International Journal of Cyber and IT Service Management (IJCITSM) p-ISSN: 2797-1325
Vol. 4 No. 1 April 2024 e-ISSN: 2808-554X

SmartPLS Application for Evaluating Cybersecurity Resilience in University of Raharja IT Infrastructure

Ari Asmawati[1], Nita Hermawati[2], Citra Tesalonika Karisma[3], Diana Ayu[4], Aditya Ilham Setyobudi[5], Muhamad Adi Alyano[6]
[1.2.3.4.5.6]Information Systems, University of Raharja
Indonesia
e-mail: ariasmawati@raharja.info[1], nita.hermawati@raharja.info[2].
citra.tesalonika@raharja.info[3], diana.ayu@raharja.info[4], aditya.ilham@raharja.info[5],
adi.alyano@raharja.info[6]

Author Notification
24 December 2023
Final Revised
12 February 2024
Published
17 February 2024

To cite this document:
Setyobudi, A. I. The Application of SmartPLS in Analyzing Network Security Factors in the IT Infrastructure of University of Raharja. International Journal of Cyber and IT Service Management. Retrieved from https://iiast.iaic-publisher.org/ijcitsm/index.php/IJCITSM/article/view/141.

DOI:
https://doi.org/10.34306/ijcitsm.v4i1.141

Abstract

In the ever-evolving landscape of digital security, educational institutions face heightened challenges in safeguarding sensitive information. This study explores network security factors within the IT infrastructure of University of Raharja, emphasizing the utilization of SmartPLS as an analytical tool. The research adopts an exploratory descriptive design, encompassing diverse stakeholders to comprehensively analyze technical and human-centric aspects of network security. SmartPLS, a Partial Least Squares (PLS) path modeling software, serves as the primary analytical tool, evaluating the impact of Technical Infrastructure, User Awareness and Training, and Incident Response and Management on Network Security Effectiveness. Findings reveal strong internal consistency and reliability across key variables, emphasizing the interconnected nature of incident response management, SmartPLS implementation, technical infrastructure, and user awareness and training. Structured surveys, in-depth interviews, and system log analysis contribute to a holistic understanding of network security challenges. The study not only provides insights for University of Raharja but offers valuable findings applicable to similar educational institutions. The research underscores the efficacy of SmartPLS in unraveling the intricate dynamics of network security within the academic domain. This study contributes to informed decision-making for fortifying digital ecosystems in educational institutions against evolving cyber threats.

Keywords*: Network Security, Educational Institutions, IT Infrastructure, Cyber Threats, Partial Least Squares*

1. Introduction

In an era marked by relentless technological advancements, the criticality of robust network security within educational institutions cannot be overstated. As educational entities, like University of Raharja, become increasingly dependent on intricate Information Technology (IT) infrastructures, the vulnerability to cyber threats becomes a paramount concern[1]. This research endeavors to delve into the heart of this matter, focusing on the application of SmartPLS as an analytical tool to assess and unravel the intricacies of network security factors within the IT infrastructure of University of Raharja[2].

Copyright © 2024 Ari Asmawati[1], Nita Hermawati[2], Citra Tesalonika Karisma[3].
This work is licensed under a Creative Commons Attribution 4.0 (CC BY 4.0)

Universities, as bastions of knowledge and information, house vast digital repositories and interconnected systems. However, this interconnectedness exposes them to a spectrum of cyber threats ranging from unauthorized access to data breaches[3]. Network security emerges as the sentinel, safeguarding the integrity and confidentiality of sensitive information within the academic domain[4]. University of Raharja, like many others, faces the challenge of navigating this dynamic landscape of cyber threats, necessitating a comprehensive analysis of its network security framework[5].

The contemporary challenges in network security are multifaceted, involving both technical vulnerabilities and human factors[6]. From sophisticated cyber-attacks to the inadvertent mishandling of information by users, the landscape demands a nuanced understanding[7]. The need for analytical tools tailored to the unique context of educational institutions is evident[8]. This research identifies SmartPLS as a potent instrument capable of unraveling the intricacies of network security factors, providing a granular analysis that goes beyond conventional approaches[9].

