Applied Community Services Journal
Vol. 01, No. 02 (2025), p. 52-64
Available online at https://serambi.org/index.php/acsj

Securing Digital Transformation in Community Services: AI-Based Solutions for Public Sector Cybersecurity

Ahmad Jamy Kohistani[1], Mohammad Nawab Turan[2*], Nasrullah Rahimi[3]

[1] Computer Engineering Department, Computer Science Faculty, Kabul Polytechnic University, Kabul, Afghanistan
[2] Network Engineering Department, Computer Science Faculty, Faryab University, Afghanistan
[3] Information Technology Department, Computer Science Faculty, Badakhshan University, Afghanistan

*Corresponding Author: mn.turan@faryab.edu.af
DOI: https://doi.org/10.61987/acsj.v1i2.1242

Abstract:
The growing digitalization of public sector and community services demands advanced cybersecurity solutions. Artificial intelligence (AI) has emerged as a vital tool to enhance cybersecurity in e-government, smart cities, and digital governance. This study systematically reviews recent literature from 2022 to 2025 to examine AI's role in improving cybersecurity, the challenges faced in implementing AI-driven solutions, and their impact on the effectiveness and trustworthiness of public services. Using databases such as IEEE, ScienceDirect, and MDPI, peer-reviewed articles were selected based on specific keywords and inclusion criteria related to AI, cybersecurity, and public/community services. The review reveals that AI improves threat detection, risk prioritization, and response efficiency, contributing to stronger infrastructure resilience and increased public trust in digital services. However, issues such as privacy concerns, ethical challenges, outdated infrastructure, and a shortage of skilled professionals hinder the full potential of AI applications. To overcome these challenges, the study emphasizes the need for ethical guidelines, infrastructure upgrades, and workforce training to support sustainable AI adoption. In summary, AI holds significant promise for enhancing cybersecurity in public services, but its success depends on addressing technical, ethical, and human factors to create secure and trustworthy digital environments.

ARTICLE HISTORY
Received August 2025
Revised September 2025
Accepted September 2025

KEY WORDS
Artificial Intelligence, Cybersecurity, Public Services, Digital Transformation, Smart Cities

INTRODUCTION

The rapid acceleration of digital transformation within public service delivery is reshaping how governments interact with and serve communities. From e-government platforms to smart city infrastructure and digital citizen engagement systems, technology now plays a critical role in advancing public access, transparency, and service efficiency. However, as community services become increasingly digitized, they also become more vulnerable to cybersecurity threats, data breaches, and AI-driven misinformation, particularly in underserved or digitally marginal populations. This shift introduces a pressing need to secure digital platforms while maintaining equitable and effective public

service. The intersection of artificial intelligence (AI) and cybersecurity presents promising solutions to address these challenges (Kshetri, 2025; Hakimi et al., 2025).

Artificial intelligence has shown significant promise in improving public service delivery by optimizing administrative processes, enabling real-time data analytics, and enhancing decision-making capabilities in government operations (Al-Ansi et al., 2024; Priyadi & Arwani, 2024). However, as these digital systems grow more interconnected through IoT and cloud platforms, they become attractive targets for cyber threats. Bokhari and Myeong (2023) highlighted that in smart cities, where e-governance systems are prevalent, cybersecurity has emerged as a critical factor in maintaining trust and functionality. Furthermore, Sethi and Verma (2025) emphasized that public safety and critical infrastructure in urban areas require robust AI-powered cybersecurity mechanisms to ensure operational continuity and citizen safety.

The integration of AI into cybersecurity systems introduces several capabilities, such as predictive threat detection, automated incident response, and advanced authentication techniques. These technologies are increasingly relevant in protecting sensitive public data and preventing service disruption (Kshetri, 2025; Mahfuri et al., 2024). Yet, while AI-enabled cybersecurity solutions are gaining momentum in sectors like banking (Rodrigues et al., 2022) and healthcare (Ndumbe & Velikov, 2024), their application in community service contexts—especially those involving public sector governance, citizen data protection, and inclusive service delivery—remains relatively underexplored.

