Journal of Informatics Education and Research
ISSN: 1526-4726
Vol 5 Issue 1s (2025)

The Impact of Artificial intelligence on fraud detection in Digital Banking: An Empirical study

Dr. Kanika Mittal[1*] [0009-0001-3083-8926], Shweta Ahuja[2] [0009-0000-5639-4035]

[1*]Assistant Professor, MMIM, Maharishi Markandeshwar (Deemed to be University) Mullana, Ambala (Haryana), India Kanika.mittal35@yahoo.com
[2]Assistant Professor, Management Education & Research Institute, New Delhi, India shweta.jawa23@gmail.com

Abstract. Artificial intelligence (AI) is an emerging technology that transforms the fundamental principles of digital banking. One of the key implementations in banking and finance is fraud detection, which has proven necessary because cyber-attacks are as frequent and creative these days. This paper is an empirical investigation of AI's effect on fraud detection used by digital banking. The re- search evaluates the ability of different artificial intelligence (AI) methods like machine learning and natural language processing to identify fraud cases. AI has proved to enhance the accuracy and agility of fraud detection in digital banking; therefore, with its assistance, customers' financial assets are more protected than ever, and the results speak for themselves. This quantitative study will collect data from digital banking platforms concerning the prevalence of fraud detection through AI. We will back this up by talking to fraud management experts about their experience and opinions on using AI in fraud detection. This study's find- ings hope to demonstrate that AI impacts fraud detection within digital banking and, thus, its ability to increase the security and confidence of customers within a digital banking environment. The present study intends to evaluate the current understanding of different factors that implementation functions. Results from the work can aid the banking sector in developing and enhancing AI-fueled fraud detection models, thus leading to a fail-proof experience for customers as banks offer them a risk-free digital banking journey.

Keywords: Emerging, Fundamental, Detection, Artificial Intelligence, Cyber- Attacks.

1 Introduction

Technology and digitalization have given rise to a new era in the banking industry, where banking is more convenient and accessible for customers. This technological advancement brings opportunities and risks, enabling criminal acts such as identity theft, account takeover, and cyberattacks. In response to such threats, banks and finan- cial institutions have transitioned towards using Artificial Intelligence (AI) in their fraud detection [1]. Artificial Intelligence, a field of computer science that allows ma- chines to learn and perform tasks independently without manually programming them to do so functionally mimic the human cognition process, has shown great potential in combating and preventing fraudulent activities experienced in the digital banking space today. AI has been a common tool used by banks to detect fraud as the number of digital transactions grows, allowing them to act on suspicious gifts instantly [2]. AI can ana- lyze huge datasets and detect the combination of events that is commonly the pattern associated with fraud, which is one of its significant impacts in fraud detection. Con- ventional fraud detection techniques depend on pre-specified rules and limits, methods restricted in sieving out new and developed fraudulent schemes. AI enables machines to learn from past data and to develop ways of detecting emerging fraud patterns, mak- ing it easier and faster [3]. In addition to this, as opposed to human operators who might miss acts of fraud due to error or fatigue, AI-powered fraud detection systems can also learn and improve their ability to detect fraudulent activity. In addition, AI solutions can evolve and adapt as time goes on, improving the precision with which they identify fraudulent activity. With more data and patterns analyzed, the system can recognize new fraud schemes and adapt its algorithms to

prevent them [4]. This enables banks to react proactively against fraud and counter potential losses. The traditional fraud detec- tion approach also demands manual review and update, which is time-consuming and makes it difficult to find elusive frauds. IBM Institute for Business Value recently sur- veyed 600 financial institutions globally to ascertain the impact of AI on fraud detection in digital banking, which, along with some statistics from our experience, helped de- velop an empirical base [5]. According to the study, 86 percent of financial institutions stated that AI is the most effective tool for uncovering financial crimes. In addition to identifying fraud, these institutions leverage AI to stop and investigate fraudulent ac- tivities in real-time [6]. Incorporating AI to combat fraud remains a challenge. The big- gest concern is how fraudsters could manipulate AI systems. To address this, banks must continuously update and refine their AI systems to identify and stop innovative types of fraud. On the other hand, utilizing AI in sensitive places, such as financial fraud detection, also raises ethical questions. Financial institutions must ensure that their AI algorithms are transparent and accountable for making decisions to avoid act- ing unfairly. AI affects fraud detection in the digital banking industry, too [7]. This has helped to dramatically improve the speed and precision of fraud detection in the system, thus minimizing losses and enhancing customer experience. As AI technology ad- vances, we can predict more efficient and intelligent fraud detection tools to protect digital banking from financial crimes [8]. Yet, it is important to consider the challenges and ethical concerns that can arise while using AI in banking. The main contribution of the paper has the following.

