American Journal of Information Science and Technology
2023; 7(2): 76-83
http://www.sciencepublishinggroup.com/j/ajist
doi: 10.11648/j.ajist.20230702.15
ISSN: 2640-057X (Print); ISSN: 2640-0588 (Online)

Improved Information Security for Enhanced Government Data Privacy at *Zanzibar Social Security Fund (ZSSF)*

Massoud Ali Juma[1], Omar Fakih[2]

[1]Department of Information Technology, Faculty of Business Administration, Zanzibar University, Zanzibar, Tanzania

[2]Department of Telecommunication, Faculty of Engineering, Zanzibar University, Zanzibar, Tanzania

Email address:
massoud.allyzbr@gmail.com (Massoud Ali Juma)

To cite this article:
Massoud Ali Juma, Omar Fakih. Improved Information Security for Enhanced Government Data Privacy at *Zanzibar Social Security Fund (ZSSF)*. *American Journal of Information Science and Technology*. Vol. 7, No. 2, 2023, pp. 76-83. doi: 10.11648/j.ajist.20230702.15

Received: April 1, 2023; **Accepted**: April 24, 2023; **Published**: May 10, 2023

Abstract: The main concern of this study was to explore the strategies for improving information security for enhancement Government data privacy in public sector, Zanzibar Social Security Fund (ZSSF) as case study. Specifically, the explore the effect of restriction of access to information on enhancement Government data privacy in ZSSF, analyses the effect of encryption of all devices on enhancement Government data privacy in ZSSF. Also, the study explores the effect of backup of the office data on enhancement Government data privacy in ZSSF and finally the study analyses the effect of strong password on enhancement Government data privacy in ZSSF. A quantitative research approach was mainly employed with appropriate method of analysis for this study. The sample size for this study consists of 79 after dropping 19 respondents who don't return the questionnaire survey. A questionnaire survey was used as data collection instrument. A descriptive statistical techniques of analysis were used to analyses the collected data from relevant respondents. The study has revealed that four predictors (Restriction of access to information, Encryption of all devices, Backup of the office data and Strong password) had a significant influence on enhancement Government data privacy in Zanzibar Social Security Fund (ZSSF). The study concluded that the information system leads to fulfill the substantial security of properties and confidentiality. Finally, the study recommended that The Information security policies should be adopted and must be developed based on standard Information Security Management System (ISMS) and data privacy.

Keywords: Restriction of Access, Encryption of All Devices, Government Data Privacy, Strong Password

1. Introduction

In most of Sub-Sahara Africa, awareness about information security in public and private sectors is minimal. To make timely choices on cyber threats and assaults, the majority of public sector or enterprises need reliable and pertinent information. [1]. It is found that information-security management and communication of security information in most of African countries government departments are very limited, yet, citizens of African countries are not aware of the risks present in cyberspace [2]. There is an evident that information security awareness is a very important in any sector in the fight against cybercrime. For that reason, it is essential for any African country that intends to implement interventions in this area to have a holistic understanding of the level of Cyber security awareness in that country [3].

Information Systems (IS) in any organization is more and more services, including those related to the registration of births and deaths, passport issuance, marriage registration, tax collection, voter registration, payroll, and public finance, among others, have been computerized or are actively being considered for automation in organizations that are already commonplace in developed countries. [4]. With an increased dependence on the IS connected over open data networks, efficient information security governance has become a crucial success feature for organizations in the developed or developing countries alike [5]. Developing countries are going through processes that developed countries went through many years ago [6].

In Zanzibar and Tanzania in general data utilization through information system especially in healthcare systems is low [7]. Available literature suggests that, despite some notable successes, the impact of information system on the decision making process within Tanzania information systems remains limited [8]. Several barriers have been reported to prevent the information system from achieving full potential in Tanzania [9]. Institutional, technological, individual, and logistical capacities are perceived factors that either enable or impede the successful implementation and use of data generated from the IS. Therefore, this research focus on the strategies that can be used to improve information system in order to enhance data privacy and security to the public sector.