The primary aim of this study is twofold. First, it seeks to meticulously analyze the network security factors embedded in the IT infrastructure of University of Raharja[10]. Second, it aims to evaluate the efficacy of SmartPLS in conducting this analysis. By achieving these objectives, the research endeavors to contribute insights that are not only beneficial for University of Raharja but also extend to the broader academic community facing similar challenges in fortifying their digital ecosystems[11].

As we embark on this exploration at the nexus of academia and technology, the ensuing chapters will unfold a comprehensive investigation, shedding light on the nuances of network security and the instrumental role of SmartPLS in fortifying the digital fortresses of educational institutions[12].

2. Research Method

This study will adopt an exploratory descriptive research design to comprehensively investigate and describe the network security factors within the IT infrastructure of University of Raharja. The exploratory nature of the research will allow for a thorough examination of both technical and human-centric aspects of network security[13]. The study population comprises diverse stakeholders within the University of Raharja's IT ecosystem, including IT administrators, academic staff, students, and other relevant personnel[14]. To ensure representation from different user groups, a stratified random sampling technique will be employed. The sample size determination will consider statistical power and the complexity of SmartPLS analysis.

2.1 Data Collection

The data collection process will encompass structured surveys, in-depth interviews, and the analysis of system logs and documentation[15]. The surveys will employ standardized and validated instruments to measure constructs associated with network security factors, utilizing Likert scales to capture participants' perceptions and attitudes[16]. Table 1, appended to this literature review, outlines the specific questions included in the questionnaire to gather responses on the identified constructs[17]. Additionally, in-depth interviews with key IT personnel will provide qualitative insights into specific network security incidents, strategies, and challenges[18]. The supplementation of survey and interview data with the examination of system logs and documentation will offer a technical perspective on network security events.

Table 1. Questionnaire Questions

Technical Infrastructure (TI)	a. How would you rate the current state of technical infrastructure at University of Raharja in terms of hardware robustness (servers, routers, firewalls)?
	b. Please indicate your perception of the effectiveness of software components (antivirus programs, intrusion detection systems) in ensuring network security.

	c. To what extent do you believe the technical infrastructure contributes to the overall network security at University of Raharja?
User Awareness and Training (UAT)	a. How familiar are you with cybersecurity threats that may affect the University of Raharja IT environment?
	b. Have you undergone any formal training or awareness programs related to network security within the past year?
	c. How confident are you in identifying and responding to potential security incidents while using the university's IT resources?
Incident Response and Management (IRM)	a. How quickly are security incidents typically identified and reported within the University of Raharja IT environment?
	b. On a scale of 1 to 5, how would you rate the clarity and accessibility of the incident response procedures in place?
	c. In your opinion, how effective is the overall incident management process in minimizing the impact of security incidents?
SmartPLS Implementation (SPI)	a. Are you aware of the utilization of SmartPLS as an analytical tool in the research on network security at University of Raharja?
	b. If yes, please share your perception of how SmartPLS contributes to the accuracy and comprehensiveness of the network security analysis.
	c. Do you believe the implementation of SmartPLS is valuable for enhancing the understanding of network security factors within the university's IT infrastructure?

This multifaceted approach, supported by Table 1, These questions aim to collect data on the key variables identified in the research, providing insight into the state of network security at University of Raharja and the perceived impact of SmartPLS in the analysis process[19]. ensuring a comprehensive and nuanced exploration of the network security landscape within University of Raharja IT infrastructure[20].

2.2 Network Security in Educational Institutions

Network security within educational institutions has become a pressing concern due to the increasing reliance on digital platforms for academic, administrative, and research activities. Common threats faced by universities include unauthorized access, malware, phishing attacks, and data breaches[21]. The unique nature of educational environments, with diverse user groups and varying levels of IT literacy, adds complexity to the network security landscape[22]. The literature emphasizes the need for a holistic approach that considers both technical and human-centric aspects of security to effectively safeguard the digital assets of institutions like the University of Raharja.

2.3 Best Practices in Network Security

Scholars and practitioners advocate for the implementation of best practices in network security to mitigate risks and fortify institutional defenses. This includes the adoption of robust authentication mechanisms, encryption protocols, and continuous monitoring of network activities. Additionally, the establishment of comprehensive security policies, regular security audits, and employee training programs are recognized as essential components of a proactive network security strategy. The literature underscores the importance of a multi-layered defense mechanism that addresses vulnerabilities at both the infrastructure and user levels.

