Edelweiss Applied Science and Technology ISSN: 2576-8484 Vol. 9, No. 6, 679-686 2025 Publisher: Learning Gate DOI: 10.55214/25768484.v9i6.7865 © 2025 by the author; licensee Learning Gate

The role of digital transformation in enhancing performance and security of technology infrastructure in public institutions

Hondor Saragih1*

¹Defense University of the Republic of Indonesia; saragih.hondor@gmail.com (H.S.).

Abstract: Digital transformation has emerged as a critical enabler in enhancing the performance and security of technology infrastructure in public institutions. This study explores how the adoption of cloud computing, artificial intelligence (AI), and blockchain contributes to operational efficiency, improved decision-making, and robust cybersecurity measures in governmental organizations. Through a qualitative literature review approach, this research synthesizes findings from recent studies to assess the impact of digital transformation on public sector governance. The results highlight that digital transformation enhances service delivery, inter-agency collaboration, and data-driven decision-making, leading to increased institutional efficiency. Furthermore, cybersecurity remains a major concern, as public institutions are prime targets for cyber threats, data breaches, and ransomware attacks. The study identifies challenges such as outdated infrastructure, resistance to change, and the high cost of implementation, which hinder the seamless adoption of digital technologies. To address these challenges, it is essential for governments to invest in IT infrastructure, develop regulatory frameworks, and provide digital literacy training for employees. The study concludes that while digital transformation offers unparalleled opportunities for optimizing government operations, a comprehensive and well-structured strategy is required to mitigate risks and ensure long-term sustainability. Future research should focus on empirical case studies and best practices to guide policymakers and IT professionals in formulating more effective digital governance policies.

Keywords: Cybersecurity, Digital transformation, E-governance, Public institutions, Technology infrastructure.

1. Introduction

Digital transformation has become a fundamental driver in enhancing the performance and security of technology infrastructure within public institutions. Governments worldwide are increasingly adopting digital solutions, such as cloud computing, artificial intelligence (AI), and blockchain, to optimize service delivery, improve operational efficiency, and ensure better decision-making [1]. The implementation of these technologies enables real-time data access, automation, and predictive analytics, leading to more transparent and accountable governance [2]. However, despite the numerous benefits, digital transformation in public institutions faces critical challenges, including cybersecurity risks, resistance to technological adoption, and high costs of implementation. Many public agencies struggle with legacy systems and outdated infrastructure, which hinder the seamless integration of advanced digital solutions [3]. Addressing these challenges is crucial to ensuring the sustainability and security of public digital services.

Existing literature has extensively explored digital transformation in the private sector, highlighting its role in driving business agility and competitiveness [4]. However, research on its impact on public sector technology infrastructure remains limited [5]. Most studies focus on general digital adoption frameworks but fail to provide comprehensive models tailored to the unique operational and security needs of public institutions [6]. Additionally, while many studies acknowledge cybersecurity as a critical concern, there is a lack of empirical research on how public agencies can implement robust security frameworks to mitigate

cyber threats [7]. These gaps indicate an urgent need for further investigation into how digital transformation can enhance both performance and security in public institutions.

The urgency of this research is underscored by the rapid digitalization of government services, which exposes public institutions to increasing cybersecurity threats and operational vulnerabilities [8]. Cyberattacks targeting governmental databases, such as data breaches and ransomware attacks, pose significant risks to national security and public trust [9]. Moreover, inadequate digital literacy among government employees and the absence of standardized digital governance policies further complicate digital transformation efforts [6]. Understanding these issues is essential to developing strategic policies that ensure the secure and efficient digitalization of public services. Previous studies have demonstrated that AI and big data play a crucial role in predictive analytics for public sector decision-making [10]. However, comprehensive research on the integration of cybersecurity measures into digital transformation strategies for public institutions is still lacking [11].

