannot guarantee the safety environment which contains security services and requirements.

The technology usage for supporting learning has been introduced and developed since the 1980s. This growth was associated to the rapid computers expansion and its diffusion for personal work at that time. Moreover, higher learning institutes and organizations have established, over the last years, diverse education approaches, such as spreading participation, long life learning, and quality assurance (Alwi and Fan, 2010). For a complete description of the e-learning growth and the development, the reader can refer to (Yassine KHLIFI and Adel BESSADOK, 2015). However, e-learning processes is related to electronic like a technology used but there is a need to change for the learning content to guarantee e-learning success. In fact, there are some common terms can be used and exchanged to reproduce the use of technology in education, including distributed education, e-learning, distance education, blended learning and online classes. Distance education is related to self-learning approaches which are depending on the learning resources kind. The learning resources are displayed using physical mail or can be accessed online or during the meeting sessions which are managed only a few times per semester. Meanwhile, the combination of face-to-face (f2f) and online learning sessions, titled blended learning, which becomes relatively popular nowadays. This education technique at a distance uses technology that combined traditional education or training through the online resources usage. In this case, numerous channels of learning information transmission are explored such as physical classrooms, virtual classrooms, email and message boards, mentoring systems, software simulations, and online collaboration as well as wireless networks (Parasuraman, 2010). E-learning approach can be presented as a nature of distance education. Moreover, the distributed education contains several of distance aspects and online education in addition it is integrated with f2f learning. Currently, e-learning procedure contains three methods of technology usage for handling f2f learning or a traditional learning, through the use of technology asynchronously and synchronously as tools for providing online course.

Nevertheless, many limitations during the e-learning practice can be identified, especially the necessity of the assurance of security services such as data integrity, users authentication and information confidentiality. In this case, the insecurity can contribute for decreasing users' satisfaction and acceptance. Moreover, it can result the reduction of e-learning processes progress and development as well as e-learning platform success. The e-learning tasks continue to propagate in the similar method with the technology requirements and improvements. Moreover, e-learning can explore Internet platform to publish the learning components and modules as well as to support the accessibility for different levels of e-learning stakeholders including, especially students and faculty members, at any time and at anywhere. E-learning can permit numerous tasks such as the registration, assessment, and posting graduation certification online. With the aim of providing an additional flexibility, several types of e-learning technologies have been presented for example mobile learning and other supports. As mentioned above, the functionality of e-learning continues to develop but to keep this development can be improved if e-learning environment becomes more protected and safety. For this reason, innovative functionality given to users will make e-learning more open and exposed to information security threats.

B. E-learning advantages and challenges

E-learning platform provides every person the opportunity for enrolling and the ability for becoming a learner. The inventive functions of e-learning, especially the two important concepts of anytime and anywhere, can eliminate the problems related to the time and distance. Also, e-learning flexibilities deliver, essentially to the students and faculty staff, the main motivation for having the extreme benefits of diverse e-learning modes including blended courses and online courses (Darab and Montazer, 2011). Furthermore, the e-learning technology tries to offer numerous various advantages, such as learning quality perfection, access enhancement to education and training, and improvement of education cost-effectiveness. E-learning offers enough flexibility to a platform of a learner-centered, attractive, interactive, efficient, simply, accessible, and meaningfully distributed and facilitated e-learning environment. In addition, learners can save money and time spent on travelling and getting the right materials for their study. They can reduce printing costs by reading the available learning materials online. Another benefit offered by e-learning is faster delivery of assessments, as lecturers can give feedback rapidly compared with the traditional method, and students as faculty members can also contribute to feedback among themselves.

The major concern in e-learning platform is to guarantee the provision of necessary security services that can protect contents and information interchanged between the shareholders against attacks. When e-learning environment is insecure then courses copyright, contents and exams evaluation cannot be protected from no-authorized access and alterations. Another issue consists how to deliver secure information and system access anytime and anywhere in order to provide the technical and social interactions between systems and individual students and faculty staff according to the course content and exchanged information. The focus of e-learning security policy is essentially to deliver the appropriate environment that can protect user's information, especially giving the ability to staff member to supervise courses contents and material. However, the present e-learning platform cannot circulate the needed information for guaranteeing a secure location according to the content requirements and stakeholders' behaviors. For this reason, security is considered as the crucial part when we focus on providing and enhancing satisfaction and acceptance of the different stakeholders. In addition, providing safety environment can contribute to the success of e-learning platform. These aforementioned requirements are not guarantee by the existing security policies and the different layers of the system, new approaches must be proposed in order to alleviate and overcome the identified shortcomings and limits.

