Recent trends in Management and Commerce

Vol: 5(2), 2024
REST Publisher; ISBN: 978-81-936097-6-7

Website: https://restpublisher.com/book-series/rmc/

DOI: https://doi.org/10.46632/rmc/5/2/3

Recent trends in Management and Commerce

REST Publisher

AI's Bipolar Effect on Mitigating and Motivating Frauds

* **Sreedevi S**
Bharathiar University & Research Associate, DKMS & Associates, Palakkad, Kerala, India.
*Corresponding Author Email: sreedeviswanathan@gmail.com

Abstract: *In the time of digital innovation, Artificial Intelligence (AI) stands at the forefront, signaling new capabilities in fraud management but also new vulnerabilities. This paper aims to dissect AI's paradoxical influence on fraud, portraying its roles in both promoting and mitigating fraudulent activities. The research seeks to bridge the gap in understanding the dual nature of AI, highlighting the need for ethical and regulatory frameworks to traverse the complications AI introduces into fraud detection and prevention. Utilising secondary data from Google News and academic databases with the keyword 'AI fraud,' this study adopts a keyword-based analysis to sift through the most relevant literature. The approach is designed to capture a comprehensive snapshot of the current discourse, underlining the bipolar impact of AI on fraud. The analysis reveals AI's significant potential in enhancing fraud detection systems through rapid data analysis and pattern recognition. However, AI technologies can be exploited to facilitate sophisticated fraud schemes. The study underscores an urgent need for evolving practices and policies that counteract AI's potential for misuse, weighing in the emerging concept of self-regulatory AI systems as a promising direction for future research. This paper contributes insights into the dualistic role of AI in fraud, adding depth to the discourse on its implications for security, ethical considerations, and regulatory challenges. It advocates for a balanced perspective on AI's capabilities.*

Keywords*: Artificial Intelligence, Fraud Detection, Fraud Prevention, Ethical AI, Regulatory Frameworks, Self-Regulatory AI.*

1. INTRODUCTION

Fraud in the digital domain has evolved, becoming an expensive challenge for organizations around the world. In response, many are adopting AI which has rapidly advanced to transform numerous industries and how we conduct our daily activities (NCBI). AI offers promising solutions for improving fraud detection and prevention efforts. However, there is a concerning aspect to its application: if leveraged improperly, AI can also be used to perpetrate fraud. This study seeks to understand AI's complex role in both enabling and thwarting fraudulent practices. The research objectives and questions aim to dissect AI's dualistic role in fraud, examining its capacity as both a protector against and a perpetrator of fraudulent acts.

2. LITERATURE REVIEW

AI has a complex role in the landscape of fraud, acting as both a facilitator and a defender. On one hand, it enables sophisticated phishing schemes and fraudulent transactions through AI-driven bots and algorithms that replicate genuine user actions, making it difficult for traditional fraud detection systems to differentiate between real and fraudulent activities. This capacity for mimicry and data analysis allows scammers to exploit AI technologies to bypass security measures covertly.

Conversely, AI is instrumental in enhancing fraud detection and prevention. Its ability to rapidly analyze vast amounts of data enables the identification of suspicious trends and anomalies, significantly reducing the impact of fraud on organizations. AI-driven systems continually adapt, learning from new data to detect emerging fraud patterns, thus maintaining a critical edge over fraudsters. The dynamic nature and speed of

AI, fueled by the aggregation of data, improve its predictive capabilities over time. Despite the inherent risks, when leveraged with an understanding of its potential and pitfalls, AI becomes a pivotal tool in the arsenal against fraud, underscoring the importance of strategic implementation and best practices in exploiting AI's capabilities for fraud prevention and detection (PwC, 2023).