Several studies have examined the transformative impact of AI and digitalization in government operations (Sharmin & Chowdhury, 2025; Djatmiko et al., 2025) and the rising importance of cybersecurity in smart city development (Sarker, 2024; Singh, 2025). However, these works often focus on technological or policy-level insights without deeply examining how AI-based cybersecurity solutions can be integrated into community service programs to enhance digital trust and accessibility. Moreover, research on marginalized or digitally excluded communities in the context of secure digital service transformation is sparse (Hakimi, Kohistani, Azimy, & Sudestra, 2025). This creates a significant gap in understanding how to practically implement secure, inclusive, and AI-augmented community services.

Therefore, the objective of this study is to investigate the role of AI-based cybersecurity solutions in securing digital transformation efforts within community service delivery. Specifically, this research seeks to explore how AI can be leveraged to enhance public sector cybersecurity frameworks while ensuring community trust, equitable access, and service sustainability. By drawing upon current advancements in AI, cybersecurity, and digital governance, this study aims to provide a comprehensive framework for integrating secure digital practices into community service programs. The findings are intended to support practitioners, policymakers, and stakeholders in building cyber-resilient public services that not only embrace innovation but also uphold public trust and data security in an increasingly digital world.

To address the critical role of artificial intelligence in strengthening cybersecurity within public and community services, this study seeks to explore key aspects of AI implementation. Understanding both the opportunities and challenges is essential for effective digital transformation in the public sector. Therefore, the following research questions guide this systematic literature review:

RQ1: How is artificial intelligence currently applied to enhance cybersecurity within public sector and community service domains?

RQ2: What are the main challenges and risks associated with implementing AI-driven cybersecurity solutions in digital transformation and e-government initiatives?

RQ3: How do AI-based cybersecurity strategies impact the effectiveness and trustworthiness of public services in smart cities and digital governance?

RESEARCH METHODS

This study employs a Systematic Literature Review (SLR) approach to comprehensively investigate the role of Artificial Intelligence (AI) in enhancing cybersecurity within the context of public sector digital transformation and community service delivery. The SLR method was selected for its methodological rigor and ability to synthesize existing evidence, identify trends, evaluate gaps, and propose future research directions (Kitchenham & Charters, 2007). Following a structured protocol, the review adheres to the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA) guidelines to ensure transparency and replicability.

Data Sources and Search Strategy

To ensure coverage of high-quality and relevant literature, this review draws from peer-reviewed articles indexed in internationally recognized scientific databases, including IEEE Xplore, ScienceDirect (Elsevier), MDPI, SpringerLink, and Taylor & Francis. These databases were selected due to their extensive coverage of topics related to AI, cybersecurity, e-governance, and digital transformation in public services.

Table 1: Search Strategy for Systematic Literature Review

Keyword Group	Search Terms	Boolean Logic
Artificial Intelligence	"artificial intelligence", "AI"	("artificial intelligence" OR "AI")
Cybersecurity	"cybersecurity", "cyber security"	("cybersecurity" OR "cyber security")
Community/Public Services	"community service", "public service", "e-government", "digital transformation"	("community service" OR "public service" OR "e-government" OR "digital transformation")
Application Context	"smart cities", "public sector"	("smart cities" OR "public sector")

The search was limited to publications between 2022 and 2025, written in English, and accessible in full text. Duplicates, non-peer-reviewed articles (e.g., blogs, white papers), and conference abstracts without full manuscripts were excluded.

Table 2: Inclusion and Exclusion Criteria

Inclusion Criteria	Exclusion Criteria
Peer-reviewed articles published between	Articles not published between 2022–

2022–2025	2025
Focus on AI applications in cybersecurity	Studies unrelated to AI or cybersecurity
Relevant to public sector, e-government, community services, or digital governance	Articles unrelated to public/community service or digital governance
Methodological transparency and clear findings	Studies lacking empirical data or a theoretical contribution
Written in English	Non-English publications
Unique, non-duplicated studies across databases	Duplicate or redundant studies across sources

The inclusion criteria focused on peer-reviewed articles published between 2022 and 2025, emphasizing studies that explore artificial intelligence applications in cybersecurity within public or community service contexts. Only articles demonstrating methodological transparency and offering clear empirical or theoretical contributions were selected. In contrast, exclusion criteria ruled out non-English publications, duplicates, and studies lacking relevance to the public sector, e-government, or digital transformation. Articles without substantial data or outside the AI and cybersecurity domain were also excluded. This selection process ensured the final set of studies was both high in quality and directly aligned with the research objectives of the review.