E-learning security services and requirements

Currently, the online learning is exposed to a set of diversity of threats and attacks including production, modification, interception and interruption. Then, e-learning information must be protected to avoid the loss of its confidentiality, integrity and availability as well as user authentication. Three diverse areas of security can be identified as follows: hardware security, information security and administration security (Weippl, 2005). The first area includes all features of physical security and emanation. The second area contains computer and communication security. Whereas the last area is related to people tend to neglect technical solutions where personnel and operation security affect this security aspect (Hair *et al.,* 2006). However, computer security deals with the prevention and detection of unauthorized actions can be performed by users of a computer system (Weippl, 2005; Hair *et al.,* 2006) Communication security involves measures and controls implemented to deny unauthorized access to information for ensuring the authenticity of the information transmission. In this work, we addressed focusing on the security services and requirements according to users' behaviors including authentication confidentiality, and integrity as well as availability.

A. Security services

We hereinafter present the security services and requirements that can be satisfied for emerging an e-learning platform and promising its success as well as user's satisfaction and acceptance, especially providing the accurate environment according to the faculty staff members' needs based on their behaviors. We can classify a set of security services including integrity, confidentiality and authentication as well as availability. For a complete description of security services, the reader can refer to (Yassine KHLIFI and Adel BESSADOK, 2015). In the sequel, we describe briefly the services explored during the design of our proposal which are summarized as follows:

- **Availability:** It is the assurance that the e-learning environment is reachable by authorized users, when required. Two sides of availability are normally discussed, which are denial of service and loss of data processing abilities. The e-learning users are dependent on the information on the Internet; consequently, the availability of materials and information to be accessed anytime and anywhere is crucial. If an e-learning platform is slow, users do not only require more time to ensure their work, but they also become frustrated, growing the negative effect on productivity. Failing to achieve this will have a main effect on e-learning users and providers. There are no active mechanisms for the prevention of denial of service, which is the opposite of availability. However, through permanent monitoring of applications and network connections one can automatically identify when a denial of service attack occurs (Weippl, 2005).
- **Confidentiality:** It consists to protect information in the system form the access of the unauthorized persons. An e-learning application can have a great number of users including students, faculty staff members or administrators who can access different information regarding one another, it is necessary to have an advanced level of confidentiality. For this reason, it is necessary to have a strong restriction between each authorized user and user groups. Then, the user will have access only to his appropriate information. The information must be encrypted after that exchanged between the e-learning infrastructure and the user's computer which can guarantee the confidentiality (Weippl, 2005).
- **Authentication:** It is mechanism that can provide the ability for identifying the user or the platform application user to give him the right to access to the application using his own account. The fact that the user claims to be represented by user ID does not essentially mean that this is true. To determine that an actual user can be mapped to a specific abstract user object in the system, and therefore be granted user rights and permissions specific to the abstract user object, the user must provide evidence to prove his identity to the system. In this case, authentication is the determining process requested user identity by verifying user-provided evidence. The evidence provided by a user in the user authentication process (Weippl, 2005).
- **Integrity:** In e-learning, integrity consists to protect data from intentional or accidental unauthorized modification then integrity depends on access controls. Hence, it is necessary to positively and uniquely identify all persons who try access. Integrity can be compromised by illegal user action, exposed downloaded files, LANs, and unauthorized programs, just because each of these threats can lead to unauthorized changes to data or programs. Ensuring the availability and integrity of information is the main goal in relation to e-learning security. Secrecy of data is closely connected to the integrity of programs and operating systems (Weippl, 2005).

B. Security requirements

To improve the protection and achieve a better security level of e-learning platform, we have found it interesting to integrate mutually security services and requirements support. For this reason, we have identified a set of security requirements including faculty staff members, students and managers. In this work, we interested to services requested by faculty staff members and students according to their requirements based on their behaviors. In the sequel, we describe only the security requirements used during the development of our proposal including faculty staff members and students. For further details on the security requirements, the readers can refer to (Yassine KHLIFI and Adel BESSADOK, 2015). The studied requirements are summarized as follows:

