Factors Influencing the Adoption of Cyber Security Standards Among Public Listed Companies in Malaysia

Mohamed Abdalla[1]
Yusri bin Arshad[4]
Faculty of Technology Management and Technopreneurship
Universiti Teknikal Malaysia Melaka
Melaka, Malaysia

Muath.Jarrah[2]
School of Information Technology, Skyline
University College, 1797
Sharjah, UAE

Ahmed Abu-Khadrah[3]
College of Computing &Informatics
Saudi Electronic University
Riyadh, Saudi Arabia

Abstract—**Employee's failure to adhere to their organization's cyber security policies contributes most of the cyber incidents. To secure information security systems, companies need to communicate behavioral and technical solutions to their employees, due to the fragility of the human factor since it plays a critically significant role in securing cyber systems. The necessity to safeguard information systems have speed up the evolution of the present method of cyber security, which should be based on adequately adopting cyber security standards to secure business enterprise's assets and users in cyberspace. This paper studies factors influencing the adoption of cyber security standards among public listed companies in Malaysia. Through online survey that was distributed among 275 Public listed companies. The findings indicated that expected related benefits and perceived ease of use had significant impact on the adoption of cyber security standards. On the other hand, perceived security had played important moderating influence on the relationship between organizational factors and the adoption of cyber security standards.**

Keywords*—*Cyber security; human factor; cyberspace; cyber security standards

I. Introduction

Cyber security standards are defined broadly to include principles, guidelines, codes of practice and technical specifications that are developed by public, private and not-for-profit entities, including government departments and agencies, national standardization bodies, industry alliances and associations [1].

Malaysian enterprise's concern regarding cyber security issues is at the peak for the last decade. Business industries striving to securer their critical infrastructures as the core value are the significance of cyber protection, which is connected to the developing knowledge of information security. According to [2] Malaysian Airlines has reported critical data breach that comprised confidential data belongs to the companies' clients. As a survey conducted by PricewaterhouseCoopers Malaysia, 42 percent of Malaysian organizations see an increased risk of cyber threats. In Malaysia, cybercriminals had hit losses equivalent to RM 1 billion, qualifying the nation to be the fifth riskiest country to cyber threats in 2019 [2].

Cyber Security, like any other application of technologies, requires standardization. As a result, a number of Cyber Security standards have been developed to govern the use of Cyber Security technologies in many fields. Specific standards, for example, exist to compel businesses to maintain safe infrastructures that limit the danger of cyber-attacks. Nowadays, Cyber Security is seen as a critical issue [3][30]. In order to secure cyber assets, organizations need to communicate technical and behavioral solutions to their employees, since the human factor has been considered the weakest line in the defense system, or at least it plays a critically significant role in securing cyber systems [4][30]. By assisting in the establishment of common security requirements and capabilities required for secure solutions, Cyber Security standards improve security and contribute to risk management. While it is impossible to remove all risks, Cyber Security standards make it more difficult for attacks to occur, or at the very least lessen the impact of those that do. The purpose of Cyber Security standards is to make information technology systems, networks, and critical infrastructures more secure [5]. If employees are not willing to accept cyber security standards, IS will not bring the full benefits of the technology to the Malaysian public listed companies [6]. Hence, the need has scaled exponentially for enterprises to adopt a new guideline of cyber security standards that could assist them mitigate data breaches, better comply with regulations and enhance cyberspace [7]. Policy makers, regulatory agencies and the industry are also increasingly agreeing that the adoption cyber security standards are required to ensure data protection, service continuity and public safety. The following are the contributions of the study:

- Perceived ease of use (PEU) is the most influential factor in the adoption of in the technological context.
- An expected related benefit is the most influential factor in the adoption of cyber security standards in the organizational context.
- Employee's innovativeness is the most influential factor in the adoption of cyber security standards in the individual context.

- Individual factors are the most influential factor in the adoption of cyber security standards in MPLC.
- Perceived security is moderated significantly by the organizational factors towards the adoption of cyber security standards.

The reminder of this paper has been organized as follows: Section 2 discusses the related works. The back ground of the study is described in Section 3. Section 4 described the theoretical framework. Methodology was discussed in Section 5 and finally, the conclusion and future words are described in Section 6.

