DETERMINANTS AND CHALLENGES OF INTELLIGENT AUTOMATION ADOPTION IN THE BANKING SECTOR: THE MODERATING ROLE OF CYBERSECURITY AWARENESS

[1]*Nurliza Binti Zainul Abidin & [2]Lee Lian Kim
[1,2]Wawasan Open University, Malaysia
Correspondence: lisanur87@yahoo.com

ABSTRACT:*The increasing integration of Intelligent Automation (IA) in the banking sector has significantly transformed financial services by enhancing efficiency, security, and customer experience. However, IA adoption in Malaysia remains in its early stages, facing barriers such as cyber security threats, workforce readiness, regulatory compliance, and technological constraints. This study aims to examine the key determinants influencing IA adoption in banking, with a focus on Individual Work Resilience, Perceived Organisational Innovativeness, and Strategic Thinking Competency, while also assessing the moderating role of Cyber security Awareness. The research employs a comprehensive literature review and theoretical framework analysis to understand how these factors impact IA adoption. Findings indicate that organisations with a culture of innovation, digital resilience, and strategic planning are more likely to adopt IA successfully. However, challenges such as cyber risks, regulatory uncertainties, and skill gaps hinder widespread implementation. Cyber security awareness plays a crucial role in mitigating risks and increasing trust in IA solutions. The study concludes that enhancing cyber security awareness, up skilling the workforce, and developing regulatory frameworks are essential for successful IA adoption. Policy recommendations include strengthening AI governance, investing in AI-driven cyber security solutions, and promoting financial institutions' digital transformation strategies. By addressing these challenges, IA can be fully leveraged to enhance banking operations, improve risk management, and ensure regulatory compliance. This research provides valuable insights for banking executives, policymakers, and researchers, facilitating the future of AI-driven financial automation.*

Keywords: Intelligent Automation (IA), Cybersecurity Awareness, Digital Transformation, Banking Sector Innovation, Regulatory Compliance in AI Adoption

1. INTRODUCTION

The rapid advancements in technology have significantly transformed various industries, with the banking sector experiencing one of the most substantial impacts. Intelligent Automation (IA) has emerged as a revolutionary innovation in banking, integrating Artificial Intelligence (AI), Robotic Process Automation (RPA), and Business Process Automation (BPA) to enhance efficiency, security, and customer satisfaction. IA is particularly relevant in Malaysia, where financial institutions are undergoing digital transformation to remain competitive globally. However, despite its numerous advantages, IA adoption in Malaysia is still in its infancy, requiring further research and strategic planning for effective implementation [1, 2]. As Industry 4.0 drives technological advancements, banks are exploring ways to leverage IA for streamlining operations, mitigating risks, and enhancing customer experiences. However, implementing IA successfully involves overcoming multiple challenges, including cybersecurity threats, workforce readiness, and regulatory compliance. Cybersecurity awareness is a growing concern in Malaysia, as it plays a critical role in ensuring safe and effective automation in banking. Therefore, this study aims to explore the background of IA in banking, its importance in Malaysia, and the key gaps that must be addressed for its successful adoption [3, 4].

IA is anadvanced technology that integrates AI, RPA, and BPA to automate complex banking operations, reducing human intervention while enhancing operational efficiency. It is widely used in fraud detection, risk assessment, customer service automation, and regulatory compliance. Using predictive analytics together with machine learning algorithms enables financial institutions to examine extensive data sets effectively and detect patterns which produce decisions with decreased mistake rates [5, 6]. The initial stage of banking automation introduced digital banking solutions coupled with ATMs alongside electronic payment systems. The expansion of banking operations together with immediate service requirements surpassed traditional automation methods' capabilities. Research demonstrated IA to be a flexible solution because it accomplished cognitive tasks that mirrored human intellectual abilities [4, 6]. Modern financial institutions across the world have adopted IA systems to process loans and on-board customers and manage regulatory compliance and defend against cyber security threats. Malaysia struggles to implement IA technology because it confronts difficulties from regulatory barriers together with cyber security risks and lack of trained personnel. The study of IA adoption in Malaysian banking needs thorough examination to identify both facing implementation hurdles and possible strategies that can lead to smooth transformations [3, 6].