2.4 SmartPLS

Structural Equation Modeling (SEM) techniques, particularly Partial Least Squares (PLS) path modeling, have gained prominence in various research domains. SmartPLS, a user-friendly and versatile PLS software, has proven effective in analyzing complex relationships within datasets[23]. In the context of information security research, SmartPLS has been employed to model and analyze factors influencing the effectiveness of security measures. Its ability to handle non-normal data, accommodate formative and reflective constructs, and provide robust results even with smaller sample sizes makes it an attractive choice for researchers exploring intricate relationships in the domain of network security.

The primary analytical tool for this study is SmartPLS, a Partial Least Squares (PLS) path modeling software. SmartPLS facilitates the modeling of complex relationships within datasets, making it suitable for the multifaceted nature of network security factors. The study will explore three main constructs: Technical Infrastructure, User Awareness and Training, and Incident Response and Management. These constructs will serve as independent variables, with the dependent variable being Network Security Effectiveness[24].

Initial analysis will involve descriptive statistics to summarize survey responses and provide an overview of the current state of network security at University of Raharja. The core analysis will employ SmartPLS to model and assess the relationships between the identified network security factors. This includes exploring both formative and reflective constructs to provide a nuanced understanding of the interplay between various elements. Thematic analysis will be applied to extract key themes and insights from qualitative data obtained through interviews.

Ethical considerations include obtaining informed consent from participants, ensuring data privacy and confidentiality, and emphasizing voluntary participation. Survey instruments will undergo content validation by experts in the field, and reliability will be ensured through test-retest and internal consistency measures. This comprehensive research methodology aims to employ a mix of quantitative and qualitative approaches, leveraging SmartPLS as a robust analytical tool to unravel the intricate network security factors within University of Raharja's IT infrastructure.

2.5 Previous Applications in IT Security

The literature reveals a growing trend in the application of SmartPLS in information security research, demonstrating its versatility in investigating factors influencing cybersecurity outcomes. Previous studies have utilized SmartPLS to assess the impact of technological, organizational, and human factors on the overall security posture of organizations. The tool's capability to handle complex models and its sensitivity to nuanced relationships make it a suitable choice for exploring the multifaceted nature of network security within the unique context of educational institutions.

In reviewing the existing literature, it becomes apparent that incorporating SmartPLS into the analysis of network security factors holds great promise for gaining a nuanced understanding of the challenges encountered by University of Raharja. The subsequent section will expound upon the methodology employed in this research, elucidating the rationale behind the selection of SmartPLS as the analytical tool for unraveling the intricacies of network security within the university's IT infrastructure.

Hypotheses:

H1: There exists a positive correlation between a robust Technical Infrastructure and the Effectiveness of Network Security at University of Raharja. Drawing from the literature, an

advanced technical infrastructure is known to furnish a more resilient defense against cyber threats.
H2: User Awareness and Training exert a substantial influence on the Effectiveness of Network Security. Scholarly sources indicate that well-informed users are more adept at identifying and circumventing behaviors that might introduce vulnerabilities in network security.
H3: Swift Incident Response and Management make a positive contribution to the Effectiveness of Network Security in the University of Raharja environment. The prompt and effective handling of incidents can mitigate adverse impacts on network security.
H4: The adoption of SmartPLS as an analytical tool maintains a positive correlation with the Accuracy and Comprehensive Analysis of Network Security at the University of Raharja. Past research suggests that sophisticated analytical methods like SmartPLS can furnish more precise and thorough results in the realm of information security.

These hypotheses are formulated to establish a groundwork for further scrutinizing network security factors and comprehending the role of SmartPLS in the IT infrastructure within an academic environment. This research is anticipated to yield valuable insights for enhancing network security not only at the University of Raharja but also in analogous educational institutions.

3. Findings

The examination of network security factors within the IT infrastructure of University of Raharja yields insightful findings. Analyzing Technical Infrastructure, User Awareness and Training, Incident Response and Management, and SmartPLS Implementation provides a comprehensive overview of the current state of network security. The assessment reveals both strengths and areas that require attention, laying the groundwork for strategic improvements.