- **Requirements for students:** When e-learning security is established, students should actively participate to define their security requirements. In this case, e-learning platform need have the ability to identify student behaviors and provide the capability to choose the utilization parameters including the usage of password, data encryption and privacy policy as well as navigation parameters. Students should not rely on access control mechanisms to avoid unauthorized access to sensitive information. All files containing sensitive information should be encrypted although encrypting each file may degrade system performance. However, many e-learning platforms do not offer a privacy policy because no one has asked faculty staff members to guarantee this. Students should create their individual list of security requirements for a risk analysis. Moreover, the email address used to send notifications of the subscribed forums. The email address is stored in a database and protected by a password which also stored in hashed form in the database. It is still appropriate not to reuse the password for other accounts. When you navigate the site your actions and your IP address will be logged.
- **Requirements for faculty staff members:** As defined before, availability, confidentiality and authentication as well as integrity, are significant security services. These services can be studied for three important teaching domains including teaching, administrative work and exams. In this context, e-learning security is not limited to the technical system but it is indispensable to cover the complete domain that guarantees the organizational procedure of teaching and administration as well as examining. Even though methods to continuous evaluation have grown popularity, the distinction between teaching and examining is still frequently drawn. Different threats and security requirements are identified in these two domains. For this purpose, a difference between teaching and examining seems a sensible issue that need

to be studied in detail. In this case, the e-learning platform must provide the suitable environment which is related to the needs of faculty staff members. These needs will be provided according to the faculty staff behaviors which are collected not only in the access to e-leaning platform and during the session usage of this platform.

Technology readiness index

A. Presentation

For detecting staff members behavior versus the use of this e-learning, Technology Readiness Index (TRI) has been selected where the term of TRI has been presented in (Cooper and Schindler, 2003). This technology has been proposed to quantity the propensity of people for embracing and using new technologies for accomplishing goals in home life and at work. In this case, TRI has become a widely known metric for studying the behavior procedure behind the adoption of technological products and services. As multiple-item scale, the TRI consisted of a 36 questions devoted for computing "technology readiness". The 36-item scale is consisted of four component dimensions of beliefs related to technology that influence a personal's level of technology readiness. These beliefs assign a willingness of person to interact with new technology (Parasuraman and Colby, 2001). From the four dimensions, two are contributors as presented in table 1 and two are inhibitors of technology adoption as defined in table 2.

Table 1. The contributors

Factor	Definition
Optimism	Being determined that technology provides increased control, flexibility and efficiency.
Innovativeness	Aptness of being technology pioneer and thought leader.

Table 2. The inhibitors

Factor	Definition
Discomfort	a perceived lack of control over technology and a feeling of being overwhelmed by it
Insecurity	It is the anxiety that people may have with technology-based transactions.

The contributors' factors, especially optimism and innovativeness are considered as the locomotive of technology readiness. In fact, a high score measured on these dimensions will generally enlarge the technology readiness. In contrast, inhibitors factors-discomfort and insecurity- prevent or delay, people's natural tendency to use new technology. Thereby, a high score measured on these dimensions will decrease the entire technology readiness (Cooper and Schindler, 2003). The four dimensions as presented in (Parasuraman and Colby, 2001) are properly independent of each other, consequently, an individual could accommodate both contributor and inhibitor feelings towards technology (Parasuraman and Colby, 2001).

Currently, the TRI has been valuable for researchers interesting in social media, mobile access and other technology services. The 36-item scales have been explored in a wide variety of service sectors such as professional services, banking, telecommunications and healthcare as well as web-based education (Cooper and Schindler, 2003).

B. Methodology

Participants in this study were 400 non graduate students attending five faculties and they are the most using of the learning management system provided by Umm Al-Qura University at Makkah Campus. After eliminating missed responses, the sample obtained composed by 384 students 23% of them were from engineering, 25% from medicine, 12% were from college science, 31% were from administration and 9% were from education. About 46% were male and 54% were female students that it has been respecting approximately the real student distribution. The survey instruments used in the TRI study as is shown in Appendix. The study questionnaire was translated in Arabic it was distributed and collected from students in classrooms comprising the demographic information of the participants. We devote a preface for the questionnaire to explain the objective of the survey by making analogy between e-learning system and technology, the assurance of confidentiality and anonymity of respondents and, the voluntary nature of respondent participation. The original technology readiness scale consists of totally 36 items divided into four dimensions as it is presented in Appendix: Optimism (10 items), innovativeness (7 items), discomfort (10 items), and insecurity (9 items). All measures were in the category of self-assessment and each item question was scored on a Liker scale from 1 to 5, with a 1 rating indicating strong disagreement and a 5 rating indicating strong agreement.