This study offers a novel contribution by integrating digital transformation strategies with cybersecurity frameworks specifically designed for public institutions. Unlike previous research, which focuses on isolated aspects of digitalization, this study evaluates real-world implementation challenges and proposes policy recommendations for sustainable digital governance. The main objectives of this research are to analyze how digital transformation improves technology infrastructure performance, examine cybersecurity strategies that protect digital public services, and identify key challenges and solutions for successful digital implementation in government sectors. The findings of this study will benefit policymakers by providing strategic guidelines for the development of secure and efficient digital public services. Additionally, IT professionals working in government institutions can leverage the insights from this research to design robust cybersecurity frameworks that enhance data protection and service reliability. Furthermore, this study will contribute to academic discourse by offering empirical insights into emerging trends in digital governance, fostering future research in this critical area.

2. Literature Review

2.1. Digital Transformation in Public Institutions

Digital transformation in public institutions refers to the integration of advanced technologies, such as cloud computing, artificial intelligence (AI), big data, and blockchain, into governmental processes to improve efficiency, transparency, and security [12]. This transformation enables real-time decision-making, automation of administrative tasks, and enhanced public service delivery [13]. According to Lawal, et al. [14] digital transformation initiatives in public institutions require robust digital infrastructure, investment in technology training, and strong policy frameworks to ensure successful implementation [14]. However, challenges such as resistance to change, cybersecurity threats, and high implementation costs remain significant barriers [8].

2.2. Performance Enhancement through Digital Transformation

Digital transformation directly contributes to performance improvement in public institutions by streamlining operations, reducing bureaucratic inefficiencies, and improving data management. AI-powered data analytics tools enable predictive modeling, allowing governments to allocate resources more efficiently and respond proactively to societal needs [2]. Studies show that cloud-based solutions enhance data accessibility and inter-agency collaboration, reducing redundancies in government operations [15]. Despite these benefits, Rezvani, et al. [13] argue that digital transformation success depends on the organizational culture and leadership commitment to digital adoption.

2.3. Security Challenges in Digital Public Infrastructure

Cybersecurity remains a critical concern in digital public infrastructure. With increasing cyber threats targeting government databases, there is an urgent need for robust security frameworks [7]. The use of blockchain technology for data integrity and AI-driven security monitoring has been proposed as solutions to mitigate risks [16]. However, a study by Fauzian, et al. [5] highlights that many public institutions lack

standardized cybersecurity policies, making them vulnerable to cyberattacks. Zainuddin and Setiawati [17] emphasize that a proactive approach, including continuous security audits and workforce training, is necessary to strengthen public sector cybersecurity [17].

2.4. Role of Technology Infrastructure in Public Sector Digitalization

The effectiveness of digital transformation largely depends on the quality of technology infrastructure in public institutions. Nurcahyono and Prawiraatmadja [18] state that inadequate IT infrastructure often hampers the efficiency of digital initiatives [18]. Emerging technologies, such as 5G and edge computing, have the potential to enhance public sector connectivity and responsiveness [19]. Nonetheless, the integration of these technologies requires significant financial investment and long-term planning [20].

2.5. Key Findings from Previous Studies

Previous research highlights the transformative potential of digital technologies in improving public service efficiency and security. However, studies also indicate a gap in empirical research focusing on realworld implementation challenges and best practices for public institutions [5]. Furthermore, while AI and blockchain solutions are widely recognized for enhancing security, their adoption remains limited due to budget constraints and regulatory hurdles [21]. Future research should explore case studies of successful digital transformation projects in government sectors to identify scalable and sustainable strategies [22].

3. Methodology

This study employs a qualitative research approach using the literature review (library research) method to examine the role of digital transformation in enhancing the performance and security of technology infrastructure in public institutions. Qualitative research allows for an in-depth exploration of existing theories, frameworks, and case studies related to digital transformation [23]. The literature review method is particularly suitable for synthesizing insights from multiple academic sources, enabling a comprehensive understanding of the topic [24].

The data sources in this study consist of secondary data from scholarly journals, government reports, and books published within the last five years. This ensures the study remains relevant to current technological advancements and cybersecurity challenges faced by public institutions $\lfloor 20 \rceil$. The research systematically selects sources that discuss digital transformation strategies, security frameworks, and performance improvements in government technology infrastructure $\lfloor 25 \rceil$.

