Artificial Intelligence for Enhanced Cybersecurity: A Mini Literature Review in the Financial Services Industry

A Term Project

Presented to the School of Accountancy, Management, Computing and Information Studies
In Partial Fulfillment of the Requirements of the Course

Social And Professional Issues In Information Technology

Submitted By:
Aggabao, Arvy T.
Albarda, Alyssa Mari
Cariño, Mark Lorenz
Razo, Ma. Lourdes Shaine
Usi, Ma. Angela Shane L.
Walis, Clester Lonyr

December 07, 2024

Table of Contents

INTRODUCTION

The finance industry has undergone significant transformation through technological advancements, particularly in developing electronic banking and financial services. A major trend in this sector is the increasing adoption of digital platforms, including online and mobile banking. Artificial Intelligence (AI) and Machine Learning (ML) in the banking industry have the potential to revolutionize operating procedures and improve services, resulting in increased productivity, efficiency, and customer satisfaction (Singh & Kaunert, 2024). However, due to the growth of this industry through cloud computing, this evolution also attracted an increased cybersecurity risk. Cyberattacks that target cloud infrastructure can pose severe concerns to data security, confidentiality, and uptime (Yue & Shyu, 2024). Cyber attackers are always targeting cloud systems, which results in a 288% increase in annual rates of cyberattacks (Munirathinam, 2020). These attacks carry serious threats, such as financial fraud, data breaches, and severe harm to one's reputation.

Advanced security measures are required for businesses to avoid such violations and warrant the efficiency of the business operations (Sigov et al., 2022). Organizations are handling security threats with enhanced machine learning algorithms (ML) and artificial intelligence (AI) technology. These kinds of developments in technology are essential to improve security measures against these transforming threats. As cyber threats become a growing challenge, automation or AI plays a critical role in assisting in implementing more efficient and effective cybersecurity measures (Wan et al., 2020). Nevertheless, even if AI can be helpful, it also has technical limitations that restrict its capabilities, such as high levels of system complexity and quality data demands. Additionally, the ethical implications of using AI in technology raise concerns about accountability, privacy, and biases, hence, AI systems require an ethical policy to cope with the potential misuse, mitigate and avoid privacy concerns, and build social trust in technology-based solutions (Levis, 2024). However, this paper primarily focuses on identifying how the integration of AI can be achieved in enhancing cybersecurity, evaluating factors and challenges, and analyzing the various ethical issues that come with integrating this technology to improve cybersecurity.

Overall, this paper focuses on these key objectives: the first is to investigate how AI might be used for advanced threat detection and fraud prevention systems, hence improving cybersecurity architecture. The next one is to understand the implementation difficulties and technological constraints of integrating AI in cybersecurity, particularly the potential scaling issues and system vulnerability concerns that may occur during this process. Lastly, it is to determine the possible ethical implementations associated with AI and risk management to mitigate the negative implications of using AI in this field. With these objectives, this study seeks to provide insights into the potential integration of AI technology into cybersecurity in the financial industry and understand the risks associated with deploying such solutions.

METHODOLOGY

Artificial intelligence (AI) technologies have come a long way, from simple automation and calculations to more sophisticated and complex procedures, such as their integration with cybersecurity. Their integration with the field of cybersecurity particularly in the finance industry highlights our evolving landscape in technology that demands a comprehensive analysis and understanding utilizing the PRISMA framework as a guide. As outlined by Page et al. (2021), PRISMA, or Preferred Reporting Items for Systematic Reviews and Meta-Analyses, is a framework that assists researchers in ensuring transparency and completeness in the process of reviewing related literature. The PRISMA framework will be used throughout this literature review to help researchers better understand and identify the implications, ramifications, and challenges of AI in the field of cybersecurity.

In addition, for this literature review, researchers will use multiple journal and article databases, including but not limited to Google Scholar, INSPEC, ResearchGate, Science Direct, and CORE to have multiple perspectives on both the positive and negative implications of using artificial intelligence (AI) and machine learning algorithms (ML) in cybersecurity. All sources from this literature review will be journals or publications published between 2015 and 2024, both internationally and locally, to ensure that the literature reviewed is current and relevant to the emerging trends in AI-powered cybersecurity infrastructure. Using the systematic approach provided by PRISMA, combined with these academic publications, this mini literature review will be able to provide a clear insight into the current status of artificial intelligence (AI) in cybersecurity in the finance field, as well as uncover gaps and their potential implications for future AI development in cybersecurity domains.

RESULTS AND DISCUSSION

Advanced Threat Detection and Fraud Prevention Systems

The rise of digital transactions, mobile banking, and e-commerce has significantly increased fraud-related activities, prompting financial institutions to adopt artificial intelligence (AI) as a paradigm-shifting approach to real-time fraud detection, revolutionizing how they combat financial offenses (Ravi Teja Potla, 2023). Integrating AI-based models into financial institutions enables real-time data monitoring, which is essential for the timely detection of suspicious activities and is considered one of the significant advantages of using AI for fraud detection (Maple et al., 2023). Real-time data analysis is essential for detecting fraud and preventing fraudulent activity before it causes severe damage. Financial transactions are tracked constantly, and any alterations to typical trends are immediately examined (Haider Ali Javaid, 2024). This contrasts conventional rule-based systems, which frequently find it challenging to keep up with complex fraud schemes because they rely on preset rules that cannot adjust to novel strategies (Gautam, n.d.).

