International Journal of Advances in Scientific Research and Engineering (ijasre)

E-ISSN : 2454-8006

DOI: 10.31695/IJASRE.2023.9.3.5

Volume 9, Issue 3
March - 2023

The Effect of Cyber Security Risks on E-Governance usage: A Case Study of Tanzanian Immigration Department

Nasra Issa[1], Kenneth Mlelwa[2]

Research Scholar[1], & Lecturer [2]

Department of Information and Communication Technology

The Mwalimu Nyerere Memorial Academy

Dar es Salaam

Tanzania

ABSTRACT

The use of e-Governance, has offered citizens a convenient, efficient and transparent manner of enjoying most important services. However, ICT services are prone to cyber security threats which can hinder the effective and efficient usage of e-Governance services. This study assessed the effect of cyber security threats and risks on the Tanzania e-Governance services usage at the Immigration department. The study has used an exploration research design to collect primary data from 113 randomly sampled respondents at the Tanzania Immigration department. The data was analysed descriptively to determine the frequency and mean relationships between the variables. Additionally, a regression model has been used to determine the direction of relationships between the independent and dependent variables. The findings revealed that 93.8% of the respondents are aware of the e-Governance services. However, this is not proportional to the e-Governance usage since only 27.4% of the responding officers indicated that they are frequent users of the service. The study further indicate that the system faces minimal security risks at the department which is a result of well-established security defense system such as the use of strong and frequent password change. The study recommends e-governance service operators should constantly monitor the systems to identify threats, develop a more user-friendly architecture, and promote adoption among Tanzanians.

Key Words: e-Governance, Cyber security, Cyber-attack, Information and Communications Technology (ICT).

1. INTRODUCTION

Nagaraja defined "E-Governance as the use of ICT to convert the usefulness, efficiency, transparency and responsibility of transfer of data and transaction between government, between government organizations, between government and citizens, between government and business" [1]. The four pillars of e-Governance include; knowledge, connectivity, data content and capital and ICT being the key component. From mere computerization, e-Governance is constantly developing to offer access, fairness and empowerment to masses [1].

The world being connected today, information security system must be set up to counter emerging vulnerabilities that may occur as a result of increasing of technology. In the complex and dynamic arena of internet, the challenges of safeguarding Information infrastructure is drastically increasing, possibly as a factor of the ubiquitous existence of services etc. depending on these networks. These networks are exposed to cyber-attacks due to various flaws in the system. Therefore, it is basically mostly importantly to increase on the security that covers the application software and infrastructure to give the governance an effective internet without any possible risk of being equipped [1].

Cyber security refers to the techniques and methods used to protect computers, network systems and the data contained, and servers from potential attacks and threats [3]. Protection may range from the prevention of physical theft to data and electronic information as well as the disruption and misdirection of services provided by these computer systems [4].Therefore, it is a discipline that involves technology, people, information, and processes to allow risk-free operations(Rea-Guaman,2017).

However, Assiret et al., indicated that, the development and adoption of e-governance services comes with associated risks such as threats and attacks. Therefore, protecting data and systems is of key importance [5], [2]. Other researcher suggested that governments and organizations must assess their information security regularly so as to improve and determine their security capability and thus review and update their information security [6].

On that note, this study intends to assess the effect of cyber security threats on the Tanzanian e-Governance services usage at the Tanzania Immigration Department as a case study.

2. LITERATURE REVIEW

Goswami, studied the impact of cyber-security in the application of e-governance [3]. He indicated that, the application of e-governance increases the participation of citizens in various programs by increasing awareness and providing up to date information in time. Thus, e-governance was shown to be of high importance in India. However, cyber security was highlighted to be an importance aspect of e-governance to combat cyber threats and attacks. The study concluded that, the security aspect of e-governance should be taken seriously. High end technology should be adopted to ensure improved confidentiality of information and transactions on the networked systems. Furthermore, Shareef, [7] reviewed the e-governance security risks, threats, and success factors. The study indicated that, despite a wide range of e-governance, it is associated with a number of threats and risks. The study recommended that, by utilizing technology, the e-governance systems should be made highly secure to ensure safety of the government and consumers. The study further emphasized that, information security is the key factor in ensuring willingness of consumers to use e-governance services and thus, government should asses the possible risks or threats and put in place an effective risk assessment strategy. It also concluded that the reasons for lower participation of people in e-governance usage were; e-governance security, attitude for development with sustainability, acceptance and awareness level also indicated that, despite the fact that e-governance simplifies the provision of government services by making services them available on-line, there exist the risk associated with the system such as privacy and online safety issues [8], [5]. They also suggest adoption of block chain technology in designing security systems for e-governance services platforms. Morya and Singh, [3] conducted a study on the latest cyber-security threats and the impact on e-governance in India. They emphasized that due to the increasing interconnectedness worldwide, information systems should be designed to combat emerging securities and threats that may develop because of the advancement of technology. They further explained that, the use of ICT system can help strengthen the four pillars of e-governance: Connectivity, Knowledge, Data Content, and Capital by protecting information, systems, and network from potential cyber-threats.