Table 3. The Pattern matrix

Pattern Matrix[a]

	Factors			
	1	2	3	4
DIS_5	.876			
DIS_4	.872			
DIS_7	.794			
DIS_6	.744			
DIS_2	.739			
DIS_8	.710			
DIS_1	.572			
OPT_3		.926		
OPT_5		.887		
OPT_4		.874		
OPT_2		.831		
OPT_1		.770		
INS_6			.809	
INS_1			.761	
INS_4			.729	
INS_3			.726	
INS_2			.667	
INS_5			.639	
INN_3				.757
INN_4				.735
INN_1				.722
INN_5				.688

Extraction Method: Maximum Likelihood.
Rotation Method: Promax with Kaiser Normalization.
a. Rotation converged in 7 iterations.

C. Data analysis and results

The pretreatment of our empirical analysis was conducted a through the examination of the data including checks for missing values, outliers, and characteristics of the variables used in our study. Confirmatory Factor Analysis (CFA) was deployed to identify the underlying structure in the TRI theoretical model data as mentioned in (Hair *et al.,* 2006). The large number of items (36 items) deployed in the study from one side, the translation of the whole text of Parasuraman questionnaire from other side let the answers provided by stuents less accurate, and then the number of factors could not be specified in advance. To increase reliability factor and to extract the dimensions of each construct of the TRI, Exploratory Factor Analysis (EFA) was conducted for several time to check the consistency of the proposed factor using IBM SPSS 20 software tools. During this validation process, from communalities table, we remove items with poor factor loadings less than 0.5 that indicate a weak correlation with all other items (Parasuraman, 2000). Thus, 15 items were excluded from technology readiness index (see appendix) and then CFA was carried out using IBM SPSS Amos 20 with the maximum likelihood estimation procedure to test the obtained measurement model as shown in Figure 1. Using the Pattern matrix shown in Table 3, we can see that variables group into factors and more precisely, they load onto TRI factors as presented in (Cooper and Schindler, 2003).

D. Reliability and validity assessment

The two major import issues in measurement theory are the reliability and validity. The reliability analysis of each factor determines its ability to yield the same results on different situation and validity refers to the measurement of what the factor is supposed to measure (Fornell *et al.,* 1981). Cronbach’s alpha (CA) is the most commonly used as an estimate of reliability that measures internal consistency. We establish convergent validity to show measures that should be related are in reality related. In addition to the internal validity measurement, the convergent validity was examined by Composite Reliability (CR) and by the Average Variance Extracted (AVE) (Bagozzi *et al.,* 1988). The recommendation level for the internal consistency reliability is at least should be 0.7 and at least 0.5 for AVE (Fornell *et al.,* 1982). As shown in Table 4, the Crombach's alpha and Composite Reliability for all constructs are above the acceptable level of 0.7. These measurements indicate a high the internal consistency. Moreover, the surpass of all constructs AVI of the level 0.5, provides strong evidence of convergent validity that ensures the real measure of the four TRI dimensions.

Table 4. Convergent validity for the measurement model

Construct	ITEMS	C.A	C.R	A.V.E
Optimism	5	0.932	0.934	0.739
Innovativeness	4	0.819	0.819	0.531
Discomfort	7	0.917	0.918	0.616
Insecurity	6	0.885	0.889	0.572

Table 5. Discriminant validity for the measurement model

Construct	Optimism	Innovativeness	Discomfort	Insecurity
Optimism	0.860			
Innovativeness	0.431	0.729		
Discomfort	0.224	0.203	0.785	
Insecurity	0.210	0.278	0.746	0.756

E. Discriminant validity

Discriminant validity refers to the extent to which factors are distinct and uncorrelated. Thus, when the correlation between any two constructs is less than the square root of the AVE then the discriminant validity is established in (Kline *et al.,* 2005). The rule is that variables should relate more strongly to their own factor than to other factor. In the Table 5, the items on the diagonal represent the square roots of the AVE and the others elements are the correlation estimates and it is shown that the square root of the AVE was greater than inter-item correlations and that conclude the approved of discriminant validity for each of the items.