2. Statement of the Problem

The adoption of information systems faces many challenges in Zanzibar such as lack of skilled personnel, financial constraint, national culture, inferior infrastructures and among others [10]. It has been noted that the increasing use of ICT in many of organization in Zanzibar, such as ZSSF, has brought some difficulties in their workflow. This is because the old and manual system has been replaced by the new flexible system (FUMIS) which helps them to overcome some problems, but not far secure and privacy. Therefore, currently, The Zanzibar Social Security Fund has created a members' web portal that makes it easier for ZSSF members to obtain information about themselves, including member details, statements, benefits, and a variety of other information.

There are several studies conducted discussing about the strategies of improving information security awareness to enhance the data privacy. However, most of them have based on private companies such as mobile phone companies. Whereby, there is a number of challenges occurred in a government sectors due to the lack of strategies for improving information security in public sector to enhance government data privacy which bring the increase of awareness in information security. For instance, data indicates that less than 50% of firms had an IT security and training program for employees, which means that more than 50% of those organizations did not train and educate their staff in IS at the time of the study. [11]. Therefore, there is a need to conduct a study on improving information security for enhancement Government data privacy in public sector. In this study, Zanzibar Social Security Fund (ZSSF) will be used as a case study so as to answer the following research questions;

1) *What is the effect of restriction of access to information on enhancement Government data privacy in ZSSF?*
2) *What is the effect of encryption of all devices on enhancement Government data privacy in ZSSF?*

3. Information System Success Model

The Information Systems Success Model (ISSM) of DeLone and McLean [12] is an established IS theory that provides an integrated view on IS success by explaining the relationships between six of the most critical dimensions of success. System Quality, Information Quality, Use, User Satisfaction, Individual Impact and Organizational Impact and their relationships to each other as depicted by arrows. This widely cited model is considered as a standard model in the field of information systems research for measuring success [12]. It is particular applicable for the field of smartphone security, because it refers to the individual context: Security in general and smartphone security in particular highly depend on the behavior of individuals. This issue is represented by the dimension Individual Impact which directly influences the organization (Figure 1).

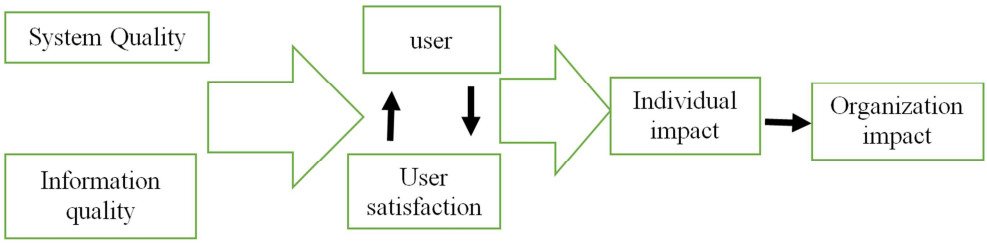

Figure 1. *Information Systems Success Model (Adapted from DeLone and McLean, 1992).*

This model will be applicable in this study since most of the domain explained in this model look like the model that are discussed in this study, where by the variables of this study includes the user of the system and how they are satisfied. The model also shows the relationship between variables like system quality and information quality where this study determining the relationship between information security and data privacy.

4. Empirical Literature Review

Dombora [13], integrated incident management model for data privacy and information security: Producing products and offering services to clients, consumers, and partners is the businesses' aim. They collect, store, transform, display, handle, and exchange information with outside entities as part of their production activities. This data may include both personal and professional information. Information may also be classified as being public, private, secret, or top-secret. Depending on their line of business and the information they handle, organizations must comply with legal regulations for information security. The legal environment consists of three types of acts: information security, data privacy and sectoral acts. The sectoral laws

may be divided into two subgroups: business related and security related. While the business-related laws imply implementation of information security measures, the sectoral information security and data privacy laws require implementation of internal rules and regulations regarding information security and data privacy.