2.1 Conceptual Framework

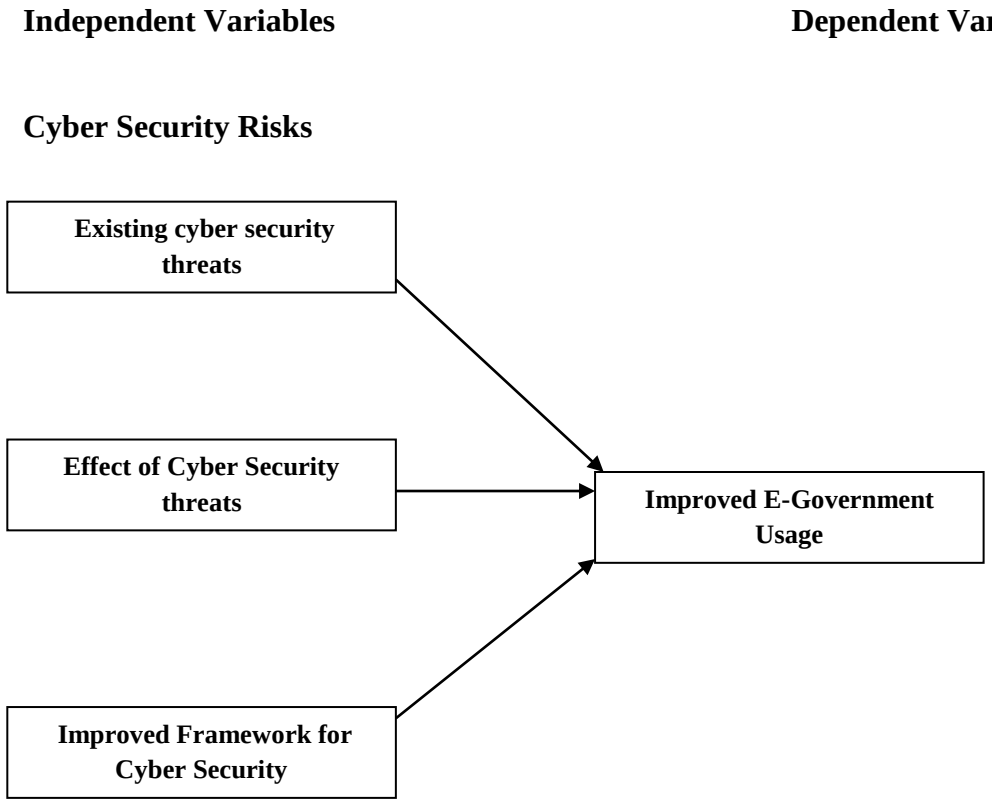

Figure No 1. Conceptual Framework

DOI: 10.31695/IJASRE.2023.9.3.5

3. METHODOLOGY

3.1 Study design and Sampling

The study adopted a quantitative research designs with a descriptive research approach. The data collected from staff of Headquarter of Immigration Department which is under the Ministry of Home Affairs in Dar es Salaam, Tanzania.

The total number of staff at Immigration headquarter is 280. The sample was selected using probability sampling technique to ensure all employees have an equal chance of being selected. On the other hand, the sample size for the study was obtained using Slovin's formula adopted from in [9].

$$n = \frac{N}{(1 + Ne^2)}$$

Where: n = Sample size; N = the number of population size; e = is the Margin of error = 7%=0.07

$$n = \frac{280}{(1+280*0.075^2)} = 108.$$

The study sample size that obtained from the formula above is 108 respondents. However, the sample size was increased by 5 respondents. Thus, the sample size used in this study was 113 respondents. Sample size increased reduce sampling error and hence increase the accuracy of the results. The table below showed the summary of role distribution of the targeted population and the sample size to be participating in the data collection of the study as calculated from the [10] approach.