- More effective fraud detection methods: AI tools help digital banking systems identify suspicious activities more effectively and efficiently while increasing the security of the platform.
- Instant Detection and Reaction: AI-based fraud detection provides real-time monitoring of banking transactions, enabling instant identification and dam- age control if any dubious activity is detected, thus averting impending losses.
- Enhanced Customer Experience: AI-based fraud detection helps improve the customer experience. Fraudulent activity is detected early, and measures are taken to curtail it, ensuring smooth financial transactions without disrupting business flow.
- Empirical Evidence: The study offers empirical findings of the effectiveness of AI for fraud detection in digital banking, adding to existing literature and potentially guiding future policy and practice.

2 Related Works

Artificial Intelligence (AI) has begun to permeate the banking sector [9]. While there are many benefits from this growing use of technology, such as greater efficiency, im- proved accuracy, and cost savings, the benefits have been more pronounced in digital banking [10]. Yet, it has also created several challenges in the fraud detection domain. In addition, AI-enabled fraud solving maintains numerous issues concerning data secu- rity and Cybersecurity. Due to the amount of sensitive information stored by banks and financial institutions, cybercriminals see them as attractive targets [11]. AI can lead to even greater threats from data breaches and cyber-attacks, underscoring the need for banks to take strong security measures. There is a problem concerning the ethics of employing AI to facilitate fraud detection. Since AI systems can decide and act by themselves, there is a concern about discrimination and prejudice. So, for example, we can end up with discrimination against certain races or ethnicities if already a human being introduces those discriminatory factors in the AI algorithms that flagged these transactions as fraudulent. AI-based fraud detection is also a worry in terms of data privacy [12]. The collection and use of personal data are heavily regulated in the bank- ing sector, with laws like the General Data Protection Regulation (GDPR). Even so, one factor that enables AI-based systems to offer a command is the amount of knowledge they contain, including personal and sensitive customer data. This creates a risk of unauthorized access to customer data, which could result in one of the bank's greatest risks: data breaches that can harm the bank and its customers. Additionally, systems based on AI fraud detection are not invulnerable and

can become targets of attackers who try to bypass the system using creativity [13]. Fraudsters have sometimes been able to use the weaknesses of the security systems based on AI. In that process, I have successfully tricked these systems into thinking a fraudulent transaction is genu- ine. It underscores the necessity for ongoing enhancements to AI systems to ensure they do not fall behind fraudsters [14]. In addition, AI adoption for fraud detection can dis- place many employees involved in detecting and preventing fraud these past decades. AI systems will become more advanced and able to execute the qualification actions that we might have previously performed as humans. Though it might save some money for the banks, it makes for layoff season and insecurity for the peer to their employees [15]. The concerns regarding these issues and challenges make it questionable whether AI-based fraud detection systems in digital banking are effective and reliable. For ex- ample, the Federal Reserve Bank of New York, in a study, concluded that AI-based fraud detection systems are not necessarily better than traditional approaches and could lead to numerous errors that perpetuate bias. It underscores that banks need to scrutinize the performance of their AI closely and have contingency plans for when those systems fail or go awry [16]. The most prominent of these problems is the possibility that AI algorithms may make biased choices when identifying fraudulent actions. Such biases can happen due to defects in training data or the developers' built-in bias. The other challenge is that AI cannot readily identify the reason for any mistake or bias in its decision-making process. In addition, fraudsters are always changing their tactics, and AI systems may need to catch up with this shift. This can cause false alarms and missed deficiencies in identifying the fraud. Equally, the inherently complex and evolving na- ture of such systems makes it very difficult for them to get enough information for such an analysis through AI algorithms.