Amato and Moscato [14] described the development of new technology capable of monitoring people's health conditions from a distance. Both medical gadgets and all other wearable technology are included in this. They discovered that the issue of data privacy is becoming more and more significant in e-health systems due to the growing use of cloud technology to manage and store sensitive data from patients. Additionally, they discovered that legal regulations govern the entire administration and storage procedures of medical records, not just service providers or users who set the privacy needs in medical domains. The use of Model Driven techniques for E-Health systems is appealing especially if formal verification of privacy requirements is enacted. In this study, they extend the Metamorphic (h) OSY modelling profile in order to explicitly consider privacy requirements for data. A novel model transformation algorithm is described for the application of Model Checking techniques to privacy verification.

Di Lorio et al. [15] described the development of new technology capable of monitoring people's health conditions from a distance. Both medical gadgets and all other wearable technology are included in this. They discovered that the issue of data privacy is becoming more and more significant in e-health systems due to the growing use of cloud technology to manage and store sensitive data from patients. Additionally, they discovered that legal regulations govern the entire administration and storage procedures of medical records, not just service providers or users who set the privacy needs in medical domains. Yet once governments impose multiple types of restrictions, it becomes harder for CSOs to adapt, resulting in fewer international shaming campaigns.

Jain et al. [16] dissemination of raw data, which is particularly important for applications in business, academia, and medicine. They added that while there are more open platforms for data collection, such as social networks and mobile devices, the amount of this data has likewise grown over time and is now moving toward becoming Big Data. Big Data's standard models do not include any level for capturing the sensitivity of both structured and unstructured data. It also needs to take into account the concepts of security and privacy, where the likelihood of disclosing private information is probabilistically minimized. This reach implies to introduced security and privacy layer between HDFS and MR Layer (Map Reduce) known as new proposed Secured Map Reduce (SMR) Layer and this model is known as SMR model. They found that the core benefit of this work is to promote data sharing for knowledge mining. This model creates a privacy and security guarantee, resolve scalability issues of privacy and maintain the privacy-utility tradeoff for data miners. In this SMR model, running time and information loss have a remarkable improvement over the existing approaches and CPU and memory usage are also optimized.

Habibzadeh et al., [17] demonstrated how the use of Cyber Physical Systems (CPSs) in smart cities has the potential to greatly enhance utilities, safety, and environmental health as well as healthcare and transportation services. These cost-saving measures and service upgrades, however, will result in greater susceptibility and risk. Smart city implementations as well as the benefits, efficiency, and cost savings they can enable have already started to expand. But there are also increasing costs and difficulties. These difficulties involve significant technological issues as well as significant organizational and policy issues. It is important to understand that these policy and technical implementation hurdles are perhaps equally likely to slow or disable smart city implementation efforts. In this study survey of the theoretical and practical challenges and opportunities are enumerated not only in terms of their technical aspects, but also in terms of policy and governance issues of concern.

According to Romanou [18] investigates how well Privacy by Design can protect personal information in a society that is changing quickly. The theoretical idea and broad guidelines of Privacy by Design, as outlined in the General Data Protection Regulation, are first succinctly explained in this paper. It will be shown why the implementation of Privacy by Design is essential in a number of sectors where specific data protection concerns arise (biometrics, e-health, and video surveillance), how it can be implemented, and examples of how it has been done.

Mtakati and Sengati, [19] in the information security is primarily a mechanism to protect information from unknown and known attacks. In this study, the Tanzanian Ministry of Education's information security vulnerabilities were examined in relation to many aspects. The analysis identified internal organizational elements that have a substantial impact on the Ministry of Education's information security risks. Additionally, research results showed a strong correlation between outside organizational issues and information security weaknesses in the Ministry of Education. Further empirical research, which could build on this study by taking a quantitative approach to the factors influencing information security vulnerabilities in various ministries and organizations, should be carried out in various regions as well as in other East African countries, the researcher recommended. Either, future studies could use the same survey tool and technique to generalize research more globally.

Abubaker et al., [20] information security and privacy can be achieved in BYOD environments: The goal of this paper is to present a current best practice methodology that businesses that employ mobile devices as part of their business strategy may use to detect and manage bring your own device (BYOD) security and privacy threats. Organizations may benefit from BYOD deployment in terms of increased employee productivity, cost savings, and work

flexibility, but there are also a number of information security and privacy concerns that are both well-known and less well-understood. This paper focuses on BYOD adoption, and its associated risks and mitigation strategies, investigating how both information security and privacy can be effectively achieved in BYOD environments.

