Indonesian Journal of Electrical Engineering and Computer Science
Vol. 16, No. 2, November 2019, pp. 1059~1064
ISSN: 2502-4752, DOI: 10.11591/ijeecs.v16.i2.pp1059-1064

Evaluation review of effectiveness and security metrics performance on information technology domain

Roshidi Din[1], Rosmadi Bakar[2] Azizan Ismail[3], Aida Mustapha[4], Sunariya Utama[5]
[1, 2,5] School of Computing, College Arts and Sciences, Universiti Utara Malaysia, Malaysia
[3,4]Faculty of Computer Science and Information Technology, Universiti Tun Hussein Onn Malaysia Parit Raja, Malaysia

Article Info

Article history:

Received Jan 29, 2019
Revised Mar 12, 2019
Accepted May 10, 2019

Keywords:

Cryptpgraphy
Information system
Parameter metric
Steganography
Wireless sensor metric

ABSTRACT

Information Technology (IT) development is the vital required for human life activities in this global era. This implementation of IT system has becomes competitive among developers to increase the quality of system performance. In order to discover the IT performance of system, it neccesary to evaluate the IT implementation performance. It determines the anticipated system output to prepare to enhance the application performance. In this paper the evaluation performance that is reviewd are effectiveness and security metrics because both of evaluations able to improve the development and protection of system. Therefore, this paper classifies some IT domain development that used in term of effectiveness and security metric approach from previous researchers' effort. It is categorized the domain based on both evaluation term of effectiveness and security metrics from specific parameter their used. The concern of this paper is to discover the important effectiveness and security metrics in IT domain performance that is anticipated to achieve expected performance.

Corresponding Author:

Roshidi Din,
School of Computing College Art and Science,
06010 Universiti Utara Malaysia, Malaysia.
Email: roshidi@uum.edu.my

1. INTRODUCTION

Nowadays, information technology (IT) implementation is a critical tool in improving the competitive development aspect of human life. It is significantly the impact that IT has influenced on the productivity of firms that are widely spread and used [1]. A lot of IT literature focus on the processes and behaviors based on trust and social enforcement that are provided with some social work and routinity of work [2]. However, the important thing for this specific requirement of implementation of IT development is the evaluation procedures as the parameters. The function of evaluation is to predict the quality of requirements of developing IT performance that deserves to be used in every aspect of life [3].

The value of evaluation as evidence to determine the level performance in some circumstances is achieved based on specific metrics. There are some evaluations that used some parameter condition in terms of security, robustness, capacity, effectiveness, efficiency etc as the parameter performance. Security parameter is used for acces control, authenticity and avoid particular risk to maintain performance of the IT system [4]. Then, capacity parameter is used in order to determine the size of IT system and adapted the system size with space of specific application that could be influence sytem performance [5]. Furthermore, robustness parameter is applied in order to avoid the risky error development and consider to safe and robust implementation that suitable is expected performance [6–8]. Moreover, The effectiveness is the capability of the system in order to perform the desired output [9]. Meanwhile, effeciency is parameter measurable quality component development to achieve the undertaking process successfuly [10, 11]. However, the effectiveness and security metrics mostly improve the performance in IT area. It is because effectiveness focus on quality

system and security metric focus on secure the system in the development of IT implementation [9, 12]. Both of performance is important to achieve in implement the goodness performance in IT systems. This paper focuses on review of effectiveness and security metrics performance in the development of IT environment in several area. It is anticipated to contribute as the guidelines the performance of effectiveness and security metrics that is developed in any methods in IT area

2. RELATED WORK

The implementation of IT in evaluation based on parameter in term of effectiveness and security metrics is expected able to achieve the appropriate performance. These are the two of the parameters applied in order to identify the quality of the system that deserved to be compared with former or another system [13]. This section is elaborated some discussion about several systems applied in order to achieve the effectiveness performance. Li and Ju [14] implemented the effectiveness system in ISMS in company so as to improve the performance some aspects. It identifies some controls to achieve the effectiveness with some implementations which are used to prevent system, reduce incident and improve understanding of roots. Those are some approaches in the company in terms of the employment and application in the industry. Then, Chebrolu [15]described some aspect in effectiveness in IT cloud such as Quality of Service, user satisfaction, and user helpfulness. It used regression analysis in order to measure the effectiveness using independent variables in the collected data. Moreover, Fu and Yu [16] declared the effectiveness in visual of cryptography consist two aspects which are contrast and security. In term of security, the third party unable to contain the secret information. Meanwhile, in contrast that is implemented human visual system able to notice the secret messages after overlapping the communication.