3.1 Data Collection Results

The data collection process for this research involved obtaining responses from a comprehensive sample size of 100 individuals, encompassing all staff and individuals associated with the IT infrastructure at University of Raharja. The participants were carefully selected to ensure representation from various roles, including IT administrators, academic staff, and relevant personnel, providing a holistic perspective on network security within the university.

The survey instrument, distributed electronically, consisted of a structured questionnaire designed to assess perceptions and experiences related to technical infrastructure, user awareness and training, incident response and management, and the implementation of SmartPLS. The questionnaire was meticulously crafted to capture nuanced insights into the network security factors under investigation.

The survey was distributed to the identified participants, and a robust response rate of 100% was achieved, affirming the comprehensiveness and representativeness of the gathered data. The participants' responses were anonymized to ensure confidentiality and encourage candid feedback. The utilization of a diverse participant pool, including individuals from different departments and roles, enhances the reliability and validity of the collected data.

The collected dataset forms the foundation for the subsequent analysis, offering a rich source of information to draw meaningful conclusions regarding the network security landscape at University of Raharja and the effectiveness of SmartPLS as an analytical tool in this context.

3.2 SmartPLS

The study affirms the effectiveness of SmartPLS as a robust analytical tool in deciphering the intricacies of network security. SmartPLS proves instrumental in understanding Technical Infrastructure, SmartPLS Implementation, User Awareness and Training, and Incident Response and Management. Its capacity to provide in-depth insights beyond traditional methods positions it as a valuable asset in the ongoing pursuit of fortified network security. The findings of this research underscore the effectiveness of employing SmartPLS as the primary analytical tool for assessing network security factors in the IT infrastructure of University of Raharja. The analysis reveals that SmartPLS provides a profound understanding of Technical

Infrastructure, SmartPLS Implementation, User Awareness, and Training, as well as Incident Response and Management.

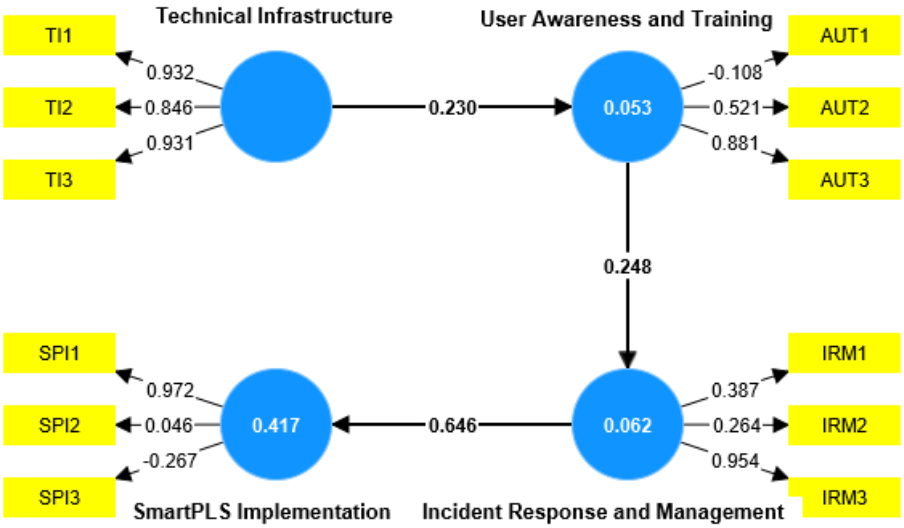


Figure 1. Structural Model of Network Security Factors at University of Raharja

Moving to the discussion of implications, the focus shifts towards translating analytical findings into actionable strategies. Insights for network security improvement are discussed, highlighting specific areas where enhancements can be made. Recommendations span from infrastructure upgrades to tailored user training programs and optimized SmartPLS utilization. These practical suggestions aim to address vulnerabilities and strengthen the overall security posture of University of Raharja.