Recent advancements in AI, particularly in generative AI (gen AI), have revolutionized business functions and posed new challenges in fraud management. There is a rapid integration of gen AI in business operations, with a significant percentage of companies adopting these tools for various functions, indicating a profound shift in organizational strategies towards AI utilization (McKinsey, 2023a). This adoption is not limited to tech departments but extends to C-suite executives, emphasizing the critical role of AI in contemporary business practices. Furthermore, the survey underscores an increase in AI investments, signifying a growing confidence in AI's potential to drive innovation and efficiency. However, it also points to an infancy stage in managing AI-related risks, particularly inaccuracies, hinting at the dual-edge of AI in business environments (McKinsey, 2023b). PwC's findings complement this view by showcasing a strong belief among organizations that AI enhances fraud detection capabilities, with 74% of respondents affirming its effectiveness in identifying fraudulent activities across various industries (PwC, 2023). AI's capacity to analyze vast data volumes in real-time, identify suspicious transactions, and adapt to emerging fraud patterns underscores its indispensable role in modern fraud prevention strategies.

Despite the optimistic outlook on AI's role in combating fraud, the literature also reflects on the challenges and evolving threats in the digital landscape. Traditional fraud detection methods are increasingly becoming obsolete against sophisticated fraud strategies, necessitating a pivot to more advanced, AI-driven solutions. These technologies, through their ability to learn from data and detect anomalies, offer a proactive approach to identifying and mitigating fraud risks, thereby safeguarding organizational assets and reputation.

This paper addresses the gap in understanding AI's dual role in fraud, focusing not only on its fraud detection aspect but also on how it can facilitate sophisticated scams. It explores the aspects of AI-related risks, ethical dilemmas, and the regulatory challenges posed by its misuse. By offering a balanced view, this study contributes to the discourse on managing AI's potential and threats in fraud prevention and detection.

3. METHODOLOGY

This study uses a keyword-based analysis to explore the role of AI in fraud within various industries. By examining sources identified through Google News and academic databases using the term 'AI fraud,' the research distinguishes between AI's use in committing versus preventing fraud. The literature review, focused on the emerging discourse, provides a foundational understanding of the key issues at the intersection of AI, fraud promotion, and fraud prevention. This approach ensures a clear and objective representation of the current state of AI's impact on fraud.

4. LIMITATIONS

The limitations of this study are primarily tied to the scope of the data and the search methodology. The keyword 'AI fraud' was used to gather relevant literature, which may not capture all instances of AI's involvement in promoting or mitigating fraud due to the variability in terminology used across sources restricted to specific dates. Moreover, the reliance on Google News and academic databases may have introduced selection bias, potentially overlooking relevant articles and reports not indexed by these platforms. Additionally, the rapid development of AI technologies means that the findings represent a snapshot that could quickly become outdated. The sentiment analysis, a subjective measure, could also be influenced by the researcher's interpretations. The categorization is inherently subjective and relies on the researcher's discernment, potentially leading to classification bias. Furthermore, due to time constraints, the analysis was limited to 20 sources, a sample size that may not provide a comprehensive view of the wider landscape of AI and fraud. This constraint on the number of sources could impact the study's breadth and depth, and findings should be interpreted with an understanding of these context limitations. These factors should be considered when extrapolating the results to broader contexts.

5. ANALYSIS AND FINDINGS

Analysis:

1. AI's Role in Motivation vs. Mitigation: The table (Annexure 1) reflects a significant dichotomy in AI's role across sectors, with a nearly equal distribution between motivating fraud and mitigating it.

AI is motivational as prominently observed in general sectors, which are related to individual fraud experiences, cyber security, and financial services, while its mitigating role is evident in government/finance, aviation, and regulation.

TABLE 1.

Sectors	Dual	Mitigate	Motivate	Total
Academic			1	1
Aviation		1		1
Cyber security	1		2	3
Finance			1	1
Financial services	2	3	1	6
General		1	4	5
Government/Finance		1		1
Medical/Healthcare			1	1
Regulation	1			1
Total	**4**	**6**	**10**	**20**

2. Recurring Key Themes: Fraud detection in mitigation and deep fakes in motivation are recurring themes across several sectors, indicating a widespread concern for these issues. The combination of machine learning and predictive AI models is often associated with fraud detection and mitigation efforts, suggesting an emphasis on proactive strategies in financial services.