Selection Process

The selection process followed three main stages:

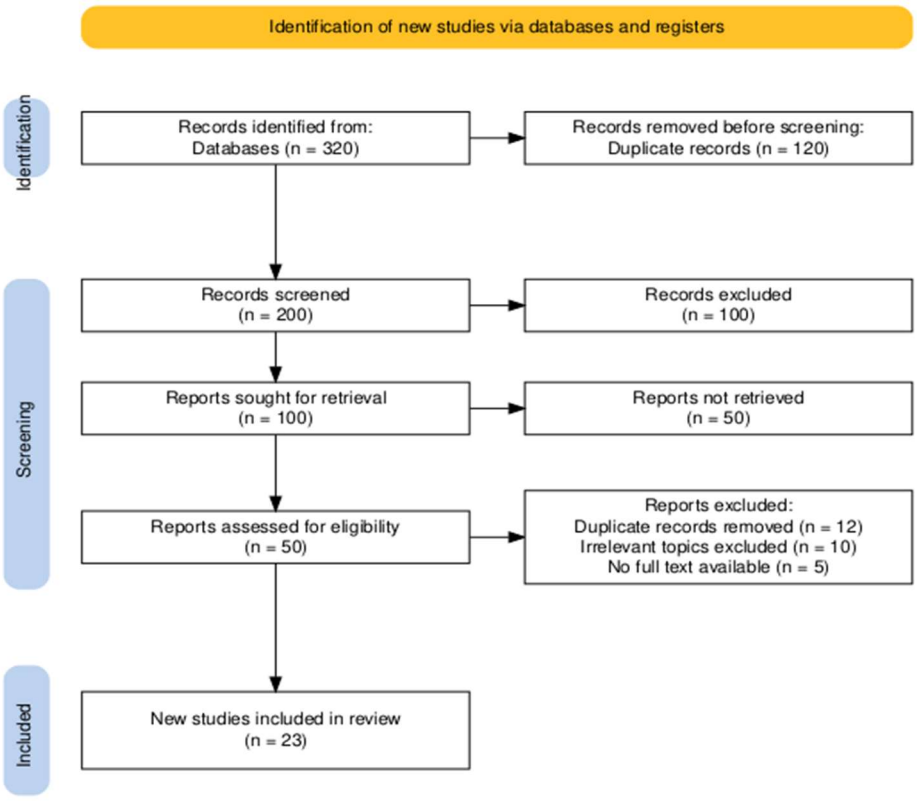

Figure 1: PRISMA Flow Diagram Illustrating the Study Selection Process

The PRISMA flow diagram (Figure 1) details the systematic selection process of studies included in this literature review. Initially, 320 records were identified from various electronic databases. After removing 120 duplicate records, 200 unique records were screened based on their titles and abstracts. Out of these, 100 records were excluded due to lack of relevance. Full texts of the remaining 100 reports were sought, but 50 were not retrieved due to access limitations. Consequently, 50 reports were assessed for eligibility. During this stage, 12 duplicate records overlooked earlier, 10 studies unrelated to AI, cybersecurity, or public service, and 5 articles without accessible full texts were excluded. Ultimately, 23 studies met all inclusion criteria and were incorporated into the systematic literature review. This rigorous selection process ensured the reliability and relevance of the data synthesized in this study.

