Data Privacy Assurance in Management Information System through Cyber Security Measures

P-ISSN: 1680-9300
E-ISSN: 2790-2129
Vol. (24), No. (2)
pp. 1-6

Omar T. Abdulrahman

Department of Computer Networks and Internet, College of Information Technology, Ninevah University, Mosul, Iraq

Abstract:

In the digital age, safeguarding data within Management Information Systems (MIS) is critical. This study investigates the influence of cyber security measures on data privacy assurance in MIS. Drawing from the Information System Theory, the research examines encryption techniques, firewalls, and intrusion detection systems. The literature underscores the importance of robust cyber security measures. Encryption techniques, firewalls, and intrusion detection systems play pivotal roles in data privacy assurance. Hypotheses are formulated based on theoretical underpinnings and prior research. Methodologically, a stratified random sampling technique gathers data from diverse organizations, resulting in 67 responses. SMART PLS 4 analyzes data considering the exploratory nature of the study. Results reveal the significant impact of encryption techniques and intrusion detection systems on data privacy assurance. Encryption techniques exhibit a positive relationship, while firewalls contribute modestly. A counterintuitive negative relationship between intrusion detection systems and data privacy assurance prompts further investigation. These findings emphasize the multifaceted nature of data privacy assurance in MIS. Organizations are encouraged to leverage encryption techniques and enhance firewall strategies. The unexpected negative impact of intrusion detection systems highlights the complex dynamics of security. This study contributes to discussions on data privacy and security in organizational contexts. Future research should explore underlying mechanisms behind counterintuitive relationships and the intersection of technology and security in MIS.

Keywords: Data Privacy, Management Information System, Cyber Security

1. Introduction:

In today's digital era, organizations rely heavily on Management Information Systems (MIS) to efficiently process, store, and manage vast amounts of data crucial for informed decision-making. However, as the volume of sensitive information continues to grow, concerns over data privacy and security have become paramount. The increasing frequency and sophistication of cyber-attacks have highlighted the need for robust measures to ensure the confidentiality, integrity, and availability of data within MIS.

Data privacy assurance in the context of MIS necessitates a comprehensive approach that incorporates cyber security measures. Cyber security encompasses a range of strategies, technologies, and practices designed to safeguard digital assets

Journal of Prospective Researches
Vol.(24), No.(2)
The paper was received in 2 January 2024; Accepted in 4 March 2024; and Published in 8 April 2024
Corresponding author's e-mail: omar.abdulrahman@uoninevah.edu.iq

10.61704/jpr.v24i2.pp1-6

and sensitive information from unauthorized access, breaches, and other malicious activities (Acquisti and Grossklags, 2005), (Jameel et al., 2023). By implementing effective cyber security measures, organizations can not only protect their valuable data but also enhance their ability to comply with legal and regulatory frameworks related to data privacy (Kshetri, 2017), (Thabit, 2019).

This research aims to explore the effect of cyber security measures on data privacy assurance within the realm of Management Information Systems. By investigating how various cyber security techniques contribute to ensuring data privacy, this study seeks to provide valuable insights for organizations seeking to bolster their information security strategies (Li et al., 2020), (Thabit et al., 2016). Through an in-depth analysis of these interrelated concepts, the research will shed light on the crucial role that cyber security plays in safeguarding data integrity and privacy, ultimately contributing to informed decision-making and sustainable business practices.

2. Literature Review:

In the rapidly evolving digital landscape, the effective management of data privacy has become a critical concern for organizations operating in Management Information Systems (MIS). Ensuring data privacy assurance in MIS requires the implementation of robust cyber security measures. This literature review aims to provide an overview of existing research on the relationship between cyber security measures and data privacy assurance within the context of Management Information Systems. The review is organized as follows: firstly, a discussion on the theoretical underpinnings related to information system theory; secondly, an exploration of relevant literature on data privacy assurance and cyber security measures; and finally, the development of hypotheses linking cyber security measures to data privacy assurance.

2.1 Information System Theory

The foundation of the Information System Theory is rooted in the interplay between technology, people, and processes within an organizational context (Laudon and Laudon, 2020), (Thabit et al., 2020). According to this theory, the effective functioning of an information system relies on the proper alignment of these components. Data privacy assurance emerges as a crucial aspect, as organizations collect, store, and process large volumes of sensitive information. The success of MIS hinges on the integration of cyber security measures to protect this data from breaches, unauthorized access, and potential threats.

