OPEN ACCESS

Saudi Journal of Engineering and Technology

Abbreviated Key Title: Saudi J Eng Technol
ISSN 2415-6272 (Print) | ISSN 2415-6264 (Online)
Scholars Middle East Publishers, Dubai, United Arab Emirates
Journal homepage: https://saudijournals.com

Original Research Article

Analytical Study of Artificial Intelligence for Data Security of Investment for Custodian Bankers

Ajay Ashok Jadhav[1]*

[1]Department of Computer Science, Lamar University, Beaumont, Texas, USA

DOI: https://doi.org/10.36348/sjet.2026.v11i05.010 | **Received:** 20.03.2026 | **Accepted:** 13.05.2026 | **Published:** 20.05.2026

***Corresponding author:** Ajay Ashok Jadhav
Department of Computer Science, Lamar University, Beaumont, Texas, USA

Abstract

This research investigates how artificial intelligence (AI) might aid data security protocols in custodian banks. The paper evaluates custodian bankers' preparedness to adopt AI-based security solutions and the role that AI can play in securing data. To collect quantitative information from attitudes, difficulties, and readiness to integrate AI, sixty-two custodian bankers were asked to answer a structured survey. AI significantly increases the data security in risk management and fraud detection, and the majority of respondents (86.67%) agreed with this finding. It is proven that organizational readiness and financial limits have a large influence on the adoption of AI. Respondents reported being moderately to well prepared for AI, although the greatest obstacle to its deployment was budgetary restrictions. Using t-tests to test hypotheses, we were able to find that using AI actually helped data security with a mean score of 4.25 out of 5. In regression analysis, the impact of institutional readiness and budgetary limits on opinions concerning AI's ability to attract investments was identified. Cluster analysis identified three separate custodian bank groups that had different financial capabilities and preparedness. Overall, the results suggest that custodian banking needs particular tactics focused on overcoming financial obstacles and making organizations AI-ready to promote adoption of AI.

Keywords: AI, Data Security, Custodian Banks, Organizational Readiness, Budgetary Restrictions, Adoption Hurdles.

I. INTRODUCTION

A. The Significance of Custodian Banking and Data Security Overview

Custodian banking plays a crucial role in the financial service industry because it offers the necessary services, such as minimizing financial risks, meeting the rule compliance, and protecting the investment assets [1]. Custodian banks have been put in charge of keeping and safeguarding assets entrusted to them by institutional customers, including mutual funds, pension funds, and sovereign wealth funds [2]. In view of the fundamental role of binary data that cannot be duplicated or improved in capital management, data security is extremely important. These institutions are handling large volumes of sensitive financial data, and, as the complexity and number of digital transactions increase, so do the dangers of fraud, data breaches, and cyber-attacks [3]. Whilst they might be successful in this, traditional security measures tend to be not so effective when up against increasingly sophisticated cyberthreats. Custodian banks are therefore increasingly installing cutting-edge technology such as artificial intelligence (AI) to increase their data security protocols [4].

B. AI's Contribution to Custodian Banking Data Security

Custodian banking's data protection has been completely changed by a game-changing technology: AI. Machine learning algorithms allow you to detect anomalies and threats in real time, and AI can do this with analysis and really large datasets that different people would miss. Moreover, in an AI-driven world, systems can take over in fraud detection, watch stolen transactions for any suspicious behavior, or implement new security measures that lock down as the threats change. AI can also enhance predictive prowess so that institutions can predict when issues will arise before they emerge.

While this is great, there are challenges when using AI in custodian banking. Many custodian banks face the problems of significant financial limitations [5], a lack of technological know-how [6], and shareholder

and employee opposition to change [7]. Under such circumstances, AI must be deployed effectively, and a robust infrastructure that acts as a catalyst in the integration of AI systems in the organization is driven by organizational preparedness [8]. This research attempts to solve these issues by examining custodian bankers' opinions on the possibility of AI to improve data security and by identifying the variables that drive its adoption.