Data Extraction and Synthesis

A structured data extraction template was used to capture key information from each study, including:

- Authors and year
- Research objective
- Methodology (quantitative, qualitative, or mixed-method)
- Key findings related to AI and cybersecurity in public/community service
- Technological focus (e.g., machine learning, IoT security, blockchain)
- Implementation context (e.g., smart cities, government platforms, citizen engagement systems)

The data were synthesized using qualitative content analysis to identify recurring themes, conceptual frameworks, and research gaps. The thematic coding process helped cluster studies around core domains, including AI-enabled threat detection, digital trust, secure e-governance, and inclusive technology design.

Quality Assessment

Table 3: Quality Assessment Criteria Based on CASP Checklist

Criteria	Description	Assessment Focus	Outcome
Clear Research Aim	Whether the study clearly states its objectives	Clarity of purpose	Included if clearly stated
Appropriate Methodology	Suitability of research design to answer the research question	Methodological appropriateness	Included if appropriate
Data Collection	Adequacy and transparency of data collection methods	Reliability and replicability	Included if methods are clear

Data Analysis	Appropriateness and rigor of data analysis techniques	Validity of findings	Included if analysis is rigorous
Results and Findings	Clarity and relevance of reported results	Contribution to research questions	Included if results are clear
Ethical Considerations	Whether ethical issues are addressed	Ethical compliance	Included if ethical standards met

To ensure the integrity and credibility of the systematic review, each selected article underwent a rigorous quality assessment using an adapted version of the Critical Appraisal Skills Programme (CASP) checklist. The evaluation focused on six key domains: clarity of research aims, appropriateness of methodology, transparency of data collection, rigor of data analysis, clarity of results, and adherence to ethical standards. Articles that failed to meet minimum standards in one or more domains—particularly regarding methodological clarity and validity—were excluded from the final synthesis. This process ensured that only studies with sound research designs and reliable findings contributed to the review, thereby enhancing the robustness and trustworthiness of the conclusions drawn.

RESULTS

This section presents the findings of the systematic literature review, organized around the three primary research questions. The results synthesize insights from recent studies published between 2022 and 2025, focusing on the application of AI in enhancing cybersecurity within public and community service domains. It also examines the key challenges and risks encountered in implementing AI-driven cybersecurity solutions during digital transformation and e-government initiatives. Finally, the section explores how these AI-based cybersecurity strategies impact the effectiveness, resilience, and trustworthiness of public services, particularly within smart cities and digital governance frameworks.

RQ1: How is artificial intelligence currently applied to enhance cybersecurity within public sector and community service domains?

Table 4: AI Applications Enhancing Cybersecurity in Public Sector and Community Services

Study	AI Application	Sector/Context	Key Findings
Bokhari & Myeong (2023)	AI-based threat detection and response	E-Governance	AI improves real-time threat identification and mitigation, reducing cyber incidents
Sarker (2024)	AI-enabled IoT cybersecurity	Smart cities	AI enhances monitoring of IoT networks, enabling faster

			response to cyber-attacks
Mahfuri et al. (2024)	Automated anomaly detection	Public sector networks	AI automates detection of irregular activities, improving security and reducing manual oversight
Rodrigues et al. (2022)	AI-powered risk assessment frameworks	Public services & banking	AI models assess cybersecurity risks to prioritize defenses efficiently
Ndumbe & Velikov (2024)	AI-supported incident prediction	Healthcare public sector	AI forecasts potential cyber threats, enhancing proactive defense measures

The review of recent studies reveals multiple ways artificial intelligence (AI) is applied to enhance cybersecurity in the public sector and community service domains. Bokhari and Myeong (2023) highlight AI's critical role in e-governance, where AI-driven threat detection systems enable real-time identification and mitigation of cyber-attacks, significantly reducing security breaches. In smart city environments, Sarker (2024) demonstrates how AI fortifies cybersecurity by continuously monitoring IoT devices and networks, allowing for rapid detection and response to emerging threats. Mahfuri et al. (2024) emphasize the automation of anomaly detection within public sector networks, which lessens reliance on manual monitoring and enhances overall security posture.

