Open Access Library Journal

A Novel Information Security Scheme for E-Learning Infrastructure Success Based on TRI Model

Yassine Khlifi[1,2], Adel Bessadok[1]

[1]Umm Al-Qura University, Mecca, KSA
[2]Research Member Digital Security Lab, SupCom, Carthage University, Tunis, Tunisia
Email: khlifi.yassine@gmail.com, yrkhlifi@uqu.edu.sa, aobessadok@uqu.edu.sa

Received 3 April 2015; accepted 18 April 2015; published 23 April 2015

Abstract

The fast growth of the Internet proposes and offers several new applications and advanced services that has greatly and quickly innovated the educational environment. The platform of e-learning represents an attractive educational field where the acceptance or utilization progresses and more and more people are taking courses or training using this technology. Mainly, e-learning platform exploits Internet infrastructure which became location for illegal events and actions, especially exposed to several kinds of threats or attacks. Furthermore, most of e-learning platforms are designed without taking into account security concerns. In this paper, we present e-learning environment, especially characteristics, development, growth, benefits and challenges. We also discussed and used TRI (Technology Readiness Index) which is considered a widely accepted metric for studying the behavior process behind the utilization of technological products and services. The results of the conducted TRI study demonstrate the need for a security scheme that incorporates students' behaviors and requirements for improving e-learning usage. For this reason, we develop a new security scheme that combines the use of information service management (ISM) and a hybrid algorithm for guaranteeing the needed security requirements. Finally, we demonstrate that our proposal can guarantee the suitable environment which provides students' satisfaction and acceptance as well as e-leaning success.

Keywords

E-Learning Platform, TRI Model, Security Requirements, E-Learning Infrastructure Success, Information Security Management

Subject Areas: **Applications of Communication Systems, Computer and Network Security**

How to cite this paper: Khlifi, Y. and Bessadok, A. (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

1. Introduction

The rapid growth of the Internet has provided several innovative services, applications and technologies, principally information and communications technology, which has major effects on people in general or users in particular. Presently, users of these technologies became able to activate and reach more Internet services due to its attractive features such as universal, openness and easiness. Today, several new services have been presented widely in the education environment that has fully detained its novel potential as learning tools through the use of the benefits of web applications. The e-learning advance has consequently led to a new learning technique and offered equivalent occurrences and opportunities to everyone for becoming learners. However, e-learning provided the training information interchange and created a novel relationship between learners and instructors regardless of time and space [1]. E-learning is the provision of a learning, training or education program by electronic resources using computer or electronic devices in other way for offering training, education or learning material [2]. In recent years, e-learning increased exponentially because it became a popular way of learning for schools, universities and businesses, and it [3].

Furthermore, e-learning users exploited web applications which were considered as the medium for supporting the popular of online services and develop the major goal of Internet attacks. Nevertheless, the Internet as a location to achieve all necessary information and knowledge, it also becomes a location for new diversities of illegal activities. To offer for e-learning users the appropriate environment and guarantee e-learning utilization success, Technology Readiness Index (TRI) is introduced for measuring tendency of the people to accept and adopt new technologies for achieving goals in home life and at work. Then, TRI has become a widely known metric for studying the behavior process behind the adoption of technological products and services [4]. The study conducted using TRI can provide, as output, the metrics which will be used to evaluate the security level requested 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 to integrate more interactivity and to develop multimedia capabilities of the system. While, these technical improvements may contribute to e-learning platform success, but in presence of insecurity, as the significant and vital services, comes to reduce user acceptance and utilization. The motivation why security can be seen as an enabling technology in this environment is that users often abstain from using insecure platforms or infrastructures. For this reason, security is a critical concern that needs to be addressed for assuring a safe running of e-learning platform with the respect of users' requirements and providing e-learning infrastructure success.

To our knowledge, several works have addressed information security in e-learning infrastructure, especially providing safety and secure system based on applications and services requirements. In most of the existing works, the authors have proposed new approaches in which they try to identify and quantify security threats as well as provide the needed security services for e-learning systems [5]. In other works, the authors have introduced novel methods related to information security management through the use the economic modeling methodology to manage security risks [6]. Other authors have attempted to offer innovative methodologies that can enable computer security threats for enhanced e-learning system resources management [7]. Even though, these works present significant contributions in the development of e-learning platform, these works have not identified some issues and limitations. Principally, the management of information security, the innovative security service utilization based on services and applications requirements which may have an important effect on user acceptance and e-learning platform success. In addition, the interchange of information associated to computer and networks security, especially information related to the use of e-learning platform requirements were little addressed. Therefore, a more complete study needs to be established for integrating information security requirements provision in e-learning infrastructure that can implement the desired mechanisms for information management.

Based on aforementioned concerns, we interested in this work for presenting e-learning environment including the different characteristics, development and growth as well as benefit which can be considered with security as a new challenge in implementing the e-learning infrastructure and its usage. Then, we explore the information security issues and threats, and the potential of information security management for reducing them and improving user acceptance as well as providing e-learning success. However, many e-learning organizations are rushing into adopting information and communication technologies without carefully understanding, design, planning and understanding the existing security concerns. Issues such as legitimate users, integrity and confidentiality of users information, course components reliability, and the guarantee of accessibility as well as other

parameters, all need to be carefully addressed for ensuring efficient e-learning platform utilization.

The remaining part of this paper is organized as follows. Section 2 briefly describes the basic concepts of e-learning characteristics, e-learning evolution. It also discusses e-learning advantages and limits. Then, section 3 presents in details the security services and requirements. Section 4 presents TRI technology which used to analyze the collected data and identify the behaviors of students to e-learning platform utilization. Section 5 details the information security management implemented for providing a secured e-learning environment. It also presents in detail the proposed security scheme and describes its associated algorithm as well as its fundamental functionality. Finally, section 6 concludes the paper.

2. E-Learning Technology

This section briefly presents the basic concepts of e-learning including characteristics, development and growth. It also discusses e-learning benefits and challenges.