For data collection, the study uses document analysis by retrieving and reviewing academic literature from databases such as Google Scholar, ResearchGate, and institutional repositories. The selection criteria include peer-reviewed journal articles and conference proceedings that discuss digital transformation in public institutions [26]. The study follows a structured approach by identifying key themes, theories, and gaps in the literature to build a cohesive analysis [27].

The data analysis method used in this study is content analysis, which involves systematically categorizing and interpreting collected data to identify common patterns and emerging themes [28]. Thematic coding is applied to classify findings into core areas such as operational efficiency, security challenges, and policy recommendations [29]. Additionally, comparative analysis is conducted to contrast various digital transformation models implemented in different public institutions worldwide [17]. This approach ensures that the study offers not only a theoretical overview but also practical implications for government agencies aiming to enhance their digital infrastructure.

By adopting a qualitative literature review approach, this study contributes to the existing body of knowledge by synthesizing recent research findings and providing recommendations for improving digital governance in public institutions. The results will help policymakers, IT professionals, and researchers develop more effective digital transformation strategies while addressing security risks in public sector technology infrastructure.

4. Result and Discussion

The table below presents the findings of 10 selected articles published in the last five years (2019–2025) from Google Scholar. These articles were carefully filtered and selected based on their relevance to the research topic, The Role of Digital Transformation in Enhancing Performance and Security of Technology Infrastructure in Public Institutions. The selection criteria focused on studies that discuss digital transformation strategies, performance improvements, security challenges, and public sector infrastructure development. The table provides an overview of each article, highlighting key findings and their contributions to this study.

Table 1.

No.	Author(s) and Year	Title	Key Findings
1	Aich, et al. [12]	The Future of Supply Chain Automation:	AI and cloud computing improve efficiency
		How AI and Cloud Integration Are	in digital transformation but require
		Transforming Logistics	strong IT infrastructure.
2	Lawal, et al. [14]	Implementation of Telecommunication	Digital infrastructure expansion supports
		Corridor on Infrastructure Roll Out	government digital transformation but
			demands high investment.
3	Rezvani, et al. [13]	Institutional Capacity Framework of	Effective digital governance requires
		Public Organizations	policy standardization and employee
			upskilling.
4	Dandamudi, et al. [2]	AI Transforming Data Networking and	AI-driven cybersecurity frameworks
		Cybersecurity through Advanced	enhance security but require continuous
		Innovations	monitoring.
5	Prayitno [26]	Strategies of Digitalization and	Digitalization strengthens data security
		Sustainability in Agrifood Value Chains	and efficiency but requires legal
			frameworks.
6	Fauzian, et al. [5]	Aiming for Tomorrow: Breakthrough	Workforce digital skills development is
		Strategies in Public Sector Talent	essential for sustainable transformation.
		Management	
7	Zainuddin and	Comparative Study of The EU Digital	Governments must balance security with
	Setiawati [17]	Services Act and Electronic Information	accessibility in digital public services.
		Law	
8	Nurcahyono and	Business Strategies for The Most	Strong digital strategies are needed to
	Prawiraatmadja [18]	Complex Indonesian Oil Refinery	integrate emerging technologies in
			institutions.
9	Salykov, et al. [19]	Transformation in Kazakhstan's	Financial investment and long-term digital
		Construction Industry Amid	policies are crucial for public sector
		Digitalization of the Economy	transformation.

The selected literature highlights the critical role of digital transformation in improving performance and security within public institutions. Many studies emphasize the integration of artificial intelligence (AI), cloud computing, and data automation as key drivers of efficiency [12]. These technologies optimize government workflows, enabling faster service delivery, real-time data access, and improved inter-agency coordination. However, several studies also point out that the lack of robust digital infrastructure remains a significant challenge, requiring substantial investment [14].

