Review on Confidentiality, Integrity and Availability in Information Security

Chai Kar Yee[1*] & Mohamad Fadli Zolkipli[2]

[1]College Arts and Sciences, School of Computing, Universiti Utara Malaysia; chai_kar yee@soc.uum.edu.my
[1]College Arts and Sciences, School of Computing, Universiti Utara Malaysia; m.fadli.zolkipli@uum.edu.my

* *Corresponding author*

To cite this article (APA): Chai, K. Y., & Zolkipli, M. F. (2021). Review on confidentiality, integrity and availability in information security. *Journal of ICT in Education, 8*(2), 34-42. https://doi.org/10.37134/jictie.vol8.2.4.2021

To link to this article: https://doi.org/10.37134/jictie.vol8.2.4.2021

Abstract

Information security is very significant needs to be secured due to people relying on networks and communication. Therefore, protecting information is a major challenge with the number of users increases rapidly in recent years. The aim of this article is to review Confidentiality, Integrity and Availability (CIA) in information security. This article focuses on the issues of information security and the requirements of information security. The articles, journals and conference papers are reviewed by researchers were published in 2016-2021. Security issues are analyzed in the recent methodologies. The result of the relationship between CIA in each information security requirement is at a moderate level. It is suggested cybersecurity risk awareness program for society is needed. Therefore, every user could get full advantages in networks and digital platforms.

Keywords: confidentiality, integrity, availability, Information Security, CIA.

INTRODUCTION

Nowadays, everyone using mobile phone or personal computer to receive and forward message or data to others. Thus, information security is a crucial matter in everyone's daily life. Also, many organisations interested in using technology services for working more efficiently, issue of protected information from risk must be concerned. The three objectives of Information Security stated to ensure protection of data which is confidentiality, integrity and availability (Alkhudhayr et al., 2019). The organisation should be able to manage from risk of information security such as unauthorized modification, illegal access and interruption. Every sector has its responsibility to enhance the knowledge in the field of information security to secure networks environment. Develop a secure network related to information in the network maintain in a private status to the users, ensure the users of the network is authenticated, and ensure the message cannot be modified and is secured during transmission can be prevent from common internet attacks.

Received Date: 09 May 2021; Accepted Date: 12 July 2021; Published Date: 14 July 2021

In an article presented by Alhassan & Adjei-Quaye (2017), the Open System Interface (OSI) model has its advantages such as flexibility, modularity, ease-of-use, and standardisation of the network protocols with different layers are easily created stacks which enable modular development. Each layer's implementation can be changed in the future without requiring any other adjustments, allowing for development flexibility. This article is presented as follows, the overview of CIA in Information Security shows in Section 2. Section 3 shows the information security issues and the requirements of information security will present at Section 4. Section 5 presents suggestions to solve the information security issue and conclusion is presented in Section 6.

LITERATURE REVIEW

Information Security

Researcher reviewed on the articles and selected conference proceedings published from 2016- 2021 through the Google Scholar and IEEE Xplore. To the sensitive information especially in the software the information security is very important on all of the field (Wang, Yao & Yu, 2018). The core concepts of information in CIA presented in article (Kumar & Bhatia, 2020) were adopted the Information Security requirements and there are commonly used in various fields of study. For example, information security in digital information may be not appropriate exposed if its confidentiality is violated, improperly changed if its integrity is jeopardised, and weakened or destroyed if its availability is threatened (Khidzir et al., 2018). A best Information Security Management System, it provides the ISO 27000x Series as a guide to practice (Aminzade, 2018). In (Alkhudhayr et al., 2019) describes Information Security as the Whitman and Mattord (2009) and ISO/IEC 27002 concept examines that the definitions are to demonstrate certain principles related to information security, such as information security is about technology or procedure not a process; additionally, information security characteristics or prosperities as in the CIA triad (Cruz de la Cruz, Romero Goyzueta, & Cahuana, 2020) shows in Figure 1.

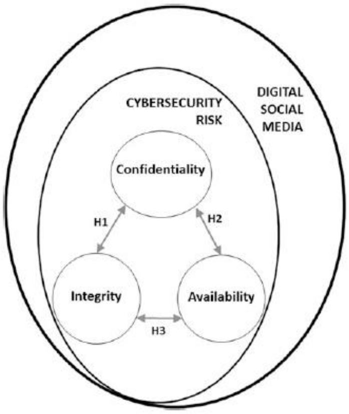

Figure 1: Shows the relationship between cybersecurity risk on CIA in digital information (Digital Social Media) (Alkhudhayr et al., 2019).