Those are some implementation of effectiveness metric in development performance. There also some related work about security metric performance in several area. According Kong, Kim and Kim [17] analysed the information security that influenced the physical security in a threat of an unnamed application security. The security measurement is important to be improved in order to avoid DOS attack and reverse the proxy group in dual control system. It measures the security level using false alarm and reduction measure in every particular technique in the system. Furthermore, Kaur[18] proposed a high security in the development video steganography. The security is improved in order to protect the hidden message from statistical attacks due to the identical bit matching substitution appliance. This is done by using a key for encryption in algorithm that provides layers form more than one user to decrypt the secret message that has the correct secret key. Then, Zaraskovsaka, Tarasov and Gluschenko [19] developed the information-measuring systems based on wireless sensor networks (WSN). The development WSN functionality is used to avoid attacks of "denial of service" or node failures. The DoS attack able to influence to the drain in the sensor battery in the system. Therefore, it used security accessibility to guarantee the service that offered by node in the WSN. The elaboration performance of effectiveness and security metrics is necessary to conduct with evaluation execution which is expected able to figure out the rates quality performance of method [20].

3. IMPLEMENTATION OF EFFECTIVENESS AND SECURITY METRICS

Based on previous section, it is mentioned the rule of effectiveness and security metric that could be defined as figure it out performance circumstances in any are of IT. This section focus on describes which IT domain that perform effectivenes and security. The implementation of effectiveness and security metric in some IT environment is shown in Figure 1 as follows.

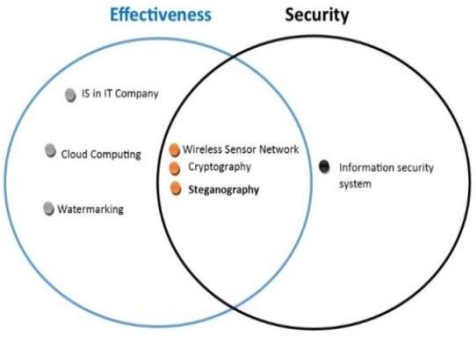

Figure 1. Area of IT that performed of effectiveness and security metric

Figure 1 shows several area of study that are related with implementation effectiveness and security performances in several area of information security study. Some area that is mentioned are the effectiveness of the study such as cloud computing, watermarking and information security in industry. Meanwhile, DoS and information security system are evaluated in the area of information security performance. However, there is also some area concerning in both of the evaluations which are wireless sensor network, cryptography and steganography. This comparison is shown in Figure 2 as follows.

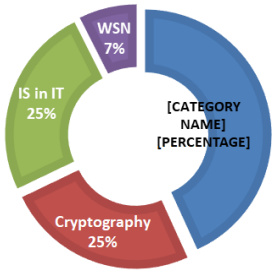

Figure 2. Domain of study that used effectiveness and security metrics

In Figure 2, the comparison of the domain study that most researchers implemented are preferred on the effectiveness on security metric on steganography with a value reach of 43%. This is followed by cryptography and information system area that share similar value 25% and wireless sensor network (WSN) 7%. In additional, the specific comparison of effectiveness and security with domain study of information security is shown in Figure 3 as follows.

Figure 3 illustatess the comparison some implementation of effectiveness and security metric performance in last decade. The highest last effort of the researcher is in the effectiveness in steganography. This is followed by the security in steganography and efectivness performances with four research efforts. Next is cryptography which four efforts in effectiveness, but zero effort in security performance. Finally, WSN has only one effort in both effectiveness and security metrics. This comparison is shown in Figure 4 as follows. Figure 4 illustrates the comparison between the effectiveness and security metric implementation. This figure generalize IT environment to divide the performance of effectiveness and security metrics that is dominant to implement.The effectiveness is mostly implemented in IT enviorment in last decade comparing that security metric. It is clearly seem that effectiveness metric reached 68% compared security metric only 32%.