Table 3.1: Population and sample size distribution

Category of respondents	Target Population	Sample Size
Human Resource Department	8	3
ICT Department	77	31
Accounts Department	22	9
Border Management Control Section	96	39
Other user of the system	77	31
Total	**280**	**113**

3.2 Data Type and Collection Methods

The study used primary data that were collected using questionnaires. A set of open and close-ended questions structured to ensure straight forwardness of questions as well as respondent's answers. Questionnaires were distributed to the 113 Immigration department staffs through physical distribution, and Google forms shared through the email and WhatsApp messaging application.

3.3 Data Analysis

Data from questionnaires were analyzed using descriptive analysis where the frequency tables were presented to explain the relationship between the dependent and independent variables. The analyses carried out using the statistical software known as the Statistical Packages for Social Sciences (IBM SPSS version 20).

3.4 Descriptive Statistics

Descriptive data analysis techniques were conducted on primary data. The data collected were analyzed using SPSS software which is more appropriate for analysis of primary data. The frequencies were calculated for each response in the questionnaire to identify most agreed alternatives in relation to combating e-governance cyber-security threats and the results presented in frequency tables.

3.5 Research Model

The study used regression analysis to assess the association between the e-Governance usage and the awareness, cyber security threats, cyber security vulnerability and users perceptions. The type of regression analysis carried is order logistic regression. The regression model is explained by the following equation:

DOI: 10.31695/IJASRE.2023.9.3.5

e-Gov_usa = α + β1Awar+β2Thrt + β3Vulnt + β4Perct + ε

Where by:e-Gov_usa = e-Government Usage; Awar = e-Governance services awareness

Thr = Cyber Security Threats; Vuln = Cyber Security Vulnerability; Perc = User Perception

α = Coefficient of the constant variable; ε = error term; β1, β2, β3, β4 = Estimated parameters in a model; t = (1, 2, …….n).

Table 3.2: Measurement of Variables

Variable Type	Variable	Measurement/Constructs	Analysis Technique	Literature Source
IV	Cyber security threats	• Log-in information • Frequent password change • Regular risk assessments • Prohibit account sharing	Descriptive Statistical and ordinal logistic regression	[12]
IV	Cyber security vulnerability	• Spam messages filter • Centrally managed and monitored system • Connection to all devices (accessibility) • Web application and protocol scanners (availability)	Descriptive Statistical and ordinal logistic regression	[13]
IV	User perceptions	• Easy to understand and use • Reliable • Fast payment method • Easy way of communicating and information sharing	Descriptive Statistical and ordinal logistic regression	[14]
DV	E-governance usage	• Improved • Trust • Security • Ability	Descriptive Statistical and ordinal logistic regression	[15]

3.6 Relative Importance Index

The relative importance indices were computed and used to see the most weighted responses as the most important. Since the questionnaires consisted of the likert-scale type questions with the responses range from strongly disagree to strongly agree, then the relative importance index is an appropriate index to measure the highly important responses. It gives the rank of responses from the most important to the least important response. The formula used to calculate the relative importance index is as presented below;

$$\text{"Relative Important Index} = \frac{5n_5 + 4n_4 + 3n_3 + 2n_2 + 1n_1)}{A * N}$$

Where;

$$n_5 = \text{Number of respondents for Strongly Agree; } n_4 = \text{Number of respondents for Agree}$$

$$n_3 = \text{Number of respondents for Neutral; } n_2 = \text{Number of respondents for Disagree}$$

$n_1 = \text{Number of respondents for Strongly Disagree"}$

3.7 Study Validity and Reliability

Validity is the extent to which the tools measure what is intended to be measured while reliability is the repeatability or consistency [11]. Reliability analysis was carried out to check internal consistency for Likert-type scale responses. The Study variables consist of likert-type scale responses, then it was necessary to check for the reliability. Relaibility index used is called Cronbach's alpha. It is the value between 0 and 1. For a variable to be reliable, the value of cronbach's alpha is at least 0.7. The reliability results are as in Table 3.Cronbach's alpha criteria are met as all the values are greater than 0.7. The likert-type scale responses were thus more reliable.

DOI: 10.31695/IJASRE.2023.9.3.5

Table 3.3: Cronbach's Alpha (Reliability test)

ITEMS	Cronbach's Alpha	No. of Items
Scale1: Existing cyber security threats on the e-Governance services usage	0.832	5
Scale2: Effect of existing cyber security vulnerability on the e-Governance services usage	0.791	5
Scale3: User perceptions on the quality of cyber security e-Governance services usage	0.950	5

4. RESULTS

4.1 Awareness and e-Governance usage at Tanzania Immigration

The findings show that most of the respondents are aware about the e-Governance services usage. It is shown in Table 4.1 that almost 93.8% responded that "Yes" they are aware about the e-Governance services. This might be the case because most of governments' officials are literate on the use of e-services especially the use of computers and smart phones in performing online transactions. However, about 6.2% (Minority) have no idea about the e-Governance services.