The banking sector of Malaysia functions as a key component in its efforts to achieve regional digital transformation leadership status. Malaysian banks have used the momentum of Industry 4.0 to implement Intelligence Automation because it helps them optimize their operations and financial services while extending access to banking services [1, 2]. The implementation of IA results in significant automation benefits which enable banks to decrease labour costs while automating both lending decisions and financial management operations along with regulatory tracking duties for enhanced business efficiency and service delivery quality

[4, 6]. The ability to withstand cyber threats determines another critical element. The growth of digital banking solutions has made Malaysian banks susceptible to rising threats of cyber attacks together with data breaches and fraudulent activities. IA bolsters safety measures through immediate fraud investigations as well as identity authentication using body features and automated detection of abnormal activities. Yeo [1] points out that Malaysia needs immediately deployed security solutions powered by AI because the country lacks an established cyber security framework [1, 3]. The implementation of IA stands essential for organizations to uphold present and upcoming customer demands. Customers today require time-sensitive personalized financial services because fintech and digital banking continue to grow. Banks implement chatbots and virtual assistants together with AI-driven recommendation systems through IA to boost customer satisfaction levels and loyalty outcomes [5, 6]. The automated system helps banks meet regulatory demands as it executes data validation together with reporting and risk assessment to fulfil AML laws and KYC protocols and Basel III risk management standards. The adoption of IA holds benefits for Malaysia but the country encounters three main obstacles including low awareness levels and unpredictable regulations and security threats. Solving these obstacles remains essential for integration success [2, 4].

2. LITERATURE REVIEW

2.1 Intelligent Automation (IA): Concept and Evolution

Intelligent Automation (IA) represents a significant technological advancement that integrates Artificial Intelligence (AI), Robotic Process Automation (RPA), and Business Process Automation (BPA) to streamline and optimize business processes. The goal of IA is to enhance operational efficiency, reduce costs, and improve decision-making capabilities through automation that mimics human cognitive abilities. The evolution of IA has been driven by Industry 4.0, where digital transformation plays a crucial role in automating complex business operations [1, 2].The concept of IA emerged from the early developments in automation and artificial intelligence, which initially focused on mechanizing repetitive tasks. However, as AI and machine learning advanced, the potential to automate decision-making processes, analyze large datasets, and predict future trends became more apparent. IA combines these technologies to offer solutions that go beyond rule-based automation, allowing systems to learn, adapt, and improve over time. According to Bornet et al., IA enables businesses to operate more efficiently by automating knowledge-based tasks that previously required human expertise [7].The banking industry has been at the forefront of IA adoption, leveraging it to enhance customer service, detect fraud, ensure regulatory compliance, and optimize back-office operations. The adoption of IA in banking has transformed traditional financial services, allowing institutions to improve security, enhance customer experience, and reduce operational costs. Despite its potential, IA adoption in Malaysia has been relatively slow, primarily due to concerns related to cybersecurity threats, regulatory challenges, and workforce readiness [1, 3]. As Malaysia continues to embrace digital banking solutions, the role of IA will become increasingly critical in ensuring sustainable banking operations.

2.2 Key Components of IA

The three fundamental elements of Intelligent Automation (IA) in banking operations are Robotic Process Automation (RPA) together with Business Process Automation (BPA) and Artificial Intelligence (AI). The combination of these three components delivers distinct functions which support automated decision systems and operational process streamlining while reducing manual work. Organizations use Robotic Process Automation (RPA) as a software-based tool to automate recurring rules-based operations and eliminate human staff involvement. Software bots operating through RPA systems conduct operations including data entry and transaction processing and customer onboarding which produces greater process efficiency with lower error rates [6]. In banking operations RPA proves vital because it cuts operational expenses while achieving better compliance standards. RPA adoption by banks has become widespread for enhancing processes involving loan processing while also improving anti-money laundering checks along with fraud prevention. Laboratory research confirms that RPA enables organizations to lower operational expenses by 30% and boost data processing precision and velocity [6] [8]. The integration of RPA technology into existing banking systems proves simple because it does not demand extensive changes to infrastructure. RPA systems confront a key restriction because they have no natural ability to make decisions outside of their predefined rules. AI-powered solutions step in at this point to enable machines to learn from data and enhance automation processes according to references [7, 8].