5. Methodology

In this study qualitative research design was used to perfect the research questions, which were prepared by the researcher to the household survey to the local context. The study was conduct at one of the government organizations located in Urban district in Urban west region. The area was select purposively based on the following criteria: it was an Urban government organization that already integrating the system of security. The target population for this study comprise staffs of Zanzibar social security and selected company and organization of urban west region. Therefore, the study population was 98 ZSSF staff in Unguja. All 98 respondents were occupied to provide information on the strategies for improving information security in public sectors to enhance government data privacy, a case of Zanzibar Social Security Fund (ZSSF). The sample size that selected were appropriate as it enabled the researcher to collect the obligatory data quickly and accurately. The self-administered questionnaire was used for this study because it enables the researcher to collect data from relatively large sample size and minimize. A descriptive statistical techniques was used for data analysis in this study.

6. Study Findings

a) Demographic profile of the respondents.

During the data collection, 98 questionnaires were distributed among the Zanzibar Social Security Fund Employees, 19 questionnaires were not returned, whereas 79 questionnaires were returned which shows that the respond rate is 81% of the total respondents. The respond rate is right to draw conclusion for the study.

The summarized results from table 1 indicates that, 4 respondents equal to (5.1%) ranges from 21 – 30, 27 (34.2%) ranges from 31 – 40, 36 (45.6%) ranges from 41 –50, 10 (12.7%) ranges from 51 – 60 and those who were 61 above were 2 respondents equal to (2.5%). Therefore, the analysis revealed that respondents were dominated by the large number of age groups of 40 to 49. This is a good age of main power in every activity in any country. Also, the 1 shows that, total of 79 respondents equal to 100% were asked in this question. 50 respondents equal to (63.3%) were male and 29 respondents equal to (36.7%) were female. These results clearly indicated that the most respondents who were participated in this study question were male, since males is a group which is most participated in fishing activities rather than female. Although, the summarized results from Table 1 show that, 54 respondents made (68.4%) were married, 19 (24.1%) were single, 4 (5.1%) were widow and those who were divorced were 2 (2.5%). This is indicated that, most of the respondents who were involved in answering questions in this study were married since, covered more than 68.4% of the total respondents. A total of 79 respondents who were involved in this study, 4 respondents equal to (5.1%) were having a' level education, 6 (7.6%) were in a certificate level, 29 (36.7%) were having diploma education, 35 (44.3%) were having bachelor degree and 5 respondents (6.3%) were having post graduate education. Therefore, the results of the study indicated that, most of the respondents involved in this study were having diploma and bachelor degree levels of education, since, it they cover by more than 70%. Finally, a total of 79 respondents who were involved in this study, 4 respondents equal to (5.1%) were having one year, 5 (6.3%) were having 1-2 years, 28 (35.4%) were having 3-4 year, 37 (46.8%) were having 5-6 years and 5 respondents (6.3%) were having 7-year experience. Therefore, the results of the study indicated that, most of the respondents involved in this study were having experience between 5-6 years, since, it they cover 46.8% of total respondents.

Table 1. *Profile of the respondents.*

Variables	Category	Frequency	Percentage
Age	21-30	4	5.1
	31-40	27	34.2
	41-50	36	45.6
	51-60	10	12.7.
	61 above	2	2.5
Gender	Male	50	63.3
	Female	29	36.7
Marital status	Married	54	68.4
	Single	19	24.1
	Widow	4	5.1
	Divorced	2	2.5
Education level	A'level	4	5.1
	Certificate	6	7.6
	Diploma	29	36.7
	Bachelor degree	35	44.3
	Post graduates	5	6.3
Work experience	One year	4	5.1
	1 – 2 years	5	6.3
	3 – 4 years	28	35.4
	5- 6 years	37	46.8
	7 years above	5	6.3

Source: Researchers, 2022

b) What is the effect of restriction of access to information on enhancement Government data privacy in ZSSF?

In this specific question, the researcher was interested to know the effect of restriction of access to information on enhancement Government data privacy in ZSSF. The respondents were supposed to select either agree, strongly agree, disagree, and strongly disagree or neutral.