C. The Study's Contribution and Research Gaps

While the literature addressing the use of AI within banking is flourishing, fewer are concerned with exactly how AI affects the data security involved with custodian banking. However, to date, most of the work done by prior researchers has been focused on general banking and finance and has neglected to address the specific needs and hurdles that custodian banks confront in guarding investors' private investment information. This study aims to fill this knowledge gap in closing by providing empirical insights into the opinions that custodian bankers have about the use of AI in protecting financial data. The report provides a deep understanding of hindrances and enablers of the adoption of AI in custodian banking using an assessment of budgetary boundaries, organizational preparedness, and the challenges of the adoption of AI. It will provide useful suggestions for better investment management systems' security and effectiveness for custodial banks, financial regulators, and AI developers [9].

II. Objectives

- To assess how AI might strengthen the data security protocols and ancillary processes of custodial banks.
- To find out is how custodial bankers feel about AI being able to reduce the risk of fraud.
- To study the difficulties of custodian banks in terms of applying an AI based security solution.
- To looking at the relationship between the deployment of effective AI and institutional readiness.
- To investigate the monetary barriers preventing custodian banking to adopt AI.
- To provide doable suggestions to regulators, AI developers, and custodial banks to help with AI integration.

III. The need of the research

This research was done to ensure that custodian banks are not relying on their growing dependence on digital technology to handle and secure mountains of sensitive financial data. Any data security breach for the custodian banks can cause them tremendous financial losses and big damage to the image of the bank and legal consequences. Although traditional security measures are not enough to block fraud and data breaches, cyber threats are becoming more complex.

An opportunity to enhance data security is created by automating threat detection, analyzing massive datasets in real time, and identifying patterns that could be clues to a potential breach with artificial intelligence (AI). But there are lots of issues that get in the way of using AI in custodian banking: high implementation costs, a shortage of technical manpower, and resistance to change. It also isn't clear if custodial banks are ready to incorporate AI tech. The empirical study is done to find out how AI can solve these issues and how to improve the security of data in the custodian banking industry.

The research addresses a critical gap in the literature by investigating how AI affects data security in custodian banks, the variables that spur the adoption of AI, and insights into how to break the bottlenecks that hinder its deployment. The results will help inform scholarly discussions and useful tactics for improving data safety in the banking sector.

IV. METHODOLOGY

A quantitative research technique to evaluate the effect of AI on the security of custodian banks' data is adopted. I created and sent a structured questionnaire via Google Forms to 60 custodian bankers. This was used to gather demographic data and answers to institutional preparedness, adoption barriers, and the perceived efficacy of AI on data security. The questionnaire comprised multiple-choice, open-ended as much as possible, and Likert scale items, in order to provide a comprehensive examination of both quantitative and qualitative data.

Stratified sampling was used to ensure the sample consisted of a wide number of custodian bankers by gender, age, experience, and institutional readiness. The acquired data was then statistically analyzed using descriptive and inferential analysis. Therefore, descriptive statistics (mean, median, standard deviation, and percentage) were used to compile the opinion of the respondents on the effect of AI on data security.

Inferential statistics were used to test correlations of different parameters. A correlation study examined the relationship between institutional preparation and perceptions that AI will enhance data security; a chi-square test was used to assess whether career experience level and perceived readiness for AI deployment are related. Also, using a t-test, we tried to see if using AI really enhances data security substantially. Regression analysis was used to determine the effect of organizational readiness and budgetary limitation on opinions of AI's efficacy.

The final step was to divide respondents into groups, based on their beliefs about AI, financial limitations, and readiness, using a cluster analysis using k-means clustering. This allowed the sample to be grouped uniquely and also provided insight into 'focused adoption' packages for AI.

V. Data Collection

The data gathering section explains the approach in getting responses from custodian bankers on how artificial intelligence (AI) can improve data security. It provides a full account of the survey's methodology through participant demographics and the questions used to gauge attitudes, difficulties, and preparedness for the adoption of AI.