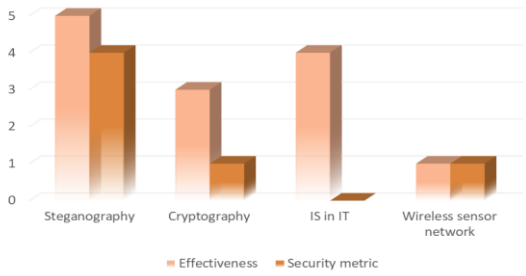

Figure 3. The comparison of effectiveness and security performances based on domain

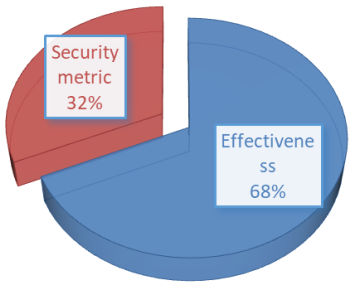

Figure 4. Comparison of implementation on effectiveness and security metrics

4. PARAMETER OF EFFECTIVENESS AND SECURITY METRICS PERFORMANCE

This section is an elaboration from the previous section that discovered the implementation of effectiveness or security metrics in the area of steganography, cryptography, IS in IT Company and also WSN. It discusses several parameters that measure the effectiveness and security metrics in the evaluation of the domain. Some parameters evaluate the effectiveness or security metric are able to be implemented in IT area as shown in the Table 1 as follows.

Table 1. Parameter Metric of Effectiveness and Secutity Metrics Performance in IT Area

	No.	Parameter Metric	**Implementation**	Metrics **Effectiveness**	**Security**
Steganography	1.	PSNR (Peak Signal to Noise Ratio)	It measure the quality of any image that compare the cover image and embed as stego image [21]–[24], restore or degrades image with detail to its reference truth image [25]. It also evaluates and compares algorithm the effectiveness and stego-image quality [26].	√	√
	2..	MSE (Mean Square Error)	It evaluates the square error representing the difference between the cover image and stego image, and also determines the image quality parameters, as to avoid problem of embedding data and improved version of the image technique [23]–[26].	√	√
	3.	NCC (Normalized Cross Correlation)	It evaluates of the similarity between the original cover image in terms of size and the stego image after embedded process [23].	√	-
	4.	PRD (Percentage Residual Difference)	It measures between the original host of ECG with result that achieved in the watermarking [27]	√	-
	5.	Accuracy measuring and standard deviation	It measures the integration of hardware and software process in negative systems with the analysis stability of information structures and security systems [28]	-	√
	6.	The pixel expansion:	It is used for comparing the level security and the adversary to determine the secret image by single share [16].	-	√
	7.	PSNR (Peak Signal to Noise Ratio)	Determine in term of the ratio between the maximum possible power of a signal in the cryptography and the power of mortifying noise that affects the fidelity of its representation [13], [18]	√	-
	8.	MSE (Mean Square Error).	It squared error of an estimator numerous methods to quantify the modification between standards values by an estimator and the correct values of the quantity that was expected [13]	√	-
	9.	Coefecient of correlation	Statistical quantity of an image pixel performance. It divides the image into 2 some image pixels blocks [29].	√	-
	10	Pixel Expansion	It is used for comparing the level security and the probability for adversary to determine that the secret image by a single share is equal[16].	-	√
Information system in IT industry	11.	Awarenes measure	It uses tools, method and procedure control in organizational security that collected data by security manager [30].	√	-
	12.	Quantitatively measurable.	Capability in measured accurately the performance control in company. It monitoring performance using proactive control to prevent the problem and reducing the incidents [14].	√	-
	13.	Function coefecient	It uses the design questionnaire to survey the personal and opinion performance of employee. The discriminant analysis based on the questionnaire classification is then used [9].	√	-
	14.	The Pearson's chi squared	It test results with respondent that evaluated the employee based on questionnaire that had been designed [15].	√	-
Wireless Sensor Network	15.	Voronoi polyhedron:	It determines the clustering system that increases life cycle and reduce power consumption in WSN environment [19].	√	-
	16.	Data-measuring systems (MSA)	Data-measuring systems (MSA) that determine the integrity that give the limited source of energy and ensure the confidentiality in securing algorithm data encryption [19].	-	√

