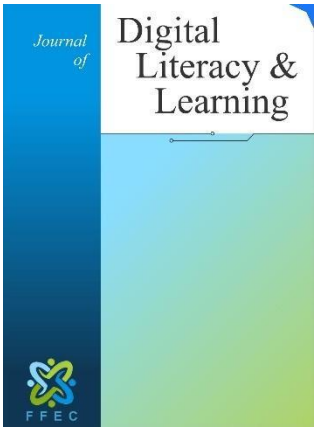
Future Front Envision Consultancy



Journal of Digital Literacy and Learning

www.futurefront.co.uk/journals/JDLL

Theoretical Approaches to Cybersecurity & Adversarial Attacks in AI-Driven Marketing: A Framework for Risk Mitigation

Dr. Munibah Munir

Article History:

Received Article: 11 January 2025

Accepted for Review: 14 January 2025

Published online: 30 January 2025

Journal of Digital Literacy and Learning, Vol. 1, No. 1, 2025

Theoretical Approaches to Cybersecurity & Adversarial Attacks in AI-Driven Marketing: A Framework for Risk Mitigation

Dr. Munibah Munir
IBADAT International University, Pakistan
Email: munibahmunirahmad@gmail.com

Abstract

The rapid development of artificial intelligence (AI) has transformed digital marketing, enabling businesses to achieve greater efficiency, improved returns on investment, and enhanced customer engagement. Despite these benefits, the widespread use of AI introduces significant challenges, including cybersecurity risks, adversarial attacks, and concerns about the unethical handling of user data. These risks threaten data privacy and consumer trust, making it essential for organizations to implement effective risk mitigation strategies. The study used the conceptual and theoretical approach to explore the integration of risk mitigation strategies in AI-driven digital marketing. By bridging the gap, this study proposed risk mitigation strategies in an AI-driven digital marketing framework. Risk mitigation strategies include advanced technological measures, ethical AI practices, and organizational policies aimed at mitigating cyber threats while enhancing customer confidence and security. Furthermore, on the principles of mediation theory, the research emphasizes the moderating role of sustainability in risk management and its contribution to ethical and long-term business practices in AI-driven marketing ecosystems.

Keywords: AI-driven digital marketing, risk mitigation strategies, cybersecurity risks, ethical AI practices, data privacy, sustainability in AI marketing.

Introduction

New technology development, particularly artificial intelligence (AI), has transformed modern digital marketing and business models over the last two decades (Kanbach, 2024). Companies now use the Internet as a digital marketing tool, specifically, after the paradigm shift, the use of the Internet become essential for companies to reach a global market (Campbell et al., 2020; Babatunde et al., 2019).

To boost internet use, AI empowers organizations to deliver unprecedented value and efficiency. Digital marketing with AI tools enhances business performance, increases return on investment and improves overall business outcomes (Almestarihi et al., 2024). However recent literature, Sarker, 2023 explained that reliance on AI opens a new window of cybersecurity risks and adversarial attacks. Such risk unfolded the possible unethical use of user data (Saura, 2021). As such, AI-based digital marketing's possible risks demand a risk mitigation strategy (Guembe,2022).

Risk mitigation strategies are used to enhance cybersecurity and improve customer confidence and sustainability to control cyber threats. Privacy paradox is lined with AI algorithms used in digital marketing strategies and highlights the ethical actions of advertisers and digital platforms tools (Willems et al, 2023). According to this privacy paradox their a discrepancy between what people do online and say about the privacy value. Dwivedi et al., (2021), explained that AI-based digital marketing strategies are nurtured and optimized over time after collecting and analysing the user data. Just relying on the privacy paradox and the numerous benefits of AI is not sufficient. Therefore, the user should be aware of such risks as companies using their data in AI-based digital marketing campaigns. However, there is a lack of risk mitigation strategies to address risks like cybersecurity risks and adversarial attacks affecting the security, customer confidence and sustainability to control cyber threats. In response to this literature gap, this present study aims to unfold the most effective risk mitigation strategies linked with AI-based digital marketing, particularly cybersecurity risk and adversarial attacks. Furthermore, this study seeks to understand the connection between risk mitigation strategies and the moderating role of sustainability in risk management. To address this study proposed a framework the answer the question: What are risk mitigation strategies linked with AI-based digital marketing, particularly cybersecurity risk exploit data and adversarial attacks? To answer this question following are the research objectives:

1. Identify the different risk mitigation strategies in AI-based digital marketing
2. Explore the risk mitigation strategies' impact on security, customer confidence and sustainability to control the cyber threats

The next section of the paper discusses the theoretical framework, risk mitigation strategies and their impact on customer confidence and sustainability to control the cyber threats in AI-based digital marketing and the last section is the conclusion.

Theoretical framework

AI-based Digital Marketing

Globalization of automation, companies make automated decisions (Rusthollkarhu et al., 2022) and use AI tools to enhance their intelligence.

AI-based digital marketing is used as an innovative tool and improves productivity (Capatina,2020; Frank,2021), AI marketing strategies are faster and more efficient than human work. AI-based marketing provides the technology solutions to marketized the product on digital platforms (Ahsan et al.,2022). Companies are using digital marketing to meet the stakeholder's and customers' needs (Ibrahim et al., 2020). Digital marketing is embedded to increase business efficiency and update their business models.

Risks and AI-based Digital Marketing

Under the mediation theory, technology plays a vital role in shaping society and human existence. Humans have the ability and responsibility for their actions, not technologies. But there are certain risks like cybersecurity risks and adversarial attacks, which can affect both the companies and customers or users of that AI-based digital marketing.

Cybersecurity is the practice of protecting data, computer systems and digital assets from cyberattacks (Smith,2021). Adversarial attacks are unauthorized access, misuse and manipulation of information in A)-based digital marketing (Jones et al., 2020). These risks affect AI-based digital marketing and have more adverse effects than positive. AI-based

digital marketing demands careful analysis and ensures user privacy and ethical protection (Kumar & Suthar 2024).

Security Customer confidence and AI-based digital marketing

The integration of artificial intelligence (AI) into digital marketing has revolutionized customer targeting and campaign efficiency but has also introduced significant security challenges. Security risks like algorithm manipulation, data breaches, and adversarial attacks have highlighted the critical concerns, customer data sensitivity and overall effect the digital marketing. Smith et al. (2021), explained in adversarial inputs AI algorithms are vulnerable which can cause system misleading, specifically customer segmentation not correct or cause a reason for fraudulent activity. All these risks not only shake the marketing specifically digital marketing systems along with customer trust which is the main element of effective digital marketing.

Customer trust has a significant role in the success of digital marketing and AI digital marketing. Over the decades consumer preferences have shifted towards data privacy and they are around 70% hesitate to share personal information if they have any doubt about security (Jones & Brown, 2020). In this case, risk mitigation strategies like secure API management, robust encryption, and AI ethical practices are effective ways to address customer confidence security. In organizations, transference of employee data, and data security measures affect the measurable improvements in customer engagement and trust (Davis et al., 2019). All these security measures will increase the customer's trust and foster overall sustainable digital marketing which will lead to data security and customer confidence.

Research Methodology

The study used the conceptual and theoretical approach to explore the integration of risk mitigation strategies in AI-driven digital marketing. This study proposed a theoretical framework rather than an empirical study. This paper's methodology is based on a systematic review and existing literature, and theoretical and conceptual analysis with the underpinning mediation theory. This theory provides the foundation to understand integration risk mitigation strategies which impact customer confidence and security with the moderating role of sustainability.