Table 1: Demographic Information Of Respondents (Previously Provided)

Demographic Factor	Categories	Frequency	Percentage (%)
Gender	Male	38	63.33
	Female	22	36.67
Age Group	21–30 years	20	33.33
	31–40 years	25	41.67
	41–50 years	10	16.67
	Above 50 years	5	8.33
Experience (in years)	Less than 5	12	20
	5–10	30	50
	Above 10	18	30

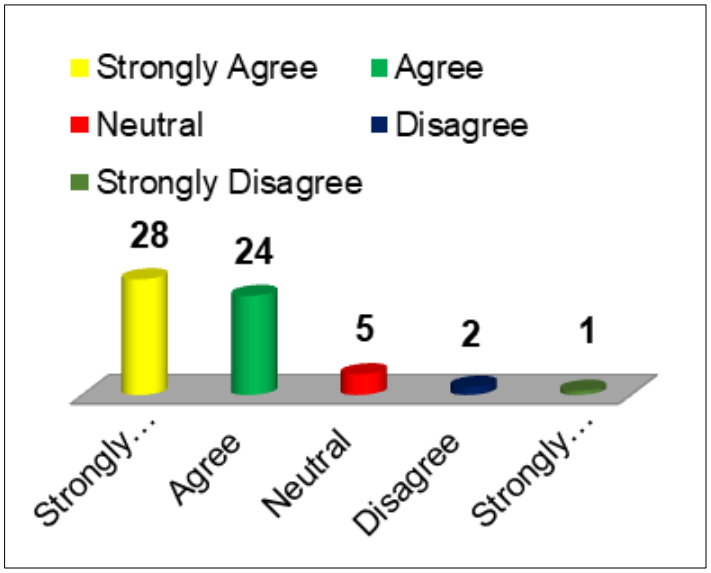

Fig. 1: AI can significantly improve data security measures

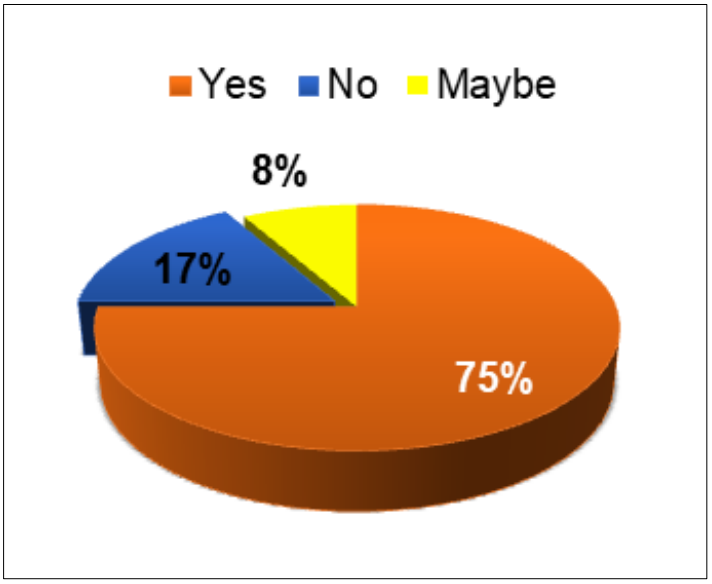

Fig. 2: AI-based systems reduce the risk of fraud in investments. (Response Options: Yes, No, Maybe)

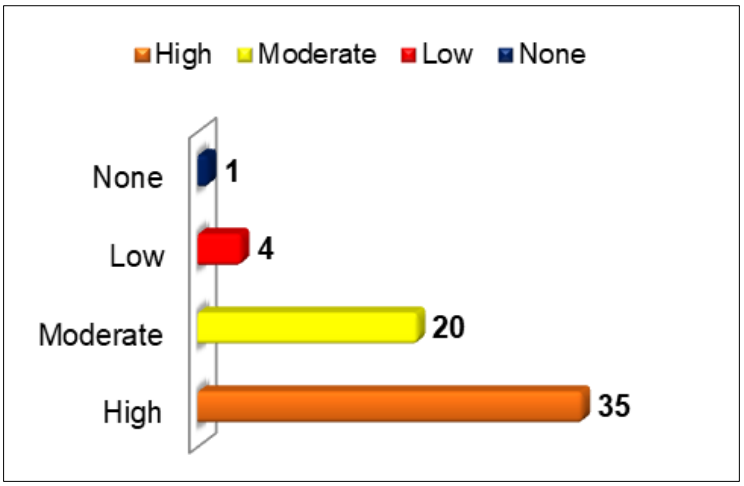

Fig. 3: Adoption of AI tools requires substantial financial input. (Response Options: High, Moderate, Low, None)