2.3 Business Process Automation (BPA)

Business Process Automation (BPA) serves as a general automation platform which enhances workflows across an entire business system beyond basic rules-controlled activities. BPA uses data analytics alongside artificial intelligence to perform automated decision projects and optimize resource deployments and improve workflow systems. Business Process Automation differs from RPA because it handles full process automation to achieve complete end-to-end support for banking operations [7, 8]. Financial institutions have used BPA implementation to enhance their operational efficiency together with regulatory compliance standards. AI-powered Business Process Automation tools support banks to fulfil their strict regulatory needs by monitoring compliance and detecting fraud and assessing risks which simultaneously enhances their service delivery [8, 9]. The analysis of customer data through BPA lets banks deliver personalized services to their clients by forecasting future financial developments. Real-time tailored loan suggestions together with investment guidance and risk evaluation reports along with predictive analytics and machine learning capabilities are now available to banks

for providing to their customers [8]. The successful deployment of BPA needs powerful cybersecurity tools to stop data breaches and cyberattacks despite being a major concern for financial establishments [9, 10].

2. 4 Artificial Intelligence (AI)

Artificial Intelligence (AI) serves as the backbone of Intelligent Automation, enabling machines to process vast amounts of data, detect patterns, and make informed decisions. AI-driven automation solutions include natural language processing (NLP), machine learning (ML), and cognitive computing, all of which contribute to enhanced decision-making in banking operations [6, 9].The implementation of AI technologies within banking automation systems has successfully improved security systems and risk assessment as well as fraud detection capabilities. Real-time transaction monitoring by AI-powered fraud detection systems enables them to detect suspicious activities which prevents fraudulent transactions. Cybersecurity operations within digital banking require AI-based systems to effectively protect against cyber threats [9]. AI technology improves customer service operations by implementing chatbots and virtual assistants as innovative components. AI-driven banking assistants deliver customized customer assistance and financial advice through automated systems that separately provide help and recommendations to users [6, 9]. The widespread adoption of AI in banking encounters resistance because of privacy concerns together with algorithmic bias and ethical problems that demand thorough examination before complete adoption [9, 10].

2.5 Previous Studies on IA Adoption in the Banking Industry

The banking field has extensively researched about IA to reveal both its operational advantages and technical obstacles as well as emerging automation prospects for financial services. Budgetary responsibilities drive the banking industry to adopt IA for greater operational efficiency alongside better security measures and regulatory compliance [7, 8]. Various research has investigated the operational effects of both RPA and BPA in banking institutions. Ribeiro et al. (2021) investigated RPA implementation throughout financial organizations and established that this technology cuts manual workloads and enhances operational performance along with maintaining regulatory standards [6]. The paper by Joseph explores AI-powered automation in sustainable banking by demonstrating how cognitive AI and machine learning power banking operations [8].

Research shows that organizations face difficulties implementing IA because of cybersecurity threats together with legislative ambiguities. Many financial institutions show reluctance toward implementing AI-based cybersecurity solutions because of their worries about data privacy matters alongside system weaknesses and compliance difficulties as per Rashed &Kassim [10]. Financial institutions must establish strong cybersecurity frameworks to defend their sensitive financial information because of the increasing need [9] [10]. The implementation of IA solutions is expected to expand at a substantial pace since organizations persist in developing their digital platforms. The Malaysian banking industry experiences swift digitalization because government initiatives and regulatory backing push for adoption of AI-based banking technology [1, 2]. Additional research is required to understand the long-term effects of IA adoption within banking enterprises while also creating best practices to handle automation risks in banking institutions [2, 3].

3. Determinants of IA Adoption in Banking Sector

The adoption of Intelligent Automation (IA) in the banking sector is influenced by multiple organizational and individual factors. Key determinants such as individual work resilience, perceived organizational innovativeness, strategic thinking competency, and cybersecurity awareness shape the intention to integrate IA technologies into banking operations. The alignment of these factors ensures successful digital transformation, fosters innovation, and enhances security measures [4], [6]. This section discusses the primary determinants affecting IA adoption in banking.

3.1 Individual Work Resilience and IA Adoption

Work resilience among individuals represents their capacity to maintain efficient performance while adapting their response to both obstacles and technological disruptions at work. Banking institutions implementing IA systems face three main consequences which include modified job positions and automated repetitive operations and technologically advanced working environments. Staff members who demonstrate resilience effectively accept job transformations and they embrace AI technologies while collaborating with automated systems [5, 7]. Resilient workers demonstrate increased ability to adapt to and accept IA-based solutions when their organizations pursue digital transformation according to research [5]. Employees need to successfully handle workplace stress and workload while working in technology-based environments to enable smooth implementation of IA in banking operations. Studies show that Wang et al. (2022) demonstrated individual resilience has a positive influence on job performance when managing digital transformation in organizations [5]. The implementation rates of IA rise when organizations create supportive atmospheres which support ongoing learning and professional growth for their members. Employees who see automation as a development chance rather than a risk become front-runners in the digital transformation process. Successful implementation of IA requires organizations to develop programs that enhance resilience because resistance to change affects the adoption outcomes [5, 6].