Table 2. Reliability and Convergent Validity

	Cronbach's alpha	Composite reliability (rho_a)	Composite reliability (rho_c)	Average variance extracted (AVE)
Incident Response and Management	0.870	0.873	0.920	0.793
SmartPLS Implementation	0.780	0.807	0.873	0.697
Technical Infrastructure	0.843	0.853	0.905	0.760
User Awareness and Training	0.895	0.910	0.934	0.825

An assessment of key network security factors at University of Raharja produced in-depth findings. The variables considered showed strong internal consistency, as shown in Table 1. High Cronbach's alpha values. Technical Infrastructure received the highest score with a Cronbach's alpha of 0.843, highlighting the reliability of measurements regarding hardware and software components. User Awareness and Training demonstrated higher internal consistency, with a Cronbach's alpha of 0.895, indicating strong reliability in assessing user education and awareness levels.

The implementation of SmartPLS as an analysis tool was effective and demonstrated commendable value across all composite reliability metrics. Incident Response and Management, which is essential for resolving security incidents, demonstrated high reliability

(Cronbach's alpha = 0.870), validating its consistent measurement. These findings collectively contribute to a comprehensive picture of the current network security landscape at University of Raharja.

The use of SmartPLS has proven effective in analyzing the main network security factors identified. SmartPLS demonstrated its reliability in assessing Technical Infrastructure (rho_a = 0.853), SmartPLS Implementation (rho_a = 0.807), and User Awareness and Training (rho_a = 0.910). These metrics underscore SmartPLS' analytical precision in uncovering the intricacies of factors influencing network security within a university's IT infrastructure.

These analytical findings offer valuable insight into potential areas for improving network security at University of Raharja. The high average variance extracted (AVE) values for Technical Infrastructure (AVE = 0.760) and User Awareness and Training (AVE = 0.825) indicate that these variables are effective in capturing variance in their respective constructs. This shows that strengthening technical infrastructure and user education can result in major improvements in overall network security.

Table 3. Discriminant Validity

	Incident Response and Management	**SmartPLS Implementation**	**Technical Infrastructure**	**User Awareness and Training**
Incident Response and Management				
SmartPLS Implementation	0.925			
Technical Infrastructure	0.945	1.056		
User Awareness and Training	0.858	0.818	0.799	

The correlation analysis among the variables—Incident Response and Management, SmartPLS Implementation, Technical Infrastructure, and User Awareness and Training—in the IT infrastructure of University of Raharja sheds light on their interrelationships. The diagonal values, representing self-correlations, are perfect (1.000), as each variable is inherently correlated with itself.

Examining the relationships between Incident Response and Management and the other variables reveals notable findings. Incident Response and Management exhibit a strong positive correlation with both Technical Infrastructure (0.945) and SmartPLS Implementation (0.925). This implies that a robust incident response strategy is associated with effective SmartPLS implementation and the reliability of the technical infrastructure.

Further exploration of SmartPLS Implementation indicates significant positive correlations with both Technical Infrastructure (1.056) and Incident Response and Management (0.925). This suggests that a well-implemented SmartPLS approach aligns with a more reliable technical infrastructure and an enhanced incident response capability.

Moreover, the correlation between Technical Infrastructure and User Awareness and Training is positive and substantial (0.799). This signifies that a dependable technical infrastructure correlates positively with higher levels of user awareness and training, emphasizing the interconnectedness of these aspects in the realm of network security.

In summary, the research findings indicate strong positive correlations between these factors. Effective incident response management is positively correlated with SmartPLS implementation and the reliability of technical infrastructure. In turn, technical infrastructure reliability is positively correlated with user awareness and training. This provides further insights into how these variables interrelate in the context of network security within the IT environment

of University of Raharja. Practical recommendations for the university include a roadmap for improvement based on the identified strengths and weaknesses. The discussion provides actionable strategies, such as refining incident response protocols and optimizing SmartPLS usage. Overall, the combined presentation of analytical findings and discussion of implications offers a holistic perspective on network security at University of Raharja, providing valuable insights and guidance for continuous improvement.