2.1. E-Learning Characteristics and Evolution

E-learning is the technology usage to support the learning procedure where information can be managed and interchanged based on the communication technology. Certainly, e-learning can be presented as the use of a set of tools and technologies including web applications and Internet infrastructure for improving the teaching, and learning techniques and methods [1]. It has similar features of many other e-services, especially e-commerce, e-banking and e-government. E-learning platform is composed of several applications and processes including web-based learning, computer-based learning, virtual classrooms, and digitals collaboration [2] [8]. E-learning users, such as teachers and students, focus on how to benefit from e-learning concerning teaching and learning purposes. However, the behaviors of e-services users are different according to their roles and needs as well as requirements. In addition, the e-learning users spend a period of time when accepting e-learning compared to traditional learning and other e-services. For this reason, several e-learning platforms try to incorporate numerous innovative functions including interactivity, flexibility and multimedia capabilities for providing user satisfaction and acceptance. While these advantages may contribute to improve user satisfaction and acceptance, 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 refrain from using systems that cannot offer the safety environment which includes security facilities and requirements.

The technology usage for supporting learning has been introduced and developed since the 1980s. This development was associated to the rapid computers expansion and its diffusion for personal employment at that time. In addition, higher learning institutes and organizations have established, over the last years, different education strategies, such as spreading participation, long life learning, and quality assurance [8]. **Table 1** displays the growth and the development of e-learning from 1983 until the recent years. As seen in the table, e-learning procedures, in the past, is related to electronic like a technology used but there is a need to change for the learning content for guaranteeing e-learning success. In fact, there are some common terms can be used and interchanged to reflect the usage of technology in education, such as distributed education, e-learning, distance education, blended learning and online classes.

Table 1. E-learning evolution [9].

Period of time	Description
Pre 1983-Era of Instructor-led Training	This was the dominant teaching tool before computers became widely available, and when interactions between the instructor and students took place in the classrooms.
1984-1993-Multimedia	Windows 3.1, Macintosh and CD ROMs were the main technology developments during this period. However, classroom interactions and dynamic presentations were lacking in this medium.
1994-2000-Web Infancy	The arrival of e-mail, media players and streaming audio/video began to change the face of multimedia mediums. Students were able to access lecture notes or materials from the web at any time and at any location.
2001 and beyond-Next-generation Web	Advanced website design, rich streaming media (real audio/video) and high bandwidth (faster data flow) will revolutionize the way in which education will be delivered. Instructor-led, interactive modes can now happen via the web, reaching far more students than before.

Distance education is related to self-learning methods which are depending on the type of used learning resources. 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, entitled blended learning, which becomes relatively popular nowadays. This technique of education at a distance exploits technology that combined traditional education or training with usage of online resources. In this situation, several channels of learning information transfer are used such as physical classrooms, virtual classrooms, email and message boards, mentoring systems, software simulations, and online collaboration as well as mobile and wireless networks [9].

As seen in **Figure 1**, e-learning mode is presented as a type of distance education. Moreover, this Figure showed that distributed education includes 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 in order to manage f2f learning or a traditional learning, based on the use of technology asynchronously and synchronously as tools for insuring online course. However, **Figure 2** describes the mode of communication of data and information which interchanged between students and teachers through the use of the e-learning platform components. However, 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 reducing users' satisfaction and acceptance. In addition, it can result the decrease of e-learning procedures progress and development as well as e-learning platform success.

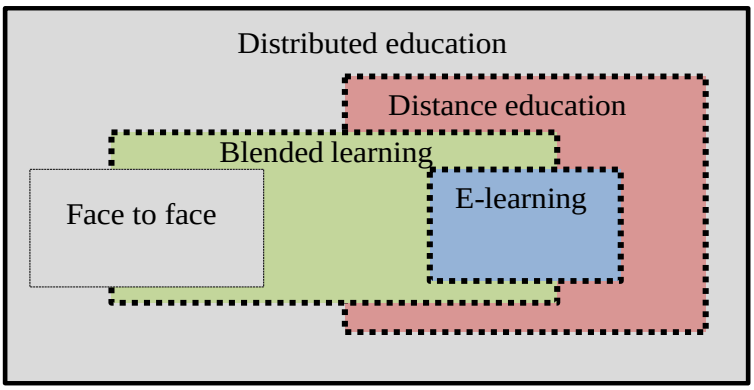

Figure 1. Relationship between e-learning and distribution learning [1].

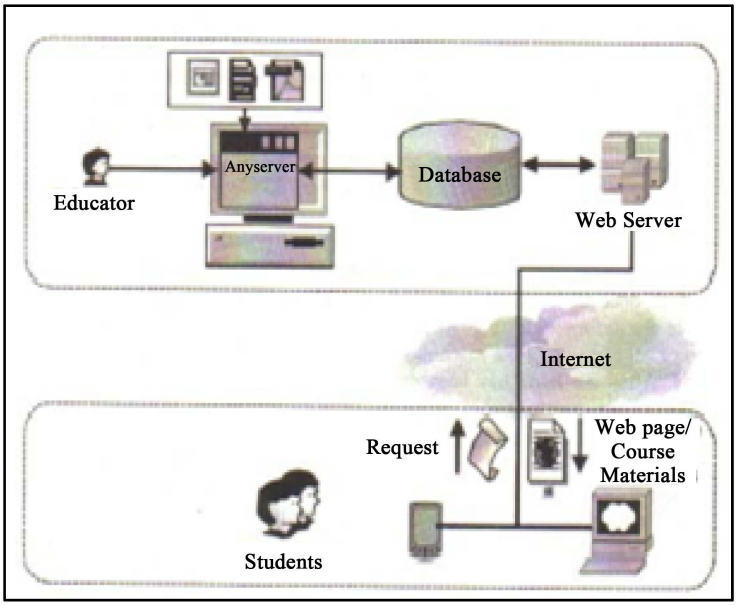

Figure 2. E-Learning systems components diagram [8].