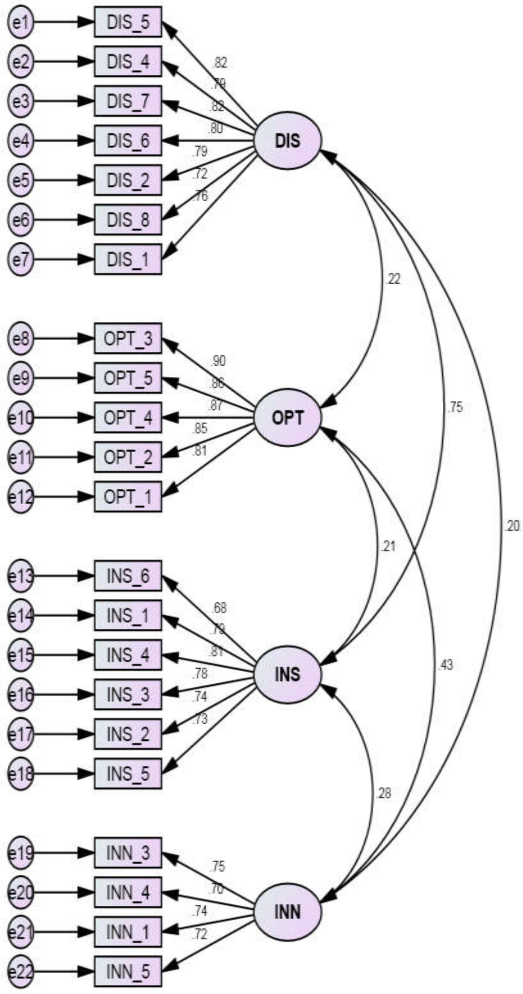

Figure 1. The measurement model fit

Table 6. The model fit indices

Fit index	Recommended Critical values	Results
X2/d.f	≤ 3	1.568
Gfi	≥ 0.9	0.922
Agfi	≥ 0.8	0.903
Cfi	≥ 0.9	0.969
Tli	≥ 0.9	0.964
Srmr	≤ 0.08	0.038
Rmsea	≤ 0.05	0.046

F. Overall model fit

The measurement model presented in Figure 1 is estimated with maximum likelihood estimation using AMOS 20. All scales remained are subject to CFA test to extract the dimensions of each construct and check the consistency of the proposed factor with actual data. The Pattern matrix illustrates a very clean factors in which convergent and discriminant validity are evident by high loadings within factors great than 0.5 (Fornell *et al.,* 1982), and no cross-loadings between factors as shown in Table 6. Factor analysis results showed 21 items loaded on four TRI factors as mentioned in Figure 1. For measuring the model fit, it is a common practice to deploy a variety of indices as it is proposed in (Yassine KHLIFI and Mohammed M. ALLEHAIBI, 2014). We can classify these indices into three categories as suggested in (Hair *et al.,* 2006). The first is the absolute fit indices category that measure how well the measurement model reproduce the observed data which include the Chi-square statistic divided by the degree of freedom, the goodness-of-fit Index (GFI) and the root mean residual (RMR). The second is the parsimonious fit indices category takes into account the model's complexity which includes the Root Mean Square Error of Approximation (RMSEA) and the adjusted goodness-of-fit Index (AGFI). The third is the incremental fit indices category that asses how well a specified model fit relative to an alternative baseline model which includes the Comparative Fit Index (CFI) and the Tucker-Lewis Index (TLI). Table 6 shows the recommended critical level of acceptable fit and the result fit indices for the research measurement model. The result, shown in Table 6, indicates that the measurement model as recommended by the three fit indices categories has an excellent fit.

G. Hypothesis research results

Table 7 presents the mean scores and standard deviation of each TRI construct. For each respondent, we calculate the overall TRI score as an average of the optimism, innovativeness, discomfort and insecurity after reverse coding the scores on discomfort and insecurity as showing in the table below and in (Cooper and Schindler, 2003). For the inhibitor dimension, the Insecurity and Discomfort factors estimated with the highest mean values of 3.7875 and 3.9374 respectively. However, for contributor dimension, Innovativeness was rated with yielded mean score, 2.7563 and the optimism was the next highest mean score, 2.2863. The overall TRI mean was 2.3294 with a standard deviation (SD) of 0.3574.

Table 7. Summary statistics for TRI related to faculty staff members

	Min	Max	Mean	S.D
Optimism	1.00	5.00	2.2863	0.7977
Innovativeness	1.00	4.75	2.7563	0.7993
Discomfort	1.00	5.00	3.7875	0.5933
Insecurity	2.00	5.00	3.9374	0.4934
Overalltri*	1.25	3.27	2.3294	0.3574

OverallTRI= [Optimism + Innovativeness + (6-Discomfort) + (6-Insecurity)]/4.