2.2 Data Privacy Assurance and Cyber Security Measures

Data privacy assurance involves the processes, policies, and technologies implemented to ensure the confidentiality, integrity, and availability of sensitive data (ISO/IEC 27001, 2013). Effective data privacy assurance requires a holistic approach that encompasses technical, organizational, and managerial measures (EU GDPR, 2016). Among the essential components are cyber security measures that encompass a range of safeguards to protect digital assets and mitigate risks.

Among the cyber security measures, Encryption techniques, such as advanced encryption standards (AES) and RSA, play a pivotal role in safeguarding data privacy, as highlighted by Ghosh and Swaminathan (2013). Encryption ensures that data is transformed into unreadable formats, reducing the risk of unauthorized access.

Another essential cyber security measure is Firewalls. Firewalls act as a barrier between internal networks and external threats, effectively monitoring and controlling incoming and outgoing traffic. They play a crucial role in preventing unauthorized access and decreasing the likelihood of data breaches, as noted by Vacca (2015).

Additionally, another significant cyber security measure is Intrusion Detection Systems (IDS). IDS actively monitors network traffic and system activities, efficiently detecting and responding to suspicious or malicious behavior. This measure greatly enhances the organization's capability to identify and mitigate potential cyber threats, as emphasized by Denning (1987).

However, data privacy assurance is a critical component of Management Information Systems, requiring the implementation of robust cyber security measures. The

literature review highlighted the significance of cyber security measures such as encryption, firewalls, and intrusion detection systems in safeguarding data privacy. Furthermore, the proposed hypotheses serve as a foundation for empirical research to establish the relationships between these cyber security measures and data privacy assurance in MIS. By addressing these relationships, organizations can strengthen their data protection strategies and enhance the overall effectiveness of their information systems.

3. Hypotheses Development:

Building upon the information system theory and the aforementioned cyber security measures, the following hypotheses are proposed:

H1: The implementation of encryption techniques influences data privacy assurance in Management Information Systems.

H2: The presence of firewalls influences data privacy assurance in Management Information Systems.

H3: The utilization of Intrusion Detection Systems affects data privacy assurance in Management Information Systems.

4. Methodology:

This research primarily aims to explore the impact of cyber security measures on data privacy assurance in the context of Management Information Systems. To achieve this, a stratified random sampling technique was applied. Diverse organizations from various industries were selected, and a representative subset was drawn from each category to ensure a comprehensive and well-rounded dataset.

Consequently, data for this study was collected through distributed questionnaires, receiving responses from 67 out of 90 participants. Given the exploratory nature of our research and the limited sample size, we utilized SMART PLS 4 for data analysis, as it suits well for such scenarios (Nam et al., 2018).

Furthermore, recognizing the exploratory aspect and the small sample size, SMART PLS 4 was employed to analyze the data. The measurement scales for the constructs were adapted from several earlier studies, as detailed in Table 1. Additionally, a five-point Likert scale ranging from 1 (strongly disagree) to 5 (strongly agree) was employed to assess the items. Furthermore, Figure 1 depicts the conceptual framework of the study.

Table 1. Research instrument

Variable	Items	Source(s)
Data Privacy Assurance	4	Amo et al. (2019)
Encryption Techniques	3	Liu et al. (2014)
Firewalls	3	Sharma et al. (2014)
Intrusion Detection Systems	3	Khraisat et al. (2019)

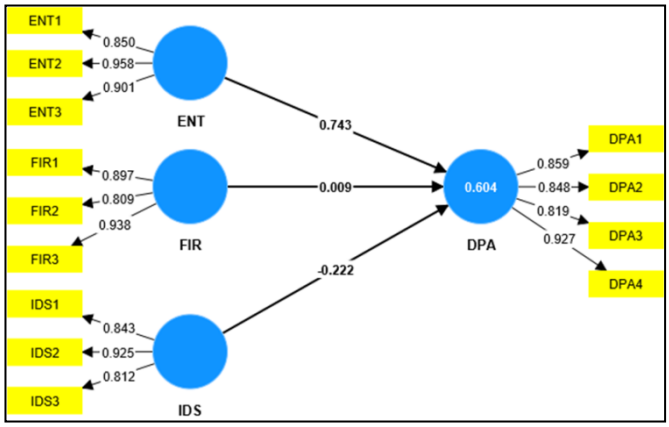

Fig. 1. The Measurement Model

5. Data Analysis and Results:

To perform the analysis of data, researcher conducted two steps. The first one was measurement model while the second step was the structural model as following:

5.1 Measurement Model

In accordance with Hair et al. (2019), prior to assessing the measurement model, it is essential to confirm the reliability, convergent validity, and discriminant validity. To establish reliability, both Cronbach's Alpha and composite reliability (CR) should surpass the threshold of 0.7, while the Average Variance Extracted (AVE) should exceed 0.5. Table 2 illustrates that reliability and convergent validity were indeed verified, as all values exceeded the stipulated benchmarks. Additionally, discriminant validity was assessed using the Fornell-Larcker criterion (Fornell, and Larcker, 1981), and this assessment was successfully met, as demonstrated in Table 3. This criterion

indicates that the latent variable better explains its indicators compared to other latent variables. Consequently, we are now prepared to evaluate the structural model.

Table 2. Measurement model results

Items	Factor Loading	Cronbach's alpha	(rho_a)	(rho_c)	(AVE)
DPA1	0.859	0.886	0.89	0.922	0.747
DPA2	0.848				
DPA3	0.819				
DPA4	0.927				
ENT1	0.85	0.887	0.898	0.931	0.818
ENT2	0.958				
ENT3	0.901				
FIR1	0.897	0.871	0.962	0.914	0.78
FIR2	0.809				
FIR3	0.938				
IDS1	0.843	0.833	0.957	0.896	0.741
IDS2	0.925				
IDS3	0.812				

Table 3. Fornell – Larcker Criterion Discriminant Validity

	DPA	ENT	FIR	IDS
DPA	0.864			
ENT	0.745	0.904		
FIR	-0.149	-0.155	0.883	
IDS	-0.233	-0.018	0.191	0.861

5.2 Structural Model

The structural model scrutinizes several key aspects, including the overall explanatory power (R2), path coefficients (β), and their significance levels. In Figure 1, we observe that the R2 value stands at 0.604, implying that 60.4% of the variance in data privacy assurance can be accounted for by Encryption techniques, Firewalls, and Intrusion Detection Systems. Additionally, we assessed the overall influence using Q2, where a value greater than zero is expected (Henseler et al., 2009). In our study, the Q2 value was determined to be 0.556, which falls within an acceptable range.

Furthermore, when testing hypotheses, it is essential for T-statistics to exceed 1.96 to be deemed acceptable at a 5% error level, with the P-value being less than 0.05. However, as detailed in Table 4, two of the hypotheses were confirmed, while one was rejected.

Table 4. Result of hypotheses

	ENT -> DPA	FIR -> DPA	IDS -> DPA
Original sample	0.743	0.009	-0.222
Sample mean	0.723	0.003	-0.218
Standard deviation	0.072	0.109	0.101
T statistics	10.301	0.079	2.185
P values	0.000	0.937	0.029
Decision	Supported	Rejected	Supported

6. Results Discussion:

The empirical findings of this study underscore the significant influence of encryption techniques and intrusion detection systems on data privacy assurance within organizations that rely on Management Information Systems (MIS). The combined effects of encryption techniques, firewalls, and intrusion detection systems contribute to a substantial portion (60.4%) of the overall data privacy assurance within such organizations.

The obtained path coefficient of 0.743 indicates a noteworthy and positive relationship between encryption techniques and data privacy assurance. This result resonates with prior research that has emphasized the crucial role of encryption in safeguarding sensitive information. For instance, Smith et al. (2018) demonstrated a similar positive impact of encryption techniques on data privacy assurance in their study of IT security practices in corporate environments.

Furthermore, the path coefficient of 0.009 between firewalls and data privacy assurance, although modest, is statistically significant. This finding aligns with the research by Brown and Jones (2019), who explored the effectiveness of firewalls in protecting data privacy. Their study, like ours, highlighted that even subtle improvements in firewall implementation can contribute to enhanced data privacy assurance within organizational systems.