II. Related Work

Cyber Security standards can be traced back as the set of practices and guidelines to protect organization's cyber infrastructure [8]. These standards are usually useful for all business enterprises, irrespective of their size, segment or industry [9]. Prior studies have examined which cyber security standards are available internationally and nationally and how could these standards be located being relative to each other and it figured out that as shown the table below [10]. Cyber security standards' compliance application in Malaysia is braced by the (NCSP). The Malaysian National Cyber Security agency keens to consolidate the critical cyber assets and promote the country's determination towards safer cyberspace besides coping with any potential cyber security crises [11]. To obtain clear picture on the most relevant international and nationals standards for cyber security, an inventory was drafted from the past studies. Approximately 180 standards were composed. Table I described the top ten most used cyber security standards in recent times [12].

Cyber security standards demonstrate a major step in information system governance. By monitoring and managing a containing risk to acceptable levels, the standards have to be entirely consistent with information system governance mechanisms and closely aligned with, and driven by the organization's cyber security guidelines [13]. The standards provide sets of benefits for the information security systems within the organizations through constant application activities, such as the security of technical and functional requirements, design and architecture, operating procedures and operational guidelines [14].

TABLE I. Cyber Security Standards Inventory (Source: Pressey et al., 2015)

Title	Source	Origin
ISO/IEC 27002	ISO/IEC	International
ISO/IEC 27001	ISO/IEC	International
NERC CIP 002-009	NERC	International
NIST SP-800 series	NIST	USA
ISA/IEC 62443	ISA	USA
AGA No.12	AGA	USA
COBIT5	ISACA	International
ISO/IEC 15408	ISO/IEC	International
API 1164	API	USA
PCI-DSS	PCI	International

III. Background of the Study

In order to increase the degree of cyber security standard's adoption and compliance to its practices, finding effective ways to adjust user's intention and decisions is essential. Despite the sophistication of the systems and how well be aligned, security methods rely on the individuals who use them. Furthermore, the users can be the major vulnerability to information systems [15].

TABLE II. Summary of Factors Influencing Cyber Security Adoption

No	Year	Author	Issue	Method	Findings
1	2019	Addae et al		Empirical study	User behavioral data for adaptive Cyber Security
2	2019	Bhuiyan et al	The influential factors of cloud adoption Security Objectives	Online survey	Relative advantages, top management support, organizational readiness and are the most influential factors in the adoption of cloud security
3	2019	Ahmad et al.	Cloud service provider security readiness model: the Malaysian perspective.	Systematic literature	The standards specified under ISO 27000 are better suitable for compliance, according to the study, because they comprise standards that complement one another and provide internationally recognised frameworks in information security management best practices
4	2018	Rafał Leszczyna	Standards on cyber security assessment of smart grid	Systematic Littauer review	The standards are more generic in nature and do not include technical specifics. They can be used as a starting point for higher-level tasks including formulating security assessment policies, allocating duties, and scheduling security assessment actions

Merely by opening infected e-mail is enough to allow criminals to place damage to the system and successfully breach organization's cyber assets [16]. According to Table II Addae et al. [17] studied user behavioral data for adaptive Cyber Security; the empirical study's findings revealed that Technology Acceptance Model (TAM) variables including perceived usefulness and perceived ease of use have significant effect on behavioral intentions and usage of Cyber Security, where Self-efficacy has also been shown to influence adoption and usage of IS. While Bhuiyan et al. [18] investigated the influential factors of cloud adoption Security Objectives. By using questionnaires to gather information from a selected IT firm that specializes in SaaS and public cloud. The results indicated that TOE model factors including, relative advantages, top management support, organizational readiness and are the most influential factors in the adoption of cloud security. In contrary, negative impacting elements include technology readiness, cloud trust, and a lack of cloud security standards was reported. Moreover, Ahmad et al. [19] studied cloud service provider security readiness model: the Malaysian perspective. The goal of the study was to provide a conceptual model that can be used to assess a CSP's readiness to comply with cloud-specific standards such as ISO/IEC 27017. The standards specified under ISO 27000 are better suitable for compliance, according to the study, because they comprise standards that complement one another and provide internationally recognized frameworks in information security management best practices. Moreover, Rafał Leszczyna [20] studied Standards on cyber security assessment of smart grid, through systematic literature review; study found that Cyber security related standards for smart grid address the issue to various extents and in different ways. The standards are more generic in nature and do not include technical specifics. They can be used as a starting point for higher-level tasks including formulating security assessment policies, allocating duties, and scheduling security assessment actions.