Numerous organizations have made several reports about the use of e-learning education, especially online courses, such as Sloan Foundation. In its report, Sloan Foundation specifies that 3.5 million students, almost 20% of US higher education students, enrolled at least in one online course during the fall 2007 term [10]. However, the reason behind this evolution is driven by new institutions are entering into the online field, combined with continuous student requests for online learning options. In addition, the entrance of a new need of knowledge of employees and staff which has also contributed to this growth. This requirement can be seen that many employees or staff requests for taking the knowledge and skills to as great a degree as possible using the easiest methods and manner that is to enroll as an e-learning student.

The e-learning functions continue to propagate in the similar method with the technology necessities and advances. Moreover, e-learning uses the Internet platform for publishing the learning components and modules for enabling the accessibility procedures for different kind of e-learning stakeholders including, especially students, at any time and at anywhere. Moreover, e-learning permits several tasks such as the registration, assessment, and posting graduation certification online. With the aim of providing more flexibility, several kinds of e-learning technologies have been presented including mobile learning which is currently underused and is not fully exploited. As seen above, the functionality of e-learning continues to grow but to keep this development can be increased if e-learning environment becomes more protected and safety. In this case, advanced functionality presented to users will make e-learning more open and exposed to information security threats.

2.2. E-Learning Advantages and Issues

E-learning technology offers every person the occasion for enrolling and capability for becoming a learner. The advanced functions of e-learning especially the two important concepts of anytime and anywhere can eliminate the problems related to the time and distance. Also, the e-learning flexibilities deliver essentially to the students the major motivation for having the extreme benefits of diverse e-learning modes including blended courses and online courses [5]. Moreover, 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 gives enough flexibility to a platform of a learner-centered, attractive, interactive, efficient, simply, accessible, and meaningfully distributed and facilitated e-learning environment. Furthermore, 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 can also contribute to feedback among themselves.

The major concern in e-learning technology is the provision of different security services that can protect contents and exchanged information between the different shareholders against the intrusions. For example in presence of insecurity, e-learning environment, courses copyright and contents as well as exams evaluation cannot be protected from the no authorized access and modifications. Another issue related to the e-learning is how to deliver a secure access anytime and anywhere for providing the technical and social interactions between systems and individual students and faculty according to the course content and interchanged data. The focus of e-learning security policy is mainly to provide the appropriate environment that can protect student information and give the ability to teachers to supervise courses contents and material. However, the present e-learning platform cannot circulate the needed information for guaranteeing a secure environment according to the content requirements. For this reason, security is considered as the crucial part when it comes to enhancing satisfaction and acceptance of students and teachers. Also, safety environment can contribute to the success of e-learning systems. Since these requirements are not guaranties by existing systems, new approaches must be proposed in order to alleviate the existing shortcomings.

3. E-Learning Security Services and Requirements

Nowadays, the information is exposed to a set of variety of threats and attacks. For this reason, information must be protected for avoiding the loss of its confidentiality, integrity and availability as well as user authentication. Three different areas of security can be identified including hardware security, information security and administration security [3]. The first area comprises 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 [11]. However, computer secu-

rity deals with the prevention and detection of unauthorized actions by users of a computer system [3] [11]. 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 security provision including secrecy, integrity, availability, non-repudiation and authenticity.

3.1. Security Services

We hereinafter present the security services and requirements that must be satisfied for emerging an e-learning platform and assuring its success as well as user's satisfaction and acceptance. We can classify four security services including secrecy, integrity and availability as well as non-repudiation. For a complete description of security services, the reader can refer to [12]. In the sequel, we describe briefly the services used during the design of our proposal, such as secrecy, integrity and non-repudiation which are summarized as follows:

- Secrecy: It represents the most well-known security requirement. It provides to users the ability to obtain access only to information for which they have received authorization. Then, users do not have the ability to access to information which have not the permission to see or to process.
- Integrity: It provides the ability that only authorized users or computer programs has the permission to change data or executable programs. Information secrecy is associated to programs and operating systems. In this case, if the integrity of operating system is violated, then the system cannot work appropriately. It is obvious that information secrecy cannot be assured when the mechanism that verifies and limits access to data is not active [3]. Thereby, it is imperative to guarantee the protection of the operating systems integrity for ensuring the data secrecy.
- Non-repudiation: It is defined that users do not have the opportunity for refusing to perform an operation or task. It can be seen as a secondary security attributes comprising the availability and integrity of the identity of users [3] [11]. For example, if a teacher deletes the results of exam, the system must have the opportunity to provide the trace back who deleted them. In this case, the use of log files can provide the related information but these files must be reliable for guaranteeing the credibility of the provided information. The mechanism auditing can be used to reach this requirement.

3.2. Security Requirements

To improve the protection and achieve a better security level over 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 authors, teachers, students and managers. In the sequel, we describe only the security requirements used during the development of our proposal such as teachers and students. For further details on the security requirements, the readers can also refer to [12]. The studied requirements are summarized as follows:

- Requirements for teachers: As defined before, secrecy, integrity, availability and non-repudiation are significant security criteria. These criteria 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 covers the organizational procedure of teaching, administration and 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.
- Requirements for students: When e-learning security is established, students should actively participate to ensure their security requirements. Students will pay attention need to choose their individual works such as a good password, data encryption and privacy policy as well as navigation parameters [11]. 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 teachers to ensure this. Students should create their individual list of security requirements for a risk analysis. In addition, 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 suitable not to reuse the password for other accounts. When you navigate the site your actions and your IP address will

be logged.

4. Technology Readiness Index

To identify students behavior versus the use of this e-learning, Technology Readiness Index (TRI) has been chosen where the term of TRI has been introduced in [4]. This technology has been proposed to measure the propensity of people for embracing and using new technologies for accomplishing goals in home life and at work. For this, 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 measuring "technology readiness". The 36-item scale was composed 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 [13]. Of the four dimensions, two are contributors and two are inhibitors of technology adoption.

