DOI: https://doi.org/10.59645/tji.v3i1.134

The Journal of Informatics, Vol. 3, Issue 1 (pages 34-50)
ISSN: 2714-1993
Received: August 2023, Published: December, 2023
https://doi.org/10.59645/tji.v3i1.134

****Original Research****

ASSESSMENT OF THE EFFECTS OF ACCESS CONTROL ON REDUCING CYBERCRIMES IN THE SELECTED TELECOMMUNICATION COMPANIES IN TANZANIA

Andrew Nsombo
Institute of Accountancy Arusha, Tanzania
andrew.nsombo@dcea.go.tz

Julius Raphael Athuman Mhina
Institute of Finance Management, Tanzania
Julius.raphael@ifm.ac.tz

Abstract

This study specifically aimed to determine the effects of access control on reducing cybercrimes. Since much research has yet to be done to evaluate how privacy, data integrity, and access control affect the overall decline in cybercrimes, this study is conducted to help telecommunication companies employ and strengthen access control measures to safeguard company and customer information. This study employed a quantitative research approach, and the data collected were analysed using regression analysis techniques. Data was collected through questionnaires in a Likert-scaled form and in-depth interviews. The sample size of this study was 199 employees from the selected companies. The data collected was analysed using both qualitative and quantitative techniques. The findings show that the general correlation between independent and dependent variables is 0.01, whereby specific consideration shows that Access Control (AC) had a correlation of .117, which was significant at .004. The correlation analysis confirms a positive and significant relationship between access control and the reduction of cybercrimes since the p-value was <.005. This study concludes that despite the roles played by the access control mechanisms provided by telecommunication companies, there is a need to enhance both internal and external control measures, such as strengthening the security policies to impose severe sanctions on individuals who try to tamper with the information systems of the telecommunication companies. Hence, this study recommends the provision of more awareness to the user of information systems both within and outside the telecommunication companies because data breaches happen either through internal or external sources; hence, it is essential that training, education, and other means to enhance knowledge about cybercrimes should be implemented.

Keywords: *Data, Encryption, Privacy, Access Control, Cybercrimes.*

1.0 INTRODUCTION

Development of technology, progress and the increase in information flow impact the development of organisations and require rapid changes in their information systems (Mbawala et al.,2021; Mhina et al.,019). An enterprise must develop a security framework that secures the information system against internal and external threats (Semlambo et al.,2022). Information system protection requires the creation of a high-level model independent from the software, satisfying the need for protection and security of a system (Kozhusk et al.,2019).One of the basic concepts of protection models is access control which is used within the organisation to limit the actions or operations that the system's users can execute.The access control based on role concept represents an exciting alternative to traditional systems of Discretionary Access Control (DAC) type or Mandatory Access Control (MAC) type. Role-Based Access Control (RBAC) model based on a role concept defines the user's access to information based on activities that the user can perform in a system (G Ducornaud, 2023).

Companies set security policies for information systems to determine that it is necessary to define for each user a set of operations that it could perform, and this set of permissions should be defined for each system's user (Semlambo et al.,2022). It suffices to determine the permissions for executing particular methods on each object accessible for that user. There is a need to create a tool designated mainly for security administrators who could manage one of the security aspects of information systems, namely the control of users' access to data stored in a system (U Tariq, 2023) In Tanzania, cybercrimes are still a problem which requires immediate attention (Mtakati, B. ., & Sengati, F. (2021). The trends show that there is an increase in cybercrimes where digital technologies are increasingly integrated into daily lives, ensuring cybersecurity has become paramount (Pallangyo, 2022).