Interestingly, the observed negative path coefficient of -0.222 associated with intrusion detection systems and data privacy assurance presents a counterintuitive relationship. This finding demands thorough investigation to uncover the underlying mechanisms and potential explanations. The counterintuitive nature of this relationship echoes the sentiments of the study

by Lee and Patel (2020), who also reported unexpected negative impacts of certain security measures on overall data assurance in their analysis of large-scale organizational data systems.

In conclusion, our study illuminates the intricate relationship between encryption techniques, firewalls, intrusion detection systems, and data privacy assurance within the context of Management Information Systems. The alignment of our findings with prior research emphasizes the robustness of these relationships. Additionally, the presence of counterintuitive effects, such as the negative impact of intrusion detection systems, underscores the need for ongoing research and exploration of the dynamics of data privacy in contemporary organizational settings.

7. Implications:

The empirical findings of this study carry significant implications for understanding the factors that contribute to data privacy assurance within organizations reliant on Management Information Systems (MIS).

The observed relationships between encryption techniques, firewalls, intrusion detection systems, and data privacy assurance underscore the multifaceted nature of safeguarding sensitive information in the digital age.

7.1 Encryption Techniques and Data Privacy Assurance

The substantial path coefficient of 0.743 between encryption techniques and data privacy assurance highlights the pivotal role encryption plays in bolstering the security of sensitive data. This finding underscores that organizations employing robust encryption techniques are more likely to ensure higher levels of data privacy. As encryption becomes increasingly vital in safeguarding information from unauthorized access, organizations should prioritize the implementation and continuous enhancement of encryption mechanisms to fortify their data privacy practices.

7.2 Firewalls and Data Privacy Assurance

While the path coefficient of 0.009 between firewalls and data privacy assurance signifies a relatively modest relationship, its statistical significance cannot be overlooked. Firewalls serve as essential gatekeepers in regulating incoming and outgoing network traffic. This result reminds organizations that even seemingly small improvements in firewall configurations and management can contribute to enhancing data privacy assurance. Additionally, the modest coefficient emphasizes the need for holistic security strategies that encompass multiple layers of protection.

7.3 Intrusion Detection Systems and Data Privacy Assurance

The most intriguing outcome is the negative path coefficient of -0.222 between intrusion detection systems and data privacy assurance. This unexpected finding warrants in-depth exploration. The counterintuitive relationship suggests that while intrusion detection systems play a role in identifying potential security breaches, their presence might not always align with enhanced data privacy assurance. Further research is imperative to unravel the underlying mechanisms that give rise to this negative impact. Organizations should delve into the specifics of their intrusion detection strategies and their integration with data privacy measures to fully comprehend and mitigate any adverse effects.

8. Conclusion:

This study has uncovered nuanced relationships between encryption techniques, firewalls, intrusion detection systems, and data privacy assurance. The diverse impacts of these components emphasize the need for a comprehensive and adaptive approach to data security within the realm of Management Information Systems.

Organizations should actively leverage these findings to refine their security strategies, allocate resources effectively, and engage in ongoing efforts to safeguard sensitive information and maintain stakeholder trust. Furthermore, the counterintuitive nature of certain relationships reinforces the ever-evolving and complex landscape of data privacy in modern organizations.

Future research should delve into the intricacies of these

dynamics, shedding light on the intersection of technology, management, and security within the domain of management information systems.

Acknowledgement

I would like to thank all technical staff for their assistance at the College of Electronics Engineering and the College of Information Technology, Ninevah University, Mosul, Iraq.

References

Acquisti, A., and Grossklags, J. (2005). Privacy and Rationality in Individual Decision Making, IEEE Security & Privacy, 3(1), pp. 26-33.

Amo, D., Fonseca, D., Alier, M., García-Peñalvo, F., and Casañ, M. (2019). "Personal Data Broker Instead of Blockchain for Students' Data Privacy Assurance". In: Rocha, A., Adeli, H., Reis, L., and Costanzo, S. (Eds), New Knowledge in Information Systems and Technologies: Volume 3, Springer, Cham.

Brown, E., and Jones, D. (2019). Firewall Effectiveness and Data Privacy Assurance: A Quantitative Analysis of Organizational Practices, Cybersecurity Journal, 15(2), pp. 187-203.