The National Institute of Standards and Technology (NIST) has described the CIA triad as one of the traditional practises for rating ICT systems used in the federal government in the United States. Professional groups and associations have also suggested using CIA in the security rating system (Shoufan & Damiani, 2017). Second, based on the concept of ISO/IEC 13335-1 and Dhillon (2007), it has defined information and communication technology security as the protection of information resources allocated in information technology systems. Finally, it has been discovered that technology and communication can be viewed as a risk factor that can be manipulated by threats in order to protect information (Alkhudhayr et al., 2019). In an article written by Al-Darwish & Choe (2019) indicates that both organisations and personal factors affect compliant actions in Information Security. The overall findings are encouraging self-efficacy, ensuring a favourable understanding of the Information Security environment, and ensuring that all levels of the company for example supervisors, co-workers and upper management apply security guidelines to their daily actions can improve compliance.

Confidentiality in Information Security

Confidentiality defines as the restrictions on the use and storage of various types of data (Khidzir et al., 2018). It can provide flexible delegation of decryption authority by generating key aggregation with a specific size. The key size is unaffected by the number of keys that must be encrypted (Kumar & Bhatia, 2020). Another method is to create privacy-aware authentication by adopting exponential growth of the number of users. Due to the insecurity of data transmission, this method has low security and privacy protection. Access control presented in this process is the method which supports data editing and prevents the replay attacks. Based on the method the user is allows to check the integrity.

Integrity in Information Security

Integrity is the guarantee that data has not been tampered with. A paper by Khidzir et al. (2018) presents a broadcast encryption method using dynamic ciphertext, which provides security guarantee for text decryption and attacks. Data replication is one of the data de-duplication processes that is used to reduce storage space and bandwidth use. The other way is creating the privacy preserving keyword search. It allows to solve the decryption and only return files that contain the specified keywords.

Availability in Information Security

The term "availability" refers to enabling that the authorized users access to the related assets and information when the users needed. Remote data integrity can be achieved using an identity-based privacy preserving method (Khidzir et al. (2018). This approach demonstrates that the data information is safe and can be used in a real time system. It also can check the data integrity effectively without necessary download the actual data. Besides, a homomorphic token is also a method for distributed erasure-coded data and scalable distributed storage. This makes it possible to perform secure and complex operations on outsourced data, such as server collusion and block alteration attacks. Because the data information is stored in the cloud computing and its integrity has been verified by third-party verifier, it is impossible to access the client data.

Received Date: 09 May 2021; Accepted Date: 12 July 2021; Published Date: 14 July 2021

INFORMATION SECURITY ISSUES

There are many information security issues concerned in all of the fields. A security issue shows in the article by Alhosani et al. (2019), in order to decrease the security incidents in bank sector, the experts agreed to provide employees with security policies awareness to understand the policy requirements. In addition, experts also provide strategies to help banks improve the security such as social engineering evaluation, privileged access (logical access or physical access), security quiz, and phishing campaign. The Bank measured the security performance by using KPIs of employees and organization. Due to continuous learning and education culture, employees who have the latest safety trends and environment would have minimal accidents. In order to support the advanced technology unit, training enables staff to resist information security risks. Threats and risks will be faced in an organisation in any fields show in Figure 2 (Pardini, Heinisch, & Parreiras, 2017).

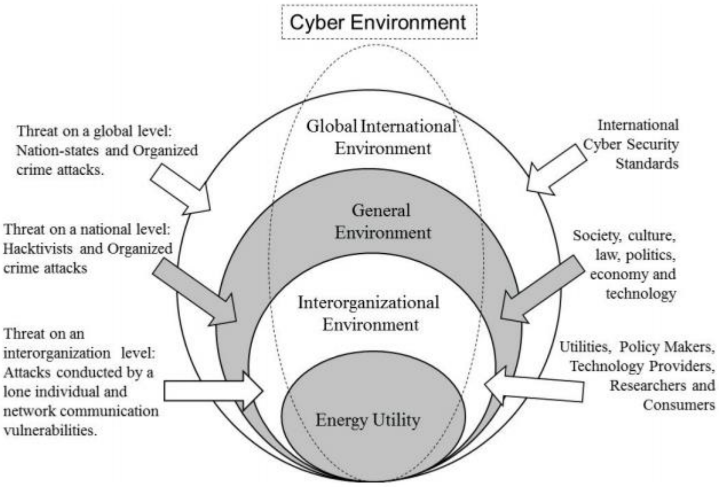
Cyber Environment
Threat on a global level: Nation-states and Organized crime attacks.
Threat on a national level: Hacktivists and Organized crime attacks
Threat on an interorganization level: Attacks conducted by a lone individual and network communication vulnerabilities.
Global International Environment
General Environment
Interorganizational Environment
Energy Utility
International Cyber Security Standards
Society, culture, law, politics, economy and technology
Utilities, Policy Makers, Technology Providers, Researchers and Consumers

Figure 2: Shows the cyber environment of an organization (Pardini, Heinisch, & Parreiras, 2017).