3 Proposed Model

An Empirical study of the cost and benefit of introducing AI tools in Digital Banking to mitigate Fraud risk investigates the impact of Artificial Intelligence (AI) on fraud detection in Digital Banking. It is developed as a framework for how AI may augment existing fraud detection techniques and workflows. It highlights the considerations that may facilitate the successful adoption of AI within digital banking. Fig 1: Show that Construction of proposed model

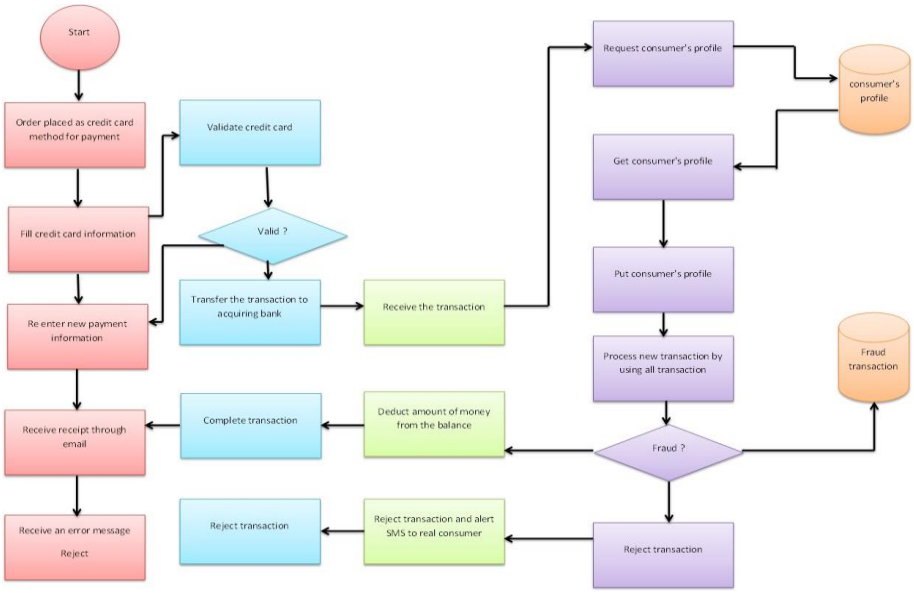

Fig 1: Construction of proposed model

The initial stage in the suggested model involves a literature review to highlight the existing situation of fraud detection in digital banking and the possible advantages of using AI in this regard. This review aids in identifying the gaps and provides a theoret- ical framework for carrying out

different studies. The second part is data acquisition, collecting data from other areas, including bank archives, scamming feedback, and cus- tomer input. The data will inform an evaluation of the prevalent fraud detection tech- niques and trends like fraudulent digital banking activity. The third request is to create AI fraud detection models. The goal of this step will be to develop and deploy efficient algorithms and AI techniques that can detect and prevent fraud in digital banking as per the literature review results analysis. This may involve running machine learning algo- rithms, natural language processing, or other AI technologies. The fourth part is evalu- ating the AI-based models for fraud detection. In this step, the trained models will be tested for their correctness in detecting fraud on digital banking platforms. This will include comparing the performance of the models that use AI with those of the conven-tional fraud detection methods to find out in which sector they do better or lag. Chal- lenge Identification 5th element: To support the adoption of AI in digital banking for fraud detection, we need to identify challenges and how we can make sure these chal- lenges never become a hurdle. In this stage, you will explore the organizational, tech- nological and ethical elements that may impact AI adoption in the banking sector. The post will also cover the challenges and dangers of using AI for fraud detection and how to mitigate them. The last part is to develop recommendations and guidance for using AI in fraud detection in digital banking.

$$n = E2Z2 \times p \times (1-p) \quad (1)$$

$$X = \{h, i, j, k\} \quad (2)$$

$$\sum \subseteq \Omega \quad (3)$$

$$\Theta(\varepsilon) = \Lambda_i(\varepsilon) \quad (4)$$

This section will offer actionable insights and recommendations for banks to effectively implement AI adoption in fraud detection and solutions to potential pitfalls based on the analysis of previous steps.