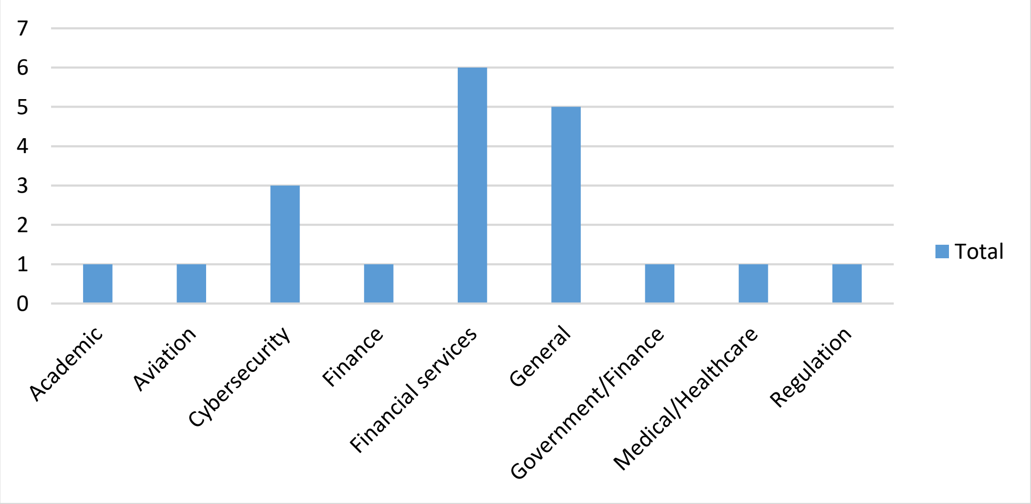

FIGURE 1.

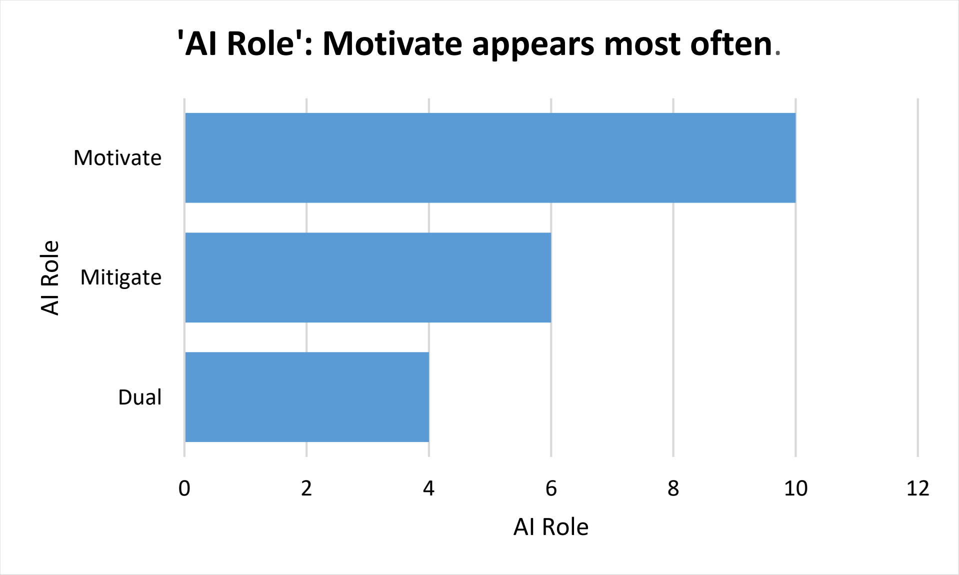

FIGURE 2.