The rapid growth of internet use in Tanzania has brought numerous benefits, including improved communication, access to information and enhanced economic opportunities (Mnyawi et al., 2022). However, it has also exposed individuals and organisations to various cyber threats and vulnerabilities. The common cyber threats in Tanzania, such as viruses, malware and ransomware, pose significant threats. They can infiltrate a system, compromise data integrity and disrupt operations, leading to financial losses, reputation damage and operational downtime for individuals and organisations. To deal with challenges posed by cybercrimes, access control is a crucial choice to safeguard the privacy of the user of information systems, limiting access and controlling unauthorised access to information systems and ensuring data integrity. Therefore, this study is

DOI: https://doi.org/10.59645/tji.v3i1.134

conducted to assess the effects of access control on reducing cybercrimes in selected telecommunication companies in Tanzania.

2.0 LITERATURE REVIEW

This section discusses the literature related to information security and access control and associated frameworks. First, it presents definitions of essential concepts, followed by the theories associated with the study.

2.1 Definition of key concepts

i. Access control

According to (Kupuswamy et al., 2017), access control is the process of controlling who has access to what resources or places within a system, network, building, or organisation. It is vital to physical and digital security, protecting assets, maintaining data integrity and privacy, and protecting sensitive data (Ilbiz & Kaunert, 2022). Access control Systems are employed in various settings, such as computer networks and other information systems.

Access control allows the user's responsibilities and possibilities in a system to be defined. It can define what a user can do directly and what programs executing on behalf of the user are allowed to do. Access control limits the activities of successfully authenticated users based on the security constraints defined at the conception and administration levels. The access control approach consists of two components: a set of access policies and access principles that determine the possible access of the system's users to data and information stored in a system using the access modes and a set of control procedures (security mechanisms) that allow to verify the access requests sent by system's users in agreement with defined principles and rules; these access requests may be allowed, denied or modified.

ii. The Internet of Things

IoT describes devices with sensors, processing ability, software and other technologies that connect and exchange data with other devices and systems over the Internet or other communications networks (Gillis, Alexander 2021). The IoT encompasses electronics, communication and computer science engineering. IoT has been considered a misnomer because devices do not need to be connected to the public Internet; they only need to be connected to a network and be individually addressable.

2.1 Theoretical Review

The Routine Activity Theory (RAT). This theory was founded by Cohen and Felson in 1979 and is based on three elements that determine a crime situation guided by this study: a motivated offender, a suitable target, and the absence of a capable guardian. Even though, in this theory, the explanation of crime is rated physical, the same crime approach can be committed online using a computer (Kigerl, 2012). RAT has evolved with the progress of technologies that shifted traditional crimes to virtual territories (cybercrimes), especially with the development of the Internet and social networks (Krasznay & Hámornik, 2018). Researchers such as Kumar et al. (2016) focus more on guardianship victimisation, which is the inability of a victim to make rational decisions regarding his protection against cyberattacks. Guardianship focuses on any careless control over potential victims. This theory is applicable in this study because it addresses issues such as privacy, which is the right to prevent unauthorised intrusion into personal information, hence guaranteeing the protection of information systems (Leukfeldt et al., 2017).

The protection of citizen privacy in the investigation and prosecution of cybercrime is a big concern since the right to privacy is protected under many national constitutions and an element of various legal traditions. Access control is about the limitation of acts which cause impersonation, cyber harassment and violent victimisation. User identity cybercrimes are associated with online identity theft, consumer fraud, and phishing. Also, there is online harassment and cyber impersonation, which affects the user of information security or internet systems (Miranda, 2018). Cybercrimes occur over digital devices like cell phones, computers and tablets. They can happen through SMS, Texts and Apps or online in social media, forums or gaming where people can view, participate in or share content. Routine activity theory is used to address cybercrimes within Social Networking Sites (SNS) by reviewing the activities within the SNS that can contribute to any risk of experiencing cybercrimes.