IV. THEORETICAL FRAMEWORK OF THE STUDY

By integrating two theoretical replicas of information systems adoption, this study developed the theoretical model for cyber security standards adoption. A combination of Technology acceptance model TAM and diffusion of innovation theory DOI, models were synthesized. TAM model focuses on the adoption decision that sometimes is based solely on voluntary situations, neglecting that users' judgments is often influenced by their peers or in response to social pressure [21]. This study seeks to synthesize theoretical frame work by joining particular number of factors originated from past models to investigate a wider standpoint which contributes in considering the adoption of cyber security standards.

A. Perceived Security (PS)

Perceived security is defined as the degree to which users perceive that using the technology will be free from any danger. Several Studies have indicated that the users' sense of control in any system is largely determined by their feeling of security [22]. Further researches that linked to perceived security are rooted in Technology acceptance model. Researches have proven the effect of perceived security on innovation adoption, including information security systems adoption [23].

Kalakota and Whinston [24] defined PS as the degree in which one feels that engaging in certain activity is free from any potential threat that creates an event or situation, in which appears to be vulnerable or unsecure. The user's decision to adopt and engage with any IS depends on their degree of security since lesser perceived security could cause a rejection of cyber security standards, adoption. Similarly, high perceived security could lead into the acceptance of information security practices [25]. In this study perceived security considers moderating variable. Fig. 1 demonstrates the theoretical framework of the study.

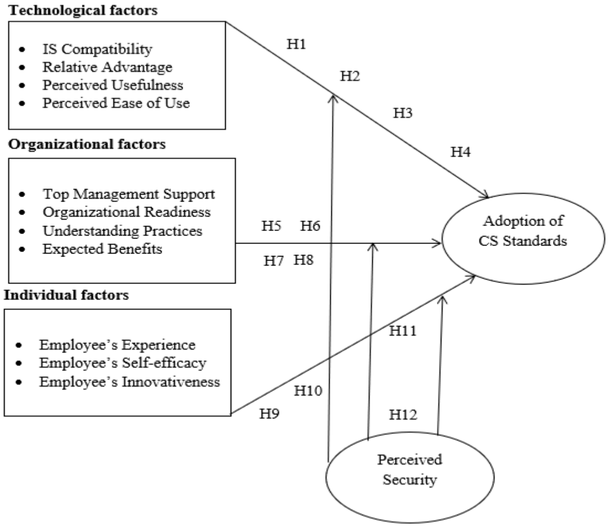

Fig. 1. Theoretical Framework.

V. METHODOLOGY

Convenience sample was used in order to collect the data for this study. Convenience sampling can be traced back as the collection of data from the targeted population members that are available and willing to provide it [26]. Therefore, this method is suitable whenever the population is broadly dispersed and the framework is unavailable in which the cluster sampling would not be sufficient [27]. Previous studies have found that this technique is commonly used in researches in the field of social science and regularly used in the organizational area studies. Yet, this study applied non-probability sampling where the researcher monitored through online each response. Hence, the responses for every characteristic were diligently observed. Consequently, the most appropriate way was to visit Bursa Malaysia Directory website to find the sampling unit and to acquire the data comprising the type of the industry or sector, the person in charge and their contacts.

A. Operational Constructs

Practically, since the study using quantitative method, it utilized specifically designed questionnaire and shaped to measure the proposed model's variables. Self-administrated questionnaire or survey was constructed by the researcher which was done by the respondents through a link (web questionnaire) that was sent by the researcher to respondents. Close-ended questions were utilized since the close-ended questions are commonly easier and quicker to be answered by the respondents. As illustrated in Table III, the questionnaire comprised two (2) sections which were section A and section B. Section A considered of questions regarding demographic information as the measurement for section A was multiple choice questions. In Section A, the questions focused on demographic profile of the company and respondents. The questionnaire contained thirty-seven (37) in two sections. On the other hand, section B contained questions regarding the factors influencing cyber security standard's adoption among Malaysian Public listed Companies, comprising: technological factors, organizational factors and individual factors. The measurement scale in section B was five-point Likert scale rating with the questions that related to the study, where the answers ranged between 1 represented strongly disagree and 5 represented strongly disagree.