3.2 Perceived Organizational Innovativeness and Readiness

Institutions that excel at quick technology adoption through effective implementation qualify as organizations with perceived organizational innovativeness. The banking sector demonstrates its willingness through investments in IA as well as building a digital culture and developing methods for automated systems integration. The adoption of IA solutions proves more likely among organizations which recognize

themselves as technologically advanced [6, 7]. According to research evidence banks that emphasize innovation in their workplace culture embrace IA at a quicker rate and with better effects when compared to institutions which oppose digital transformation. The research by Bornet et al. [6] reveals that organizations focusing on innovation with digitalization gain market advantage through automated systems for better operational efficiency and service excellence [7]. The essential indicators for organizational readiness in adopting IA are listed in Table 1.

Table 1: Indicators of Organizational Readiness for IA Adoption

Indicators	Description
Digital Infrastructure	Presence of cloud computing, AI platforms, and automation tools
Leadership Support	Commitment of top management towards IA investments
Employee Training Programs	Upskilling initiatives for employees to adapt to IA
Cybersecurity Preparedness	Implementation of AI-driven cybersecurity measures
Regulatory Compliance Strategies	Readiness to align with financial regulations

Source: Adapted from [6, 7].

An approach to automation which stays ahead of problems results in better risk control along with enhanced user satisfaction and more efficient banking procedures. Organizations which lack readiness towards IA implementation experience solution implementation delays together with elevated operational perils and decreased adoption rates of their IA solutions [6, 8].

3.3 Strategic Thinking Competency and Its Role in Technology Adoption

Organizations need strategic thinking competency to enable their adoption of IA because it helps them establish effective planning and execution as well as optimization of automation technologies. Strategic foresight among employees and decision-makers enables them to predict future banking operational effects of IA while establishing automation strategies based on business targets and projecting upcoming challenges [6,7]. The banking industry faces quick expansion which demands leaders to develop strategic thinking abilities for steering technology-based organizational change. The combination of strategic planning scope and automation investments produces better efficiency along with superior risk management performance in banking institutions according to Joseph (2023) [8]. Strategic leaders create open collaboration areas to keep workers involved in automation adoption activities instead of seeing AI implementation as disruptive. Strategic decision-making requires banks to create guidelines that address AI governance as well as cybersecurity standards and ethical frameworks in banking automation practices [7, 8].

3.4 Moderating Effect of Cybersecurity Awareness

Financial institutions process and handle automation technology risks through cybersecurity awareness which acts as a key moderating factor for adopting information security measures. The increasing adoption of AI-based solutions faces crucial security barriers to adoption which include data breaches and cyberattacks alongside identity theft incidents [9, 10].

Table 2: Cybersecurity Challenges in IA Adoption

Cybersecurity Challenge	Impact on IA Adoption
Data Breaches and Unauthorized Access	Weakens trust in IA-powered banking systems
Phishing and AI-Based Cyber Threats	Increases vulnerabilities in financial transactions
Regulatory Compliance Issues	Slows down IA implementation due to stringent security laws
Lack of Employee Awareness	Creates risks in AI-enabled fraud detection systems

Source: Adapted from [9, 10].

Organizations that establish strong cybersecurity cultures together with employee awareness programs become more capable of deploying IA while maintaining secure data [9]. To gain user confidence financial institutions need to dedicate funds to AI-based cyber security programs and compliance initiatives for automation solutions [10].

4. Challenges and Barriers in IA Adoption

IA adoption faces resistance in banking institutions because of technical limitations alongside regulatory constraints as well as workforce capacity issues and financial barriers. To achieve optimum automation potential and proper integration financial institutions need to resolve existing obstacles. The main obstacle preventing organizations from adopting IA stems from their insufficient technological infrastructure. Banking organizations face challenges because their current legacy systems do not integrate well with artificial intelligence automation solutions which produces operational inefficiency and integration problems [4], [6]. The inability to scale automation applications thus limits banks in their efforts to expand automated software beyond individual branches or departments. Implementing large-scale IA requires banks to spend on cloud computing technology as well as big data analytics and AI infrastructure according to studies [4, 6].