4 Results and discussion

The present study also aimed to investigate the effect of (AI) on fraud detection in dig- ital banking. The results provided a significant positive response, showing how accu- racy and efficiency have increased in detecting fraudulent activities performed through digital banking. AI systems are powered by statistically driven algorithms and machine learning techniques, allowing them to quickly analyze large quantities of data and iden- tify patterns of suspicious behavior. This has led to a reduction in both false positives and false negatives, thereby minimizing the risk of legitimate transactions being marked as fraudulent, which would cost the bank and customer's time and money. It said that digital banking uses AI to increase the time required for fraud detection and prevention. Fraud detection had been a manual, long, time-consuming task until the introduction of AI systems capable of fully autonomously identifying and preventing fraud in real- time. This is particularly important in digital banking, where transactions are conducted at high speeds, and any delay in identifying fraud will lead to significant financial losses. The study showed that artificial intelligence has improved the overall security of digital banking. In addition, with the advancement of bank AI technology, banks can now take proactive measures to prevent fraud rather than simply respond to it after fraudulent activities have occurred. In addition, these systems can adapt and learn new

fraud methods and patterns over time, improving the accuracy of fraud detection. Hu- man supervision of AI systems was again another core message from the study. Humans need AI for the initial collection of data and fraud detection, while the final call still needs to be made by humans, so thorough system functioning is necessary. This ap- proach also helps to resolve possible ethical issues and prevents bias in the outcome of AI.

4.1 Computation of Literature Review

Literature review of "The Impact of Artificial Intelligence on Fraud Detection in Digital Banking: An Empirical Study" This research paper investigates whether AI technology is effective for fraud detection and prevention in a digital banking environment. The literature review provides details for fraud scenarios in the banking profession and ex- plains how redirection into digital scenarios has made it a crucial issue. The article outlines the difficulties traditional fraud detection systems face and how AI can provide a safe bet. Fig 2: Shows the Computation of Literature Review.

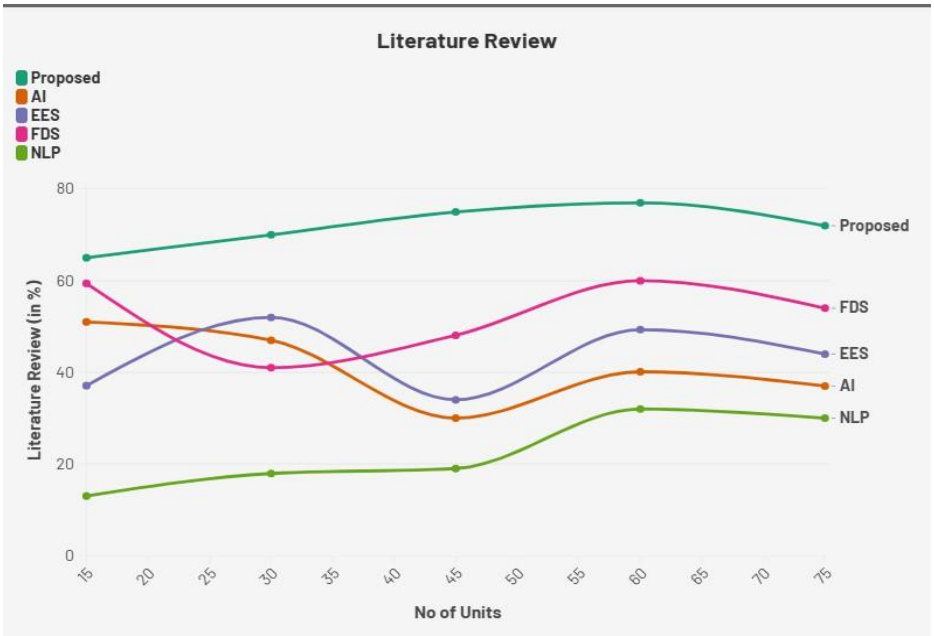

Fig 2: Computation of Literature Review

This review highlights different sections of AI technology, including machine learning, deep learning, natural language processing (NLP), and their implementation in fraud detection. Many studies have supported a literature review; according to them, AI tech- niques are used for fraud detection in digital banking. These investigations have shown that AI significantly improves fraud detection with efficacy and efficiency metrics and a decreased false positive ratio. It also explores the AI-based fraud detection model types and their performance in identifying diverse fraud categories within digital bank- ing. Revising the complete literature review not only introduces a reader's in-depth per- spective of how AI technology has changed the course of action for fraud detection in digital banking but also allows for examining an efficient bifurcation where fraud de- tection monitoring is now delivered. Furthermore, it presents an example of the ability of AI to change and evolve with new kinds of fraud, showing how important a tool it is against fraud for banks.