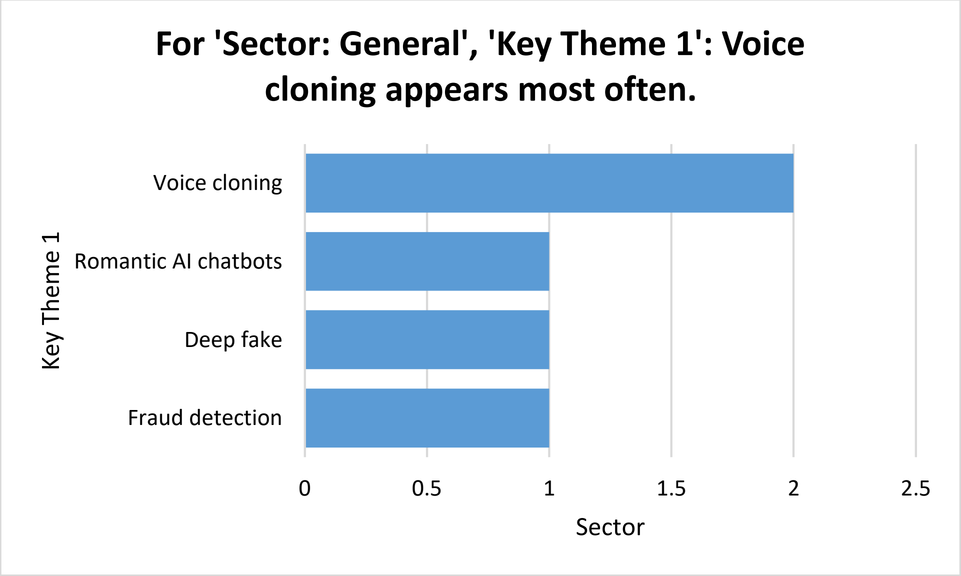

FIGURE 3.

3. Sentiment Analysis: The sentiment associated with articles varies, with motivations for fraud skewing negative, as seen with voice cloning, generative AI in scams, and deep fakes. In contrast, AI's role in mitigation, such as fraud prevention and detection, shows a more positive sentiment.
4. Sector-Specific Concerns: Cybersecurity is a sector where AI's role in motivation (voice scams and hacking) is as important as its role in mitigation, showing the dual capacity of AI to influence the security landscape.

Findings:
Cyber security and Finance are seen as hotspots. These sectors show significant activity in both fraud motivation and mitigation, underscoring the serious importance of AI in their fraud strategies. However, we can see negative sentiment in Academic and General Sectors. Instances of plagiarism, misuse of generative AI, and romantic AI chatbots targeting data privacy raise ethical and security concerns, reflecting broader societal apprehension towards AI misuse. A rather positive reception for AI in mitigation is seen in the news articles and reports sources which indicate a positive reception for AI's role in fraud prevention, especially when enhanced by sophisticated machine learning techniques and models.

6. IMPLICATIONS AND FUTURE DIRECTIONS

The study on the bipolar effect of AI in the case of promoting or mitigating frauds shows that it can both enable and prevent fraudulent actions. The key takeaway is the need for careful use and monitoring of AI to harness its benefits while minimizing risks.

Ethical considerations are necessary, as AI's deployment in fraud detection must respect privacy and avoid bias. The findings suggest a need for updated practices and policies that balance AI's potential against its dangers. Importantly, the concept of self-regulatory or co-regulatory AI emerges as a promising area for future exploration, aiming to make AI systems capable of identifying and mitigating risks autonomously. Future research should aim to improve AI's effectiveness in fraud prevention, delve into ethical AI use, and develop advanced strategies against AI-assisted fraud. Moving forward, striking the right balance between innovation and security will be key to maintaining trust in digital platforms.