4.2 Cybersecurity Risks and Compliance Issues

Banking institutions face considerable cybersecurity challenges which prevent widespread adoption of information automation systems. The adoption of artificial intelligence in automated systems exposes financial institutions to increased cyber threats which forces them to create robust protection measures for data security [9, 10]. To guarantee secure AI implementation in financial transactions institutions must properly follow PSD2 and GDPR regulatory standards. Failure to comply with standards results in legal liabilities together with potential damage to reputation for institutions [9] and [10]. When institutions implement IA there arises concern for job displacement that creates employee resistance to automation processes. A majority of employees view IA as an existence threat to their jobs making them reluctant to adopt it [5, 7]. The implementation of IA faces difficulties because financial institutions lack adequate capabilities in AI and machine learning combined with data analytics skills. Financial institutions need to develop employee training initiatives which enable staff to adjust to AI-operated banking

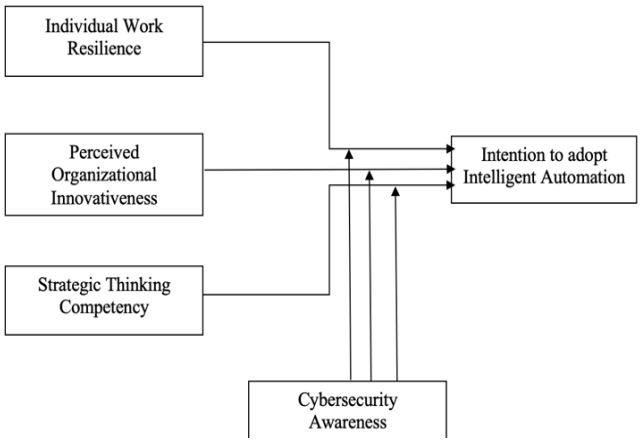
operations [5, 7]. The implementation expense of IA solutions creates an obstacle mainly affecting financial institutions that operate between mid-sized and small banking segments. Banks need to weigh their startup expenses against anticipated future returns over a long period [8, 10].

Table 3: Cost-Benefit Analysis of IA Adoption in Banking

Cost Factor	Potential Benefits
High Initial Investment	Long-term cost reduction and efficiency gains
AI Infrastructure Maintenance Costs	Enhanced customer experience and operational agility
Compliance and Regulatory Costs	Improved security and fraud detection

Source: Adapted from [8, 10].

5. Conceptual Framework Development



The conceptual framework showcases three main influencing factors for Banking sector adoption of Intelligent Automation through Individual Work Resilience and Perceived Organizational Innovativeness and Strategic Thinking Competency while Cybersecurity Awareness functions as a moderating influence. The resilience of individual work enables employees to face automation changes through improved digital abilities and training. Organizational perception about embracing new technologies indicates how willing banks become to advance digital transformation through emerging technologies. The strategic thinking competency helps organizations to direct information automation projects toward business objectives and maintain regulatory compliance and risk management standards. The role of Cybersecurity Awareness becomes vital because it controls how individuals perceive risk while they adopt security protocols and build their trust in automation systems. Organizations that establish robust cybersecurity practices together with employee awareness tend to implement Intelligent Automation successfully even though organizations without such measures can encounter implementation challenges because of data protection concerns and regulatory compliance specifications as well as operational perils. The framework demonstrates how readiness and resilience together with security awareness form a system that drives Information Assurance adoption processes.

6. CONCLUSION

The adoption of Intelligent Automation (IA) in banking signifies a major transformation, integrating Artificial Intelligence (AI), Robotic Process Automation (RPA), and Business Process Automation (BPA) to enhance efficiency, security, and customer service. This study explored key determinants influencing IA adoption, including Individual Work Resilience, Perceived Organizational Innovativeness, and Strategic Thinking Competency, with Cybersecurity Awareness as a moderating factor. Findings suggest that organizations fostering resilience, innovation, and strategic planning are more likely to adopt IA successfully. However, barriers such as cybersecurity concerns, regulatory challenges, workforce readiness, and cost constraints remain critical. A systematic research agenda combined with suggested policies together with enhanced cybersecurity training will enable smooth implementation of IA solutions.