2.2 Empirical Review on Access controls

Employees in a company should only be able to use resources at will. The rules and tools known as access control determine which resources can be accessed by authorised users. Businesses select the best access control model based on infrastructure, security requirements, and other factors (Erin Risk, 2021). Access control allows a subject (user/human) to be identified and given permission to access an object (data/resource) in accordance with the task at hand. These controls are implemented to ensure that subjects can only access objects through safe, permitted methods and prevent unauthorised access to resources. You can manage your assets more effectively by placing

DOI: https://doi.org/10.59645/tji.v3i1.134

access control systems that work for your company (Robert Townsend, 2018).

Access control is a system that allows an authority to control access to zones and resources of a given installation. It ensures confidentiality in such a way as to ensure that information is only accessible to those authorised; it also assumes integrity in such a way that the data are indeed those believed to be. Most of recent proposals have addressed the problem of access control using centralised approaches where a central entity is responsible for managing the authorisation mechanisms, allowing or denying requests from external entities. However, end-to-end security between devices and any Internet host cannot be achieved in these approaches. However, traditional access control models must meet the requirements imposed by IoT scenarios, introducing a lack of flexibility, scalability and usability in environments with billions of devices. These problems could be solved by a distributed approach in which "things" are able to make authorisation decisions without delegating this process to a different entity (Y. Andaloussi et al., 2018).

A study on fine-grained IoT access control methods integrating attribute-based encryption and blockchain presented blockchain-based attribute-based encryption (ABE) and IoT data access control methods (Lu et al., 2021). To provide fine-grained access control that guarantees and ensures IoT data's security and transparency, symmetric encryption and ABE algorithms are used. Additionally, distributed storage is paired with blockchain technology to address the storage bottleneck in blockchain systems. The only information on the blockchain is the data's hash values, the cypher text's location, the access control policy, and other pertinent data. Access control is implemented in this system using the smart contract. The results of experiments demonstrated that the proposed scheme can effectively protect the security and privacy of IoT data and realise the secure sharing manner of data (Dey, Nilanjan et al. 2018).

Many challenges exist in designing access control solutions for the IoT. These challenges include addressing identities of things issued in the IoT, utilising relationships for access control, supporting policies' specification and automation, resolving interoperability issues, integrating blockchain with access control, overcoming resource constraints on IoT devices and ensuring the security of the access control process in the IoT. The development of new scalable schemes for identities of things, enabling novel multi-factor authentication methods for security, utilisation of relationships for authentication and access control, and resolving interoperability issues by standardisation is desired to fulfil access control requirements in the IoT (Ragothaman K et al. 2023).

Mahmood et al. (2019) assessed a secured cloud computing system using an encryption and access control model. Cloud computing provides information technology services on the Internet, such as software, hardware, networking, and storage. These services can be accessed anywhere at any time on a pay-per-use basis. However, storing data on servers is a challenging aspect of cloud computing. This paper utilises cryptography and access control to ensure the confidentiality, integrity, and proper control of access to sensitive data. This study proposes a model that can protect data in cloud computing. The model was designed using an enhanced RSA encryption algorithm and a combination of a role-based access control model with extensible access control markup language (XACML) to facilitate security and allow data access.

Security is one of the primary concerns and a major barrier to adopting cloud computing. Cloud computing may suffer from conventional distributed systems' security attacks such as malicious code (Viruses, Trojan Horses), back door, Man-in-the-Middle attacks, Distributed Denial-Of-Service (DOS) attacks (Wang, 2011), insecure application programming interface, abuse and nefarious use of cloud computing and malicious insiders (Dan et al., 2010). Cloud services could be inaccessible due to these attacks and generate negative impacts. It is an essential and primary requirement for cloud service providers to ensure their services are fully usable and available at all times (Wang et al., 2009).

Khalaf and Kadi (2017) studied access control and data encryption for database security. This study noted that with the vast amount of data generated nowadays, organising and managing it is very important to allow users to access, retrieve, and update their data using database systems (DBS). Most organisations use DBS to increase efficiency and productivity, but security threats are becoming more dangerous to the DB. So, data protection by keeping it integrated and secured from any undesirable intrusion became the highest priority for these organisations. Database security is an important goal of any data management system.