The contributors can be presented as follows:

- Optimism: It is defined as a positive view of technology and a belief that offers people increased control, flexibility, and efficiency in their lives [13]. It describes the expecting from the positive pertinence of technology.
- Innovativeness: It is defined as a tendency to be a technology pioneer and thought leader [13]. It is about the authority of using technology.
- However, the inhibitors can be mentioned as follows:
- Discomfort: It is defined as a perceived lack of control over technology and a feeling of being overwhelmed by it [13]. It is the doubt about the guarantee that concerns ordinary people experience with technology.
- Insecurity: It is defined as distrust of technology and skepticism about its ability to work properly [13]. It is the risk that people may have with technology-based transactions.

As contributors, optimism and innovativeness are the locomotive of technology readiness. In fact, a high score measured on these dimensions will generally enlarge the technology readiness. In contrast, 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 [4]. The four dimensions as shown in **Figure 3** are fairly independent of each other, therefore, an individual could accommodate both contributor and inhibitor feelings towards technology [13].

From many years, the TRI has been precious for researchers interesting in social media, mobile access and other technology services. The 36-item scales have been used in a wide variety of service sectors including education, banking, telecommunications, healthcare, and professional services [4].

4.1. Classification of Technology Readiness

Classification is a meaningful way to capture the complexities of people's beliefs related to the use of new technology. Based on the technology readiness scores, as described in [13], they describe five classes of tech-

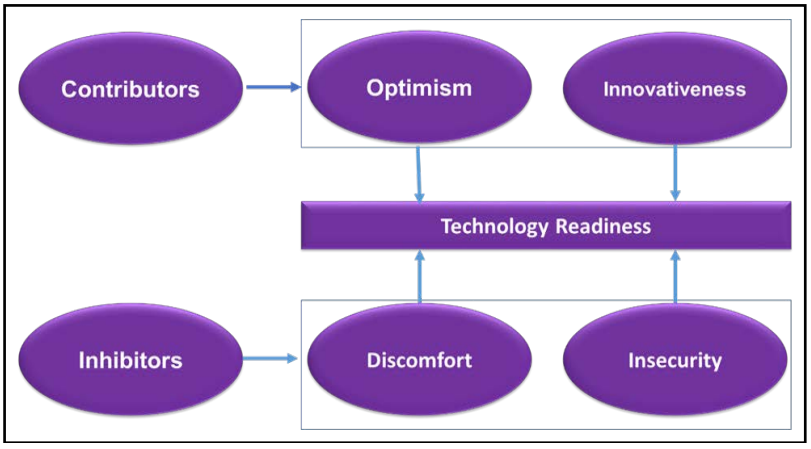

Figure 3. Drivers of technology readiness [9].

nology readiness users as following:

- Explorers: who the first people to adopt technology, who are highly motivated and who are a relatively easy group to attract when a new technology product or service is introduced because they have no fears about it.
- Pioneers: who the next to adopt technology, who desire the benefits of new technology by sharing the optimism and innovative views of explorers, but are more realistic about the difficulties and dangers by feeling some discomfort and insecurity.
- Sceptics: who are low motivated and need to be tended and to be convinced of the benefits of using the emerging technology.
- Paranoids: who are may find technology interesting, but at the same time they are feeling insecure; and
- Laggards: who are the resistant ones possess few motivations toward technology, which are the last to adopt technology unless they are forced to do so.

4.2. Model Hypothesis

In view of these TRI factors as specific characteristic between technology motivated and non-motivated, as seeing in **Figure 3**, we can considered the following hypotheses.

- H1: The optimism factor, defined as a positive vision of technology, and the belief that it greater control, flexibility and efficiency in people's lives, is a differentiating element between users and non-users of e-learning courses.
- H2: The innovativeness factor, defined as a tendency to be a pioneer, leader or opinion-former in the use of technology, is a differentiating element between users and non-users of e-learning courses.
- H3: The discomfort factor, defined as perception of lack of control over technology and the feeling of being pressured or oppressed by it, is a differentiating element between users and non-users of e-learning courses.
- H4: The insecurity factor, defined as distrust of technology and skepticism of one's own abilities to use it appropriately, is a differentiating element between users and non-users of e-learning courses.

4.3. 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 Likert scale from 1 to 5, with a 1 rating indicating strong disagreement and a 5 rating indicating strong agreement.

4.4. 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 [11]. 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 students 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 SPSS 20 software tool. 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 [9]. Thus, 15 items were excluded from technology readiness index (see **Appendix**) and then CFA was carried out using Amos 20 with the maximum likelihood estimation procedure to test the obtained measurement model as shown in **Figure 3**. Using the Pattern matrix shown in **Table 2**, we can see that variables group into factors and more precisely, they load onto TRI factors as presented in [4].

4.5. 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 [14]. Cronbach's alpha 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) [15]. The recommendation level for the internal consistency reliability is at least should be 0.7 and at least 0.5 for AVE [16]. As shown in **Table 3**, 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 2. The Pattern matrix.

	Factor			
	1	2	3	4
Ins_4	0.914			
Ins_2	0.895			
Ins_3	0.868			
Ins_7	0.796			
Ins_1	0.701			
Inn_6		0.798		
Inn_1		0.793		
Inn_3		0.746		
Inn_4		0.725		
Inn_2		0.655		
Inn_5		0.632		
Opt_3			0.858	
Opt_5			0.832	
Opt_7			0.784	
Opt_6			0.753	
Opt_8			0.635	
Dis_2				0.909
Dis_1				0.794
Dis_3				0.781
Dis_4				0.658
Dis_7				0.615

Table 3. The Crombach's alpha and composite reliability.

Construct	Items	Crombach's alpha	Composite reliability	Average variance extraction
Optimism	5	0.889	0.894	0.629
Innovativeness	6	0.882	0.886	0.565
Discomfort	5	0.873	0.876	0.588
Insecurity	5	0.920	0.921	0.702

4.6. 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 [17]. The rule is that variables should relate more strongly to their own factor than to other factor. In the **Table 4**, 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.