TABLE III. STRUCTURE OF THE QUESTIONNAIRE

Question	**Measurement**	**Location in questionnaire**	**Total items**
Respondents' profile	Multiple choice questions	Section A: Q1-4	4
IS Compatibility	Five-point Likert scale rating	Section B: Q5-7	3
Relative Advantage	Five-point Likert scale rating	Section B: Q8-10	3
Perceived Usefulness	Five-point Likert scale rating	Section B: Q11-13	3
Perceived Ease of Use	Five-point Likert scale rating	Section B: Q14-16	3
Top Management Support	Five-point Likert scale rating	Section B: Q17-19	3
Organizational Readiness	Five-point Likert scale rating	Section B: Q20-22	3
Understanding Practices	Five-point Likert scale rating	Section B: Q23-25	3
Expected Benefits	Five-point Likert scale rating	Section B: Q26-28	3
Employee's Experience	Five-point Likert scale rating	Section B: Q29-31	3
Employee's Self-efficacy	Five-point Likert scale rating	Section B: Q32-34	3
Employees' Innovativeness	Five-point Likert scale rating	Section B: Q35-37	3

1) Data analysis procedure: To analysis the data and reveal the findings accurately, two forms of most used statistical tools discoverer the relationships and compare between groups must be presented. Data were prepared for analysis, prior to the analysis. Editing the data and coding it along with the data entry were achieved. Editing the data comprises of inspecting the instrument of the filed-up survey to define and reduce errors to the minimum, misclassification, incompleteness, and gaps in the information attained from the respondents [28].

VI. Analysis and Findings

A. Demographic Profile Analysis

According to Table IV, the number of males were the majority with one 130 employees while the number of females was 44 employees. The Technological sector were from Telecommunication, ICT and Technology manufacturing, financial services, media and digital followed by the food, beverage and tobacco manufacturing and also palm oil mining and real estate services. The majority number of the respondents where from digital, media and financial services with (46%), (27%) of the respondents where from the ICT, telecommunication and technology Manufacturing sectors whereas and food, beverage and tobacco manufacturing with 24.1 percent while the number of respondents from real estate services were 1.7%. 0.6% from palm oil mining which was the lowest.

Refereeing to the results, the year of the creation of the companies shows that 40.8% of the companies were established prior to 2000 where 38.5% were founded between 2000 and 2005. 14.5% was created at the period between 2005 to 2010, while 6.3% was established after 2010. 79.3% which is overwhelming majority of the public listed companies in Malaysia have applied cyber security policies where the rest 20.7% have not implemented any cyber security policies.

1) Reliability test: According to Table V, reliability can be traced back as the replication, accuracy and consistency of a measurement procedure [27]. Cronbach's alpha considers among of the most commonly used reliability ranging between 0 and 1 value. For exploratory research, a Cronbach's alpha that is bigger than six (6) is usually accepted to indicate reliability for the measurement though it is more preferable if the value greater than 0.70.

TABLE IV. RESPONDENT'S PROFILE

Characteristics	**Items**	**Number (N=174)**	**Percentage**
gender	Male Female	130 44	74 25.3
Sector of Technology	Telecommunication, ICT and technology manufacturing media, digital, and financial services Beverage, food and Tobacco manufacturing Real estate Palm oil and mining	48 80 42 3 1	27.6 46 27.6 1.7 0.6
Year of company established	Prior to 2000 between 2000 to 2005 between 2005 to 2010 After 2010	71 67 25 11	40.8 38.5 14.4 6.3
Has your company implemented any cyber security polices	Yes No	138 36	79.3 20.7