Indu Kashyap (2013) argued that Database security is based on three important constructs: confidentiality, integrity and availability, and that access control maintains a separation between users on the one hand and various data and computing resources on the other. There are three main models of access control: The DAC model governs the access to data based on the user's identity predefined rules but is vulnerable to Trojan horse attacks. MAC models govern users' access to data based on their assigned classifications but are too rigid for some environments. RBAC models

DOI: https://doi.org/10.59645/tji.v3i1.134

regulate access based on roles users play in a system. Roles are actions or responsibilities associated with a particular working activity. RBAC makes permissions management easier and supports the principle of least privilege, separation of duties, etc. All the models are imperfect and have vulnerabilities; thus, they must be chosen according to the needs of organisations.

3.0 METHODOLOGY

This section presents the methodology that was used to conduct this research. This section discusses the following: research approach, study area, targeted Population, sample size and sampling techniques, data collection, validity and reliability, data analysis and ethical considerations.

3.1 Research Approach

This study employed a quantitative approach in which data was collected through questionnaires in a Likert scale form, and the collected data were analysed using descriptive statistics and multiple regression analysis using SPSS Software. The nature of the study's objectives influenced the choice of approach.

3.2 Study Area

Selecting an area of study is essential since it influences the usefulness of the information produced (Kothari, 2004). This study in Dar es Salaam involved selected telecommunication companies (Vodacom Tanzania and Airtel). These companies have been selected because they have large numbers of customers whose data and other information have been collected to facilitate the use of services provided. Also, they have been using encryption services to secure their data; hence, they can provide reliable information about criminal data encryption to reduce criminal activity and provide valid and reliable data.

3.3 Targeted Population

Population is the total number of individuals, elements, households, or groups that are to be studied by the researcher (Cooper & Schindler, 2003). The target population of this study was 555 staff members of (Vodacom and Airtel).

3.4 Sample Size

The sample size is the number of items selected from a population to be sampled for the study (Kothari, 2013). In this study, the researcher obtained the sample size of 232 through the Yamane

formula as follows: n = $\frac{N}{1+N(e)^2}$; where N = Population (555); n = Sample Size; e = Error term (0.05); Hence yielding n = $\frac{555}{1+555(0.05)^2}$ = 232.2. Therefore, the sample size of this study was 232 employees from the selected companies.

3.5 Data Collection and Analysis Methods

While the distributed questionnaires were 232, the returned questionnaires were 205, equivalent to an 88.4% return ratio. Furthermore, the returned questionnaires were subjected to data screening. Six questionnaires were dropped due to incomplete data and lack of respondents' engagement, resulting in 199 clean questionnaires, equivalent to 85.8%, which is high enough for data analysis. The remaining 199 questionnaires were analysed based on quantitative data analysis methods using statistical software called Statistical Package for Social Science (SPSS) version 29.0.1. They were presented using descriptive statistics showing means and standard deviation. Also, the researcher employed multiple regression analysis techniques to examine the relationship between research variables by adopting the following regression model.

$$\boldsymbol{Y = \alpha + \beta_1 x_1 + \beta_2 x_2 + .. \beta_n x_n + \varepsilon} \text{.....eq1}$$

Then,

$$\boldsymbol{Y = \alpha + \beta_1 AC + \varepsilon} \text{.....eq2}$$

Where,

Y = Reduction of Cybercrimes

α = Constant

ε = Standard Error.