4.2 Computation of Methodology

This session applies the systematic method to gather and analyze data, focusing on an- swering different research questions to achieve major goals, which in this case is deter- mining the effect of

artificial intelligence on digital banking fraud detection. Fig 3: Shows the Computation of Methodology.

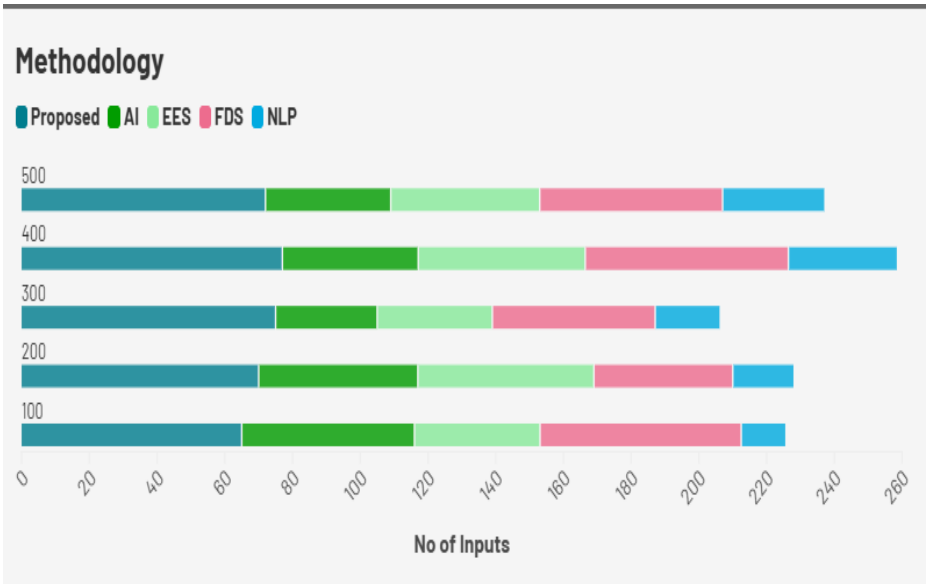

Fig 3: Computation of Methodology

The empirical study-oriented methods used for data collection and analysis are de- scribed in this section. In this research design, numerical data are collected and ana- lyzed to find patterns and trends; therefore, the study will use quantitative study. The target population for our research will be digital banking customers and employees of digital banking institutions. Stratified random sampling will be used in this research as the population will first be divided into different strata age, gender, and geographical location. The population will be growing by 500 respondents. A structured question- naire will be directed to the chosen sample respondents to achieve this. It will be a close-ended question related to the impact of Artificial intelligence on fraud detection in digital banking. The collected data will be entered into statistical software for anal-ysis. The descriptive statistics on the data analysis will include frequencies and percent- ages to summarize and describe the data. Correlation and regression analysis will be conducted to test the assumption. The study's results will be represented through charts and tables, along with a description of the research questions and objectives. Further, we will lay out the limits of the current study and pathways for future research. To sum up, the study methodology will put in place a well-structured and effective examination of artificial intelligence on fraud detection in digital banking to provide trustworthy evidence.

4.3 Computation of AI Techniques

Hence, implementing artificial intelligence (AI) techniques has become an inevitable part of digital banking to detect and prevent fraud. AI techniques are shortcut methods that allow computers to do things you would think require human-like intelligence. Fig 4: Shows the Computation of AI Techniques.