TABLE V. CRONBACH'S ALPHA TEST RESULT

Construct variables	**Number of items in scales**	**Places in the questionnaire**	**Cronbach's alpha**
Technology factors			
IS compatibility (ISC) Relative Advantage (RA) Perceived Usefulness (PU) Perceived Ease of Use (PEU)	3 3 3 3	Q5 Q6 Q7 Q8	0.876 0.678 0.908 0.90
Organization factors			
Top management Support (TMS) Organizational Readiness (OR) Expected Benefits (EB) Understanding Practices (UP)	3 3 3 3	Q9 Q10 Q11 Q12	0.834 0.686 0.897 0.907
Individual factors			
Employee's Experience (EE) Employee's Self-efficacy (ES) Employee's Innovativeness (EI)	3 3 3	Q13 Q14 Q15	0.854 0.723 0.728

B. Multi Linear Regressions

In order to analyze the effect of technological, organization and individual factors of cyber security standards adoption, regression analysis was utilized as shown in Table VI. The R-square (R^2) for technological factors indicated 0.332, which indicates that 33.2 percent of the variance in the adoption of cyber security standards. Technological factors contribute to enhance information security ((β= 0.082, p= 0.000). Thus, H1 is supported where the technological factors contribute to the adoption of cyber security standards. Technology factors played significant role in cyber security standards adoption according to the regression analysis in the study.

Moreover, R^2 for organizational factors showed 0.361, which indicated 36.1% of the variance in the adoption of cyber security standards could be forecasted from the relationship of all independent variables in organizational predictors. For individual factors R^2 is calculated as 0.301 which means that 30.1% of the variance in cyber security standards adoption might be projected from relationship of all independent variables in individual predictors. The findings indicated that these predictors played significant roles of cyber security standards adoption. Therefore, H3 is supported by the analysis where individual factors had significant positive relationship with the adoption of cyber security standards.

Table VII, Illustrated the R-square (R^2) showed 0.332 for technological factors (TF), which means that 33.2% percent of the variance in the adoption of cyber security standards can be predicated from the relationship of all independent variables in technological factors. Regression analysis results have proven that perceived ease of use (B= 0.220, p= 0.000) had significant influence on the adoption of cyber security standards. However, Information system compatibility, relative advantage and perceived usefulness have not had significant influence on the adoption of cyber security standards. Moreover, R^2 for organizational factors showed 0.361 which mean that 36.1% of the variance can be predicted from association off all independent variables in organizational factors (OF). According to the results expected benefits (B= 0.630), p= 0.000) played important roles in influencing the adoption of cyber security standards. On the other hand, Top managements support, organizational readiness and understating practices had no significant influence on Cyber Security standards adoption. R^2 for individual factors was 0.301, which represents that 30.1% of the variance in the adoption of cyber security standards could be predicted from the association of all independent variables in individual factors (IF). Three significant variables that explained cyber security standards adoption in individual factors, including employee's experience (B=0.210, p= 0.037), employee's self-efficacy (B=0.084, p= 0.0341), as well as employee's innovativeness (B=0.432, p= 0.000).

TABLE VI. RESULT OF MULTIPLE REGRESSION ANALYSIS (N=174)

Variables	Constant	Unstandardized coefficient (B)	Standardized coefficient (b)	p-value	R-square (R^2)
Technological factors	1.550	0.037	0.082	0.000	0.332
Organizational factors	-320	0.142	0.287	0.000	0.361
Individual factors	3.809	0.183	0.395	0.000	0.301

TABLE VII. ANALYSIS OF CONSTRUCTS

Construct	Model	Unstandardized coefficient (B)	Standardized coefficient (b)	p-value	R-square (R^2)
TF	1				
ISC		0.014	0.12	0.503	0.332
RA		0.143	0.085	0.867	
PU		0.220	0.129	0.090	
PEU		0.586	0.080	0.000	
OF	2				
TMS		-0.191	-0.116	0.288	0.361
OR		0.284	0.188	0.072	
UP		0.339	0.223	0.012	
EB		0.630	0.509	0.000	
IF	3				
EE		0.210	0.154	0.037	0.301
ES		0.084	0.180	0.0341	
EI		0.432	0.406	0.000	