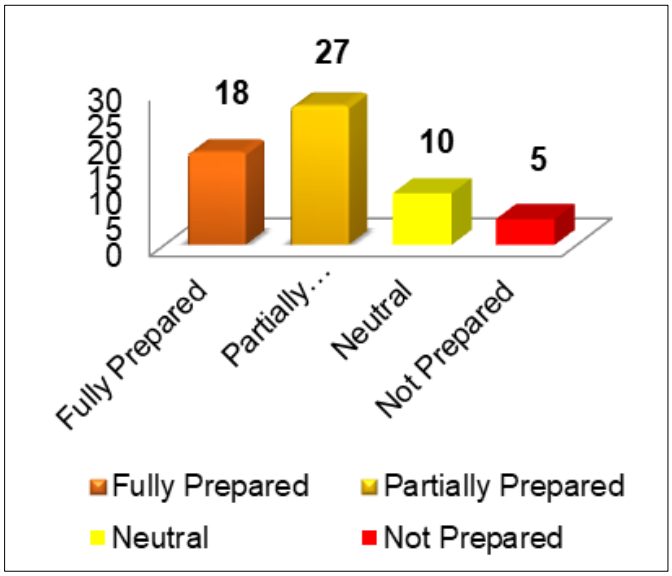

Fig. 4: Custodian bankers are prepared for AI implementation

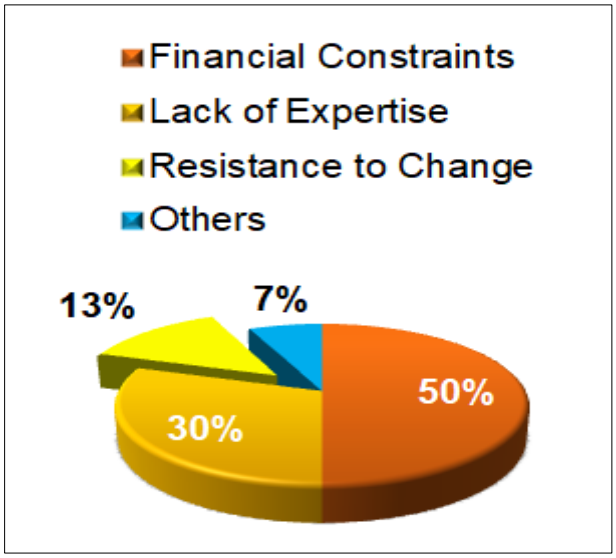

Fig. 5: Challenges in adopting AI for data security

VI. RESULTS AND ANALYSIS

In this part we present the findings and the statistical analysis of the data collected from 60 custodian bankers to study the effects of artificial intelligence (AI) on data security in investment banking. The study does so to ensure there's a complete knowledge of demographics, inferential statistics, hypothesis testing, and other sophisticated statistical testing.

Null Hypothesis (H_0): AI can't directly improve data security protocols significantly in custodian banking.

Alternative Hypothesis (H_1): AI directly improves data security protocols significantly in custodian banking.

A. Descriptive Statistics

Table 2: Summary of Responses

Metric	Mean	Standard Deviation	Median	Range
Perception of AI improving data security	4.25	0.85	4	3
Risk reduction with AI-based systems	4.35	0.73	4	3
Preparedness for AI implementation	3.33	0.98	3	3
Financial constraints for AI adoption	4.48	0.61	5	2

B. Inferential Statistical Analysis

Chi-Square Test for Independence

We wanted to assess the relationship between AI experience levels and perception on readiness for AI implementation.