Conversely, Artificial Intelligence plays a significant role in fraud detection by employing sophisticated algorithms to analyze behavior, find irregularities, and detect fraud in massive data sets. Because AI systems learn from their past experiences, they can adjust to new technologies employed by scammers over time, improving their ability to forecast and spot fraud, allowing institutions to reduce financial losses, and react quickly to possible threats (Xu et al., 2024). This capability is critical in the connected and fast-paced world of today's changing financial environment when prompt action is necessary to reduce risks and avoid financial crimes (Zhang & Chen, 2024).

Implementation Challenges and Technical Limitations

Integrating AI in the financial industry, including the banking sector, poses many benefits as well as challenges. Like many others, AI has since changed the landscape of the financial industries, starting with its integration in an attempt by organizations to keep up with the ever-evolving technology. Some of the many utilized functions of AI are improving financial services by streamlining operations, boosting customer satisfaction, and enhancing security measures (Yalavarthi et al., 2024). Despite the many advantages of AI in banking, financial institutions face multiple challenges. For one, ensuring data quality and its proper management is crucial for AI systems to function properly, whereas banks often deal with inconsistent data storage and formats, making it difficult to maintain the integrity and accuracy of AI performance. The banking industry is also subject to strict regulations to which AI implementations and integrations must also adhere, posing complex and demanding risks of additional oversight. As AI models also reflect biases based on their training data, unfair outcomes and customer treatment may also tend to happen, which is why it is important to watch out for such biases and correct them to ensure fair customer service (Derilova et al., 2024). There are numerous aspects of utilizing AI technology that need to be kept in check in the financial sector. This is why the banking industry must be properly equipped to manage the risks and get the most out of the multiple benefits that AI systems have to offer.

Ethical Implications and Risk Management

Data risks of AI systems in finance are the possible threats affecting the confidentiality, integrity, and availability of AI data and systems (Stephens, 2024). Implementing AI in credit scoring can lead to discrimination issues (Fernandez, 2019). Additionally, integrating AI in fraud prevention could infringe on individuals' privacy rights (Patil, 2024). Therefore, adopting privacy-preserving techniques will be essential for the ethical use of AI (Dialzara, 2024). Bias in AI algorithms can also be minimized by adjusting data models and results (Dataheroes, 2023). Financial institutions must address the risks associated with AI, ensure compliance with relevant regulations (Jack, 2023), and address biases from black box AI systems by actively working to enhance the explainability of their AI systems through techniques such as explainable AI (Mastercard, n.d.). Additionally, regulators require financial institutions to establish frameworks that promote the ethical use of AI, ensuring transparency in AI-generated outcomes (Sandridge, 2024). Embracing the principles underlying the regulations of the General Data Protection Regulation (GDPR) and Data Privacy Act (DPA) can ensure that their AI systems are fair, transparent, and respectful of privacy (Udig, 2018). Over-reliance on AI in the financial system can make it more fragile and vulnerable to failures and cyberattacks (Leitner et al., 2024). While AI can automate tasks and improve decision-making, it may unintentionally undermine critical thinking and reasoning skills (Kim, 2024). A balanced approach that combines technology with human support can result in more efficient financial services. The growing reliance on AI (LinkedIn, 2024) offers significant opportunities. However, it highlights the importance of addressing challenges of AI algorithms to ensure fairness and accountability (Gomez, 2024).

CONCLUSION

This study highlighted advanced threat detection and fraud prevention, implementation challenges and technical limitations, and ethical implications and risk management. The findings show that the integration of Artificial Intelligence in cybersecurity offers significant benefits that include real-time fraud detection, proactive threat identification, and responses that are adaptive to emerging risks (Ravi Teja Potla, 2023; Xu et al., 2024). These benefits, however, also have a number of challenges that include the need for high-quality data, compliance with regulation, and ethical implications (Derilova et al., 2024; Patil, 2024).

The discussion revealed that the implementation of Artificial Intelligence systems is constrained by technical limitations despite Artificial Intelligence systems learning from threats (Stephens, 2024; Mastercard, n.d.). In order to address the challenges, a multifaceted approach is required. This approach involves AI model refinements, regulatory framework transparency, and commitment to ethical practices involving Artificial Intelligence (Sandridge, 2024; Gomez, 2024). Furthermore, there is a risk of undermining critical thinking and the increasing fragility of the system, which becomes apparent with over-reliance on Artificial Intelligence (Kim, 2024; Leitner et al., 2024).

To fully realize the potential of artificial intelligence, financial institutions must implement solid risk management frameworks and explainable AI methodologies, and comply with data protection rules such as DPA and GDPR (Udig, 2018; Sandridge, 2024). Finally, our literature study revealed that combining human experience with advanced AI systems is highly recommended to assure trust in AI-driven cybersecurity solutions as well as technological efficiency.