In medical fields, there have creating medical mobile apps for data transmission. A mobile medical application provides many functions and must meet the regulatory standards of all medical devices. Transmission of the patients' data need to be concerned because there are many deployment scenarios of medical mobile applications that need to be considered to ensure the security of data. The Ponemon report on mobile application security in 2015 emphasized that the investment in mobile application security is not enough. Consequently, numerous incidents have occured, for example, hackers target mobile applications in the form of malicious software to gain access to the servers or databases, unexpected data leaks, users download malicious software in the form of another application or bypassing most inbound filters are usually connected with corporate devices, making them vulnerable to malware attacks, download or an update from an untrustworthy source (Treacy & Mccaffery, 2017).

REQUIREMENTS OF INFORMATION SECURITY

Protecting network security includes securing the system objects, whether tangible or intangible, and preventing unauthorized access and modification from internal and external. The example of tangible objects are the hardware tools (Awang et al., 2020), while intangible objects are the information and data, including transformation and static storage. End-user objects such as keyboards and mice, network and communication channels to prevent hackers from intercepting the network communications, and the example of network objects need to be protected such as routers, switches, gateways, firewalls, and hubs. Then, CIA is the basic requirements for the protecting software resources (Treacy & Mccaffery, 2017). Besides that, there are two important security features which is forward secrecy and backward secrecy. Forward secrecy means when an IoT-aware node leaves the network, it must prevent any subsequent messages. When a new IoT-aware node is connected to the network, it must be stopped from reading any previously transmitted messages, which is known as backward secrecy (Alkhudhayr, 2019).

Confidentiality defines protection of information to prevent information from being leaked to unauthorized people. Integrity refers to the prevention of unauthorised parties from altering data. Availability refers to the ability of approved parties to access information when it is required. Within the development of usable devices, the purpose of data safety and protection is to preserve data integrity and availability for necessary use while also maintaining user privacy through confidentiality. When evaluating data security risks for mobile applications, it's critical to figure out what kinds of security threats can be avoided (Tsaregorodtsev, 2018). Security threats came from variety threat sources for example from attacks, other mobile applications, the users, mobile platforms, network carriers, and operating systems. When the unauthorized access to the data stored or to the functions on supporting devices are considered, these security risks will be further expanded. In the process of data transmission, the possibility of CIA data leakage is greatly enlarged by these circumstances. For protection and privacy in digital communication, many security standards and protocols are used, such as Secure Socket Layer (SSL), Secure Hypertext Transfer Protocol (S-HTTP), secure e-mail (Pretty Good Privacy PGP), and Secure Shell (SSH).

SUGGESTION TO SOLVE THE INFORMATION SECURITY ISSUE

Individual Level

This section aims to explore what kind of role a person can play in the overall success of strategic information security usage. There were no constituent elements of Information Security Strategy (ISSiO) at the individual level, which is surprising since it is generally agreed that overall protection is dependent on the weakest link, which is usually the individual (Home, Maynard, & Ahmad, 2017). When user using cloud services or other media on Internet there are two kinds of people which is the person planning to use the services and the kind of people who is familiar with the services (Gao et al., 2019). So, not all the people are familiar with the security attributes. Data replication, regenerating code, erasure code, homomorphic encryption, redundant residue number system, and secret sharing schemes are six basic methods used to improve the efficiency and confidentiality of data processing and storage shows in Tchernykh et al. (2019) can use in both levels. To map a collection of tasks to a set of resources, there are two approaches: static scheduling and dynamic scheduling.

Since the network topology and detailed information about processor and job characteristics are known in advance with static scheduling, it is possible to obtain a near-optimal schedule for certain problems. When a task is complete, the static method creates a schedule. Unfortunately, since these tools are not devoted to a single person, it is difficult to predict how well it will do. Besides, a method by using encrypted the video data from unauthorized user which is a visual security technology to protect the confidentiality of data (Yu, Kim, & Kim, 2021).