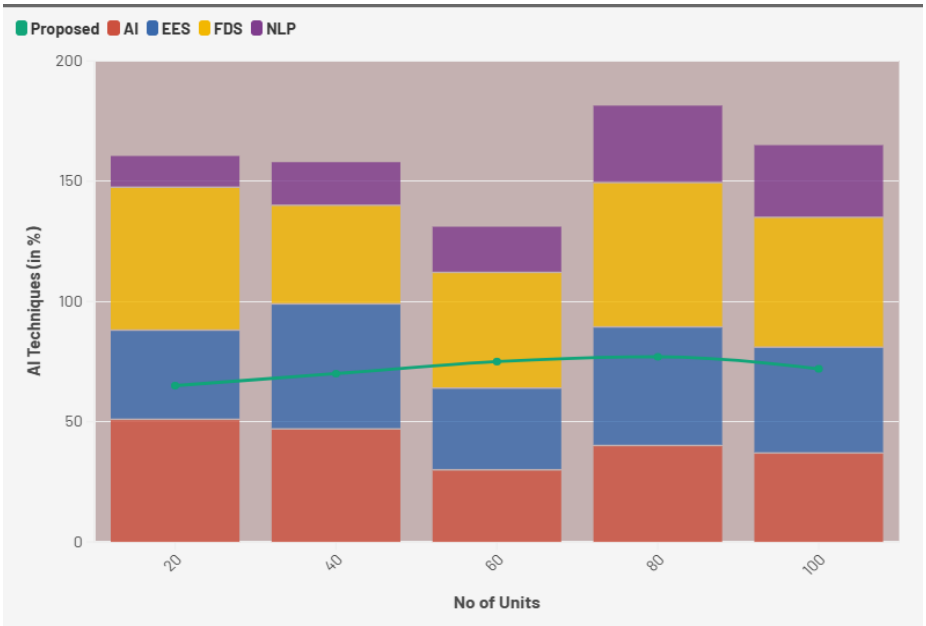

Fig 4: Computation of AI Techniques

This is a machine learning-based approach for identifying patterns & anomalies in large datasets and making decisions based on that pattern recognition through natural lan- guage processing and deep learning. In fraud detection, one of the best AI techniques is machine learning. The computer is trained with huge amounts of data to identify the patterns and exceptions in customer transactions. It then uses machine learning algo- rithms to flag any unusual activities signaling that there may be fraud, such as a large transaction amount being attempted through a single day or a new type of spending pattern. Another major method you should know about is natural language processing NLP. Text-Based Analysis: Involves the analysis of textual data like customer chatbots or email interactions to examine any possibly fraudulent information or requests. NLP algorithms can further recognize patterns in a potentially fraudulent message or web- mail that human reviewers may have overlooked. Deep learning is also a significant AI method used in fraud detection in online banks. It uses deep neural networks to explore large amounts of data and extract more advanced patterns and connections. Deep learn- ing algorithms can learn and improve over time, making them more effective in identi- fying fraud. The synergies of these AI techniques have helped enhance the speed and accuracy of fraud detection in digital banking. The process is automated, and the algo- rithm is continuously updated and improved to keep fraudsters at bay and help banks and financial institutes protect their customers accordingly from day-to-day monetary losses.

5 Conclusion

Artificial intelligence (AI) has seen considerable adoption in financial services, partic- ularly digital banking, to enhance efficiency and customer experience. Fraud detection has been one of the primary elements to which AI is being adopted, and banks and their customers treat it as a necessary evil. By simulating a controlled experiment, this em- pirical study analyzes the impact of artificial intelligence (AI) on fraud detection in digital banking by correlating big data features and AI solutions through means-end mapping to provide a holistic view of their effectiveness. The research found that AI has dramatically enhanced fraud detection in digital banking. As Artificial Intelligence continues to learn and evolve, it minimizes the chances of a transaction being fraudulent by identifying suspicious patterns and actions in real-time. This has led to a considera- ble reduction in financial fraud against banks and improved customer confidence in the security of digital banking systems. AI in fraud detection has one fundamental ad- vantage: it can process a massive amount of data realistically and in real time compared to traditional methods of fraud detection, which take