Table4.1: E-Governance services Awareness among employees at Immigration

Awareness	Frequency	Percent	Valid Percent
Yes	106	93.8	93.8
No	7	6.2	6.2
Total	**113**	**100**	**100**

The Results in Table 6 show that Most of the respondents are using e-Governance services. It is shown in Table 4.2 that 61.1% said that they sometimes use e-Governance services and 27.4% of them they use it very often. However they are very few of them (Only 11.5% approximately) who do not use the e-Governance services.

Table 4.2: E-Governance services usage at Immigration

e-Gov usage	Frequency	Percent	Valid Percent
Very often	31	27.4	27.4
Sometimes	69	61.1	61.1
Not using	13	11.5	11.5
Total	**113**	**100**	**100**

4.2 The existing cyber security threats on e-Governance usage

The descriptive analysis on the existing cyber security threats was conducted and the results are in Table 4.3.The assessment was in term of likert-scale type of questions. The respondents were provided the statements and they had to choose one of the responses (likert-scale type) either "Strongly Disagree, Disagree, Neutral, Agree or Strongly Agree". In Table 3.3"SD=Strongly Disagree, DA=Disagree, N=Neutral, A=Agree, SA=Strongly Agree".

Table 4.3: Examining Existing threats on e-Governance usage

	SD	DA	N	A	SA	Total
	Freq (%)	Freq (%)	Freq (%)	Freq (%)	Freq (%)	Freq (%)
T1	15 (13%)	20 (18%)	44 (39%)	26 (23%)	8 (7%)	113 (100%)
T2	24 (21%)	18(16%)	13 (12%)	40 (35%)	18 (16%)	113 (100%)
T3	14 (12%)	23 (20.4)	50(44.2)	21 (19%)	5 (4.4%)	113 (100%)
T4	11(10%)	18 (16%)	30(26.5)	29(25.6)	25 (22%)	113 (100%)
T5	16 (14%)	18 (16%)	32 (28%)	33 (29%)	14 (12%)	113 (100%)

The descriptions of the statements; "T1= our system has log information that highlight any important issues; T2= Our system prompt us to change passwords every few months, T3=Our system undergo regular risk assessments to evaluate the security, T4=Our system prohibit account sharing across all services and users, and T5=Our system control and monitor what applications your users are allowed to install and use". Most of the respondents (more than 51%) either agreed or strong agreed to T2.

Relative importance indices computed to see the statement (s) with greater weight. The results are in Table 4.4.

DOI: 10.31695/IJASRE.2023.9.3.5

Table 4.4: Computation of Relative Important Index

	SD (1)	DA (2)	N (3)	A (4)	SA (5)	Total	Total (N)	A*N	RII	RANK
T1	15	40	132	104	40	331	113	565	0.586	4
T2	24	36	39	160	90	349	113	565	0.618	3
T3	14	46	150	84	25	319	113	565	0.565	5
T4	11	36	90	116	125	378	113	565	0.669	1
T5	16	36	96	132	70	350	113	565	0.619	2

Table 4.4 shows the relative importance in each of the statements. The column named RII stand for the "relative importance index" which shows how each statement received the response.

Table 3.4 shows that the more important is given to the statement T4. On the other hand the statement given less importance is T3. This implies that at Immigration department they do not perform regular risk assessments to evaluate the risk of e-Governance usage.

The study also examined the existing threat and vulnerabilities by assessing five statements namely; E1=I receive a lot of spam messages in my email, E2= Our system is centrally managed and monitored for all user accounts and login events at our network, E3=My email has a lot of prompt messages, E4=Our system allows connection of all devices to access the ICT network and E5=Our system have web application and protocol scanners to check for potential attacks.

Table 4.5 shows the results, in the columns headings in Table 4.5; SD=Strongly Disagree, DA=Disagree, N=Neutral, A=Agree, SA=Strongly Agree.