4.7. Overall Model Fit

The measurement model presented in **Figure 4** 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 [16], and no cross-loadings between factors as shown in **Table 4**.

Factor analysis results showed 21 items loaded on four TRI factors as mentioned in **Figure 4**. For measuring the model fit, it is a common practice to deploy a variety of indices as it is proposed in [18]. We can classify these indices into three categories as suggested in [11]. 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 5** shows the recommended critical level of acceptable fit and the result fit indices for the research measurement model. The result, shown in **Table 5**, indicates that the measurement model as recommended by the three fit indices categories has an excellent fit.

4.8. Hypothesis Research Results

Table 6 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 [4]. For contributor dimension, Innovativeness was rated with highest mean score, 3.938 and the optimism was the next highest mean score, 3.772. However, for the inhibitor dimension, the discomfort and insecurity factors yielded mean values of 2.856 and 3.585 respectively. The overall TRI mean was 3.317 with a standard deviation of 0.296.

Overall TRI = [Optimism + Innovativeness + (6 − Discomfort) + (6 − Insecurity)]/4.

5. Information Security Management

Based on conducted TRI study and the aforementioned results, we can realize that the students can be categorized into paranoid's class according to the classification of technology readiness users. The different obtained metrics can reveal that the students are interesting to e-learning usage but at the same time they are feeling insecure. In addition, students are characterized by their optimism and discomfort as well as students' behavior is related to insecurity level or to security provision. In this case, e-learning success is related to the platform utili-

Table 4. The Crombach's alpha and composite reliability.

Construct	Optimism	Innovativeness	Discomfort	Insecurity
Optimism	0.793			
Innovativeness	0.733	0.752		
Discomfort	0.344	0.405	0.767	
Insecurity	0.468	0.484	0.530	0.838

Table 5. The model fit indices.

Fit Index	Recommended Critical Value	Result
Chi-Square/Degree of Freedom	≤3	287.089:183
GFI	≥0.9	0.934
AGIF	≥0.8	0.917
CFI	≥0.9	0.979
TLI	≥0.9	0.976
RMR	≤0.08	0.023
RMSEA	≤0.05	0.039

Table 6. The model fit indices.

	Min	Max	Mean	Standard deviation
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

zation and its success needs facing the whole issues addressed in implementing e-learning, specifically the security challenge. In this case, to reduce insecurity status can contribute to build a secure e-learning environment and students can benefit from using an adequate e-learning infrastructure and sustainable investments.

5.1. Toward a Security Management Scheme

While the existing approaches can be considered as an important contribution in e-learning security platform, 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 students. This makes controlling and managing very difficult for monitoring the information processing. Consequently, there is a need for synchronization between the students' requirements, and the design and implementation of e-learning infrastructure. One of the main aspects of these enhancements is the realization of e-learning environment, where security services are associated to students requirements are processed during the phases of platform exploitation without any restriction. The motivation behind this idea is to enable the security management in the different of e-learning components, which significantly enhances the students' usage and improves students' satisfaction. Furthermore, e-learning will evolve towards security measures for supporting the multiples students' needs with variable requirements.

5.2. Security Management Scheme

The proposed security management scheme (SMS) attempts to guarantee several specific aims such as providing

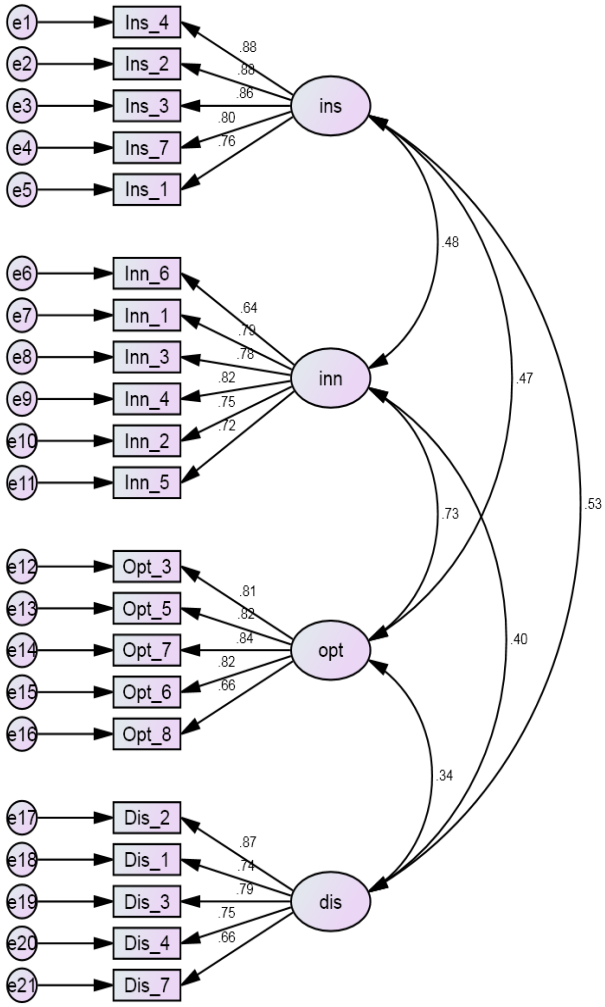

Figure 4. The measurement model fit.

the needed processes to protect information from a wide variety of threats, ensuring procedure continuity, reducing risk occurrence during e-learning platform deployment. The main objective of the scheme is concerned with detecting and preventing unauthorized users actions. Moreover, it tries to guarantee the suitable environment for information interchange during the use of e-learning platform. Also, it encourages students to benefit from the significant educational objectives of e-learning platform. Then, Information security is achieved by a suitable set of control tasks known as Information Security Management (ISM). ISM includes rules, process, procedures, and organizational structures as well as software and hardware functions that need to be implemented for managing students' risks. Furthermore, such controls need to be implemented, monitored and upgraded for ensuring the specific security objectives and providing students' needs.