Table 2. *Restriction of access to information.*

Statements/Level of Agreement	SD		D		PA		A		SA	
	F	%	F	%	F	%	F	%	F	%
It keeps data safe from remote access attacks	5	6.3	3	3.8	5	6.3	21	26.6	45	57.0
It helps to blocks important content from being viewed	2	2.5	4	5.1	9	11.4	23	29.1	41	51.9
It provides a firewall against potential hacking attempts	2	2.5	4	5.1	9	11.4	34	43.0	30	38.0
Could help to reduce identity theft incidents	2	2.5	2	2.5	3	3.8	31	39.2	41	51.9
It allows the organization to control the employees	1	1.3	3	3.8	5	6.3	31	39.2	39	49.4

Source: Researchers, 2022

The summarized results from table 2 indicated that, out of 79 respondents involved in this study, 5 equal to (6.3%) strongly agreed, 3 (3.8%) agreed, but 5 respondents equal to (6.3%) were neutral, those who disagreed were 21 equal to (26.6%), and those who strongly disagreed were 45 equal to (57.0%.). Therefore, the study clearly indicated that, the restriction of access to information it keeps data safe from remote access attacks because respondents 57% strongly disagreed. This is supported by the study of Amato and Moscato, [14] which clarified the development of new technology capable of tele monitoring people's health. The study discovered that the issue of ensuring data privacy is becoming more and more crucial in E-Health systems due to the growing use of Cloud technologies to manage and store sensitive data from patients. Additionally, they discovered that legal regulations govern the entire administration and storage procedures of medical records, not just service providers or users who set the privacy needs in medical domains.

Also, the result from the table above indicated that, out of 79 respondents involved in this study, 2 equal to (2.5%) strongly agreed, 4 (5.1%) agreed, but 9 respondents equal to (11.4%) were neutral, those who disagreed were 23 equal to (29.1%) and those who strongly disagreed were 41 equal to (51.9%.). Therefore, 51.9% of all respondents strongly disagree that the restriction of access to information it helps to blocks important content from being viewed. In line with the study of Smidt et al. [15] support these results when they conducted a study on stopping the flow of information; some governments restrict CSOs. The study clarified that the organizations may mobilize against restrictions and find new ways of delivering information on human rights violations to international publics. In addition, the findings indicated that, out of 79 respondents involved in this study, 30 equal to (38.0%) strongly agreed, 34 (43.0%) agreed, but 9 respondents equal to (11.4%) were neutral, those who disagreed were 4 equal to (5.1%) and those who strongly disagreed were 2 equal to (2.5%.). Therefore, the findings of the study revealed that, restriction of access to information it provides a firewall against potential hacking attempts, since a large group of the respondents of 43% of the total respondents agreed. Siponen and Oinas-Kukkonen [21] support these results by identifying four security issues (access to Information Systems, secure communication, security management, development of secure Information Systems), and examines the extent to which these security issues have been addressed by existing research efforts.

Although, the researchers elaborated that, out of 79 respondents involved in this study, 41 equal to (51.9%) strongly agreed, 31 (39.2%) agreed, but 3 respondents equal to (3.8%) were neutral, those who disagreed were 2 equal to (2.5%) and those who strongly disagreed were 2 equal to (2.5%.). Therefore, the findings of the study revealed that, the restriction of access to information could help to reduce identity theft incidents in government data privacy, since a large group of the respondents more that 50% of the total respondents strongly agreed. Tsohou et al., [22] supported these results on the study of exploring information security awareness focusing on individual and/or organizational aspects. This paper argues that security awareness processes are associated with interrelated changes that occur at the organizational, the technological and the individual level. They introduce an integrated analytical framework that has been developed through action research in a public sector organization, comprising actor-network theory (ANT), structuration theory and contextualize. They develop and use this framework to analyses and manage changes introduced by the implementation of a security awareness programme in the research setting.