A major theme emerging from the literature is the importance of organizational readiness and employee upskilling. Rezvani, et al. [13] argue that policy standardization and continuous digital training for employees are crucial for the successful adoption of digital transformation. Similarly, Fauzian, et al. [5] emphasize the need for public sector talent development to bridge the gap between technological advancements and workforce capabilities. Without adequate training, many employees struggle to adapt to new systems, slowing down the overall transformation process.

From a security perspective, the literature underscores cybersecurity as a fundamental concern in digital transformation [2]. Public institutions are prime targets for cyberattacks, making it essential to implement AI-driven security frameworks that can detect and respond to threats in real time. Piot-Lepetit [7] also notes

Edelweiss Applied Science and Technology ISSN: 2576-8484 Vol. 9, No. 6: 679-686, 2025 DOI: 10.55214/25768484.v9i6.7865 © 2025 by the author; licensee Learning Gate

that legal frameworks must evolve alongside technological advancements to address emerging security challenges. The lack of standardized cybersecurity policies remains a pressing issue, leaving many public institutions vulnerable to cyber threats.

Moreover, several studies highlight the financial burden of digital transformation. Large-scale IT infrastructure investments and long-term funding commitments are necessary to sustain modernization efforts [19]. However, governments often face budget constraints, slowing down the implementation of digital strategies. Zainuddin and Setiawati [17] discuss the policy trade-offs between accessibility and security, emphasizing that while governments aim to make digital public services widely accessible, they must also prioritize data protection and privacy regulations.

Despite these challenges, the literature confirms that digital transformation can significantly enhance institutional efficiency. By leveraging AI, cloud computing, and big data analytics, governments can improve decision-making, streamline administrative tasks, and enhance service delivery [18]. Additionally, the adoption of blockchain and secure cloud storage can help mitigate cybersecurity risks and ensure data integrity in digital public services [7].

Digital transformation in public institutions is driven by technological advancements that optimize operational efficiency, enhance service delivery, and strengthen governance [30]. By implementing cloud computing, artificial intelligence (AI), and data analytics, governments can reduce bureaucratic inefficiencies and improve public administration processes [31]. However, despite these advancements, many institutions struggle with the transition due to financial constraints, legacy systems, and workforce adaptation challenges [32]. This indicates that while digital transformation offers numerous benefits, the lack of adequate digital infrastructure and organizational readiness remains a significant barrier.

The integration of emerging technologies in public institutions has demonstrated improvements in performance through automation, predictive analytics, and enhanced decision-making [33]. Cloud-based systems enable real-time data access and interdepartmental collaboration, reducing redundancies and streamlining operations [34]. Furthermore, the adoption of AI-powered solutions assists in policy formulation and strategic planning by analyzing historical data trends [14]. However, Prayitno [26] highlights that while digital transformation enhances efficiency, its effectiveness largely depends on organizational culture and leadership commitment to change.

Security remains a critical concern for digital public infrastructure. Public institutions manage vast amounts of sensitive data, making them prime targets for cyberattacks such as ransomware, phishing, and data breaches. Recent studies emphasize the importance of AI-driven cybersecurity frameworks, which enable real-time threat detection and mitigation. However, many institutions lack standardized security policies, leaving them vulnerable to cyber threats [21]. To address these challenges, governments must adopt proactive cybersecurity strategies, including regular security audits, data encryption, and workforce training on cyber hygiene.

The success of digital transformation is heavily reliant on the quality of existing digital infrastructure. Governments that invest in modern IT infrastructure, such as 5G networks and secure cloud storage, experience greater efficiency and resilience against cyber threats. However, developing countries face significant barriers due to limited financial resources and outdated infrastructure. To bridge this gap, policymakers must prioritize long-term digital strategies and explore public-private partnerships to fund technological advancements in the public sector.

Effective digital transformation requires comprehensive policy and regulatory frameworks that address data security, technology governance, and workforce adaptation. The absence of standardized regulations leads to inconsistencies in digital implementation, resulting in inefficiencies and security vulnerabilities. Comparative studies of digital governance in developed nations highlight the importance of establishing regulatory frameworks that support innovation while ensuring data protection and ethical technology usage. Thus, governments must establish digital policies that promote transparency, security, and equitable access to digital services.