The security can be realized through the use of technical means and appropriate management procedures. Identifying which controls can be made involves careful planning also requires participation of different shareholders, especially students and teachers applied in that order. Several domains of security management can be identified, specifically risk management, computer architecture and system security, operation and physical security. The implementation of an ISM 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 achieving e-learning platform achievement and also for avoiding and reducing the relevant risks. Therefore, the proposed SMS scheme considers the management of the information usage during the student session in order to provide the suitable functions for guaranteeing the interchange of the information. Moreover, a suitable algorithm has been

proposed for handling the claimed security requirements and the offered security services through a real time information transaction. This scheme is necessary for preserving students' usage and acceptance as well as e-learning platform success.

5.3. Information Security Management in E-Learning

Information security technologies including hardware and software security have been used to secure e-learning environment. An accurate scheme will provide the necessity of having active mechanisms for security, and privacy control and management. Ensuring a control without an appropriate planning policy cannot support for decreasing threats in e-learning. However, the management of access control using incorrect way can result access of internal or external malicious actions. Therefore, it is not only the solution which matter but the management of security, which will define the success of the security controls of the solution. Despite examining the hardware and software solution, the information security can be achieved by an appropriate set of controls. A second approach can emphasis the main elements 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 SMS scheme is integrated in ISM in e-learning environment in order to offer the flexibility to the user at the same time ensuring integrity confidentiality and non-repudiation of information as well as the authentication. Then, based on the students' behaviors and requirements during the e-learning platform usage, the proposed scheme activates the security procedures related to the specially needed for e-learning.

5.4. ISM Framework for Students Satisfaction

ISM 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 ISM framework which can be used as a guide in assisting for users of the e-learning platforms in order to manage the e-learning information security. The proposed SMS security scheme (**Figure 5**) will be integrated in the ISM framework that we have proposed in [12]. The SMS scheme will extend the proposed ISM 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, ISM 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 ISM, the users benefit with the secured e-learning platform and enhance their acceptances as well as improve e-learning success.

5.5. SMS Algorithms

To implement aforementioned needs and provide the suitable environment, we develop the ISM algorithm that combines the usage of the security algorithms depending on students' behaviors and requirements. The proposed algorithm insures online and real transfer the needed information related to the users, especially during access step of students or teachers to significantly monitor the resources availability and utilization based on students' requirements and security needs. The algorithm is performed at each access to e-learning platform during the data work session. Then, when the work session started and the user transmitted the individual data, the e-learning platform identifies the needed services and performs the proposed algorithm depending on the users' parameters for providing the suitable environment using the advanced security functions. When, the students do not specify the security needs, the proposed scheme triggers the hybrid tasks which activate the estimation of the accurate environment and provide the suitable security functions. In the following, we present the considered parameters handled by the work session and the different system components.

Algorithm 1: SMS students' scheme
Begin
1. **Identify** security services (integrity, confidentiality, non-repudiation, auhentication)
2. **Identify** security requirements (students requirements)
3. **Identify** students' data
4. Begin tasks = 1
5. End tasks = n

```
6.    Data = input
7.    Interigty request = True
8.    Confidentiality request = True
9.    Non-repudiation request = True
10.   Auhentication request = True
11.   While Begin tasks ≤ End tasks
12.       If Begin tasks = 1 & Interigty request = True
13.           Accept students' data
14.           Perform Data integrity task
15.           If Integrity request = True
16.               Perform Data confidentiality task
17.               If Confidentiality request = True
18.                   Perform Data non-repudiation task
19.                   If Non-repudiation request = True
20.                       Perform Data non-repudiation task
21.                       If Auhentication request = True
22.                           Perform Data authenticity task
23.                       Else
24.                           Begin tasks = End tasks
25.                       Endif
26.                   Else
27.                       Begin tasks = End tasks
28.                   Endif
29.               Else
30.                   Begin tasks = End tasks
31.               Endif
32.           Else
33.               Begin tasks = End tasks
34.           Endif
35.       Else
36.           Perform Data tasks
37.       Endif
38.   Begin tasks = Begin tasks +1
39.   Enddo.
End Algorithm
```

```
Data integrity_task
Begin
1.    Identify student-behaviors
2.    Identify requirements
3.    Generate integrity_level
4.    If Integrity level = 1
5.            Perform Sha1
6.        Else
7.            If Integrity level = 2
8.                Perform Md5
9.            Else
10.               If Integrity level = 2
11.                   Perform CRC32
12.               Else
13.                   student-behaviors = False
14.                   requirements = False
15.                   Perform Hybrid_Task
16.           Endif
17.       Endif
End task
```

```
Data confidentiality_task
Begin
1.    Identify student-behaviors
2.    Identify requirements
3.    Generate non-repudiation_level
4.    If non-repudiation_level = 1
5.            Perform DES
6.    Else
7.        If non-repudiation_level = 2
8.            Perform 3DES
9.        Else
10.           If non-repudiation_level = 3
11.               Perform AES
12.           Else
```

```
13.                     If non-repudiation_level = 4
14.                         Perform RSA
15.                     Else
16.                         If non-repudiation_level = 5
17.                             Perform diffie-hellman
18.                         Else
19.                             student-behaviors = False
20.                             requirements = False
21.                             Perform Hybrid_Task
22.                         Endif
23.                     Endif
24.                 Endif
25.             Endif
26.     Endif
End task
```

```
Data non-repudiation_task
Begin
1.  Identify student-behaviors
2.  Identify requirements
3.  Generate non-repudiation_level
4.  student-behaviors = False
5.  requirements = False
6.  Perform Hybrid_Task
7.  Endif
End task
```

```
Data authentication_task
Begin
1.  Identify student-behaviors
2.  Identify requirements
3.  Generate authentication_level
4.  student-behaviors = False
5.  requirements = False
6.  Perform Hybrid_Task
End task
```

```
Data Hybrid_task
Begin
1.  Identify student-behaviors
2.  If student-behaviors = False
3.      Identify requirements
4.      If requirements = False
5.          Create student-behaviors
6.          Create requirements
7.          Generate integrity_level
8.          Generate confidentiality_level
9.          Generate non-repudiation_level
10.         Generate authentication_level
11.         Perform security-task
12.     Else
13.         Determine requirements
14.     Endif
15. Else
16.     Determine requirements
17. Endif
End task
```