TABLE 2. Annexure 1

Source ID	Publication Date	Source Type	Sector	AI Role	Key Theme 1	Key Theme 2	Key Theme 3	Sentiment	Citation
1	07/03/24	News Article	General	Motivate	Voice cloning	Ransom scam	-	Negative	5
2	28/02/24	News Article	Government /Finance	Mitigate	Fraud detection	Machine learning	-	Positive	6
3	14/02/24	News Article	Finance	Motivate	Generative AI	Phishing	Financial scams	Negative	7
4	16/02/24	News Article	Regulation	Dual	Deep fake	Impersonation	-	Neutral	8
5	13/06/23	News Article	Cyber security	Motivate	Generative AI	Voice scams	-	Negative	9
6	04/03/24	News Article	Cyber security	Motivate	Hacking	Consumer protection	-	Neutral	10
7	05/02/24	News Article	Academic	Motivate	Plagiarism	Chat GPT	-	Negative	11
8	11/03/24	News Article	Aviation	Mitigate	Fraud prevention	-	-	Positive	12
9	04/05/20	Blog	Financial services	Mitigate	Fraud prevention	-	-	Positive	13
10	17/12/23	News Article	General	Motivate	Voice cloning	-	-	Negative	14
11	09/03/24	News Article	Financial services	Mitigate	Fraud detection	Consumer spending pattern	-	Positive	15
12	11/03/24	News Article	Cybersecurity	Dual	Deep fakes	Identity theft	Proactive prevention	Neutral	16
13	12/08/23	News Article	General	Motivate	Deep fake	Video scams	-	Negative	17
14	07/03/24	Blog	Financial services	Dual	Fraud detection	Predictive AI	-	Neutral	18
15	10/05/23	Journal article	Financial services	Mitigate	Fraud detection	ML models	Feature engineering	Positive	19
16	31/05/23	Journal article	Medical/Healthcare	Motivate	Fraudulent scientific articles	Ethical implications	AI content	Negative	1
17	01/12/23	Research report	Financial services	Dual	Fraud detection	Sophistication	Fraud volume	Neutral	20
18	24/11/20	Book Chapter	General	Mitigate	Fraud detection	Machine learning	-	Positive	21
19	05/02/24	News Article	Financial services	Motivate	Deep fake	Video scams	-	Negative	22
20	07/03/24	News Article	General	Motivate	Romantic AI chatbots	Data privacy	Security vulnerability	Negative	23

REFERENCES

[1]. Májovský, M., Černý, M., Kasal, M., Komarc, M., & Netuka, D. (2023). Artificial Intelligence Can Generate Fraudulent but Authentic-Looking Scientific Medical Articles: Pandora's Box Has Been Opened. Journal of medical Internet research, 25, e46924. https://doi.org/10.2196/46924

[2]. McKinsey & Company. (2023, August 1). The state of AI in 2023: Generative AI’s breakout year. Survey. Retrieved from https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-in-2023-generative-ais-breakout-year

[3]. McKinsey & Company. (2023, June 14). The economic potential of generative AI: The next productivity frontier. Report. Retrieved from https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-economic-potential-of-generative-ai-the-next-productivity-frontier

[4]. PricewaterhouseCoopers (PwC). (2023, June 15). Artificial Intelligence & its role in the fight against fraud. Digital Upskilling tech background. Publication. Retrieved from https://www.pwc.com/mt/en/publications/other/artificial-intelligence-role-in-the-fight-against-fraud.html

[5]. Bethea, C. (2024, March 7). The terrifying A.I. scam that uses your loved one's voice. The New Yorker. https://www.newyorker.com/science/annals-of-artificial-intelligence/the-terrifying-ai-scam-that-uses-your-loved-ones-voice

[6]. Egan, M. (2024, February 28). AI is Uncle Sam's new secret weapon to fight fraud. CNN. https://edition.cnn.com/2024/02/28/business/artificial-intelligence-fraud-treasury-ai/index.html

[7]. Sheng, E. (2024, February 14). Generative AI financial scammers are getting very good at duping work email. CNBC. Updated February 16, 2024. https://www.cnbc.com/2024/02/14/generative-ai-financial-scammers-are-getting-very-good-at-duping-work-email.html

[8]. Bomey, N. (2024, February 16). FTC seeks to ban impersonation fraud as AI enables deepfakes. Axios. https://www.axios.com/2024/02/16/ftc-ban-impersonation-fraud-ai-deepfakes