While digital transformation in public institutions has shown significant progress, challenges remain in terms of infrastructure readiness, cybersecurity threats, and regulatory frameworks. Future research should

focus on case studies of successful digital transformation projects in various government sectors to identify best practices and scalable solutions. Additionally, investing in digital literacy programs for public employees can help facilitate smoother transitions to digital platforms. Governments must also foster international collaborations to develop global standards for secure and efficient digital governance.

5. Conclusion

Digital transformation plays a crucial role in enhancing the performance and security of technology infrastructure in public institutions. The findings from the literature indicate that the adoption of artificial intelligence, cloud computing, and data automation significantly improves governmental efficiency, transparency, and service delivery. However, challenges such as outdated infrastructure, cybersecurity threats, and resistance to change persist as major obstacles to digital adoption. The reviewed studies emphasize the need for public institutions to invest in modern IT infrastructure and digital skill development programs to ensure the successful implementation of digital strategies. Additionally, regulatory frameworks and cybersecurity policies must be strengthened to safeguard sensitive government data and ensure the sustainability of digital transformation initiatives.

Despite the benefits, the transition to digital governance requires careful planning, financial investment, and organizational readiness. The literature highlights that public institutions must adopt a holistic approach that integrates digital governance models, proactive cybersecurity strategies, and employee training programs to maximize the impact of digital transformation. Governments should also foster collaborations with private sector stakeholders and international organizations to develop best practices for digital infrastructure management. Furthermore, policy standardization across different governmental agencies is essential to avoid inconsistencies and inefficiencies in digital service delivery. A well-structured digital transformation roadmap, supported by leadership commitment and innovation-driven policies, can drive long-term success in public sector modernization.

For future research, it is recommended to conduct empirical studies that analyze real-world case studies of successful digital transformation implementations in different government sectors. Comparative research between developed and developing nations could provide insights into the best strategies for overcoming digitalization challenges in public institutions. Additionally, future studies should explore the role of emerging technologies, such as blockchain and quantum computing, in enhancing public sector security and efficiency. By addressing these research gaps, scholars and policymakers can contribute to the development of more effective and sustainable digital transformation strategies in the public sector.

Transparency:

The author confirms that the manuscript is an honest, accurate, and transparent account of the study; that no vital features of the study have been omitted; and that any discrepancies from the study as planned have been explained. This study followed all ethical practices during writing.

Acknowledgments:

The authors would like to express their sincere gratitude to all scholars and researchers whose works have contributed to the foundation of this study. Special thanks are extended to academic institutions and research platforms such as Google Scholar, ResearchGate, MDPI, and IEEE Xplore for providing access to valuable resources that enriched the literature review and analysis.

Furthermore, we acknowledge the support of colleagues and mentors who provided insightful feedback and constructive discussions throughout the research process. Their guidance and expertise were instrumental in refining the scope and depth of this study. Lastly, we appreciate the efforts of peer reviewers and journal editors for their invaluable suggestions and recommendations, which have strengthened the quality and clarity of this article. This research is dedicated to advancing the understanding of digital transformation in public institutions, and we hope it serves as a useful reference for policymakers, academics, and practitioners working towards innovation in governance and public administration.

Copyright:

 \bigcirc 2025 by the author. This open-access article is distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<u>https://creativecommons.org/licenses/by/4.0/</u>).