6. Conclusion

E-learning employment continues to increase in which the development depends on more and more of Internet platform that becomes a place of illegitimate actions. These actions expose e-learning users, especially students and teachers, to several kinds of threats. In this paper, we mainly addressed the benefits and challenges of e-learning technology. We also discuss e-learning security services and requirements that need to be implemented for providing e-learning success. Moreover, we explore TRI technology for studying the behavior behind technological products and services uses. The conducted study shows that the students need for security services and requirements during the e-learning platform use. Based on the output metric of TRI study, we develop a new scheme in which a novel algorithm is implemented and used during the users' session. This algorithm is activated according to the students' behaviors and security requirements in that order. The proposed algorithm

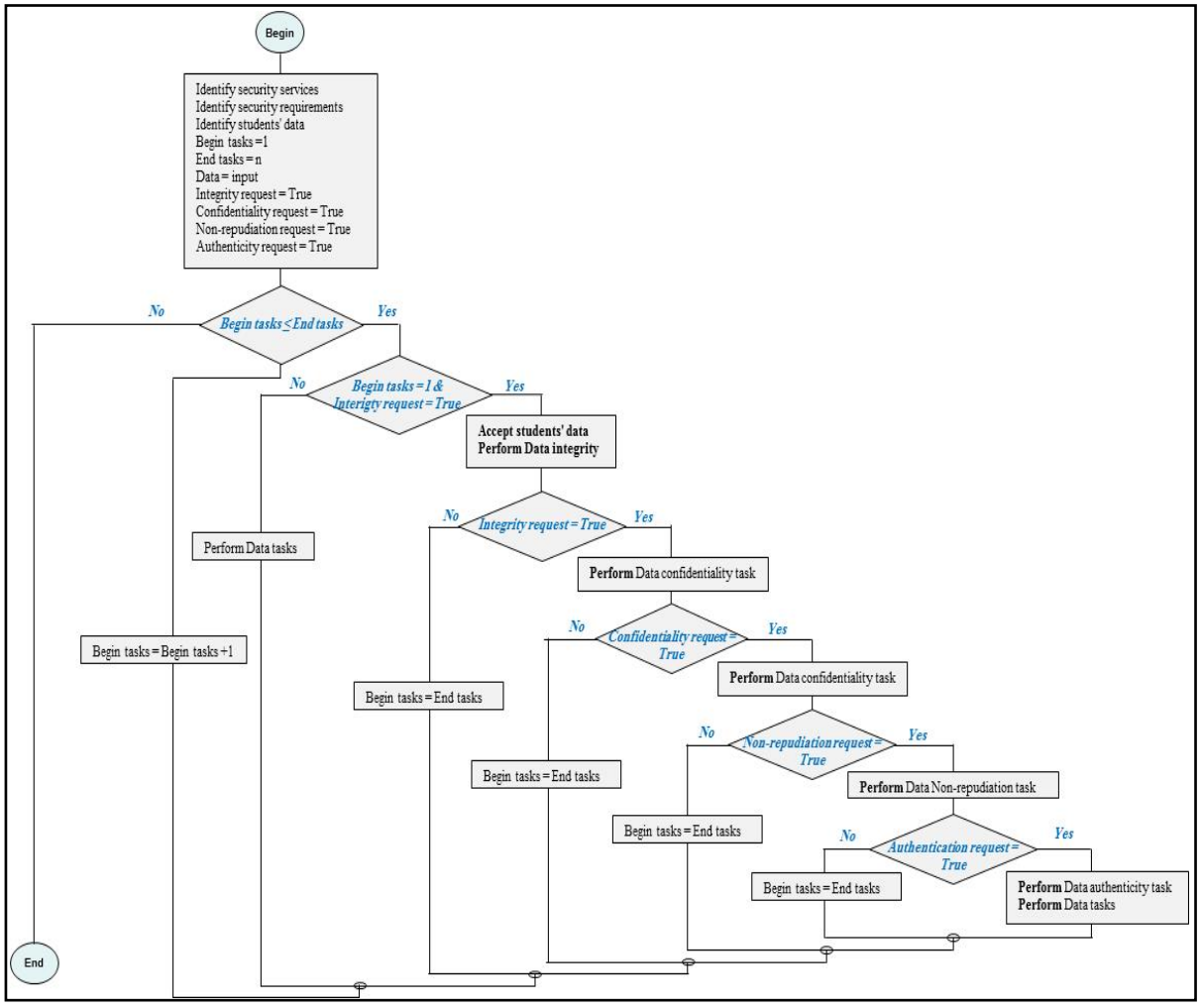

Figure 5. SMS security scheme.

tries also to correlate the collected behaviors of students and their suggested security requirements for providing a safer e-learning environment and improving students acceptance and satisfaction. The scheme is integrated with ISM for reinforcing the e-learning environment security which becomes effective if the security is able to associate the students' activities and needs. In addition, the ISM 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 students' behaviors and requirements.

References

[1] Sun, P.C., Ray, J.T., Finger, G., Chen, Y.Y. and Yeh, D. (2008) What Drives a Successful E-Learning? An Empirical Investigation of the Critical Factors Influencing Learner Satisfaction. *Computers and Education*, Elsevier, **50**, 1183-1202. http://dx.doi.org/10.1016/j.compedu.2006.11.007

[2] Sung, Y.T., Chang, K.E. and Yu, W.C. (2011) Evaluating the Reliability and Impact of a Quality Assurance System for E-Learning Courseware. *Computers & Education*, **57**, 1615-1627. http://dx.doi.org/10.1016/j.compedu.2011.01.020

[3] Weippl, E.R. (2005) Advances in Information Security. *Security in e-Learning*, Springer.