Table 8. Summary statistics for TRI related to students

	Min	Max	Mean	S.D
Optimism	1.00	5.00	3.7724	0.61823
Innovativeness	2.00	5.00	3.9384	0.4866
Discomfort	1.00	5.00	2.8568	0.71901
Insecurity	1.00	5.00	3.5854	0.77453
Overalltri*	2.40	4.50	3.3171	0.29614

Information security management

Based on the obtained results using TRI study, we can realize that the faculty staff members can be categorized into paranoid's class according to the classification of technology readiness users. The innovativeness mean value mentioned in table 5 can reveal that the faculty staff members are motivating to e-learning deployment. However, the insecurity value can show that the faculty staff members are feeling insecure. But, the faculty staff members are characterized by their optimism and discomfort as well as the behavior of faculty staff members is related to insecurity level. Moreover, based on the content of the tables 5 and 6, we can remark that faculty staff members and students have the same preoccupation versus insecurity concern. But, faculty staff members find that the security provision for e-learning platform is more significant as obligation or duty for data courses and exams management. While, the students consider that the security is also imperative but as users' usage and for personnel data management. For this reason, e-learning success is correlated to the faculty staff members' use and its success needs facing the whole issues addressed in implementing e-learning, specifically the security behavior for faculty staff members and students. In this case, to moderate insecurity challenges can be presented by integrating the needed secured services and requirements over e-learning platform. Then, E-learning users, especially faculty staff members, can benefit from using a secured e-learning infrastructure at same time profit from viable investments.

A. Toward a security management scheme

While the proposed approaches in the existing works can be considered as an important contribution in e-learning security, other extensions to these works can be investigated for implementing advanced security services or functions. Whereas security is important issues in e-learning environment, most of the proposed strategies did not take into account security requirements related to stakeholder of e-learning platform, particularly for faculty staff members. This makes control and management very critical to supervise or monitor the information processing tasks. Therefore, there is a need for synchronization between the stakeholder requirements, and the design and implementation for the improvement of e-learning infrastructure. The major key aspects of these improvements is the provision of e-learning environment, where security services are depending on stakeholder needs which are handled during the platform employment. The motivation behind this idea is to support the security mechanisms in the different level of e-learning infrastructure utilization, which significantly enhances the stakeholders' usage and improves users' satisfaction. For this reason, e-learning infrastructure will collect and supervise security services measures for supporting the multiples users' needs with variable requirements.

B. Security supervision scheme

The proposed security supervision scheme will attempt to provide several definite goals including offering the desired mechanisms to protect information from a wide variety of threats, ensuring procedure continuity, reducing risk occurrences during e-learning platform utilization. The principal objective of the scheme consists to identify faculty staff members' requirements and prevent unauthorized users events. Also, it attempts to insure the appropriate environment for information transaction during the e-learning platform utilization. In this case, it encourages users to benefit from the important educational objectives of e-learning platform. Then, Information security is achieved by a suitable set of control tasks known as security supervision scheme (SSS). SSS includes rules, process, procedures, and organizational structures as well as software and hardware functions that need to be implemented for managing users' risks. Additionally, such process and procedures need to be implemented, monitored and upgraded for insuring the specific security objectives and providing users' needs. The security can be realized through the use of technical means and suitable supervision actions. Identifying which controls can be made involves careful design and planning also requires participation of diverse shareholders, especially faculty staff members.

Several fields of security supervision can be identified, specifically risk administration, computer architecture and system security, operation and physical security. The SSS scheme implementation is influenced by professional and objectives, resulting security requirements and the active process. Information security is important for both public and private areas, and when trying to protect critical infrastructures. In both areas, security will function as an enabler for reaching e-learning platform achievement and also for overcoming and reducing the significant risks. Therefore, the proposed SSS scheme considers supervision of the information usage during the faculty staff members' sessions for providing the appropriate functions and guaranteeing the information interchange. Furthermore, an appropriate algorithm has been proposed for handling the requested security needs and the offered security services through a real time information transaction. This scheme can strongly contribute for improving users' usage and acceptance as well as e-learning platform success.

C. Information security supervision in e-learning

Information security supervision will include hardware and software security procedure which will be used to provide a safer e-learning environment. An accurate supervision scheme will provide the needs having active mechanisms for security, and privacy control and management as well as supervision. Attempting to guarantee a control without a suitable supervision policy cannot decrease attacks and threats as well as can result the loss of security services, especially authentication and integrity. However, the inaccurate supervision of the security parameters related to users' behavior can result access of internal or external malicious actions. Therefore, it is not only the solution which matter but the security supervision, which will define the success of the security controls of the solution. Despite examining the hardware and software solution, the information security can be accomplished by a suitable set of control tasks. A second approach can emphasis the key features of information security within e-learning environment. This approach can be based on e-learning information assurance, security governance, creating information security policy and procedures, implementing and monitoring information security countermeasures. The proposed SSS scheme is integrated in information security management in e-learning environment in order to offer the flexibility to the user at the same time ensuring integrity confidentiality of information and the authentication as well as availability. Then, based on the faculty staff members' behaviors and requirements during the e-learning platform usage, the proposed scheme activates the security procedures related to the particularly needed for e-learning.