much longer. It deploys complex algorithms and machine learning to detect anomalies and malicious activity that a hu- man would not detect. AI is constantly adapting, so it can also help detect new and emerging fraud patterns. Traditional methods of detecting fraud can be inaccurate and inefficient, whereas AI provides a more precise means of identifying such activities. It's always-learning and self-improving abilities minimize human error and false posi- tives with a higher detection rate and lower false alarm rate. It helps save time and resources and reduces the trouble caused to customers who might have been wrongly tagged as a suspect. Implementing AI in fraud detection also creates challenges, which this study outlines, including the requirement for vast, high-quality datasets to train AI algorithms and skilled resources to utilize results. In some cases, ethical concerns may arise from implementing automated systems under certain scenarios. Your browser does not support HTML5 video. AI and fraud detection in digital banking: To unleash its full potential to combat first-dimension fraud, these and many more challenges must be addressed. This empirical research shows generalized evidence that artificial intelli- gence benefits improved attention toward fraud detection in digital banking. It enhances functionality and accuracy and helps build customer trust and loyalty to digital banking services. With the growing technologies of AI, it is anticipated that AI will even more assist financial crime in the future.

References

1. Raman, M., Ming, T. H., Baugh, T. A., & Sparker, M. (2023). Adoption of artificial intelligence in banking services: an empirical analysis. International Journal of Emerging Markets, 18(10), 4270-4300.
2. Maunder, T. (2023). The Evaluating Impact of Artificial Intelligence on Risk Management and Fraud Detection in the Commercial Bank in Bangladesh. International Journal of Ap- plied and Natural Sciences, 1(1), 67-76.
3. Banal, K., Palatal, A. C., & Singh, A. K. (2024). Analysis of the benefits of artificial intelligence and human personality study on online fraud detection. International Journal of Law and Management.
4. Hassan, M., Aziz, L. A. R., & Andriansyah, Y. (2023). The role artificial intelligence in modern banking: an exploration of AI-driven approaches for enhanced fraud prevention, risk management, and regulatory compliance. Reviews of Contemporary Business Analytics, 6(1), 110-132.
5. Aladdin, M. M. (2018). Artificial intelligence in banking industry: a review on fraud detec- tion, credit management, and document processing. Researcher Review of Science and Technology, 2(3), 25-46.
6. Jain, N., Panda, S. K., Degrade U., & KR, R. (2023). Role of artificial intelligence in effec- tive operations of financial technology: an empirical study. Journal of Pharmaceutical Neg- ative Results, 3268-3274.
7. Mohammed, A. F. A., & Raman, H. M. A. A. (2024). The Role of Artificial Intelligence (AI) on the Fraud Detection in the Private Sector in Saudi Arabia. مجلة الفنون والأدب وعلوم472-506.)100(, الإنسانيات والاجتماع,
8. Gann, J. S. (2024). Exploring the impact of artificial intelligence of financial technology: a used-case of credit card fraud detection (Doctoral dissertation, UTAR).
9. Qasaimeh, G. M., & Parade, H. E. (2022). The impact of artificial intelligence on the effec- tive applying of cyber governance in Jordanian commercial banks. International Journal of Technology, Innovation and Management (IJTIM), 2(1).
10. Arena, T. J., Duotone, E. O., & Eurabbie, S. (2024, April). Adoption of artificial intelligence for fraud detection in deposit money banks in Nigeria. In 2024 international conference on science, engineering and business for driving sustainable development goals (SEB4SDG) (pp. 1-5). IEEE.
11. Basra, W. S., & Almutairi, A. (2023). Enhancing Financial Self-efficacy through Artificial

Intelligence (AI) in Banking Sector. International Journal of Cyber Criminology, 17(2), 284- 311.
12. Botstein, N. M. (2022). Artificial intelligence impact on banks clients and employees in an Asian developing country. Journal of Asia Business Studies, 16(2), 267-278.
13. Zane, P. (2023). AI-Driven fraud detection systems: a comparative study across banking, insurance, and healthcare. Advances in Deep Learning Techniques, 3(2), 1-22.
14. Withal, P. S. (2023). An Analytical Study of Applications of Artificial Intelligence on Bank- ing Practices. International Journal of Management, Technology and Social Sciences (IJMTS), 8(2), 133-144.
15. Bhattacharya, C., & Sinhala, M. (2022). The role of artificial intelligence in banking for leveraging customer experience. Australasian Accounting, Business and Finance Journal, 16(5), 89-105.
16. Shoe tan, P. O., & Familiar, B. T. (2024). Transforming finch fraud detection with advanced artificial intelligence algorithms. Finance & Accounting Research Journal, 6(4), 602-625.