The research established Individual Work Resilience as a fundamental quality which enables employees to adapt to automation while decreasing their opposition to change. The perceptual innovativeness of organizations sets bank readiness to implement IA solutions while Strategic Thinking Competency aids business follow-up with fundamental corporate objectives and risk reduction initiatives. The level of cybersecurity awareness affects these relationships because better security measures combined with reduced hesitation in IA adoption result from increased awareness levels. Inadequate cybersecurity practices cause institutions to hold back because of worries about data breaches and compliance risks and regulatory uncertainties.

A combination of empirical research should examine the implementation of Intelligent Automation in Malaysian banking sectors and its sustained impact on employment stability together with organization performance alongside AI bias and data privacy challenges. Public officials need to create guidelines that manage AI governance alongside cybersecurity requirements along with programs to advance workforce capabilities. Wholesale banks need to improve customer cybersecurity knowledge by conducting training programs and deploying AI security systems together with educational programs targeting bank customers. Financial institutions can achieve successful implementation of IA with risk mitigation by building strong cybersecurity strategies and maintaining regulatory compliance. The research gives essential guidance to banking executives and policymakers and researchers for designing financial sector automation developments.

REFERENCES

1. Yeo, H. R. (2022). *Design and development of Malaysian cybersecurity profiling framework: Towards creating a recommendation system to combat cybercrime* (Doctoral dissertation, UTAR).
2. Mohamad, E., Abd Rahman, M. S., Rahman, A. A., Mohamad, N., Azlan, N. N., &Saptari, A. (2021).

Investigation of the awareness level in Malaysia's manufacturing industries on the implementation of industry 4.0. *JIE Scientific Journal on Research and Application of Industrial System*, *6*(1), 53-66.

3. Subramaniam, S. R. (2017). Cyber security awareness among Malaysian pre-university students. *Proceeding of the 6th Global Summit on Education*, 1-14.
4. Lu, Y., Wang, L., Nassehi, A., & Wan, J. (2024). Smart manufacturing enabled by intelligent technologies. *International Journal of Computer Integrated Manufacturing*, *37*(1–2), 1–3.
5. Wang, A., Tang, C., Song, J., Fan, C., Wang, W., Chen, Z., … & Yin, W. (2022). Association of individual resilience with organizational resilience, perceived social support, and job performance among healthcare professionals in township health centers of china during the covid-19 pandemic. Frontiers in Psychology, 13.
6. Ribeiro, J., Lima, R., Eckhardt, T., & Paiva, S. (2021). Robotic Process Automation and Artificial Intelligence in Industry 4.0 - A Literature review. *Procedia Computer Science*, *181*, 51–58.
7. Bornet, P., Barkin, I., & Wirtz, J. (2021).*Intelligent Automation: Welcome to The World ffHyperautomation: Learn How to Harness Artificial Intelligence to Boost Business & Make Our World More Human*
8. Joseph, O. (2023). Sustainable banking through robotic process automation: what role does esg and cognitive ai play?. Journal of Digitovation and Information System, 3(1), 116-140.
9. Kaloudi, N., &Jingyue, L. I. (2020). The AI-based cyber threat landscape: A survey. *ACM Computing Surveys*, *53*(1).
10. Rashed, M., & Kassim, N. M. (2023). Factors influencing user's intention to adopt AI-based cybersecurity systems in the UAE. *Interdisciplinary journal of information, knowledge, and management*, *18*, 459-486.
11. Ansari, M. F. (2021). *The Relationship between Employees' Risk Scores and the Effectiveness of the AI-Based Security Awareness Training Program*. University of the Cumberlands.
12. Ren, Y. (2024). *Factors Impacting the Adoption of Artificial Intelligence Powered Cybersecurity Virtual Assistant: A Quantitative Study* (Doctoral dissertation, National University).
13. Yan, B., & Teng, Y. (2025). The double-edged sword effect of artificial intelligence awareness on organisational citizenship behaviour: a study based on knowledge workers. *Behaviour & Information Technology*, 1-17.
14. Khan, S. K., Shiwakoti, N., Stasinopoulos, P., Chen, Y., & Warren, M. (2024). The impact of perceived cyber-risks on automated vehicle acceptance: Insights from a survey of participants from the United States, the United Kingdom, New Zealand, and Australia. *Transport policy*, *152*, 87-101.
15. Oprea, S. V., Nica, I., Bâra, A., & Georgescu, I. A. (2024). Are skepticism and moderation dominating attitudes toward AI- based technologies?. *American Journal of Economics and Sociology*, *83*(3), 567-607.