D. SSS framework for faculty staff member satisfaction

SSS framework is the only real instance for an infrastructure to build an effective security architecture which can match current status and growing information security threats. For this reason, e-learning requires a special SSS framework which can be used as a guide in assisting for users of the e-learning platforms in order to accomplish the e-learning information security. The proposed SSS security scheme will be integrated in the information security management framework that we have proposed in (Yassine KHLIFI and Adel BESSADOK, 2015). The SSS scheme will extend the proposed information management framework by introducing the proposed enhancements that overcome the discussed shortcomings and provide more efficiency to e-learning platform. The enhancements will contain numerous details on policies, process, procedures, and software functions for improving security performance. Based on this extension, SSS framework can give the e-learning system the required security procedure that can manage the need security services and suggest the suitable security controls. Moreover, based on the use of SSS scheme, the users benefit with the secured e-learning platform and enhance their acceptances as well as improve e-learning success.

E. SSS algorithms

To implement the abovementioned needs and provide the appropriate environment, we develop the SSS algorithm that combines the security algorithms usage depending on faculty staff members' behaviors and requirements. The proposed algorithm insures a real transfer of the required information or attributes related to the users, especially during access step of faculty staff members to significantly monitor the platform availability and utilization. During the access process, the platform identifies faculty staff members' requirements and security needs then it provides the suitable use of the e-learning platform. In this case, the proposed algorithm is performed at each access to e-learning platform during the authentication working session. Once the work session started, the faculty staff member communicated the individual data to the e-learning platform which identifies the needed security services and triggers the proposed algorithm depending on the identified parameters for providing the requested environment using the advanced security functions. When, the faculty staff members do not specify the security needs, the proposed scheme triggers the hybrid tasks which activate the estimation of the accurate environment and trigger the suitable security functions. In the following, we present the considered parameters handled by the work session and the different system components.

Algorithm: Supervision scheme

```
Begin

Perform authentication {attributs: type-user, email, password, Date-last-session, Date- Recent--session, number-session}
Identify user-kind {faculty staff members' data: attributs: type-user}
Status-tasks =True {begin or end of tasks}
While Status-tasks =True
    Accept faculty staff members ' data
If security-services == {}
    Generate security requirements
    Else
        Identify user-behaviors {attributs: email, password, security services}
        Perform Security-services
    Endif
    If data == end-session
        Status-tasks = False
    Endif
Enddo.
End.
```

Security-services

```
Begin
```

```
Identify user-type
Identify user-session
Perform Authentication
Generate security-level
If security-level==
    [1]  Perform Integrity
    [2]  Perform Confidentiality
    [3]  Perform Integrity, Perform Confidentiality
    Else  Perform Hybrid-behavior-generation
Endif
End
Hybrid-behavior-generation
Begin

Read user-attributes{email, password, type-user, user-access-number}
Read Past-behavior, Date-last-session, Date-new-session
Compute number-session,  Period-time
Identify user-behaviors
If user-access-number==0
    Generate Recent-behavior
Else
    Compare new-behavior with last-behavior
   If Recent-behavior <> Past-behavior
      If period-time < week
          Store Recent-behavior
      Endif
   Endif
Endif
End.
Integrity
Begin
Generate integrity-level
If Integrity-level ==
   [1]  Perform Sha1
   [2]  Perform Md5
   [3]  Perform CRC32
Endif
End.
Confidentiality
Begin
Generate Confidentiality-level
If Confidentiality-level==
   [1]  Perform DES
   [2]  Perform 3DES
   [3]  Perform AES
   [4]  Perform RSA
   [5]  Perform diffie-hellman
Endif
End.
Authentication
Begin
Identify user-attributes {email, password, type-user, user-access-number}.
If Authentication-level ==
   [1]  Perform Model-authentication1
   [2]  Perform Model-authentication2
   [3]  Perform Model-authentication3
   [4]  Perform Model-authentication4
   [5]  Perform Model-authentication5
Endif
Create security-level
Create user-attributes
End.
Model-authentication1
Begin
Generate Password-authentication
Generate user-behaviors
End.
Model-authentication2
Begin
Generate Identity-authentication
Generate user-behaviors
End.
Model-authentication3
Begin
Generate Identity-Geographic-position
Generate user-behaviors
End.
```