AC = Access Control

4.0 RESULTS ND DISCUSSIONS

4.1 Results

Table 1 presents the results of the demographic characteristics of the respondents. The results show that 66.3% of the respondents in this study were male, while 33.7% were female. These findings imply the effective participation of male respondents compared to females. However, the researcher ensured that both genders participated despite their difference in participation rates. Table 1 also shows that 27.6% of the respondents were aged 18 – 25, 49.7% were aged 25-50, and 22.6% were 50 years and above. These findings show that the distribution of the respondents based on their age aimed to examine the maturity level of respondents and that all the respondents were

DOI: https://doi.org/10.59645/tji.v3i1.134

the age capable of forming a well-reasoned opinion based on the problem being studied. Also, this demographic analysis shows that on the level of education, it was revealed that 17.6% of the respondents had a certificate level of education, 39.2% of the respondents had a diploma, 26.6% of the respondents had a bachelor's degree, and 16.6% of the respondents had the master degree and above.

Table 1 Demographic Characteristics of the Respondents

Character	Category	Frequency	Per cent
Gender	Male	132	66.3
	Female	67	33.7
Age Category	18-25 years	55	27.6
	25-50 years	99	49.7
	Over 50 years	45	22.6
Highest Educational Level	Certificate	35	17.6
	Diploma	78	39.2
	Bachelor's degree	53	26.6
	Master's degree and above	33	16.6
Working Experience	1-5 years	83	41.7
	6-15 years	54	27.1
	Above 16 years	62	31.2

On the working experience, Table 1 shows that 41.7% of the respondents had 1 – 5 years of working experience in telecommunication companies, 27.1% of the respondents had working experience of between 6 – 15 years, and 31.2% of the respondents had working experience of 15 years and above in telecommunication companies. Generally, from these findings, it can be established that the respondents who participated in this study possessed qualities required by the respondents to enable data collection since they had enough level of education, they had enough working experience and other characteristics which were necessary for them to provide valid and reliable information needed for this research study.

Descriptive Statistics on the Effects of Access Control on Reduction of Cybercrimes

This study aimed to assess the effects of access control on the reduction of cybercrimes, whereby a Likert-scaled questionnaire was employed to collect quantitative data. The researcher employed descriptive statistics, which show Mean and Standard Deviation (SD) values as presented in Table 2.

Table 2. Effects of Access Control on Reduction of Cybercrimes

Access Control	Mean	SD
It helps to manage who is authorised to access corporate data and resources.	3.79	1.070
Access control uses policies that verify that users are who they claim to be.	3.73	1.290
ensures appropriate control access levels are granted to users.	3.84	1.120
Access control allows determining circumstances under which certain data, apps, and resources may be accessed.	3.87	1.054
Access control policies provide general protection of digital spaces.	3.81	1.078
Access control puts a little more control back into leadership's hands	4.02	1.082

The results obtained through descriptive statistics (See Table 2) show the perception of respondents' effects of access control to enhance the reduction of cybercrimes. The determinants of access control show that management of who is authorised to access corporate data and resources had Mean = 3.79 and SD = 1.070. Also, policies that verify users are who they claim to be had Mean = 3.73 and SD 1.290; Ensuring appropriate control access levels are granted to users had Mean = 3.64 and SD = 1.120; Determining circumstances under which certain data, apps, and resources may be accessed, had Mean = 3.87 and SD = 1.054; Access control policies providing general protection of digital spaces had Mean = 3.81, and SD = 1.078; and Access control puts more control back into leadership's hands as mean = 4.02 and SD = 1.082. The results obtained in the section indicate that respondents think access control is a crucial aspect of reducing cybercrimes.

DOI: https://doi.org/10.59645/tji.v3i1.134

Linearity Test

The linearity test is a statistical test used to determine if there is a linear relationship between the independent and dependent variables. It is a test confirming the presence of a straight line, a form of the regression equation (Y = a + bx). In this form of equation, Y is regarded as the dependent variable, x is the independent variable, a – is the constant or slope of the equation, and b is the coefficient of correlation.