Moreover, Rodrigues et al. (2022) discuss AI-powered risk assessment frameworks applied in public services and banking sectors to efficiently prioritize cybersecurity defenses based on risk levels. In healthcare—a critical public service domain—Ndumbe and Velikov (2024) illustrate how AI models predict potential cyber incidents, facilitating proactive measures that safeguard sensitive data. Collectively, these applications demonstrate AI's versatile and impactful contribution to strengthening cybersecurity infrastructures in public and community service settings, fostering resilience and trust in digital governance.

RQ2: What are the main challenges and risks associated with implementing AI-driven cybersecurity solutions in digital transformation and e-government initiatives?

Table 5: Challenges and Risks in Implementing AI-Driven Cybersecurity for Digital Transformation and E-Government

Study	Challenge/Risk	Context	Key Insights
Hakimi et al. (2024)	Data privacy and ethical concerns	E-Government	Concerns over data misuse and ethical issues limit AI adoption
Singh (2025)	High complexity and cost	Digital transformation	Implementation complexity and financial burden hinder

			projects
Tyagi et al. (2024)	Lack of transparency and explainability	Cybersecurity systems	Black-box AI models reduce trust and accountability
Mahfuri et al. (2024)	Integration with legacy systems	Public sector infrastructure	Compatibility issues cause delays and security vulnerabilities
Rodrigues et al. (2022)	Skilled workforce shortage	Public sector & banking	Insufficient AI expertise limits effective deployment

The implementation of AI-driven cybersecurity solutions in digital transformation and e-government initiatives faces several critical challenges and risks. Hakimi et al. (2024) identify data privacy and ethical concerns as primary barriers, emphasizing fears of data misuse and the need for ethical governance frameworks to guide AI deployment. Singh (2025) highlights the high complexity and associated costs of integrating AI systems, which can limit the scalability and sustainability of such initiatives within public sector budgets.

A significant technical challenge is the lack of transparency and explainability in AI models, often described as "black-box" systems. Tyagi et al. (2024) note this opacity reduces user trust and complicates accountability in cybersecurity decision-making. Additionally, integration challenges with legacy systems are prominent; Mahfuri et al. (2024) report that outdated infrastructure in many public organizations hinders seamless AI adoption, increasing vulnerability risks during transitions.

Rodrigues et al. (2022) further emphasize the shortage of skilled professionals capable of developing, deploying, and managing AI-based cybersecurity tools, which restricts effective implementation and operational efficiency. Collectively, these challenges underscore the need for balanced strategies that address technical, ethical, and resource constraints to realize AI's full potential in securing digital government services.

RQ3: How do AI-based cybersecurity strategies impact the effectiveness and trustworthiness of public services in smart cities and digital governance?

Table 6: Impact of AI-Based Cybersecurity Strategies on Effectiveness and Trustworthiness in Smart Cities and Digital Governance

Study	Impact Area	Context	Key Findings
De Azambuja et al. (2023)	Enhanced threat detection and response	Smart cities	AI improves the speed and accuracy of detecting cyber threats, leading to more resilient city infrastructure
Sethi & Verma (2025)	Protection of critical	Smart cities	AI-based strategies reduce vulnerabilities in essential

	infrastructure		services, enhancing public safety and service continuity
Sharmin & Chowdhury (2025)	Increased transparency and accountability	Digital governance	AI tools enhance monitoring and auditing capabilities, promoting trust among citizens
Rodrigues et al. (2022)	Improved risk prioritization	Public sector services	AI enables efficient allocation of resources by prioritizing high-risk threats, improving service reliability
Ndumbe & Velikov (2024)	Strengthened citizen trust	Healthcare and public services	AI-based cybersecurity fosters greater citizen confidence in digital services by safeguarding sensitive data

AI-based cybersecurity strategies significantly impact the effectiveness and trustworthiness of public services, especially within smart cities and digital governance frameworks. De Azambuja et al. (2023) show that AI enhances threat detection and response capabilities, enabling smart cities to react swiftly and accurately to cyber incidents, which increases overall infrastructure resilience. This capability is crucial in protecting critical urban services, as noted by Sethi and Verma (2025), who emphasize that AI reduces vulnerabilities in essential systems, ensuring public safety and uninterrupted service delivery.