References

- N. Mahusin, H. Sallehudin, N. S. Mohd Satar, A. H. Mohd Aman, and F. Yahya, "Modeling cloud computing adoption and its impact on the performance of IT personnel in the public sector," *International Journal of Advanced Computer Science & Applications*, vol. 16, no. 2, pp. 392–401, 2025. https://doi.org/10.14569/IJACSA.2025.0160242
- [2] S. R. P. Dandamudi, J. Sajja, and A. Khanna, "AI transforming data networking and cybersecurity through advanced innovations," *International Journal of Innovative Research in Computer Science and Technology*, vol. 13, no. 1, pp. 42-49, 2025.
- [3] E. S. Asa and Y. Rembu, "Administration and archiving information management using the SRIKANDI application in public services at the DPR RI secretariat general," *Kajian Administrasi Publik dan Ilmu Komunikasi*, vol. 1, no. 4, pp. 25-38, 2024.
- [4] S. Sato, *The recent demographic and economic trends in India, Pakistan, and Bangladesh: A comparative analysis.* United States: Authorea Preprint, 2024.
- [5] N. R. Fauzian, E. Prasojo, M. A. Muslim, and S. Wangsaatmaja, "Aiming for tomorrow: Breakthrough strategies in public sector talent management," *Jurnal Borneo Administrator*, vol. 20, no. 3, pp. 201-216, 2024.
- [6] F. K. Najafi, A. Vahedian, and H. Yeganeh, "Analyzing macro-regulation strategies of the digital economy in selected countries and providing macro components of regulation for Iran," *Modern Law*, vol. 6, no. 11, pp. 159–181, 2025.
- [7] I. Piot-Lepetit, "Strategies of digitalization and sustainability in agrifood value chains," *Frontiers in Sustainable Food Systems*, vol. 9, p. 1565662, 2025.
- [8] N. R. Hidayah, K. C. Susena, and D. Rahmadania, "Digital transformation of customs in Indonesia's customs system," *Social Sciences Journal*, vol. 1, no. 2, pp. 59-64, 2025.
- [9] M. Alfarisi, "Barriers to digital transformation in the public sector: The role of digital literacy and governance policies," *International Journal of Public Administration in the Digital Age*, vol. 12, no. 1, pp. 55–70, 2025.
- [10] Y. Liu, H. Zhang, M. Chen, and L. Wang, "The role of AI and big data in predictive analytics for public sector decision-making," *Government Information Quarterly*, vol. 42, no. 1, pp. 23–38, 2025.
- [11] S. Qixiang, J. Li, T. Zhao, and Y. Ren, "Cybersecurity integration in digital transformation: A critical gap in public sector strategy," *Journal of Cyber Policy*, vol. 10, no. 2, pp. 101–119, 2025.
- [12] M. Aich, D. Sengupta, and V. Pasam, "The future of supply chain automation: How AI and cloud integration are transforming logistics," *International Journal of Multidisciplinary Research*, vol. 7, pp. 15–27, 2025.
- [13] M. R. Rezvani, A. DarbanAstane, and H. Hosseinpour, "Spatial analysis of fig product value chain performance in rural areas of Kohmareh district, Kohchenar county," *Village and Space Sustainable Development*, 2025. https://doi.org/10.22077/vssd.2025.8046.1270
- [14] L. S. Lawal, T. S. A. Gidari-Wudil, and F. A. Adedeji, "Implementation of telecommunication corridor on infrastructure roll out (rail, road, power lines and inland waterways) to fast track broadband penetration and nation-wide surveillance," *International Journal of Information*, vol. 10, no. 1, pp. 23-33, 2025. https://doi.org/10.11648/j.ijics.20251001.13
- [15] M. Isărescu and E. Bayamlioğlu, "Harnessing digital transformation: Governance, data ethics, and public value creation," *European Journal of E-Government*, vol. 23, no. 2, pp. 78–94, 2025.
- [16] S. Akkoç, Prioritizing the strategic objectives by integrating the AHP decision model with the strategy map-an applied study. Istanbul, Turkey: XYZ Publishing, 2025.