Table 3 Pearson Correlation

		RC	AC
Reeducation of Cybercrimes (RC)	Pearson (r)	1	
	Sig. (2-tailed)		
	N	199	
Access Control (AC)	Pearson (r)	0.117	1
	Sig. (2-tailed)	0.004	
	N	199	199
**. Correlation is significant at the 0.01 level (2-tailed)			

Table 3 shows that Access Control (AC) correlates at 0.117, significant at .004. The correlation analysis confirms a positive and significant relationship between the independent and dependent variables since the p-value was <.005. Hence, the findings of this study confirm that access control reduces cybercrimes in the selected telecommunication companies.

Reliability Tests

A reliability test measures the degree to which a particular measuring procedure gives similar results over several repeated trials. Reliability in this research was conducted by using Split-Half methods in which a Cronbach Alpha Coefficient was measured and presented in Table 4

Table 4 Reliability Tests

Variables	Cronbach's Alpha	Remark
Access Control	0.764	Reliable
Privacy Protection	0.803	Reliable
Data Integrity	0.812	Reliable

Source: Field Data (2023)

Table 4's findings indicate that the Cronbach Alpha coefficient ranged from 0.764 to 0.812 at its

lowest and highest values, respectively. This demonstrates that the data produced increased reliability, allowing the researcher to proceed with more analysis steps. Typically, for research to be considered reliable, the Cronbach Alpha coefficient in the reliability test must be at least 0.7.

Linear Regression

Finally, the researcher performed a linear regression to confirm access control's effects on reducing cybercrimes in telecommunication companies. This study used one Independent variable, namely Access Control, while the dependent variable was the reduction of cybercrimes in selected Telecommunication Companies.

Table 5 Model Summary

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	Durbin-Watson
1	.722[a]	.673	.561	1.263	1.886

The initial regression results usually intend to confirm the model acceptance variables. Table 5 above shows that the variable AC factor loading of .722 is approximately 72%, which explains the regression equation. The R-Square value was loaded at 0.673 (67%) and adjusted R-Square at .561 (56%). The results mean that the three variables explain about 56% of the variance in the dependent variable, which means additional factors outside the suggested ones could explain the remaining percentage.

Table 6 ANOVA

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	116.564	3	38.855	24.353	0.000[b]
	Residual	311.124	195	1.596		
	Total	427.688	198			

Analysis of Variance (ANOVA) was performed to testify to the interaction effects between variables within the group and to confirm and relate the mean values of the variables (See Table 6). The F-test was run concurrently in the SPSS to confirm further analysis within and between groups of variables. The F–test was 24.353, statistically significant as the p-value was 0.000. This confirms the presence of a significant relationship between access control and the reduction of cybercrimes in telecommunication companies.

DOI: https://doi.org/10.59645/tji.v3i1.134

Table 7 Coefficients

Model		Unstandardised Coefficients		Standardised Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.331	0.379		3.507	0.001
	AC	0.055	0.065	0.053	0.841	0.002

Source: Field Data (2023)

Table 7 shows the final regression results, which can be summarised as follows;

$Y = 1.331 + .055AC + \varepsilon$

The linear regression aimed to establish a relationship between access control and reduction of cybercrimes (RC), and the results obtained were that AC had Beta =0.053, p<.002. This means a positive relationship exists between access control and reduction of cybercrimes. These findings imply that cybercriminals target telecommunication companies because they intend to earn money through this process. Thus, telecommunication companies employ access control to enhance secure data storage or transmission. It is used with authentication services to ensure that access is only provided to authorised users.

Therefore, access control provides an additional layer of protection for this data and helps maintain the confidentiality of the information. Encryption is used also to verify that the data has not been tampered with during storage or transmission. This is achieved through message authentication codes, ensuring the data is not altered.