Table 4.5: Effects of cyber security vulnerability (RII)

	SD (1)	DA (2)	N(3)	A(4)	SA (5)	Total	Total (N)	A*N	RII	RANK
E1	37	72	93	20	20	242	113	565	0.428	5
E2	18	44	108	100	60	330	113	565	0.584	1
E3	21	36	189	20	30	296	113	565	0.524	3
E4	25	54	108	84	20	291	113	565	0.515	4
E5	20	48	129	72	40	309	113	565	0.547	2

In Table 4.5, statement E2 has the largest RII and therefore it is said to be given more importance by the respondents. The implication is that, at Immigration department most of the respondents given more important on the effect of security vulnerability that, "system is centrally managed and monitored for all user accounts and login events at their network" and hence the system is not vulnerable.

Also the statement E5 is the next most important since its RII greater next to the statement E2. This is to say; at Immigration department the system have web application and protocol scanners to check for potential attacks.

4.3 Regression model

The study used ordered logistic regression to explain the relationship between the dependent variable (e-Governance usage) and the independent variables (awareness of e-Governance services, cyber security threats and cyber security vulnerability). The ordered regression results are given in Table 4.6 and Table 4.7. The test was conducted using 5% (0.05) significance level and the result was significance since p value (Sig.) is 0.000 which is less than 0.05.

Table 4.6: Model Fitting Information

Model	-2 Log Likelihood	Chi-Square	df	Sig.
Intercept Only	204.487			
Final	.000	204.487	63	.000

Table 4.7 contains the regression Parameter Estimates of the independent variables which are significant .The estimates are interpreted using their signs (positive or negative signs). For a positive sign, implication is that, for every increase in independent

DOI: 10.31695/IJASRE.2023.9.3.5

variable there is an increase in dependent variable. Whereas, for a negative sign, implication is that, for every increase in independent variable, there will be a decrease of the dependent variable.

Table 4.7: Regression coefficients and significance tests

Parameter Estimates								
							95% Confidence Interval	
		Estimate	Std. Error	Wald	df	Sig.	Lower Bound	Upper Bound
Threshold	[e_Gov_USAGE = 0]	14.14	10.13	1.948	1	.163	-5.72	34.01
	[e_Gov_USAGE = 1]	32.14	11.61	7.669	1	.006	9.39	54.895
Location	[Awareness=1]	26.64	8.60	9.600	1	.002	9.79	43.495
	[Awareness=2]	0[a]			0			
	[System has log information that highlight any important issues=2]	12.79	5.30	5.828	1	.016	2.41	23.179
	[System has log information that highlight any important issues=3]	7.50	3.23	5.398	1	.020	1.17	13.834
	[[System has log information that highlight any important issues=5]	0[a]			0			
	[[System has log information that highlight any important issues=2]	-9.31	4.72	3.902	1	.048	-18.56	-.072
	[System has log information that highlight any important issues=5]	0[a]			0			
	[System have web application and protocol scanners to check for potential =4]	-18.744	8.688	4.655	1	.031	-35.772	-1.716
	[System have web application and protocol scanners to check for potential =5]	0[a]			0			

Table 4.7 show that the independent variables which are significant are; the awareness of e-Governance services, cyber security threat (T1=System has log information that highlight any important issues and T4=System prohibit account sharing across all services and users) and Effect of cyber security vulnerability (E5=system have web application and protocol scanners to check for potential attacks).Regression analysis results show that there are some threats if taken into account might help to improve the cyber security system. In Table 4.7, the awareness of e-Governance has significant effect to the usage of e-Governance services. It shows that the increase in the awareness by a unit will lead to the higher e-Governance usage by 26 units. Thus the awareness should be raised to the users so as to increase e-Governance usage. The threats seem to have an impact on the usage of e-Governance. The system with system log information that highlights any important issues (For Disagree category) has the influence on the e-Governance usage. Table 4.7 shows that, with reference category (strongly agree) as the system increase log information which highlights important issues, the e-Governance usage will be higher by 12 units. However, a variable "system prohibit account sharing across all services and users" with the Disagree category has a negative effect to the usage of e-Governance. The increase of this variable (system prohibit account sharing across all services and users, for disagree) will the lower e-Governance usage by 9 units.

5.0 CONCLUSION

The study found that at Immigration the system prompt the users to change password every time. This may cause the users to be at risk of unsecured system. Another threat at Immigration department is that the system does not undergo regular risk assessments to evaluate the security.

DOI: 10.31695/IJASRE.2023.9.3.5

The extent of security vulnerability is not high since the respondents did not mention about them receiving any attacks through emails and other means. It was observed that their system is centrally managed and monitored for all user accounts and login events at their network and that the system has web application and protocol scanners to check for potential attacks.