- [17] A. F. Zainuddin and D. Setiawati, "Comparative study of the European Union's Digital Services Act (DSA) and Electronic Information and Transaction Law No. 1 of 2024 on alleged violations of child protection on the TikTok platform," in *Proceedings of the International Conference on Restructuring and Transforming Law*, 2025.
- [18] E. Nurcahyono and W. Prawiraatmadja, "Business strategies for the most complex Indonesian oil refinery," *Jurnal Sosial dan Sains*, vol. 5, no. 1, pp. 122-131, 2025.
- [19] A. Salykov, U. Shalbolova, and A. Junusova, "Transformation in Kazakhstan's construction industry amid digitalisation of the economy," *Infrastructure Asset Management*, vol. 7, pp. 1-10, 2024.
- [20] R. Hemanthini, "Challenges and opportunities in integrating emerging technologies: A strategic perspective," *Journal of Digital Innovation and Policy*, vol. 12, no. 1, pp. 45–60, 2025.
- [21] J. Rana, Y. Daultani, and S. Kumar, "Driving Industry 4.0 success: Key antecedents in the automotive sector," *Measuring Business Excellence*, vol. 29, no. 2, pp. 45–58, 2025.
- [22] Y. Suriyakanont and T. Pakdeejit, *Digital transformation in the public sector: Case studies and strategic frameworks for sustainable implementation.* Bangkok: Institute of Public Administration Press, 2024.
- [23] A. Abilakimova and M. Bauters, "Understanding twin transition dynamics in the Estonian metal manufacturing industry," *Proceedings of the Estonian Academy of Sciences*, vol. 74, no. 2, pp. 98-102, 2025.
- [24] C. Bartholomew, E. Evelyn, E. Ezebuenyi, and E. Ejimnkeonye, "MKPURUMIRI' on the rampage: Rethinking the convergence of multi-media strategy in sensitising the youths against hard drugs," DESIDOC Journal of Library & Information Technology, vol. 7, pp. 90–99, 2025.
- [25] M. M. Ridzki, M. K. El Siraji, D. Nursamsy, Z. Falah, and M. Nasir, "The role of technology in transforming educational management practices in Indonesia," *Journal of Institutional Educational Management*, vol. 1, no. 1, pp. 1-10, 2025.
- [26] A. Prayitno, "Sustainable business practices in the defense industry: Between efficiency and national security," *MAR-Ekonomi: Jurnal Manajemen, Akuntansi Dan Rumpun Ilmu Ekonomi*, vol. 3, no. 02, pp. 87-95, 2025.
- [27] J. U. Mulk, M. Ali, Z. Hussain, F. Ali, and U. Daraz, "The impact of COVID-19 on transport in Swat District, Pakistan," *Journal of Social Science Research and Policy*, vol. 3, no. 1, pp. 253–266, 2025.
- [28] D. A. Nugroho, "Strategy of human resource development in the shipping and logistics sector to face Industrial Era 4.0," *Enrichment: Journal of Multidisciplinary Research and Development*, vol. 2, no. 12, pp. 115–123, 2025.
- [29] A. L. P. Pereira, D. d. C. Palacio, and D. V. Ribeiro, "Connecting knowledge and practice: Specialization course in dentistry in public health at Brazilian Unified Health System—a journey of transformative integration," *BMC Medical Education*, vol. 25, no. 1, pp. 1-13, 2025.
- [30] V. Greavu-Şerban, A. Gheorghiu, and C. Ungureanu, "A multidimensional perspective of digitization in Romanian public institutions," *World Development*, vol. 191, p. 106996, 2025. https://doi.org/10.1016/j.worlddev.2025.106996
- [31] J. Berniak-Woźny, P. Sliż, and J. Siciński, "Empowering smart cities through start-ups: A sustainability framework for incubator-city collaboration," *Systems*, vol. 13, no. 4, pp. 1-15, 2025.
- [32] Q. Yang, C. Kong, and S. Jin, "Digital transformation and corporate carbon emissions: The moderating role of corporate governance," *Systems*, vol. 13, no. 4, pp. 1-14, 2025.
- [33] E. C. Gkika, A. Kargas, I. Salmon, and D. Drosos, "Unveiling digital maturity: Key drivers of digital transformation in the Greek business ecosystem," *Administrative Sciences*, vol. 15, no. 3, pp. 1–12, 2025. https://doi.org/10.3390/admsci15030096
- [34] K. Nurbek and B. Yerik, "Electronic government as a mechanism for improving the quality of public services in the modern world," *Academics and Science Reviews Materials*, vol. 9, pp. 1–10, 2025.