[4] Parasuraman, A. (2000) Technology Readiness Index (TRI) a Multiple-Item Scale to Measure Readiness to Embrace New Technologies. *Journal of Service Research*, **2**, 307-320. http://dx.doi.org/10.1177/109467050024001

[5] Ben Arfa Rabai, L., Rjaibi, N. and Ben Aissa, A. (2011) Quantifying Security Threats for E-Learning Systems. *Inter-*

national Conference on Education and e-Learning Innovations.

[6] Naaji, A. and Herman, C. (2011) Implementation of an E-Learning System: Optimization and Security Aspects. *Proceedings of the* 15*th WSEAS International Conference on Computers*.

[7] Rjaibi, N., *et al*. (2012) Cyber Security Measurement in Depth for E-learning Systems. *International Journal of Advanced Research in Computer Science and Software Engineering*, 1-15.

[8] Alwi, N.H.M. and Fan, I.S. (2010) E-Learning and Information Security Management. *International Journal of Digital Society* (*IJDS*), **1**, 148-156.

[9] Gefen, D., Straub, D. and Boudreau, M.-C. (2000) Structural Equation Modeling and Regression: Guidelines for Research Practice. *Communications of the Association for Information Systems* 4.1.

[10] Mason, R. and Rennie, F. (2006) E-Learning: The Key Concepts. Routlege, Abingdon Great Britain.

[11] Hair Jr., J.F., Black, W.C., Babin, B.J., Anderson, R.E. and Tatham, R.L. (2006) Multivariate Data Analysis. 6th Edition, Prentice-Hall International, New Jersey.

[12] Khlifi, Y. and Allehaibi, M.M. (2014) Information Security Services and Requirements for E-learning Infrastructure Success. 2014 *World Congress on E-Learning*, *Education and Computer Science* (*WCEECS*'2014), Hammamet.

[13] Parasuraman, A. and Colby, C.L. (2001) Techno-Ready Marketing: How and Why Your Customers Adopt Technology. The Free Press, New York.

[14] Cooper, D.R. and Schindler, P.S. (2003) Business Research Methods. 8th Edition, McGraw-Hill Irwin, Boston.

[15] Fornell, C. and Larcker, D.F. (1981) Evaluating Structural Equation Models with Unobservable Variables and Measurement Error. *Journal of Marketing Research*, 39-50. http://dx.doi.org/10.2307/3151312

[16] Bagozzi, R.P. and Youjae, Yi. (1988) On the Evaluation of Structural Equation Models. *Journal of the Academy of Marketing Science*, **16**, 74-94. http://dx.doi.org/10.1007/BF02723327

[17] Fornell, C., Tellis, G.J. and Zinkhan, G.M. (1982) Validity Assessment: A Structural Equations Approach Using Partial Least Squares. *Proceedings of the American Marketing Association Educators*' *Conference*.

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

Appendix

Optimism	
Opt_1*	Technology gives more control over their daily lives
Opt_2*	Products and services that use the newest technologies are much more convenient to use
Opt_3	You like the idea of doing business via computers because you are not limited to regular business hours
Opt_4*	You prefer to use the most advanced technology available
Opt_5	You like computer programs that allow you to tailor things to fit your own needs
Opt_6	Technology makes you more efficient in your occupation
Opt_7	You find new technologies to be mentally stimulating
Opt_8	Technology gives you more freedom of mobility
Opt_9*	Learning about technology can be as rewarding as the technology itself\\
Opt_10*	You feel confident that machines will follow through with what you instructed them to do
Innovativeness	
Inn_1	Other people come to you for advice on new technologies
Inn_2	It seems your friends are learning more about the newest technologies than you are [reverse scored]\\
Inn_3	In general, you are among the first in your circle of friends to acquire new technology when it appears
Inn_4	You can usually figure out new high-tech products and services without help from others
Inn_5	You keep up with the latest technological developments in your areas of interest
Inn_6	You enjoy the challenge of figuring out high-tech gadgets
Inn_7*	You find you have fewer problems than other people in making technology work for you
Discomfort	
Dis_1	Technical support lines are not helpful because they do not explain things in terms you understand
Dis_2	Sometimes, you think that technology systems are not designed for use by ordinary people
Dis_3	There is no such thing as a manual for a high-tech product or service that is written in plain language
Dis_4	When you get technical support from a provider of a high-tech product or service, you sometimes feel as if you are being taken advantage of by someone who knows more than you do
Dis_5*	If you buy a high-tech product or service, you prefer to have the basic model over one with a lot of extra features
Dis_6*	It is embarrassing when you have trouble with a high-tech gadget while people are watching
Dis_7	There should be caution in replacing important people-tasks with technology because new technology can breakdown or get disconnected
Dis_8*	Many new technologies have health or safety risks that are not discovered until after people have used them
Dis_9*	New technology makes it too easy for governments and companies to spy on people
Dis_10*	Technology always seems to fail at the worst possible time
Insecurity	
Ins_1	You do not consider it safe giving out a credit card number over a computer
Ins_2	You do not consider it safe to do any kind of financial business online
Ins_3	You worry that information you send over the Internet will be seen by other people
Ins_4	You do not feel confident doing business with a place that can only be reached online
Ins_5*	Any business transaction you do electronically should be confirmed later with something in writing
Ins_6*	Whenever something gets automated, you need to check carefully that the machine or computer is not making mistakes
Ins_7	The human touch is very important when doing business with a company
Ins_8*	When you call a business, you prefer to talk to a person rather than a machine
Ins_9*	If you provide information to a machine or over the Internet, you can never be sure it really gets to right place

*item excluded from the analysis with low loading (less than 0.5).