[9]. Bomey, N. (2023, June 13). Generative AI is making voice scams easier to believe. Axios Closer. https://www.axios.com/2023/06/13/generative-ai-voice-scams-easier-identity-fraud

[10]. Chieffi, T. (2024, March 4). AI hacking scams are on the rise – here's how to protect your money, points and miles. The Points Guy. https://www.axios.com/2023/06/13/generative-ai-voice-scams-easier-identity-fraud

[11]. Wolkovich, E. M. (2024, February 5). 'Obviously ChatGPT' — how reviewers accused me of scientific fraud. Nature. https://www.nature.com/articles/d41586-024-00349-5

[12]. Wixted, J. (2024, March 11). Fighting fraud: why AI will propel airlines towards a profitable future. Airport Technology. https://www.airport-technology.com/comment/fighting-fraud-why-ai-will-propel-airlines-towards-a-profitable-future

[13]. Swain, H. (2020, May 04). More financial services providers turn to Gen-AI for fraud prevention. GlobalData. https://www.globaldata.com/newsletter/details/more-financial-services-providers-turn-to-gen-ai-for-fraud-prevention_89886/

[14]. Times of India (TOI). (2023, November 20). Woman loses Rs 1.4 lakh to AI voice scam: What is it and how not to become a victim. The Times of India. https://timesofindia.indiatimes.com/gadgets-news/woman-loses-rs-1-4-lakh-to-ai-voice-scam-what-is-it-and-how-not-to-become-a-victim/articleshow/105298323.cms

[15]. Fonseca, L. (2024, March 9). The role of AI in analysing consumer spending patterns. Financial Express. https://www.financialexpress.com/business/digital-transformation-the-role-of-ai-in-analysing-consumer-spending-patterns-3419199/

[16]. Raynel, T. (2024 March 11). EON report warns of complex fraud challenges ahead in 2024. Security Brief. https://securitybrief.co.nz/story/seon-report-warns-of-complex-fraud-challenges-ahead-in-2024

[17]. Manohar, A. (2023, August 12). Online AI fraud: Beware of scamsters using video call trick to con you. Mint. https://www.livemint.com/money/personal-finance/online-air-intelligence-ai-fraud-beware-of-scamsters-using-video-call-trick-to-con-you-11691820631343.html

[18]. Dierks, D. (2024, March 7). Why data is the backbone of predictive AI. Finextra. https://www.finextra.com/the-long-read/967/why-data-is-the-backbone-of-predictive-ai

[19]. Mytnyk, B., Tkachyk, O., Shakhovska, N., Fedushko, S., & Syerov, Y. (2023). Application of Artificial Intelligence for Fraudulent Banking Operations Recognition. Big Data and Cognitive Computing, 7(2), 93. https://doi.org/10.3390/bdcc7020093

[20]. PwC. (2023). Impact of AI on fraud and scams. PricewaterhouseCoopers. https://www.pwc.co.uk/forensic-services/assets/impact-of-ai-on-fraud-and-scams.pdf

[21]. Bao, Y., Hilary, G., & Ke, B. (2020). Artificial Intelligence and Fraud Detection. In V. Babich, J. Birge, & G. Hilary (Eds.), Innovative Technology at the interface of Finance and Operations. Springer Series in Supply Chain Management. Springer Nature.

[22]. Edwards, B. (2024, February 5). Deepfake scammer walks off with $25 million in first-of-its-kind AI heist. Ars Technica.URL https://arstechnica.com/information-technology/2024/02/deepfake-scammer-walks-off-with-25-million-in-first-of-its-kind-ai-heist/

[23]. Sapkale, Y. (2024, March 7). Fraud Alert: Romantic AI Chatbots Are NOT Your Friend or Girlfriend. Moneylife. https://moneylife.in/article/fraud-alert-romantic-ai-chatbots-are-not-your-friend-or-girlfriend/73636.html