The study revealed that awareness of e-Governance services, cyber security threats and vulnerability influence the e-Governance usage. The study by Rajandran and Mohamed [8], examined the reason for the less participation of the people in e-government transactions in India and concluded that e-governance security, lack of sustainability, development measures, system acceptance and awareness level, were significant in influencing usability. Similarly, our study has found that most of the staffs at the Immigration department are aware of the e-governance and hence are using it. The findings in the current study are superior in the sense that, the sample size is larger than that adopted by previously study [8].

While studying cyber security vulnerability of the digital economy which relies upon the ability of cybersecurity technical solution with non-technical areas happening at the same time with business units, executives, providers, and end-users to prevent any cyberattacks which might occur [16]. The study reveals that software security vulnerabilities, poor designed networks, weak configuration as the major vulnerabilities that are exploited to carry out successful attacks on the critical infrastructures. Similarly, our study has found that most of the staff at the Immigration department agrees that the system is centrally managed and monitored for all user accounts and login events at their network .Thus to have the system of such kind should help to reduce the security vulnerability.

6. RECOMMENDATIONS

Based on the findings, there may be a need for similar study to be conducted to different class of people, not only government officials but also other people even those who are at the informal sectors. Furthermore, the study recommends that other scholarly to extend this study beyond the assessment of cyber security threats and vulnerability, to suggest an effective framework to address such threats in developing nations.

REFERENCES

[1] Nagaraja, K. (2016) e-Governance in India: Issues and Challenges. IOSR Journal of Economics and Finance, 7(5), 50-54.

[2] Morya, K., & Singh, M. (2020). Study of Latest Cyber security Threats to IT/OT and their Impact on e-Governance in India .International Journal on EmergingTechnologies,939-947.

[3] Goswami, A. (2018). Impact of Cyber Security in Different Application of e-Governance. Journal of Advances and Scholarly Researches in Allied Education, 65-71.

[4] Nadikattu, R. R. (2020). New Ways of Implementing Cyber Security to Help in Protecting America (May 14, 2020). Journal of Xidian University, VOLUME 14, ISSUE 5, 2020, Page No: 6004 - 6015, Available at SSRN: https://ssrn.com/abstract=3622822

[5] Assir, H., Nanda, P., & Mohanty, M. (2020).Secure e-Governance Using Blockchain. Easy Chair Reprints, 1-8.

[6] Otero, A. R. (2014). An Information Security Control Assessment for Organization. Nova Southeastern University.

[7] Shareef, M. S. (2017).Security of e-government; Risks, Threats, and Success Factors. Journal of Raparin University, 61-79.

[8] Mohamed, R. and Rajandran K. A. (2017) Study on Cyber Security in E-Governance with Reference to Areas of Thanjavur District, Tamil Nadu.

[9] Tejada, J.J., & Paunzalan, J. (2012).On the Misuse of Slovin's Formular. The Philippine Statistician, 129-13

[10] Yamane, Taro. (1967). Statistics: An Introductory Analysis, 2nd Edition, New York: Harper and Row.

[11] Bolarinwa, O. A. (2015) Principles and methods of validity and reliability testing of questionnaires used in social and health science researches. Niger Postgrad Med J 2015; 22:195-201.

[12] Chen, J. V., Jubilado, R. J. M., Capistrano, E. P. S., and Yen, D. C., (2015). "Factors affecting online tax filing – An application of the IS Success Model and trust theory. Computers in Human Behavior". 43, 251–262.

[13] Mufti, N. M., Alshayeb, M., and Mahmood, S. (2018). "A Readiness Model for Security Requirements Engineering", IEEE Access, vol. 6, pp. 28611-28631

[14] Kalsi, N.S. and Kiran, R. (2015) "A strategic framework for good governance through e-governance optimization: a case study of Punjab in India", Program, Vol. 49, No. 2, pp.170204.

[15] Alzahrani, L., Al-Karagholi, W., and Weerakkody, V., (2017). "Analysing the critical factors influencing trust in e-government adoption from citizen's perspective: A systematic review and a conceptual framework". International Business Review, Volume 26, Issue 1, February 2017, 164–175.

[16] Rea-Guaman, A.M., Sa´nchez-Garcı´a, I.D., San Feliu, T., Calvo Manzano, J. A. (2017) Maturity Models in Cybersecurity: a systematic review. In: 12th ConferenciaIbe´rica de Sistemas y Tecnologı´as de Informacio´n (CISTI'17). Lisbon

DOI: 10.31695/IJASRE.2023.9.3.5