An Integrated Framework to Ensure Information Security Over the Internet

El-Sayed M. Towfek El-kenawy
Department of Communications and Electronics,
Delta Higher Institute for Engineering &Technology (DHIET)), Mansoura, Egypt

M. Saber
Department of Comm. & Comp., Faculty of Engineering, Delta University for science & Technology

Reham Arnous
Department of Communications and Electronics,
Delta Higher Institute for Engineering &Technology (DHIET)), Mansoura, Egypt

ABSTRACT
Information security is not a new concept in the technological industry. Information security is one of the major study areas in computer information systems. Due to the increasing popularity and dependency over internet, the need for proper information security has increased. There are new security paradigms arising every day to increase the information security. Determining the quality and value of the information, to set the proper system qualities to implement proper security is of high importance. However, the requirement of a more effective solution to be implemented in order to prevent the increasing security threats against the information on internet. Information security requires the integration of different perspectives including mathematical evaluation, technical evaluation, economic perspective and social perspective. Hence, in this paper, we are proposing an integrated framework to ensure information security over the internet. In the proposed framework, we incorporate mathematical and logical analysis techniques by incorporating methodological strategies and procedures along with different analysis techniques which will have different factors causing risk as the input parameters and generates one output – risk, which is expressed as in terms of probability. Thus, the proposed framework for information security system stands above the existing systems in producing better results

Keywords
Information Security, internet, Integrated Framework

1. INTRODUCTION
Information security is the field of study that deals with the protection of data and information against unauthorized access, use, piracy and leakage while used online. It can be used to protect both digital and physical information. The importance of the need for effective security management is increasing day by day. We have witnessed the information technologies (IT) and Internet changing our world at an unbelievable speed. The CIA triad which is about maintaining the confidentiality, integrity, and availability throughout keeping the information safe is followed by the information security professionals throughout the world [1]. The CIA triad itself is the key concepts of information security. To ensure proper security for the data and information, maintaining up to date security management system is also required. Basic analysis of the level of risk involved, determining the accurate budget and classifying the data and information based on the level of confidentiality is to be considered while considering the framework for information security [2]. In this paper, we are proposing a framework for information security which provides a new procedure and strategy for information security management. As mentioned in [3] "Information security nowadays is no longer an isolated and scattered but a very complicated systems engineering problem." Hence the requirement for a comprehensive analysis and implementation of information security has emerged.

2. METHODS
There has been many previous studies and researches conducted on improving information security. However, we cannot land on a permanent solution since the technology is vast developing and the security threat keeps arising. The responsibility of the security experts to secure the data and information form compromising the integrity of data is becoming more challenging. The increase in network dependency has also exposed the data and information to a high risk. Another important factor which creates unusual threat to information security is the hardware authentication procedure which is extremely important when it comes to internet of things. The latest technology uses authentication process with a new Core vPro processor that belongs to the sixth generation of processors to ensure security [4]. To ensure continuous improvement of the existing security methods and programs, there should be a constant review and continuous evolution of latest technologies and trends in information security ("LSC"). The emergence of cloud technology has also created a significant impact on the security of information system. So, we have to utilize the data security center by using IaaS. The increase in use of machine learning and artificial intelligence also has a relevant interest of purpose in the security of information systems of these technologies as well [4].

We are utilizing the concepts of information security engineering (ISE) to propose a comprehensive framework for maintaining information systems security. To achieve this, we have conducted a study based on the information security engineering perspective. Based on the study, there were four different problems faced by the current information security system. The problems are in the measures which are adopted to ensure secure communication, in the planning and development of information systems, methods and policies involved in the development of the information systems and the control of access to the information stored in the systems [3]. There are various previous researches which studies the issues and information security in conceptual, technological and organizational approaches. However, in this paper, we are proposing a conceptual framework of information security engineering which integrates procedures, strategies and methodology to contribute to an effective information security

management system.

The process flow of system engineering is considered for this system which is customized according to the information systems engineering. In the first step which identifies the requirements, in the process flow of information systems engineering, we consider the identification of requirements for information security. Likewise, in the second step, the functionalities of the information system are defined. In the third step, the information security system is defined. In the next step, we implement the information security system and finally the effectiveness of the system is evaluated [5]. In the proposed system, we describe the framework as four levels: definition level, basic theory level, methodology level and application level. The definition level consists of the objectives, definitions, research theories and other disciplines. In the basic theory level, we define the mathematical functions, logical calculations, philosophical basics and psychological considerations of information systems engineering. In the methodology level, we define the analysis and evaluation methods which are used in the proposed system. Finally, in the application level, the information security management and the required technologies for maintaining information security are defined. This framework covers all the basic approaches in methodological and technical aspects. This will help to overcome the issues of communication security, access of information and systems, security management and secure information system development, which were earlier identified. Thus, the proposed system will be more effective in managing information systems security than the existing systems.