VII. Discussion and Implications

Malaysia has progressed toward being an advanced digital economy where cyberspace increases in volume and complexity. Consequently, cyber-threats are increasing rapidly; as a result, businesses are facing high possibility security risks in cyberspace lately [29]. Findings have indicated perceived ease of use played significant part in the adoption of cyber security standards in the technology context. The conflicting findings could be explained by adopters' perceptions that cyber security standards are easy to adopt since it will help to protect and secure their systems and because the adoption procedure doesn't require any mental or physical effort. Furthermore, expected related benefits and is significant predictor to adopt cyber security standards in Public listed companies in Malaysia, to enhance their information security systems in organizational context [30]. Organizational factors can be traced back as the techniques that the company approaches to solve the problem in the networks. Though, the magnitude of security risks and proposed practices make it gradually challenging for users to decide which standards should be applied [31]. Employee's experience, employee's self-efficacy and employee's innovativeness, are the most influential factors determining the adoption of cyber security standards in individual context, which can be interpreted that the adopter's perception of their employee's experience knowledge and skills enable them to adapt cyber security standards more quickly. Moreover, the adopters perceive that their employee's self-efficacy, and their ability to handle the challenges contribute to the adoption of cyber security standards. Meanwhile, the role of the innovativeness and creativeness in the adoption of cyber security standards in public listed companies in Malaysia is crucial, in specific, there was extensive investigations by scientists in this area about of innovativeness that has essentially been defined as the degree to which person adopts innovations sooner than other members of their same social context [32].

VIII. Conclusion

This paper studied factor influencing the adoption of cyber security standards due to the need for enterprises to adopt cyber security standards in order to mitigate data breaches internally or external. While it is impossible to remove all risks, cyber security standards make it more difficult for attacks to occur, or at the very least lessen the impact of those that do. The purpose of cyber security standards is to make information systems more secure. The study focuses on specific factors including technological, organizational, and individual factors. other factors may lead into the adoption of cyber security standards including environmental, social, and motivation factors. Investigating these factors may bring more insights and clearer image from future research.

References

[1] Leszczyna, R. "Cyber Security and privacy in standards for smart grids – A comprehensive survey," Computer Standards and Interfaces, 56, pp. 62–73, 2018.

[2] Security magazine, "Malaysian Airlines is breached: 2021 cyber security news," Security. [article]. Available https://www.securitymagazine.com/articles/94738-malaysian-airlines-is-breached.

[3] Hamdani, S. W. A., Abbas, H., Janjua, A. R., Shahid, W. Bin, Amjad, M. F., Malik, J., Murtaza, M. H., Atiquzzaman, M., & Khan, A. W, "Cyber Security Standards in the Context of Operating System. ACM Computing Surveys, 54(3), pp. 1-5., 2021.

[4] M. N. Al-Mhiqani, R. Ahmad, Z. Z. Abidin, W. Yassin, A. Hassan, and A. N. Mohammad, "New insider threat detection method based on recurrent neural networks," Indonesian Journal of Electrical Engineering and Computer Science, 17(3), pp. 1474–1479, 2019.

[5] Peng, S. Y. "Private Cyber Security standards? Cyberspace Governance, Multistakeholderism, and the (Ir)relevance of the TBT Regime" Cornell International Law Journal, 51(2) pp. 445–469, 2018.

[6] Suhazimah, D. "Social Factors Influencing the Information Security" Australasian Conference on Information Systems, 2016, pp. 1-9.

[7] Kiilu, K.P.C., and M.D., Nzuki, "Factors Affecting Adoption of Information Security Management Systems" International Journal of Science and Research (IJSR), 5(12), pp. 161-162, 2015.

[8] Pressey, A.R.L., Adam, P., and Adam, P. "Inventory and classification of cyber security standards" mdpi, 118(1), pp.81–101, 2015a.

[9] Zachary A.C., and Linkov. I., "Cyber Security Standards: Managing Risk and Creating Resilience" IEEE Computer Society, 4(1), pp. 134-137, 2018.

[10] Pressey, A.R.L., Adam, P., and Adam, P. "Inventory and classification of cyber security standards" mdpi, 118(1), pp.81–101, 2015b.

[11] Muazzam, M., 2015. Cyber security standards Compliance: A Vital Measure to Critical Infrastructure Protection. Malaysia, KBMG.

[12] Pressey, A.R.L., Adam, P., and Adam, P. "Inventory and classification of cyber security standards" mdpi, 118(1), pp.81–101, 2015c.