Organizational Level

The organisational level is where the most internal control can be exercised to promote an externally focused strategic implementation of information security and it deserves particular consideration in the review of IS literature. ISSiO can be used to incrementally increase the quality of an organisation's information security programme. To be effective, there must be a strong connection between the ISSiO and the business strategic plan (Home, Maynard, & Ahmad, 2017). Probability theory and statistical methods are used in the scheduling to deal with uncertainties from various sources. The use of fuzzy and stochastic approaches, as well as critical scheduling flexibility and robustness problems are discussed. Two major frameworks are considered uncertainty about the future which is online scheduling and stochastic scheduling. Online scheduling is referring by not knowing the future work arrival. Organisation can make decision when the work has arrived. This makes the works more efficient in all fields. Organizations may also use stochastic scheduling to solve the issue of task attributes such as due dates, turnaround times, and arrival times being modelled as random variables whose exact values are unknown before they arrive and finish (Tchernykh et al., 2019).

Load balancing is one of the possible methods for resolving ambiguity-related computation and communication imbalances, allowing for better resource allocation. It is critical to specify the following concepts for effective load balancing which is the number of jobs to be migrated, who and when initialises load balancing, the time slot used for migration, device underload or overload, and the number of Virtual Machines chosen for migration. It aids in the effective and equitable distribution of computing resources, resulting in high resource utilisation and QoS. The elastic load balancing algorithm distributes incoming traffic, such as Virtual Machines, requests, and jobs, through several instances to achieve higher QoS. When the operating system is overburdened, it will scale down. Capacity can be decreased or increased in real time depending on the network resources and computing used. Elasticity allows for the handling of a fluctuating workload while avoiding overloading. In order to prevent work from overload and starvation, the admissibility of resources should be considered in load balancing techniques when only a small collection of resources is selected for a job execution (Tchernykh et al., 2019).

In the context of software security, ORAM such a tool for hiding storage access patterns. Robust ORAM is able to enhance the CIA by using linear network coding to store data in the servers and build redundant coded blocks. The customer chooses linear network encoding rather than encryption or decryption because of the encoded blocks are simple and direct combination of blocks in an existing file, so customers can create new encoded blocks without having to reorganise blocks in the original file (Thao et al., 2017).

CONCLUSION

This paper review on the CIA in information security. Therefore, researcher presented the issues, requirements and the techniques of information security in multiple fields. Every user and organisations should take responsibility in protecting their own information and data will not be attacked by hackers (Alhassan & Adjei-Quaye, 2017). In the information security strategy (ISSiO), it is necessary to enhance personal use, and organisation can make progress by following the strategy provided for the protection of digital information. This study extended the security awareness of organisations in private or public sectors still in developing stage. There are some tools can be use to improve the security, for example machine learning algorithms can define the impact of attacks and provide the best security solutions. The result of the relationship between CIA in each information security requirement is at the moderate level. Thus, it is suggested cybersecurity risk awareness programme for society is needed. Therefore, every user can get the full advantages in networks and digital platforms.

LIMITATION

The Information Security Strategy (ISSiO) has the potential to be extremely beneficial to organisation. This approach has some limitations used in organisation for example identifies the structure as a static document, there is no dynamic processes to ensure its efficacy in reacting to immediate changes in the external environment. It focusses mainly on the organisational point of view, and the researcher have not adequately clarified the dimensions of measuring ISSiO (Home, Maynard, & Ahmad, 2017). If the influence of people on security is included in an appropriate way, the requirements of the CIA are not enough for individuals or the organisations purpose (Lundgren, B., & Möller, 2017).

FUTURE RESEARCH

In the article published by Home, Maynard, & Ahmad (2017) declared that many information system scholars have studied the theoretical basis of ISSiO to help organisations to improve in information security.

Received Date: 09 May 2021; Accepted Date: 12 July 2021; Published Date: 14 July 2021

ACKNOWLEDGEMENT

The authors would like to thank to all School of Computing members who involved in this study. This study was conducted for the purpose of System and Network Security Research Project. This work was supported by Ministry of Higher Education Malaysia and Universiti Utara Malaysia.

REFERENCES

Al-Darwish, A. I., & Choe, P. (2019, July). A framework of information security integrated with human factors. In *International Conference on Human-Computer Interaction* (pp. 217-229). Springer, Cham.

Alhassan, M. & Adjei-Quaye, A. (2017). Information Security in an Organization. *International Journal of Computer (IJC).* pp 100-116.

Alhosani, K. E., Khalid, S. K., Samsudin, N. A., Jamel, S., & Mohamad, K. M. (2019). A policy driven, human oriented information security model: A case study in UAE banking sector. IEEE Conference on Application, Information and Network Security (AINS).