In terms of governance, Sharmin and Chowdhury (2025) highlight how AI-driven tools improve transparency and accountability through enhanced monitoring and auditing of digital processes, which in turn fosters greater citizen trust. Rodrigues et al. (2022) further demonstrate that AI's ability to prioritize risks allows public sector organizations to allocate cybersecurity resources more effectively, contributing to reliable and secure services.

Finally, Ndumbe and Velikov (2024) find that AI's role in protecting sensitive healthcare and public service data strengthens citizen confidence in e-government initiatives. Together, these findings underscore AI's transformative potential in securing digital governance, improving operational effectiveness, and building public trust in smart city environments.

DISCUSSION

The findings of this systematic review highlight the transformative potential of artificial intelligence (AI) in enhancing cybersecurity within public sector and community service domains, yet they also reveal substantial challenges that need to be addressed for successful implementation. AI's role in threat detection, anomaly identification, and risk prioritization is widely recognized as pivotal in strengthening cybersecurity infrastructures, especially in the context of digital governance and smart cities (Bokhari & Myeong, 2023; Sarker, 2024; De Azambuja et al., 2023). These applications enable

faster and more accurate responses to cyber threats, which is crucial given the increasing complexity and volume of cyber-attacks targeting public services.

However, the integration of AI-driven cybersecurity solutions faces significant hurdles. Privacy concerns and ethical considerations stand out as major barriers, reflecting fears about data misuse and insufficient regulatory frameworks (Hakimi et al., 2024). This aligns with prior studies emphasizing the need for transparent, ethical AI frameworks to build public trust (Tyagi et al., 2024). Furthermore, the technical challenge of integrating AI with legacy public sector systems limits the scalability of AI solutions (Mahfuri et al., 2024). Many public organizations still rely on outdated infrastructure, which complicates smooth adoption and introduces security vulnerabilities during transition phases.

The shortage of skilled professionals in AI and cybersecurity further exacerbates these challenges (Rodrigues et al., 2022). Without adequate expertise, even the most advanced AI tools cannot be effectively deployed or managed, limiting their impact. This calls for increased investment in workforce development and capacity building in the public sector to support digital transformation initiatives.

Importantly, the study also highlights the positive impact of AI-based cybersecurity on the effectiveness and trustworthiness of public services. Enhanced threat detection and proactive risk management improve the resilience of critical infrastructure, directly benefiting public safety and service continuity (Sethi & Verma, 2025; De Azambuja et al., 2023). Moreover, AI-driven transparency and accountability measures contribute to higher citizen trust in digital governance systems, which is essential for broader adoption and success of e-government services (Sharmin & Chowdhury, 2025; Ndumbe & Velikov, 2024).

Overall, while AI offers promising avenues for securing digital public services, a balanced approach that addresses ethical, technical, and human factors is essential. Policymakers and practitioners should focus on establishing robust ethical guidelines, upgrading infrastructure, and fostering a skilled workforce to fully leverage AI's capabilities in enhancing cybersecurity and digital governance.

CONCLUSION

The review of AI-driven cybersecurity in public sector and community services reveals both promising opportunities and significant challenges. Artificial intelligence has demonstrated strong potential to enhance the security, efficiency, and responsiveness of digital services, particularly within smart cities and e-government frameworks. Its ability to detect threats rapidly, prioritize risks, and improve system resilience contributes directly to safeguarding critical infrastructure and protecting sensitive data. This, in turn, strengthens public trust and confidence in digital governance, which is essential for successful digital transformation.

However, the adoption of AI-based cybersecurity solutions is not without obstacles. Privacy concerns, ethical considerations, and the lack of transparency in AI models pose risks that can undermine trust if left unaddressed. Additionally, many public sector organizations struggle with outdated infrastructure that complicates the integration of advanced technologies, creating vulnerabilities during transitional periods. The scarcity of skilled professionals further hampers effective implementation and long-term sustainability of AI cybersecurity measures.