Finally, the researchers showed that, out of 79 respondents involved in this study, 39 equal to (49.2%) strongly agreed, 31 (39.2%) agreed, but 5 respondents equal to (6.3%) were neutral, those who disagreed were 3 equal to (3.8%), and those who strongly disagreed were 1 equal to (1.3%.). Therefore, the findings of the study revealed that, 49% of all the respondents agree that restriction of access to information it allows the organization to control the employees. Flowerday and Tuyikeze, [23] supported these results by developing the information security policy involves more than mere policy formulation and implementation. This paper argues that an information security policy has an entire life cycle through which it must pass during its useful lifetime. A formal content analysis of information security policy development methods was conducted using secondary sources.

c) What is the effect of encryption of all devices on enhancement Government data privacy in ZSSF?

The existing information system with the respect of data privacy of ZSSF were described according to the study results. A descriptive statistical techniques analysis was used to analyses this objective using frequency distribution. The respondents were supposed rate their opinion by selecting either agree, strongly agree, disagree, and strongly disagree or neutral.

Table 3. *Encryption of all devices.*

Statements/Level of Agreement	SD		D		PA		A		SA	
	F	%	F	%	F	%	F	%	F	%
It Can Help to Protect Remote Workers	3	3.8	4	5.1	6	7.6	34	43.0	32	40.5
Increases the Integrity of organization Data	1	1.3	2	2.5	6	7.6	44	55.7	26	32.9
Can Increase Employees Trust	4	5.1	1	1.3	4	5.1	17	21.5	53	67.1
It Could Help the organization to Avoid Regulatory Fines	2	2.5	2	2.5	4	5.1	41	51.9	30	38.0
It Supports Data Integrity	2	2.5	2	2.5	7	8.9	34	43.0	34	43.0

Source: Researchers, 2022

The summarized results from table 3 indicated that, out of 79 respondents involved in this study 32 equal to (40.5%) strongly agreed, 34 (43.0%) agreed, but 6 respondents equal to (7.6%) were neutral, those who disagreed were 4 equal to (5.1%) and those who strongly disagreed were 3 equal to (3.8%.). Therefore, the findings of the study revealed that, the effect of encryption of all devices on enhancement Government data privacy in ZSSF Help to Protect Remote Workers, since a large group of the respondents more that 80% of the total respondents strongly agreed and agreed. This is strongly supported by Di Iorio et al., [15] on the evaluation of the risk's seriousness and the suitability of the actions taken to adhere to the General Data Protection Regulation (GDPR) of the European Union (EU). According to this study, there is significant variation in how privacy principles are implemented across 10 European nations. The main areas of concern were underlined for: data linkage (median, range of adoption: 45%, 30%–80%), access and accuracy of personal data (50%, 0%–100%) and anonymization procedures (56%, 11%–100%).

Also, the study indicated that, out of 79 respondents involved in this study, 26 equal to (32.9%) strongly agreed, 44 (55.7%) agreed, but 6 respondents equal to (7.6%) were neutral those who disagreed were 2 equal to (2.5%) and those who strongly disagreed were 1 equal to (1.3%.). Therefore, the findings of the study revealed that, the effect of encryption of all devices on enhancement Government data privacy in ZSSF Increases the integrity of organization Data, since more than 55% of all respondents agreed. In line with Oualha and Olivereau [24] discussed sensor and data privacy in industrial wireless sensor networks to support these findings. Due to their capacity to regulate and keep an eye on physical environments, sensor networks are particularly intriguing. However, a number of security issues prevent that integration. The self-organizing nature of WSN architecture and the limited sensor resources make privacy protection a particularly difficult issue.

Furthermore, the table 3 indicated that, out of 79 respondents involved in this study, 53 equal to (67.1%) strongly agreed, 17 (21.5%) agreed, but 4 respondents equal to (5.1%) were neutral, those who disagreed were 1 equal to (1.3%) and those who strongly disagreed were 4 equal to (5.1%.). Therefore, the findings of the study revealed that, the effect of encryption of all devices on enhancement Government data privacy in ZSSF can increase employees trust since more than 67.1% of all respondents strongly agreed. The results are supported with the study of Malin [25] by clarifying that the protection of patients' privacy is severely jeopardized by the inclusion of genetic data in personal medical records. As a result, numerous patient privacy protection systems for shared genetic data have been created and put into use. The author identifies patterns of protection failure and goes over a number of the factors that make these systems vulnerable. The studies and discussion here offer guidelines for creating cutting-edge security measures that can withstand formal proofs.