Based on Table 1, several parameters metric are implemented in some area of IT focusing on effectiveness, security and both metric performances. In steganography, it is showed two parameters focus on effectiveness metric performance, two parameters metric security metric and two parameters focus on both of the metrics performance. In cryptography, most of parameter focus on effectiveness metric and only one parameter focus on security metric performance. In IT company all of paremeters focus on effectiveness

metric performance, while in WSN, one parameter focuses on the effectiveness metric and one parameter focuses on security metric. However, there is one the unique thing list in Table 1; PSNR and MSE metrics in steganography focus on both metrics performance, while both of same parameter metrics in cryptography only focus on the effectiveness metric performance.

5. CONCLUSION

This paper studies about the effectiveness and security metrics that is a concern in development to achieve the quality of IT performance. From the two metrics of the performance, this paper is analyzed some domain of study that concern with evalution in effectiveness and security metric performances. The domain study that used in the area both evaluation performances which are steganography, cryptography, IS in IT Company and WSN. This paper reviews most of effectiveness and security performance is used in IT area. It is discovered effectiveness and security metric as become some concern of this study. Both of performance important to evaluate with some parameter to achieve the expected performance in develop a system in IT area. However, the exact parameters that evaluate effectiveness and security metric is necessary to determine the performance of steganography as the future work that is related with this study.

ACKNOWLEDGEMENTS

The author wish to thank the Ministry of Higher Education Malaysia in funding grant under the University Grant Non-PI with S/O 13850, RIMC of Universiti Utara Malaysia, Kedah.

REFERENCES

[1] T. Herath and H. R. Rao, "Encouraging information security behaviors in organizations : Role of penalties, pressures and perceived effectiveness," *Decis. Support Syst.*, vol. 47, no. 2, pp. 154–165, 2009.
[2] R. Kishore, H. R. Rao, and K. Nam, "^^ m Qjarterly The Role of Service Level Agreements of Information Technology Management An Empirical Study1 Outsourcing :," vol. 33, no. 1, pp. 119–145, 2015.
[3] N. Voloshina, S. Bezzateev, A. Prudanov, M. Vasilev, and A. Gorbunov, "Effectiveness of LSB and MLSB information embedding for BMP images," *Conf. Open Innov. Assoc. Fruct*, vol. 2016–Septe, pp. 378–384, 2016.
[4] D. Kutscher and I. I. T. O. S. N. Etworks, "It ' s the Network : Towards Better Security and Transport Performance in 5G," 2016.
[5] C. Mohan, "Steganography based information security with high embedding capacity," pp. 17–21, 2015.
[6] L. Aolaritei, D. Lee, T. L. Vu, and K. Turitsyn, "A Robustness Measure of Transient Stability under Operational Constraints in Power Systems," *IEEE Control Syst. Lett.*, vol. PP, no. c, p. 1, 2018.
[7] S. Norussaadah, M. Salleh, R. Din, N. H. Zakaria, and A. Mustapha, "A Review on Structured Scheme Representation on Data Security Application," vol. 11, no. 2, pp. 733–739, 2018.
[8] R. S. Sabri, R. Dini, and A. Mustapha, "Analysis Review on Performance Metrics for Extraction Schemes in Text Steganography," vol. 11, no. 2, pp. 761–767, 2018.
[9] A. Almubark, N. Hatanaka, O. Uchida, and Y. Ikeda, "The Effectiveness of Corporate Culture Toward Information Security Incidents," vol. 6, 2015.
[10] W. T. Lin, "The business value of information technology as measured by technical ef fi ciency : Evidence from country-level data," *Decis. Support Syst.*, vol. 46, no. 4, pp. 865–874, 2009.
[11] R. Din, S. Utama, and A. Mustapha, "Evaluation Review on Effectiveness and Security Performances of Text Steganography Technique," vol. 11, no. 2, pp. 747–754, 2018.
[12] R. Din, R. S. Sabri, A. Mustapha, and S. Utama, "A Comparative Review on Data Hiding Schemes," vol. 11, no. 2, pp. 768–774, 2018.
[13] K. Anusudha, N. Venkateswaran, and J. Valaramathi, "Selective Plane Replacement Watermarking and Cryptography (SPRWC)," vol. 9, no. December, pp. 1–7, 2016.
[14] L. Hong-li and Z. Ying-ju, "Measuring Effectiveness of Information Security Management," *Comput. Netw. Multimed. Technol. 2009. CNMT 2009. Int. Symp.*, pp. 1–4, 2009.
[15] S. B. Chebrolu, "How do cloud capabilities impact various aspects of IT effectiveness?," *Proc. - 2012 IEEE 5th Int. Conf. Cloud Comput. CLOUD 2012*, no. May 2010, pp. 932–940, 2012.
[16] Z. X. Fu and B. Yu, "A Modified Multi-Secret Visual Cryptography with Ring Shares," *Adv. Eng. Forum*, vol. 6–7, pp. 343–349, 2012.
[17] B. S. Kong, M. S. Kim, and K. J. Kim, "A study on improvement measures of unmanned security system against security threats," *2013 Int. Conf. IT Converg. Secur. ICITCS 2013*, pp. 1–3, 2013.
[18] N. Kaur, "An embedded extended visual cryptography scheme for color image using LPG with PCA," vol. 1, no. 6, pp. 41–47, 2016.
[19] E. Zakasovskaya, V. Tarasov, and A. Glushchenko, "Information Security Issues in the Distributed Information Measurement System," *2017 Int. Conf. Ind. Eng. Appl. Manuf.*, no. Ml, 2017.
[20] R. G. Sargent, "Proceedings of the 2013 Winter Simulation Conference R. Pasupathy, S.-H. Kim, A. Tolk, R. Hill, and M. E. Kuhl, eds," pp. 321–327, 2013.