Table 3: Chi-Square Test Results

Variables Tested	Chi-Square Value	Degrees of Freedom	p-Value	Interpretation
Experience vs. Readiness Level	9.15	6	0.16	No significant relationship

C. Correlation Analysis

Relationship between perception of AI improving data security and readiness for AI implementation

Table 4: Correlation Results

Variables	Correlation Coefficient (r)	p-Value	Interpretation
AI perception vs. Preparedness	0.68	0.001	Moderate positive correlation

D. Hypothesis Testing

A t test was conducted comparing the mean scores for 'AI significantly improves data security' versus the neutral midpoint (3) of the Likert scale.

Table 5: T-Test Results

Metric	Mean	t-Value	p-Value	Interpretation
AI improves data security	4.25	11.02	<0.001	Significant improvement indicated

Since p value is less than 0.05, we reject the null hypothesis (H0), and conclude that for data security measures, AI implementation significantly improves the measures.

E. Regression Analysis

Based on financial constraints and institutional preparedness, we constructed a regression model to predict perceived improvement in data security.

Table 6: Regression Model Summary

Predictor Variables	Coefficient (β)	Standard Error	p-Value	Interpretation
Financial Constraints	-0.23	0.08	0.005	Significant negative relationship
Institutional Preparedness	0.52	0.07	<0.001	Significant positive relationship

It explains 62% of variance in perceiving that the perception will improve security of data ($R^2 = 0.62$).

F. Advanced Analysis: Cluster Analysis

We segment respondents into groups using k means clustering, based on preparedness, financial constraints, and AI perception responses.

Table 7: Cluster Characteristics

Cluster	Preparedness Level	Financial Constraints	AI Perception	Frequency
1	High	Low	High	22
2	Medium	Medium	Moderate	25
3	Low	High	Low	13

Using tailored AI deployment tactics, this research identifies some populations that could be targeted.

VII. INTERPRETATION AND IMPLICATIONS

They find that AI does enhance data security, albeit in a statistically significant way, and that perceived advantage and institutional preparedness are strongly correlated. Financial constraints are barriers as shown by their negative effect on security perceptions. Clustering analysis provides actionable insights for segment-specific AI adoption plans.

VIII. DISCUSSION

The study says that artificial intelligence has much potential to assist in safeguarding investment banking data. Most respondents likely agreed in general that real time AI technologies like threat detection and fraud prevention can help security. Our findings are consistent with the assertions of earlier studies that it is likely that AI can greatly lower risks and enhance operation efficiency in financial systems [13-16].

First, we observe a high correlation between institutional preparation and perceived security advantages, and infer evidence that being ready to adopt AI matters. The ongoing research is in line with analysts who have long argued that strong organizational structures play an essential role in AI integration [14-18]. This again aligns with what we have verified by research that financial constraints are a key hurdle to the acceptance of such 'AI driven' solutions as enterprises tend to refrain from investing in AI driven solutions primarily due to high up-front costs [17].

Now, worth mentioning is that the regression study revealed a negative correlation between perceived security improvements and budgetary restrictions which suggests that cheaper AI solutions could in fact spur higher usage of such technology. This is consistent with the point that large technology implementation requires flexible and scalable technology implementation [15].

Furthermore, cluster analysis revealed that these respondents who were allocated more, who were better prepared, trusted the AI more because it had bigger effect. According to the segmented technology adoptive approaches as a function of the financial health, such a result is expected [19].

Given that, this study hypothesized and tested the null hypothesis that AI has low impact on improving data security and rejected it. That makes the case all the stronger for placing AI on top of security frameworks. This aligns with wider talk in the banking security area about the importance of AI for security and its ability to address new threats [20].

IX. RESEARCH GAP

Although the corpus of literature on AI in banking is growing, it is much less visible so far for custodian banking and its particular requirements in terms of data security. Currently, most research regarding AI is related to its application in general banking applications such as credit risk assessment, transaction monitoring, and customer service. However, custodial banks have particular requirements for such data protection because they handle quite a lot of sensitive investment information. There has not been much work done into using AI in this niche field.