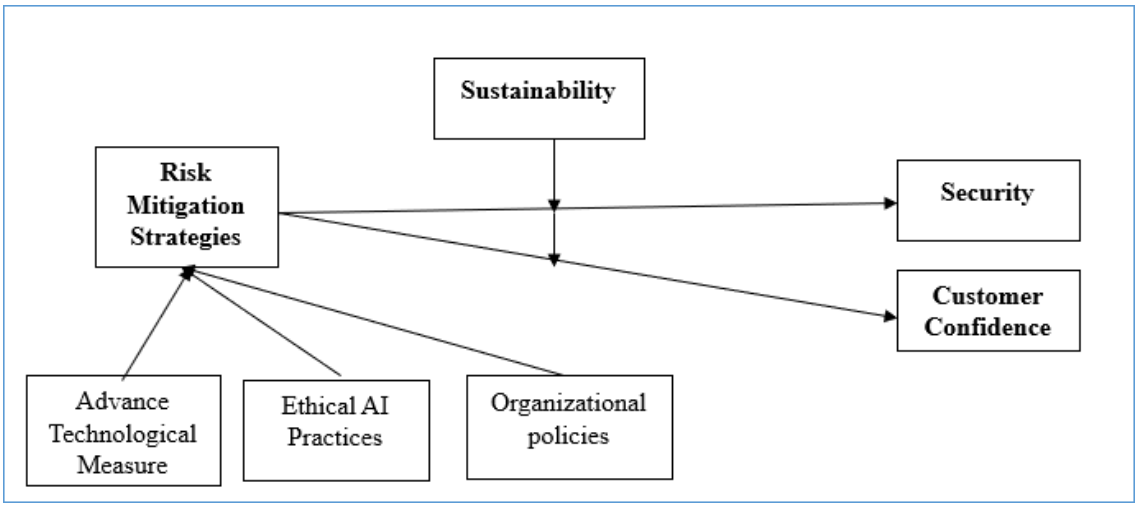


Figure 01: Risk Mitigation Strategies in AI Digital Marketing Framework

The above figure-01 of risk mitigation strategies in AI digital marketing proposed framework. Risk mitigation strategies are advanced technology, ethical AI practices and organizational policies which impact data security and customer confidence. All these strategies to mitigate the risk have been aimed to mitigate the cyber threats and enhance the digital marketing systems' customer trust. Furthermore, this relationship has an adaptable and long- run viable risk mitigation efforts sustainability as moderator strengthen the relationship. According to mediation theory, risk mitigation has an indirect role in strengthening security and customer confidence with sustainable practices. This will contribute to successful and stable AI digital marketing.

Customer confidence is fostered by effective risk mitigation techniques, which guarantee the security of financial operations, operations, and data. Businesses that strive to lower risks can improve the security of assets and transactions, by creating a more reliable and secure stable brand image that customers are ready to interact with as their information is protected.

In this model, sustainability serves as the moderator, affecting how risk mitigation strategies impact data security and customer confidence. The moderating role of sustainability covers both environmental and organizational sustainability practices which reinforce the effectiveness of risk mitigation strategies. Companies with sustainable practices in AI digital marketing might mitigate risks more effectively and enhance data security and customer confidence. Furthermore, mediation theory suggests that sustainable practices indirectly shape risk mitigation strategies to foster customer confidence and data security. Businesses use sustainability as a strategic move to enhance risk mitigation in AI-digital marketing.

This approach underscores the importance of creating an integrated model where risk reduction leads to both tangible and intangible benefits, particularly in an era where consumers increasingly value ethical practices and long-term viability in their engagement with brands. These risk mitigation strategies emphasize the significance of developing an integrated model where risk mitigation leads towards data security and improves customer confidence, particularly in the era of high customer concerns for ethical practices in AI digital marketing.

Conclusion

Artificial intelligence (AI) has revolutionized business models through increased customer interaction, accuracy, and efficiency in digital marketing. Nevertheless, there are serious drawbacks to these developments, such as hostile risks and cyber-security concerns, which can jeopardize data security and erode customer confidence. To overcome these obstacles, this paper highlights the importance of putting risk mitigation strategies and sustainable practice. In addition to enhancing security and customer confidence, these tactics support sustainability, guaranteeing the moral and long-term use of AI in digital marketing.