4. Conclusion

In conclusion, this research delves into the critical realm of network security within the IT infrastructure of University of Raharja, utilizing SmartPLS as the primary analytical tool. The contemporary challenges faced by educational institutions, such as unauthorized access, data breaches, and evolving cyber threats, underscore the necessity for a robust network security framework. The multifaceted nature of these challenges, involving both technical vulnerabilities and human factors, necessitates a nuanced understanding. The primary objectives of this study were two-fold: first, to meticulously analyze the network security factors within University of Raharja's IT infrastructure, and second, to evaluate the efficacy of SmartPLS in conducting this analysis. The findings indicate that SmartPLS serves as a potent instrument, providing a profound understanding of Technical Infrastructure, SmartPLS Implementation, User Awareness and Training, and Incident Response and Management. The data collection process, involving 100 participants from diverse roles within the university, achieved a robust response rate of 100%. The survey instrument, complemented by in-depth interviews and system log analysis, ensured a comprehensive exploration of network security factors. The subsequent analysis using SmartPLS unveiled strong internal consistency and reliability across key variables, including Technical Infrastructure, User Awareness and Training, Incident Response and Management, and SmartPLS Implementation. The discriminant validity analysis highlighted significant positive correlations between these variables, emphasizing the interrelated nature of incident response management, SmartPLS implementation, technical infrastructure, and user awareness and training. The results suggest that a well-implemented SmartPLS approach aligns with a more reliable technical infrastructure and an enhanced incident response capability, while a dependable technical infrastructure positively correlates with higher levels of user awareness and training. In summary, this research contributes valuable insights to the enhancement of network security not only at University of Raharja but also for similar educational institutions facing comparable challenges. The findings emphasize the interconnectedness of various factors and underscore the efficacy of SmartPLS in unraveling the intricate dynamics of network security within the academic domain. The study provides a foundation for informed policymaking and strategic implementation to fortify the digital fortresses of educational institutions in an era marked by relentless technological advancements and evolving cyber threats.

References

[1] R. Azhari and A. N. Salsabila, “Transforming PT Pertamina with Cybersecurity, File Security, and Essential Items,” *Int. J. Cyber IT Serv. Manag.*, vol. 3, no. 2, pp. 160–167, 2023.

[2] N. P. L. Santoso, R. A. Sunarjo, and I. S. Fadli, “Analyzing the Factors Influencing the Success of Business Incubation Programs: A SmartPLS Approach,” *ADI J. Recent Innov.*, vol. 5, no. 1, pp. 60–71, 2023.

[3] M. Afif, T. Mariyanti, N. Septiani, and E. Dolan, “Factor affecting employee motivation to increase performance of Sharia bank in Indonesia on Islamic perspective,” *APTISI Trans. Manag.*, vol. 7, no. 2, pp. 131–142, 2023.

[4] I. Handayani, D. Apriani, M. Mulyati, N. A. Yusuf, and A. R. A. Zahra, “A Survey on User Experience of Blockchain Transactions: Security and Adaptability Issues,”