The summarized results from table 3 indicated that, out of 79 respondents involved in this study, 30 equal to (38.0%) strongly agreed, 41 (51.9%) agreed, but 4 respondents equal to (5.1%) were neutral, those who disagreed were 2 equal to (2.5%) and those who strongly disagreed were 2 equal to (2.5%.). Therefore, the findings of the study revealed that, the effect of encryption of all devices on enhancement Government data privacy in ZSSF could help the organization to avoid regulatory fines since more than 51% of all respondents agreed. This is supported by Reidenberg and Schaub [26] about the Data privacy are a combustible mix. The improvement of education and the protection of student privacy are key societal values. This article explores how learning technologies also create ethical tensions between privacy and the use of Big Data for educational improvement. The study argues for the need to demonstrate the efficacy of learning systems while respecting privacy and how to build accountability and oversight into learning technologies.

The study indicated that, out of 79 respondents involved in this study, 34 equal to (43.0%) strongly agreed, 34 (43.0%) agreed, but 7 respondents equal to (8.9%) were neutral, those who disagreed were 2 equal to (2.5%) and those who strongly disagreed were 2 equal to (2.5%.). Therefore, the findings of the study revealed that, the effect of encryption of all devices on enhancement Government data privacy in ZSSF could supports data integrity, since more than 80% of all respondents agreed and strongly agreed. These results supported by Guarda et al., [27] by explaining that, lack of monitoring of Id system lead to the most of business practices involve personal data-processing of customers and employees failed. This paper presents a declarative framework to support the specification of information system designs, purpose-aware access control policies, and the legal requirements derived from the European Data Protection Directive. This allows for compliance checking via a reduction to policy refinement that is supported by available automated tools.

7. Conclusion

To explore the effect of restriction of access to information on enhancement Government data privacy in ZSSF, the study indicated that, the development of technology does not create a big challenge in the administration in public sector. Also, it is resolved that, the use of internet does not create a big challenge in the administration in public sector. In addition, come up with the idea that the information system leads to fulfill the substantial security of properties and confidentiality. Whereby, lack of trust and transparency in information system design can affect information security. To analyses the effect of encryption of all devices on enhancement Government data privacy in ZSSF, here, the study decided that, the use of computer security incidents helps in reducing hacking process and destructive cyber-attacks. Also, the development and the spread of e-services system helps in data privacy. Finally, it reach to the agreement that unauthorized access of information system might impact the government operation and reveal citizen's private information. Whereby, the confidentiality of data and systems that use or generate personal data helps in data praxis. And the tack of monitoring/surveillance of id systems or other databases holding person helps in data privacy.

8. Recommendation of the Study

Since information security and data privacy are very crucial, the special attention to protection of personal data in the public sector should be enhanced. It introduces a number of significant changes and restrictions. Therefore, a careful assessment must be done, as not all provisions are applicable. Especially the exceptions should be carefully considered before the general rule is applied. The government of Zanzibar should take the special effort to enhance the significance of information security and privacy in the public organization, official offices as well as to emphasis different companies to establish reliable system that could protect the data from hacking in our country.

References

[1] Kamariza, Y. (2017). Implementation of information security policies in public organizations: Top management as a success factor.

[2] Zhao, H., Wang, Y., & Liu, X. (2022). The assessment of smart city information security risk in China based on zGT2FSs and IAA method. Scientific reports, 12 (1), 1-14.

[3] Ezingeard, J. N., & Bowen-Schrire, M. (2007). Triggers of change in information security management practices. Journal of General Management, 32 (4), 53-72.

[4] Laurini, R. (2018). Information systems for urban planning: a hypermedia cooperative approach. CRC Press.

[5] Al-Emran, M., Mezhuyev, V., Kamaludin, A., & Shaalan, K. (2018). The impact of knowledge management processes on information systems: A systematic review. *International Journal of Information Management*, *43*, 173-187.

[6] Abualoush, S. H., Obeidat, A. M., Tarhini, A., & Al-Badi, A. (2018). The role of employees' empowerment as an intermediary variable between knowledge management and information systems on employees' performance. *VINE Journal of Information and Knowledge Management Systems*.