3. .RESULTS

Using the proposed framework for information security system will provide an integrated solution to information security issues by incorporating methodological strategies and procedures. As described earlier, the framework has four levels: definition level, basic theory level, methodology level and application level. We have included the objectives, definitions, research theories and other disciplines in the definition level which will be the basics of the information security engineering research. The basic theory level integrates the mathematical logistics which incorporates logical calculations, functions, probability analysis, random events study and basics of information theory. Integration of mathematical functions into the framework will create effective results in information security since it will increase the efficiency of designed algorithm through mathematical analysis. This level also includes the philosophical basics which can be used to study the structure of associated security breach and risks, qualitative and quantitative analysis of the applied technology in the framework and the accuracy of the developed end system. We also deal with the various ideas of human system, human computer interactions and technology interventions which may cause the breach. This result in understanding almost all possible glitches and risks involved in the information security system and building an efficient framework and system design.

We have also integrated various analysis and evaluation methods which are used in the proposed system along with the above-mentioned features. To ensure proper security and functioning of the system, we can incorporate various analysis techniques into this. This has helped to recognize the threats and vulnerabilities the infrastructure is facing [6]. In this enterprise architecture of the proposed framework of the system, we have utilized several information security risk analysis solutions based on the enterprise architecture. We have used quantitative risk analysis methods which are based on a combination of well-established and validated methods along with Event and Fault analysis and Casual analysis methods [6]. The risk analysis methods evaluate the threats, previous attack patterns and scenarios, and controls and analyses the risk probabilities. This feature works very effectively since we incorporate multiple analysis techniques in a single framework to ensure improved security. The method will have different factors causing risk as the input parameters and generates one output – risk, which is expressed as in terms of probability. The proposed analysis system of risk identification and administration strategy is outlined to be quantitative and effectively pertinent to probabilistic assessment [6].

The proposed framework also includes the information security management and the required technologies for maintaining information security in the application level. The basic management standards, management processes, policies and regulations and also the previously identified risk factors of communication security issues, security management issues, access issues and security in the information security system development is also incorporated into this framework at this level. Thus, by addressing all the basic risk factors, risk probability analysis and the already identified security issues, this proposed framework can provide a better system for providing information security in the existing database. Using multiple analysis techniques also facilitates the identification of future risk causes and thus saves the system from requirement of frequent updates.

4. CONCLUSION

From the methodological strategies and procedures incorporated along with the multiple mathematical and logical analysis techniques, the proposed framework will definitely be able to perform much better than the existing systems for information security for the given set of data or information. As mentioned earlier, the need for an integrated framework for information security system has become an absolute necessity these days as the dependency on the internet and the transfer of data and information over the internet has increased considerably. A simple combination of these technologies might not work as expected. However, incorporating the technologies of complex information security engineering adds to the success of the framework. Our framework not only secures the information shared online, but also the various risk analysis methods incorporated analysis of the risk and previous attack patterns to ensure safety and regular updating of the information security system. This research can considerably increase the standard of security provided for the data and information shared or stored online.

5. REFERENCES

[1] "Importance Of Information Security - Video & Lesson TranscriptStudy.Com". Study.Com,2018,https://study.com/academy/lesson/importance-of-information-security.html. Accessed 26 July 2018.

[2] "LSC". Lsc.Co.Za, 2018, https://www.lsc.co.za/blog/risk-security/insights/the-importance-of-effective-security management. Accessed 26 July 2018.

[3] Li, Meng'gang, and Mincong Tang. "Information Security Engineering: A Framework For Research And Practices". International Journal Of Computers Communications & Control, vol 8, no. 4, 2013, p. 578. Agora University Of Oradea,

doi:10.15837/ijccc.2013.4.579.

[4] Tripwire, Inc. "3 Emerging Innovations In Technology That Will Impact Cyber Security". The State Of Security, 2018, https://www.tripwire.com/state-of-security/featured/emerging-technology-cyber-security/. Accessed 26 July 2018.

[5] Staff, National Research Council. Systems Analysis And Systems Engineering In Environmental Remediation Programs At The Department Of Energy Hanford Site. National Academies Press, 1998.

[6] Janulevičius, justinas. method of information security risk analysis for virtualized systems. vilnius gediminas technical university, 2016, http://dspace.vgtu.lt/bitstream/1/3026/1/J_Janulevicius_dissertation_LEIDYKLAI1.pdf. Accessed 26 July 2018.