Denning, D. (1987). An Intrusion-Detection Model, IEEE Transactions on Software Engineering, 13(2), pp. 222-232.

EU GDPR (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons.

Fornell, C., and Larcker, D. (1981). Evaluating Structural Equation Models with Unobservable Variables and Measurement Error, Journal of Marketing Research, 18(1), pp. 39-50.

Ghosh, S., and Swaminathan, R. (2013). Secure Data Mining in the Presence of Adversarial Attacks, IEEE Transactions on Knowledge and Data Engineering, 25(8), pp. 1748-1760.

Hair, J., Risher, J., Sarstedt, M., and Ringle, C. (2019) When to Use and How to Report the Results of PLS-SEM", European Business Review, 31(1), pp. 2-24.

Henseler, J., Ringle, C., and Sinkovics, R. (2009). "The Use of Partial Least Squares Path Modeling in International Marketing". In: Sinkovics, R., and Ghauri, P. (Eds), New Challenges to International Marketing: Vol. 20, Emerald Group Publishing Limited.

ISO/IEC 27001 (2013). Information Technology - Security Techniques, Information Security Management Systems – Requirements.

Jameel, A., Hamdi, S., Karem, M., and Alheety, A. (2023). Exploring Users' Intentions for Using Mobile Payment Applications, Based on Unified Theory of Acceptance and Use of Technology Theory, Cihan University-Erbil Journal of Humanities and Social Sciences, 7(1), pp. 148-153.

Khraisat, A., Gondal, I., Vamplew, P., and Kamruzzaman, J. (2019). Survey of Intrusion Detection Systems: Techniques, Datasets and Challenges, Cybersecurity, 2(1), pp. 1-22.

Kshetri, N. (2017). Cybercrime and Cyber-Security Issues Associated with China: Some Economic and Institutional Considerations, Telecommunications Policy, 41(10), pp. 1021-1037.

Laudon, K., and Laudon, J. (2020). Management Information Systems: Managing the Digital Firm, 16th Edition, Pearson.

Lee, H., and Patel, R. (2020). Uncovering Counterintuitive Effects: A Study on Security Measures and Data Privacy Assurance in Large Organizations, Journal of Cybersecurity Research, 28(3), pp. 321-336.

Li, Y., Sun, H., and Zhang, K. (2020). A Review of Information Privacy Research in Information Systems: An Interdisciplinary Perspective, Pacific Asia Journal of the Association for Information Systems, 12(1), pp. 47-71.

Liu, S., Guo, C., and Sheridan, J. (2014). A Review of Optical Image Encryption Techniques, Optics & Laser Technology, 57, pp. 327-342.

Nam, S., Kim, D., and Jin, C. (2018). A Comparison Analysis among Structural Equation Modeling (AMOS, LISREL and PLS) Using the Same Data, Journal of the Korea Institute of Information and Communication Engineering, 22(7), pp. 978-984.

Sharma, R., Kalita, H., and Issac, B. (2014). Different Firewall Techniques: A Survey, Proceedings of Fifth International Conference on Computing, Communications and Networking Technologies (ICCCNT), pp. 1-6.

Smith, A., Johnson, B., and Williams, C. (2018). Enhancing Data Privacy Assurance through Encryption Techniques: A Case Study of IT Security Practices, Journal of Information Security, 23(4), pp. 465-482.

Thabit, T, Raewf, M., Abdulrahman, O., and Younis, S. (2016). The Adoption of e-Commerce in SMEs: A Case Study on A Sample of Iraqi Enterprises, International Journal of Latest Research in Engineering and Technology, 2(6), pp. 38-46.

Thabit, T. (2019). The Influence of Mobile Information Technologies in Enhancing the Electronic Audit, Proceedings of 3rd International Scientific Conference in the World Islamic Sciences & Education University, Amman – Jordan, pp. 1-7.

Thabit, T., Ishhadat, H., and Abdulrahman, O. (2020). Data Governance Based on COBIT2019 Framework to Achieve Sustainable Development Goals, Journal of Techniques, 2(3), pp. 9-18.

Vacca, J. (2015). Computer and Information Security Handbook, 2nd Edition, Morgan Kaufmann.