[7] Ismagilova, E., Hughes, L., Dwivedi, Y. K., & Raman, K. R. (2019). Smart cities: Advances in research—An information systems perspective. *International Journal of Information Management*, *47*, 88-100.

[8] Koivisto, J., & Hamari, J. (2019). The rise of motivational information systems: A review of gamification research. *International Journal of Information Management*, *45*, 191-210.

[9] Stair, R., & Reynolds, G. (2020). *Principles of information systems*. Cengage Learning.

[10] Hoxha, K., Hung, Y. W., Irwin, B. R., & Grépin, K. A. (2020). Understanding the challenges associated with the use of data from routine health information systems in low-and middle-income countries: A systematic review. *Health Information Management Journal*, 1833358320928729.

[11] Scholl, M. (2018). Play the Game! Analogue Gamification for Raising Information Security Awareness. Systemics, Cybernetics and Informatics, 16 (3), 32-35.

[12] DeLone, W. H., & McLean, E. R. (2002, January). Information systems success revisited. In Proceedings of the 35th Annual Hawaii International Conference on System Sciences (pp. 2966-2976). IEEE.

[13] Dombora, S. (2018). Integrated incident management model for data privacy and information security. In *BOOK OF PROCEEDINGS* (p. 319).

[14] Amato, F., & Moscato, F. (2015). A model driven approach to data privacy verification in E-Health systems. *Trans. Data Priv.*, *8* (3), 273-296.

[15] Di Iorio, C. T., Carinci, F., Oderkirk, J., Smith, D., Siano, M., de Marco, D. A., ... & Benedetti, M. M. (2021). Assessing data protection and governance in health information systems: a novel methodology of Privacy and Ethics Impact and Performance Assessment (PEIPA). *Journal of Medical Ethics*, *47* (12), e23-e23.

[16] Jain, P., Gyanchandani, M., & Khare, N. (2019). Enhanced secured map reduce layer for big data privacy and security. *Journal of Big Data*, *6* (1), 1-17.

[17] Habibzadeh, H., Nussbaum, B. H., Anjomshoa, F., Kantarci, B., & Soyata, T. (2019). A survey on cybersecurity, data privacy, and policy issues in cyber-physical system deployments in smart cities. *Sustainable Cities and Society*, *50*, 101660.

[18] Romanou, A. (2018). The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. *Computer law & security review*, *34* (1), 99-110.

[19] Mtakati, B., & Sengati, F. (2021). Cybersecurity Posture of Higher Learning Institutions in Tanzania. *The Journal of Informatics: 2714-1993*, *1* (1).

[20] Abubaker, N., Dervishi, L., & Ayday, E. (2017, October). Privacy-preserving fog computing paradigm. In *2017 IEEE Conference on Communications and Network Security (CNS)* (pp. 502-509). IEEE.

[21] Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 38 (1), 60-80.

[22] Tsohou, A., Karyda, M., Kokolakis, S., & Kiountouzis, E. (2015). Managing the introduction of information security awareness programmes in organisations. *European Journal of Information Systems*, *24* (1), 38-58.

[23] Flowerday, S. V., & Tuyikeze, T. (2016). Information security policy development and implementation: The what, how and who. *computers & security*, *61*, 169-183.

[24] Oualha, N., & Olivereau, A. (2011, May). Sensor and data privacy in industrial wireless sensor networks. In *2011 Conference on Network and Information Systems Security* (pp. 1-8). IEEE.

[25] Malin, B. A. (2005). An evaluation of the current state of genomic data privacy protection technology and a roadmap for the future. *Journal of the American Medical Informatics Association*, *12* (1), 28-34.

[26] Reidenberg, J. R., & Schaub, F. (2018). Achieving big data privacy in education. *Theory and Research in Education*, *16* (3), 263-279.

[27] Guarda, P., Ranise, S., & Siswantoro, H. (2017, June). Security analysis and legal compliance checking for the design of privacy-friendly information systems. In *Proceedings of the 22nd ACM on Symposium on Access Control Models and Technologies* (pp. 247-254).