[13] Tofan, D.C. "Information Security Standards" Journal of Mobile, Embedded and Distributed Systems, 3(3), pp. 15-20, 2011.

[14] Calder, A., and Carter, N. "Understadnding cyber security standards" CGI, 2019. [online] Available: https://www.cgi.com/en/media/white-paper/understanding-Cyber Security-standards.

[15] Nasser Al-Mhiqani, M., Ahmed, R., Zainal Abidin, Z. A., & Isnin, S. N. "An Integrated Imbalanced Learning and Deep Neural Network Model for Insider Threat Detection" International Journal of Advanced Computer Science and Applications, 12(1), pp. 573–577, 2021.

[16] Huang, C.C., 2017. "Cognitive factors in predicting continued use of information systems with technology adoption models" information research Journal, 22(2), pp. 45-55, 2017.

[17] Addae, J. H., Sun, X., Towey, D., & Radenkovic, M. "Exploring user behavioral data for adaptive Cyber Security" User Modeling and User-Adapted Interaction, 29(3), pp. 701–750, 2019.

[18] Bhuiyan, M. Y., Othman, S. H., & Raja Mohd. Radzi, R. Z. "An Enhancement of TOE Model by Investigating the Influential Factors of Cloud Adoption Security Objectives" International Journal of Innovative Computing, 9(1), pp. 55–67, 2019.

[19] Ahmad, N. I., Mohamed, I., Daud, M., Jarno, A. D., & Hamid, N. A. "Cloud Service Provider Security Readiness Model: The Malaysian Perspective" Proceedings of the International Conference on Electrical Engineering and Informatics, pp. 705-714, 2019.

[20] Leszczyna, R. "Cyber Security and privacy in standards for smart grids – A comprehensive survey" Computer Standards and Interfaces, 56, pp. 62–73, 2018ab.

[21] Mumtaz, A.H. and Arachchilage, S. "A Conceptual Model for the Organisational Adoption of information system innovations. Journal of Computer Engineering & Information Technology, pp. 317-339, 2017.

[22] Shin, D.H. "The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. ScienceDirect, 22(5), pp. 428-438, 2010.

[23] Edward, H., & Clyde, H., Ki-Yoon, K., Kwan-Sik, N., and James, S., "Measuring Perceived Security in B2C Electronic Commerce Website Usage: A Respecification and Validation" science direct, 62, pp.11-12, 2014.

[24] Carlos, R. J., García, J. and José, V.J., "The importance of perceived trust, security and privacy in online trading systems" Emarald insight, 17(2), pp. 96-113, 2019.

[25] Huang, C.C., "Cognitive factors in predicting continued use of information systems with technology adoption models" information research Journal, 22(2), pp. 45-55, 2017.

[26] Etikan I., 2016. "Comparison of Convenience Sampling and Purposive Sampling" American Journal of Theoretical and Applied Statistics, 5(1), pp. 1-4, 2016.

[27] Saunders, M., Lewis, P., and Thornhill, A., "Research Methods for Business Students.7th ed., England: Pearson Education Limited, 2016a.

[28] Kumar. R., "Research methodology: A step by step guide for beginners, 3rd ed, London: Sage, 2011.

[29] Saunders, M., Lewis, P., and Thornhill, A., "Research Methods for Business Students.7th ed., England: Pearson Education Limited, 2016b

[30] Al-Mhiqani, M. N., Ahmad, R., Abidin, Z. Z., Yassin, W. M., Hassan, A., Mohammad, A. N., & Clarke, N. L. "A new taxonomy of insider threats: an initial step in understanding authorised attack. International Journal of Information Systems and Management, 1(4), pp. 343-359, 2018.

[31] Li, L., He, W., Xu, L., Ash, I., Anwar, M., Yuan, X., "Investigating the impact of cyber security policy awareness on employees' cyber security behavior" International Journal of Information Management, 45, pp. 13-24, 2019.

[32] Marcati, A., Guido, G., and Peluso, A.M., 2008. "The role of SME entrepreneurs' innovativeness and personality in the adoption of innovations" ScienceDirect, 37(9), pp. 1579-1590, 2008.