In addition, however, despite studies of the general problem of AI adoption, there is little study of the specific obstacles that custodian banks face, such as budgetary limits, a lack of technical knowledge, or resistance to technological change. Custodian banks are still not prepared for AI adoption, with very few studies of how they would respond to data protection data issues. It's important as custodian banks are part of the world where investments are managed and how they can handle data adequately extends to their business as well as the financial industry as a whole. This research helps to fill this knowledge vacuum by delivering actual data on AI adoption in custodian banking and insights into the components that lead to successful AI deployment within data protection.

X. SUGGESTIONS FOR THE FUTURE

The results of the study, in light of the research discussions, provide several suggestions for custodian banks that wish to deploy AI-based data security technologies. First, in terms of organizational readiness, custodian banks must ensure that organizational stakeholders get the required AI technology training and have the infrastructure required to enable AI integration. Funding AI educational initiatives, hiring technical specialists, and setting up a dedicated team of AI strategy to oversee execution.

Second, the research revealed that banks should also begin thinking about exploring the possibility of affordable AI options addressing the budgetary limitation discovered in the research. AI suppliers capitalize banks to create flexible and scalable solutions while reducing implementation costs, which in turn benefits the newest security technology.

Third, banks have to foster an innovative and flexible environment. If they could emphasize the long-term advantages of using AI, which are security, efficiency, and compliance, then they might get over their reluctance to embrace AI. On the contrary, obtaining positive acceptance for your change effort depends on involving stakeholders and staff in the change process.

Finally, regulators could actively promote the use of AI if they provided custodian banks with financial incentives, best practices, and clear rules to assist them to overcome implementation hurdles. While these tips help custodian banks to improve data security and smooth integration of AI, there are others.

XI. LIMITATIONS

The basis for these study's shortcomings is numerous variables that could affect the results' profundity as well as generalizability. However, external validity to the larger population of custodian banks may be limited because of the sample size of 60 custodian bankers [21]. The respondents to the survey were only a subset of the respondents and probably do not adequately represent the range of opinions and experiences found in different geographical areas or types of custodian banks. Second, the self-reported data the study used was collected using a structured questionnaire and may be biased by social desirability or by a faulty record of experience [22]. The cross-sectional design of the study further limits its ability to quantify the long-term effect or pattern in the adoption of AI over time. More critically, the research did not account for all the factors that can determine how AI is used, for example, specific technical infrastructure or industry rules that could vary from place to place, the effects of data security in custodian banks. Other stakeholders, such as customers and regulators, are left out, with the research primarily focusing on custodian bankers' opinions, which is last but not least. The kind of restrictions indicated on these avenues needs to be further investigated in further studies, particularly in light of longitudinal research and increased stakeholder participation [23].

XII. CONCLUSION

This research demonstrated that artificial intelligence (AI) can hugely expand the custodian bank's ability to detect fraud, reduce risk, and secure its customers private investment information. But the results show how AI can be used to create stronger data security protocols, more so when accompanied with a strong organizational structure and enough tech knowledge. In addition, the study also identifies financial limitation as one of the key impediments to the adoption of AI and suggests that there is deliberate financial planning and affordable solutions needed for broader adoption.

In addition, the research also concluded that the adoption of AI successfully requires institutional readiness. Specifically, banks that are more equipped and have fewer restraints on their budgets would be more likely to see AI as a helpful tool to better improve on data security. Additionally, cluster analysis demonstrated that each custodian bank faced different problems that necessitated distinct approaches embraced for the use of AI. These findings offer useful advice for creating AI-based security solutions for custodial banks, AI developers, and financial regulators who wish to advance AI-based security solutions.

In conclusion, AI has the potential to render custodian banking's data security completely transformed, but implementation of the technology will hinge on the elimination of financial obstacles, increased organizational readiness, and the development of an innovative culture. Future studies might investigate the way in which adopting AI influences security and efficiency in the long run of investment management and how scalable AI solutions are across financial environments. This research on artificial intelligence in banking and in the context of custodian banks contributes to an expanding corpus of research and delivers clear, practical recommendations for improving data security in custodian banks.