To fully realize the benefits of AI in enhancing public sector cybersecurity, a comprehensive and balanced approach is necessary. This includes developing clear ethical frameworks to govern AI use, investing in modernizing legacy systems, and fostering the growth of expertise within the workforce. Encouraging collaboration among policymakers, technologists, and community stakeholders will also be crucial to designing solutions that are both effective and socially responsible.

In conclusion, AI has the potential to revolutionize cybersecurity in community services and digital governance, offering improved protection, operational efficiency, and citizen trust. Yet, addressing the multifaceted challenges related to ethics, technology, and human resources is vital to ensuring these advancements are both impactful and sustainable. The future of secure, trustworthy public services lies in harnessing AI responsibly while maintaining a strong focus on transparency, inclusiveness, and adaptability.

REFERENCES

Al-Ansi, A. M., Garad, A., Jaboob, M., & Al-Ansi, A. (2024). Elevating e-government: unleashing the power of AI and IoT for enhanced public services. *Heliyon*, *10*(23). https://hammingate.com/index.php/GRPCGPM/article/view/2023-11-07

Bokhari, S. A. A., & Myeong, S. (2023). The influence of artificial intelligence on e-Governance and cybersecurity in smart cities: A stakeholder's perspective. *IEEE Access*, *11*, 69783-69797. https://doi.org/10.1109/ACCESS.2023.3293480

De Azambuja, A. J. G., Plesker, C., Schützer, K., Anderl, R., Schleich, B., & Almeida, V. R. (2023). Artificial intelligence-based cyber security in the context of industry 4.0—a survey. *Electronics*, *12*(8), 1920. https://doi.org/10.3390/electronics12081920

Djatmiko, G. H., Sinaga, O., & Pawirosumarto, S. (2025). Digital transformation and social inclusion in public services: A qualitative analysis of e-government adoption for marginalized communities in sustainable governance. *Sustainability*, *17*(7), 2908. https://doi.org/10.3390/su17072908

Hakimi, M., Ezam, Z., Totakhail, A., & Ghafory, H. (2024). Transformative Impact of Artificial Intelligence on IoT Applications: A Systematic Reviewof Advancements, Challenges, and Future Trends. *International Journal of Academic and Practical Research*, *3*(1), 1-1. https://www.ejournals.ph/article.php?id=24184

Hakimi, M., Kohistani, A. J., Sahnosh, F. A., Samadzai, A. W., & Enayat, W. (2025). Enhancing Customer Awareness of Cybersecurity Threats in E-Banking: A Study on the Role of AI-based Risk Communication Tools. *Jurnal Ilmiah Manajemen dan Bisnis*, *10*(1), 100-110. https://doi.org/10.38043/jimb.v10i1.6762

Hakimi, M., Rahmani, K. R., Ezam, Z., & Shahbazi, H. (2024). Integrating Blockchain Technology for Secure E-Government Services: Opportunities and Challenges. *Journal of Social Science Utilizing Technology*, *2*(3), 317-335. https://doi.org/10.70177/jssut.v2i3.1266

Hakimi, M., Kohistani, A. J., Azimy, A. S., & Sudestra, I. M. A. (2025). THE INFLUENCE OF EMERGING TECHNOLOGIES ON COMMUNICATION PRACTICES IN THE DIGITAL AGE. *Jurnal Ilmiah Dinamika Sosial*, *9*(1), 136-153.https://doi.org/10.38043/jids.v9i1.6500

Hakimi, M., Sediqi, M., Kohistani, A. J., & Quraishi, T. (2025). THE ROLE OF DIGITAL LITERACY AND TECHNOLOGY ADOPTION IN FACILITATING SOCIAL

TRANSFORMATION IN AFGHANISTAN. *Jurnal Ilmiah Dinamika Sosial*, *9*(2), 175-191. https://doi.org/10.38043/jids.v9i2.6809