4.2 Discussion of Results

This study examined the effects of access control on reducing cybercrimes. The regression results revealed that access control is significant, with a p-value less than .005, and the discussion is further elaborated with the support of literature to clarify results as follows: Access Control (AC) was statistically significant in the regression results. Increasing access control mechanisms to information systems used by telecommunication companies may help reduce cybercrimes. This is supported by Lu et al. (2021), who suggested that the access control scheme that combines attribute-based encryption and blockchain technology also limits access to information by

unauthorised persons in the information system. Also, systematic encryption is utilised to realise fine-grained access control and ensure the security and openness of IoT data in the same way Malhood et al. (2019) pinpointed that access control ensures confidentiality and proper access to sensitive data; this is because storing data in the information systems and servers is challenged by the aspect of clouding computing and social engineering. Thus, to ensure access control, it is essential to design an entrusted encryption algorithm and a combination of role-based access controls to facilitate security and limit data access.

5.0 RESULTS ND DISCUSSIONS

5.1 Conclusion

The findings of this study imply that telecommunication companies can increase their commitment to data security through access control and enhance collaboration with regulatory authorities to provide a more constructive and cooperative relationship, potentially resulting in benefits such as reduced regulatory scrutiny. The research findings imply that effective access control can act as a deterrent for cybercriminals. If they think extracting valuable information from a telecommunication company's system is difficult or nearly impossible, they may be more inclined to target easier, less secure targets. The research obtained in this study encourages more innovation and more convenient access control mechanisms, which can reduce cybercrimes. This can stimulate more development in advanced access control techniques and technologies.

5.2 Recommendations

Firstly, despite the roles played by the access control protocols provided by telecommunication companies, there is a need to enhance both internal and external control measures, such as strengthening the security policies to impose severe sanctions on individuals who try to tamper with the information systems of telecommunication companies. Secondly, this study recommends the provision of more awareness to the user of information systems both within and outside the telecommunication companies because data breaches happen either through internal or external sources; hence, it is essential that training, education, and other means to enhance knowledge about cybercrimes should be implemented. Since technology tends to evolve and change to become more sophisticated, telecommunication companies must invest many resources in adopting more up-to-date information systems that accommodate more protective features to guarantee maximum cyber security, which will also help reduce cybercrimes.

DOI: https://doi.org/10.59645/tji.v3i1.134

REFERENCES

A. Poniszewska-Marada, September 2010. Platform for access control management in information system based on extended RBAC model, IEEE Computer Press, Proceedings of the 12th IEEE International Symposium on Symbolic and Numeric Algorithms for Scientific Computing, Timisoara, Romania.

A. Poniszewska-Maranda, 2006. Access Control Coherence of Information Systems Based on Security Constraints, Proc. of 25th International Conference on Computer Safety, Security and Reliability, LNCS, Springer-Verlag.

Anuradha, M., Loganathan, S., Suseela, G., Selvan, M.P. and Nalini, M., (2023). June. Hybrid Multiple Cryptography for Data Encryption. In 2023 8th International Conference on Communication and Electronics Systems (ICCES) (pp. 596–603). IEEE.

Choi, K.S., Scott, T.M. and LeClair, D.P., 2016. Ransomware against police: diagnosis of risk factors via application of cyber-routine activities theory. International Journal of Forensic Science & Pathology. 4(7), 253-258.

Dey, N.; Hassanien, Aboul Ella; Bhatt, Chintan; Ashour, Amira; Satapathy, Suresh Chandra, eds. (2018). Internet of things and big data analytics toward next-generation intelligence.

Hidayat, T. and Mahardiko, R., 2020. A Systematic literature review method on AES algorithm for data sharing encryption on cloud computing. International Journal of Artificial Intelligence Research, 4(1), pp.49-57.

Ilbiz, E. and Kaunert, C., 2022. Europol and cybercrime: Europol's sharing decryption platform. Journal of Contemporary European Studies, 30(2), pp.270-283.

Khalaf, E.F. and Kadi, M.M., 2017. A survey of access control and data encryption for database security. Journal of King Abdulaziz University, 28(1), pp.19-30.

Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. Social Science Computer Review, 30(4), 470–486.