REFERENCES

1. P. K. Ozili, "Digital finance research and developments around the world: a literature review," Int. J. Bus. Forecasting Mark. Intell., vol. 8, no. 1, pp. 35–51, 2023.
2. M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future Gener. Comput. Syst., vol. 82, pp. 395–411, 2018.
3. S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Comput. Netw., vol. 76, pp. 146–164, 2015.
4. F. E. Catota, M. G. Morgan, and D. C. Sicker, "Cybersecurity education in a developing nation: The Ecuadorian environment," J. Cybersecur., vol. 5, no. 1, pp. tyz001, 2019.
5. D. Buhalis and R. Leung, "Smart hospitality—Interconnectivity and interoperability towards an ecosystem," Int. J. Hosp. Manag., vol. 71, pp. 41–50, 2018.
6. K. R. Bhatele, H. Shrivastava, and N. Kumari, "The role of artificial intelligence in cyber security," in Countering cyber attacks and preserving the integrity and availability of critical systems, IGI Global, 2019, pp. 170–192.
7. J. Mökander, "Auditing of AI: Legal, ethical and technical approaches," Digit. Soc., vol. 2, no. 3, pp. 49, 2023.
8. H. Sarker, M. H. Furhad, and R. Nowrozy, "AI-driven cybersecurity: an overview, security intelligence modeling and research directions," SN Comput. Sci., vol. 2, no. 3, pp. 173, 2021.
9. Y. K. Dwivedi et al., "Artificial Intelligence (AI): Multidisciplinary perspectives on emerging

challenges, opportunities, and agenda for research, practice and policy," Int. J. Inf. Manag., vol. 57, pp. 101994, 2021.
10. M. M. Khan and M. Fasih, "Impact of service quality on customer satisfaction and customer loyalty: Evidence from banking sector," Pakistan J. Commer. Soc. Sci., vol. 8, no. 2, pp. 331–354, 2014.
11. K. Hakala, "Robo-advisors as a form of artificial intelligence in private customers' investment advisory services," Bachelor's thesis, 2019.
12. J. Manyika et al., "A future that works: AI, automation, employment, and productivity," McKinsey Glob. Inst. Res., Tech. Rep, vol. 60, pp. 1–135, 2017.
13. D. W. Arner, J. N. Barberis, and R. P. Buckley, "The evolution of Fintech: A new post-crisis paradigm," Georgetown Law J., vol. 108, no. 4, pp. 1271–1319, 2020.
14. T. H. Davenport and J. Kirby, "Only humans need apply: Winners and losers in the age of smart machines," HarperBusiness, 2016.
15. Gartner, "Top Strategic Technology Trends," Gartner, 2021.
16. P. Gomber, R. Koch, and M. Siering, "Digital Finance and Fintech: current research and future research directions," J. Bus. Econ., vol. 87, no. 5, pp. 537–580, 2017.
17. J. Manyika et al., "A future that works: Automation, employment, and productivity," McKinsey Glob. Inst., 2017.
18. OECD, "Recommendation of the Council on Artificial Intelligence," OECD, 2019.
19. E. M. Rogers, Diffusion of innovations, 5th ed., Free Press, 2003.
20. D. Schatsky, C. Muraskin, and R. Gurumurthy, "Cognitive technologies in financial services," Deloitte University Press, 2018.
21. S. Rahi, M. M. Khan, and M. Alghizzawi, "Extension of technology continuance theory (TCT) with task technology fit (TTF) in the context of Internet banking user continuance intention," Int. J. Qual. Reliab. Manag., vol. 38, no. 4, pp. 986–1004, 2021.
22. N. Schwarz, "Self-reports: How the questions shape the answers," Am. Psychol., vol. 54, no. 2, pp. 93, 1999.
23. V. Venkatesh, M. G. Morris, G. B. Davis, and F. D. Davis, "User acceptance of information technology: Toward a unified view," MIS Q., vol. 27, no. 3, pp. 425–478, 2003.