Hakimi, M., Suranata, I. W. A., Ezam, Z., Samadzai, A. W., Enayat, W., Quraishi, T., & Fazil, A. W. (2025). Generative AI in Enhancing Hydroponic Nutrient Solution Monitoring. *Jurnal Ilmiah Telsinas Elektro, Sipil dan Teknik Informasi*, *8*(1), 94-103. https://doi.org/10.38043/telsinas.v8i1.6242

Ionescu, R. (2025). Adopting Cloud Computing and Big Data Analytics to Enhance Public Sector Transparency and Accountability Through Artificial Intelligence. *Nuvern Machine Learning Reviews*, *2*(1), 1-18. https://nuvern.com/index.php/nmlr/article/view/4

Kshetri, N. (2025). Transforming cybersecurity with agentic AI to combat emerging cyber threats. *Telecommunications Policy*, 102976. https://doi.org/10.1016/j.telpol.2025.102976

Mahfuri, M., Ghwanmeh, S., Almajed, R., Alhasan, W., Salahat, M., Lee, J. H., & Ghazal, T. M. (2024, February). Transforming Cybersecurity in the Digital Era: The Power of AI. In *2024 2nd International Conference on Cyber Resilience (ICCR)* (pp. 1-8). IEEE. https://doi.org/10.1109/ICCR61006.2024.10533072

Mishra, S. (2023). Exploring the impact of AI-based cyber security financial sector management. *Applied Sciences*, *13*(10), 5875. https://doi.org/10.3390/app13105875

Ndumbe, S.I., Velikov, P. (2024). Government Strategies on Cybersecurity and How Artificial Intelligence Can Impact Cybersecurity in Healthcare with Special Reference to the UK. In: Jahankhani, H., Bowen, G., Sharif, M.S., Hussien, O. (eds) Cybersecurity and Artificial Intelligence. Advanced Sciences and Technologies for Security Applications. Springer, Cham. https://doi.org/10.1007/978-3-031-52272-7_9

Priyadi, U., & Arwani, A. (2024). Digital transformation: Artificial intelligence shaping the future of public sector. *New Applied Studies in Management, Economics & Accounting*, *7*(4), 54-67. https://doi.org/10.22034/nasmea.2024.193544

Rodrigues, A. R. D., Ferreira, F. A., Teixeira, F. J., & Zopounidis, C. (2022). Artificial intelligence, digital transformation and cybersecurity in the banking sector: A multi-stakeholder cognition-driven framework. *Research in International Business and Finance*, *60*, 101616. https://doi.org/10.22034/nasmea.2024.193544

Sarcea, O. A. (2024, July). AI & Cybersecurity–connection, impacts, way ahead. In *International Conference on Machine Intelligence & Security for Smart Cities (TRUST) Proceedings* (Vol. 1, pp. 17-26). https://www.scrd.eu/index.php/trust/article/view/543

Sarker, I.H. (2024). AI-Enabled Cybersecurity for IoT and Smart City Applications. In: AI-Driven Cybersecurity and Threat Intelligence. Springer, Cham. https://doi.org/10.1007/978-3-031-54497-2_7

Sethi, M., & Verma, V. (2025, May). Protecting Public Safety and Critical Infrastructure Systems in Smart Cities via Cybersecurity: AI-Based Threat Detection and Response. In *2025 Global Conference in Emerging Technology (GINOTECH)* (pp. 1-6). IEEE. https://doi.org/10.1109/GINOTECH63460.2025.11077039

Sharmin, S., & Chowdhury, R. H. (2025). Digital transformation in governance: The impact of e-governance on public administration and transparency. *Journal of Computer Science and Technology Studies*, *7*(1), 362-379.

https://doi.org/10.32996/jcsts.2025.7.1.27
Singh, H. (2025). Cybersecurity for Smart Cities Protecting Infrastructure in the Era of Digitalization. *Available at SSRN 5267856*. https://dx.doi.org/10.2139/ssrn.5267856
Tyagi, A. K., Kumari, S., & Richa. (2024). Artificial Intelligence-Based Cyber Security and Digital Forensics: A Review. *Artificial Intelligence-Enabled Digital Twin for Smart Manufacturing*, 391-419. https://doi.org/10.1002/9781394303601.ch18