[21] P. Yadav, N. Mishra, and S. Sharma, "A secure video steganography with encryption based on LSB technique," *2013 IEEE Int. Conf. Comput. Intell. Comput. Res. IEEE ICCIC 2013*, 2013.
[22] D. Baby, J. Thomas, G. Augustine, E. George, and N. R. Michael, "A novel DWT based image securing method using steganography," *Procedia Comput. Sci.*, vol. 46, no. Icict 2014, pp. 612–618, 2015.
[23] P. Sehgal and V. K. Sharma, "Eliminating Cover Image Requirement in Discrete Wavelet Transform based Digital Image Steganography," *Int. J. Comput. Appl.*, vol. 68, no. 3, pp. 37–42, 2013.
[24] M. Tayel, H. Shawky, and A. E. S. Hafez, "A New Chaos Steganography Algorithm for Hiding Multimedia Data," *4th Int. Conf.*, pp. 208–212, 2012.
[25] Z. A. Alqadi, M. K. A. Zalata, and G. M. Qaryouti, "Comparative Analysis of Color Image Comparative Analysis of Color Image Steganography," *Int. J. Comput. Sci. Mob. Comput.*, vol. 5, no. 11, pp. 37–43, 2016.
[26] H. R. Kanan and B. Nazeri, "A novel image steganography scheme with high embedding capacity and tunable visual image quality based on a genetic algorithm," *Expert Syst. Appl.*, vol. 41, no. 14, pp. 6123–6130, 2014.
[27] A. Ibaida and I. Khalil, "Wavelet-based ECG steganography for protecting patient confidential information in point-of-care systems," *IEEE Trans. Biomed. Eng.*, vol. 60, no. 12, pp. 3322–3330, 2013.
[28] O. V Isaev, A. S. Kravchenko, and V. P. Irkhin, "Method for Modeling Accuracy Measuring in Evaluation of Sustainability of Information Structure Security System in Terms of Negative Impacts," no. 1, pp. 205–210, 2017.
[29] S. Bhowmik and S. Acharyya, "Image cryptography: The genetic algorithm approach," *Proc. - 2011 IEEE Int. Conf. Comput. Sci. Autom. Eng. CSAE 2011*, vol. 2, pp. 223–227, 2011.
[30] A. Odeh, K. Elleithy, and M. Faezipour, "Steganography in Arabic text using Kashida variation algorithm (KVA)," *Syst. Appl*, 2013.