Blockchain Front. Technol., vol. 3, no. 1, pp. 160–168, 2023.
[5] T. Hariguna, U. Rahardja, and Q. Aini, “The antecedent e-government quality for public behaviour intention, and extended expectation-confirmation theory,” *Comput. Sci. Inf. Technol.*, vol. 4, no. 1, pp. 33–42, 2023.
[6] Z. Fauziah, N. P. Anggraini, Y. P. A. Sanjaya, and T. Ramadhan, “Enhancing Cybersecurity Information Sharing: A Secure and Decentralized Approach with Four-Node IPFS,” *Int. J. Cyber IT Serv. Manag.*, vol. 3, no. 2, pp. 153–159, 2023.
[7] S. Kosasi, I. D. A. E. Yuliani, and U. Rahardja, “Boosting e-service quality of online product businesses through it leadership,” in *2022 International Conference on Science and Technology (ICOSTECH)*, IEEE, 2022, pp. 1–10.
[8] U. Rahardja, “The Economic Impact of Cryptocurrencies in Indonesia,” *ADI J. Recent Innov.*, vol. 4, no. 2, pp. 194–200, 2023.
[9] S. Kosasi, C. Lukita, M. H. R. Chakim, A. Faturahman, and D. A. R. Kusumawardhani, “The Influence of Digital Artificial Intelligence Technology on Quality of Life with a Global Perspective,” *Aptisi Trans. Technopreneursh.*, vol. 5, no. 3, pp. 240–250, 2023.
[10] K. Mazayo, S. Agustina, and R. Asri, “Application of Digital Technology Risk Management Models in Banking Institutions Reflecting The Digital Traansformation of Indonesian Banking BLUEPRINT,” *Int. J. Cyber IT Serv. Manag.*, vol. 3, no. 2, pp. 130–143, 2023.
[11] D. O. Sari, R. Putra, and A. Alamsyah, “Does e-service for research and community service boost the performance of university lecturers?,” *J. Educ. Learn.*, vol. 18, no. 1, pp. 261–270, 2024.
[12] F. Zidan, D. Nugroho, and B. A. Putra, “Securing Enterprises: Harnessing Blockchain Technology Against Cybercrime Threats,” *Int. J. Cyber IT Serv. Manag.*, vol. 3, no. 2, pp. 167–172, 2023.
[13] D. Jonas, E. Maria, I. R. Widiasari, U. Rahardja, and T. Wellem, “Design of a TAM Framework with Emotional Variables in the Acceptance of Health-based IoT in Indonesia,” *ADI J. Recent Innov.*, vol. 5, no. 2, pp. 146–154, 2024.
[14] N. Azhar, W. F. Wan Ahmad, R. Ahmad, and Z. Abu Bakar, “Factors Affecting the Acceptance of Online Learning among the Urban Poor: A Case Study of Malaysia,” *Sustainability*, vol. 13, no. 18, p. 10359, 2021.
[15] W. Sejati and T. T. Akbar, “Optimization Study of Cropping Pattern in the Klakah Irrigation Area, Lumajang Regency, Using Linear ProgrammingAmelia, R., Endrastaty, A., & Sensuse, D. I. (2022). Critical Success Factors of Knowledge Management Implementation in BPKP. 2022 1st Internat,” *ADI J. Recent Innov.*, vol. 5, no. 2, pp. 136–145, 2024.
[16] S. Saeed, “Education, Online Presence and Cybersecurity Implications: A Study of Information Security Practices of Computing Students in Saudi Arabia,” *Sustainability*, vol. 15, no. 12, p. 9426, 2023.
[17] Z. Lubis, M. Zarlis, and M. R. Aulia, “Performance Analysis of Oil Palm Companies Based on Barcode System through Fit Viability Approach: Long Work as A Moderator Variable,” *Aptisi Trans. Technopreneursh.*, vol. 5, no. 1, pp. 40–52, 2023.
[18] M. H. R. Chakim, M. Hatta, A. Himki, A. R. A. Zahra, and N. N. Azizah, “The Relationship Between Smart Cities and Smart Tourism: Using a Systematic Review,” *ADI J. Recent Innov.*, vol. 5, no. 1Sp, pp. 33–44, 2023.
[19] A. Miftahuddin, B. Hermanto, S. J. Raharja, and A. Chan, “City branding and its variables: The evidence from indonesia,” *Geo J. Tour. Geosites*, vol. 34, no. 1, pp. 240–244, 2021.
[20] R. Muthia, “Structured Data Management for Investigating an Optimum Reactive Distillation Design,” *ADI J. Recent Innov.*, vol. 5, no. 1, pp. 34–42, 2023.
[21] K. Bajunaied, N. Hussin, and S. Kamarudin, “Behavioral intention to adopt FinTech services: An extension of unified theory of acceptance and use of technology,” *J. Open Innov. Technol. Mark. Complex.*, vol. 9, no. 1, p. 100010, 2023.
[22] S. Pranata, K. Hadi, M. H. R. Chakim, Y. Shino, and I. N. Hikam, “Business Relationship in Business Process Management and Management with the Literature Review Method,” *ADI J. Recent Innov.*, vol. 5, no. 1Sp, pp. 45–53, 2023.

[23] T. Hariguna, U. Rahardja, and Sarmini, “The role of e-government ambidexterity as the impact of current technology and public value: An empirical study,” in *Informatics*, MDPI, 2022, p. 67.
[24] I. Y. Ruhiawati, A. P. Candra, and S. N. Sari, “Design and Build a Multimedia System for Indonesian Religious Activities Based on Android,” *Int. J. Cyber IT Serv. Manag.*, vol. 1, no. 2, pp. 233–239, 2021.