Conclusion

E-learning employment continues to grow in which the development depends on more and more of Internet platform which is considered a place of illegal activities. These activities expose e-learning users, especially faculty staff members, to some kinds of threats. In this work, we mainly addressed the benefits and challenges of e-learning infrastructure. We also discussed e-learning security needs and requirements that must be implemented for providing e-learning success. In addition, we explore TRI technology for studying the behavior behind technological products and services uses. The conducted study show that the faculty staff members need for security services and requirements during the e-learning platform utilization. Based on the output metric of TRI study, we develop a new scheme in which a novel algorithm is implemented and used during the work session. This algorithm is activated according to the faculty staff members' behaviors and security requirements in that order. The proposed algorithm attempts also to correlate the collected behaviors of faculty staff members and their suggested security requirements for providing a safer e-learning environment and improving faculty staff members acceptance and satisfaction. The scheme is proposed for reinforcing the e-learning environment security which becomes effective if the security is able to associate the activities and needs of the faculty staff members. In addition, the SSS scheme managed user behaviors and proposed as security framework which can act as a guide in assisting the e-learning stakeholders in supervision of the information security within the e-learning environment. Finally, the conducted TRI study opens new security algorithm directions that can be developed based on correlation of two security input levels related to the prediction of users' behaviors and requirements.

REFERENCES

Alwi, N.H.M., I. S. Fan 2010. "E-Learning and Information Security Management*", International Journal of Digital Society (IJDS),* June 2010, vol. 1, Issue 2, pp. 148-156.

Baby, A. and A.Kannammal, 2014. "Information Security Modeling In an E-Learning Environment," International Journal of Computer Science Issues, Vol. 11, Issue 1, No 1.

Bagozzi, Richard P., and Youjae Yi, 1988. "On the evaluation of structural equation models." Journal of the academy of marketing science 16.1 (): 74-94.

Bariket, N. and S. Karforma, 2012. “Risks and Remedies in E-learning System” *International Journal of Network Security & Its Applications (IJNSA),* Vol.4, No.1, January 2012.

Cooper, D.R., and Schindler, P.S. 2003. Business Research Methods. (8th ed.). Boston: 15 McGraw-Hill Irwin.

Darab, B. and Gh.A. Montazer, 2011. “An eclectic model for assessing e-learning readiness in the Iranian universities,” *Computers & Education*, Issue 56, pp. 900-910.

Fornell, C., Tellis, G. J., and Zinkhan, G. M. 1982. Validity assessment: A structural equations approach using partial least squares. Proceedings, American Marketing Association Educators’ Conference.

Fornell, Claes, and David F. Larcker, 1981. "Evaluating structural equation models with unobservable variables and measurement error." Journal of marketing research: 39-50.

Hair, J. F., Jr., Black, W. C., Babin, B. J., Anderson, R. E., & Tatham, R. L. 2006. Multivariate data analysis (6th ed.). New Jersey: Prentice-Hall International.

Kline, R.B. 2005. Principles and Practice of Structural Equation Modeling (2nd Edition ed.). New York: The Guilford Press.

Parasuraman, A., and Colby, C. L. 2001. Techno-ready marketing: how and why your customers adopt technology. New York: The Free Press. Parasuraman, A., & Colby, C. L. Techno-ready marketing: how and why your customers adopt technology. New York: The Free Press.

Parasuraman, Arun, 2000. "Technology Readiness Index (TRI) a multiple-item scale to measure readiness to embrace new technologies." *Journal of Service Research*, 2.4: 307-320.

Sun, P.C., J.T. Ray, G. Finger, Y.Y. Chen, and D. Yeh, 2008. “What drives a successful E-learning? an empirical investigation of the critical factors influencing learner satisfaction,” Computers and Education, Elsevier, vol. 50, pp.1183–1202.

Sung, Y.T., K. E. Chang, and W. C. Yu, 2011. “Evaluating the reliability and impact of a quality assurance system for E-learning courseware,” *Computers & Education*, vol. 57, No. 2, pp. 1615–1627.

Weippl, E.R. 2005. Advances in Information Security, Security in e-learning, Springer.

Yassine KHLIFI and Adel BESSADOK, 2015. “A Novel Information Security Scheme for E-Learning Infrastructure Success Based on TRI Model”, Open Access Library Journal, 2: e1424. http://dx.doi.org/10.4236/oalib.1101424.

Yassine KHLIFI and Mohammed M. ALLEHAIBI 2014. “Information Security Services and Requirements for E-learning Infrastructure Success”, 2014 World Congress on E-Learning, Education and Computer Science (WCEECS’2014), Hammamet, Tunisia.

Yong Chen and Wu He, “Security Risks and Protection in Online Learning: A Survey,” *The International Review of Reseach in open and Distance Learning*, Vol. 14, N. 5, pp. 109-126, 2013.

****