The proposed model, which is based on mediation theory, emphasizes sustainability as a crucial moderating component that affects how well risk mitigation strategies work. Businesses can manage cybersecurity threats holistically by integrating sustainable practices and creating a framework for digital marketing that is safe and reliable. This research fills the important gap by highlighting the risk mitigation strategies for AI digital marketing while addressing customer confidence and data security. To further improve the resilience of AI-driven marketing ecosystems, future research might examine the relationship between

sustainability, risk management, and technology developments in different industries and secondary data.

References

Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., & Connolly, J. F. (2022). Cybersecurity threats and their mitigation approaches using Machine Learning—A Review. *Journal of Cybersecurity and Privacy*, *2*(3), 527-555.

Almestarihi, R., Ahmad, A. Y. A. B., Frangieh, R., Abu-AlSondos, I., Nser, K., & Ziani, A. (2024). Measuring the ROI of paid advertising campaigns in digital marketing and its effect on business profitability. *Uncertain Supply Chain Management*, *12*(2), 1275-1284.

Babatunde, S. (2019). Governmental financial reporting reforms and relationship marketing: An analysis of International Public Sector Accounting Standards Implementation. *Journal of Promotion Management*, *25*(5), 700-721.

Campbell, M. C., Inman, J. J., Kirmani, A., & Price, L. L. (2020). In times of trouble: A framework for understanding consumers' responses to threats. *Journal of Consumer Research*, *47*(3), 311-326.

Capatina, A., Kachour, M., Lichy, J., Micu, A., Micu, A. E., & Codignola, F. (2020). Matching the future capabilities of artificial intelligence-based software for social media marketing with potential users' expectations. *Technological Forecasting and Social Change*, *151*, 119794.

Davis, L., et al. (2019). *Building Trust Through Secure AI Marketing Practices*. Journal of Consumer Behavior

Dwivedi, Y. K., Ismagilova, E., Hughes, D. L., Carlson, J., Filieri, R., Jacobson, J., ... & Wang, Y. (2021). Setting the future of digital and social media marketing research: Perspectives and research propositions. *International journal of information management*, *59*, 102168.

Frank, B. (2021). Artificial intelligence-enabled environmental sustainability of products: Marketing benefits and their variation by consumer, location, and product types. *Journal of Cleaner Production*, *285*, 125242.

Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The emerging threat of AI-driven cyber attacks: A review. *Applied Artificial Intelligence*, *36*(1), 2037254.

Ibrahim, A., Thiruvady, D., Schneider, J. G., & Abdelrazek, M. (2020). The challenges of leveraging threat intelligence to stop data breaches. *Frontiers in Computer Science*, *2*, 36.

Jones, T., & Brown, R. (2020). *Data Privacy in the Digital Age*. Marketing Analytics Review.

Kanbach, D. K., Heiduk, L., Blueher, G., Schreiter, M., & Lahmann, A. (2024). The GenAI is out of the bottle: generative artificial intelligence from a business model innovation perspective. *Review of Managerial Science*, *18*(4), 1189-1220.

Kumar, D., & Suthar, N. (2024). Ethical and legal challenges of AI in marketing: an exploration of solutions. *Journal of Information, Communication and Ethics in Society*, *22*(1), 124-144.

Rustholllkarhu, S., Toukola, S., Aarikka-Stenroos, L., & Mahlamäki, T. (2022). Managing B2B customer journeys in the digital era: Four management activities with artificial intelligence-empowered tools. *Industrial Marketing Management, 104*, 241–257. https://doi.org/10.1016/j.indmarman.2022.04.014

Sarker, I. H. (2023). Multi-aspects AI-based modelling and adversarial learning for cybersecurity intelligence and robustness: A comprehensive overview. *Security and Privacy*, *6*(5), e295.

Smith, J., et al. (2021). *Adversarial Vulnerabilities in AI Systems*. Cybersecurity Journal.

Williams, J., Prawiyogi, A. G., Rodriguez, M., & Kovac, I. (2024). Enhancing circular economy with digital technologies: A pls-sem approach. *International Transactions on Education Technology (ITEE)*, *2*(2), 140-151.