Alkhudhayr, F., Alfarraj, S., Aljameeli, B., & Elkhdiri, S. (2019, May). Information security: A review of information security issues and Techniques. In *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)* (pp. 1-6). IEEE.

Aminzade, M. (2018). Confidentiality, integrity and availability–finding a balanced IT framework. *Network Security, 2018*(5), 9-11.

Awang, N., Samy, G. N., Hassan, N. H., Maarop, N., Magalingam, P., & Kamaruddin, N. (2020). Identification of information security threats using data mining approach in campus network. *Journal of Physics: Conference Series, 1551*(1), 012006 (11pp).

Cruz de la Cruz, J. E., Romero Goyzueta, C. A., & Cahuana, C. D. (2020). Open VProxy: Low Cost Squid Proxy Based Teleworking Environment with OpenVPN Encrypted Tunnels to Provide Confidentiality, Integrity and Availability. *IEEE Engineering International Research Conference (EIRCON)*, Lima, Peru, pp. 1-4. https://doi.org/10.1109/EIRCON51178.2020.9253767

Gao, T., Li, T., Jiang, R., Yang, M., & Zhu, R. (2019). Research on Cloud Service Security Measurement Based on Information Entropy. *Int. J. Netw. Secur., 21*, 1003-1013.

Horne, C. A., Maynard, S. B., & Ahmad, A. (2017). Organisational Information Security Strategy: Review, Discussion and Future Research. *Australasian Journal of Information Systems*, *21*. https://doi.org/10.3127/ajis.v21i0.1427

Khidzir, N. Z., Daud, K. A. M., Ismail, A. R., Ghani, M. S. A. A., & Ibrahim, M. A. H. (2018). Information Security Requirement: The Relationship Between Cybersecurity Risk Confidentiality, Integrity and Availability in Digital Social Media. In Regional Conference on Science, Technology and Social Sciences (RCSTSS 2016) (pp. 229-237). Springer, Singapore.

Kumar, R., & Bhatia, M. P. S. (2020). A Systematic Review of the Security in Cloud Computing: Data Integrity, Confidentiality and Availability, *IEEE International Conference on Computing, Power and Communication Technologies (GUCON)*, Greater Noida, India, pp. 334-337. https://doi.org/10.1109/GUCON48875.2020.9231255

Lundgren, B., & Möller, N. (2017). Defining Information Security. *Science and Engineering Ethics, 25*(2), 419–441.

Pardini, D. J., Heinisch, A. M. C., & Parreiras, F. S. (2017). Cyber security governance and management for smart grids in Brazilian energy utilities. *JISTEM J.Inf.Syst. Technol. Manag. 14*(3), 385-400. https://doi.org/10.4301/s1807-17752017000300006

Shoufan, A., & Damiani, E. (2017). On inter-rater reliability of information security experts. *Journal of Information Security and Applications, 37*, 101–111, 2017.

Tchernykh, A., Schwiegelsohn, U., Talbi, E. G., & Babenko, M. (2019). Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. *Journal of Computational Science*, *36*, 100581.

Thao, T. P., Miyaji, A., Rahman, M. S., Kiyomoto, S., & Kubota, A. (2017). Robust ORAM: Enhancing Availability, Confidentiality and Integrity. *IEEE 22nd Pacific Rim International Symposium on Dependable Computing (PRDC),* Christchurch, New Zealand, 30-39. https://doi.org/10.1109/PRDC.2017.14

Treacy, C., & Mccaffery, F. (2017). Data Security Overview for Medical Mobile Apps Assuring the Confidentiality, Integrity and Availability of Data in Transmission. *International Journal on Advances in Security. 9*(3&4), 146-157.

Tsaregorodtsev, A. V., Kravets, O. J., Choporov, O. N., & Zelenina, A. N. (2018). Information security risk estimation for cloud infrastructure. *International Journal on Information Technologies & Security*, *10*(4).

Wang, Y., Yao, J., & Yu, X. (2018). Information Security Protection in Software Testing, *2018 14th International Conference on Computational Intelligence and Security (CIS),* Hangzhou, China, pp. 449-452. https://doi.org/10.1109/CIS2018.2018.00106

Yu, J. -Y., Kim, Y., & Kim, Y. -G. (2021). Intelligent Video Data Security: A Survey and Open Challenges. *IEEE Access*, *9*, 26948-26967. https://doi.org/10.1109/ACCESS.2021.3057605