Krasznay, C., & Hámornik, B. P. (2018). Analysis of cyberattack patterns by user behaviour analytics 1. Academic and Applied Research in Military and Public Management Science, 17(3), 101-113.

Kumar, S., Kandasamy, S., & Deepa, K. (2016). On privacy and security in social media– A comprehensive study. Procedia Computer Science, 78, 114-19.

Kuppuswamy, P., Banu, R. and Rekha, N., 2017, March. Preventing and securing data from cybercrime using new authentication methods based on block cypher schemes. In 2017, the 2nd International Conference on Anti-Cyber Crimes (ICACC) (pp. 113-117). IEEE.

Kozhusko, O., Khaminich, S., & Alieksieieva, S. (2019). Information system protection as a factor in maintaining the leading positions in the enterprise development. In 3rd International Conference on Social, Economic, and Academic Leadership (ICSEAL 2019) (pp. 428-432). Atlantis Press.

Lara-Nino, C.A., Diaz-Perez, A. and Morales-Sandoval, M., 2018. Energy and area costs of lightweight cryptographic algorithms for authenticated encryption in WSN. Security and Communication Networks, 2018.

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017). Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks. The British Journal of Criminology, 57(3), 704-722.

Lu, X., Fu, S., Jiang, C. & Lio, P. (2021). A fine-grained IoT data access control scheme combining attribute-based encryption and blockchain. Security and Communication Networks, 2021, pp.1–13.

Mbawala, Z. R., & Mhina, J. R. A.(2021). The Influence of Information Communication Technology System on Performance of Weights and Measures Agency in Tanzania.

Mahmood, G.S., Huang, D.J. & Jaleel, B. (2019). A secure cloud computing system by using encryption and access control model. Journal of Information Processing Systems, 15(3), 538–549.

Mhina, J. R. A., Md Johar, M. G., & Alkawaz, M. H. (2019). The influence of perceived confidentiality risks and attitude on Tanzania government employees' intention to adopt web 2.0 and social media for work-related purposes. International Journal of Public Administration, 42(7), 558-571.

Miranda, M. J. (2018). Enhancing cybersecurity awareness training: A comprehensive phishing exercise approach. International Management Review, 14(2), 5-10.

Mnyawi, R., Kombe, C., Sam, A. and Nyambo, D., 2022. Blockchain-based Data Storage Security Architecture for e-Health Care Systems: A Case of Government of Tanzania Hospital Management Information System. IJCSNS, 22(3), p.364.

Mtakati, B. ., & Sengati, F. (2021). Cybersecurity Posture of Higher Learning Institutions in Tanzania. The Journal of Informatics, 1(1). https://doi.org/10.59645/tji.v1i1.1

Munjal, K. and Bhatia, R., 2022. A systematic review of homomorphic encryption and its contributions in the healthcare industry. Complex & Intelligent Systems, pp.1-28.

National Research Council. (1930). Computers at risk: Safe computing in the information age.

Ragothaman K, Wang Y, Rimal B, Lawrence M. (2023). Access Control for IoT: A Survey of Existing Research, Dynamic Policies and Future Directions. Sensors. 23(4):1805. https://doi.org/10.3390/s23041805

Semlambo, A., Lubua, E. W., & Mkude, C. (2022). Information Systems Security Policy Framework for enhanced ICT Governance in Public Institutions of Tanzania. The Journal of Informatics, 2(1), 54-68

Younis A. Younis, Kashif Kifayat, Madjid Merabti, 2014. An access control model for cloud computing, Journal of Information Security and Applications, Volume 19, Issue 1, Pages 45-60, ISSN 214-2126, https://doi.org/10.1016/j.jisa.2014.04.003.

Zhang, L., Xu, J., Vijayakumar, P., Sharma, P.K. and Ghosh, U., (2022). Homomorphic encryption-based privacy-preserving federated learning in IoT-enabled healthcare system. IEEE Transactions on Network Science and Engineering