References

Dataheroes. (2023, August 2). *What is Bias Mitigation*. DataHeroes. https://dataheroes.ai/glossary/bias-mitigation/

Dialzara. (2024, May 23). *Privacy-Preserving AI: Techniques & Frameworks*. Dialzara.com. https://dialzara.com/blog/privacy-preserving-ai-techniques-and-frameworks/

Fernandez, M. (2019, September 5). *Algorithm Bias in Credit Scoring: What's Inside the Black Box? | Blog | CGAP*. Www.cgap.org. https://www.cgap.org/blog/algorithm-bias-in-credit-scoring-whats-inside-black-box

Galvanize. (2021, April 8). *Understanding the Risks of Machine Learning*. Galvanize. https://www.wegalvanize.com/risk/understanding-the-risks-of-machine-learning/

Gomez, A. (2024). *Can AI Detect and Prevent Fraud? | ADKF*. Adkf.com. https://www.adkf.com/news/can-ai-detect-and-prevent-fraud

jack. (2023, August 16). *The Challenges of Artificial Intelligence Adoption and Regulatory Compliance - Ethico*. Ethico. https://ethico.com/blog/the-challenges-of-artificial-intelligence-adoption-and-regulatory-compliance/

Kim. (2024, August 6). *The Unintended Consequences of Generative AI*. INSEAD Knowledge. https://knowledge.insead.edu/strategy/unintended-consequences-generative-ai

Leitner, G., Singh, J., van der Kraaij, A., & Zsámboki, B. (2024). The rise of artificial intelligence: benefits and risks for financial stability. *Financial Stability Review*. https://www.ecb.europa.eu/press/financial-stability-publications/fsr/special/html/ecb.fsrart202405_02~58c3ce5246.en.html

Levis, M. (2024). *Understanding The Limitations Of AI (Artificial Intelligence)*. Medium. https://medium.com/@marklevisebook/understanding-the-limitations-of-ai-artificial-intelligence-a264c1e0b8ab

Linkedin. (2024). *You're navigating the world of financial services. How do you balance automation with human connection?* Linkedin.com. https://www.linkedin.com/advice/1/youre-navigating-world-financial-services-how-yazpf

Mastercard. (n.d.). *Explainable AI: From Black Box to Transparency | Brighterion AI | A Mastercard Company*. B2b.mastercard.com. https://b2b.mastercard.com/news-and-insights/blog/explainable-ai-from-black-box-to-transparency/

Mhlanga, D. (2020). Industry 4.0 in Finance: The Impact of Artificial Intelligence (AI) on Digital Financial Inclusion. *International Journal of Financial Studies*, *8*(3), 45. mdpi. https://doi.org/10.3390/ijfs8030045

Munirathinam, S. (2020). *Chapter Six - Industry 4.0: Industrial Internet of Things (IIOT)* (P. Raj & P. Evangeline, Eds.). ScienceDirect; Elsevier. https://www.sciencedirect.com/science/article/abs/pii/S0065245819300634?via%3Dihub

Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., & McGuinness, L. A. (2021). The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. *Systematic Reviews*, *10*(1). https://systematicreviewsjournal.biomedcentral.com/articles/10.1186/s13643-021-01626-4

Patil, D. (2024, November 8). *Artificial intelligence in financial risk assessment and fraud detection: Opportunities and ethical concerns*. https://www.researchgate.net/publication/385746635_Artificial_intelligence_in_financial_risk_assessment_and_fraud_detection_Opportunities_and_ethical_concerns

Sandridge, T. (2024, August 12). *Maximizing compliance: Integrating gen AI into the financial regulatory framework*. IBM Blog; Security Intelligence. https://www.ibm.com/blog/maximizing-compliance-integrating-gen-ai-into-the-financial-regulatory-framework/

Sigov, A., Ratkin, L., Ivanov, L. A., & Xu, L. D. (2022). Emerging Enabling Technologies for Industry 4.0 and Beyond. *Information Systems Frontiers: A Journal of Research and Innovation*, 1–11. https://doi.org/10.1007/s10796-021-10213-w

Singh, B., & Kaunert, C. (2024). Vertical Assimilation of Artificial Intelligence and Machine Learning in Safeguarding Financial Data. *Advances in Finance, Accounting, and Economics Book Series*, 169–197. https://doi.org/10.4018/979-8-3693-3633-5.ch010

Stephens, T. (2024, June 5). *AI risks in accounting and finance*. Www.bccpa.ca. https://www.bccpa.ca/news-events/cpabc-newsroom/2024/june/ai-risks-in-accounting-and-finance/

Udig. (2018). *GDPR & CCPA Implications for Banks Using AI*. Udig.com. https://www.udig.com/insights/blog/gdpr-ccpa-implications-banks-ai

Wan, J., Yang, J., Wang, Z., & Hua, Q. (2018). Artificial Intelligence for Cloud-Assisted Smart Factory. *IEEE Access*, *6*, 55419–55430. https://doi.org/10.1109/access.2018.2871724

Yue, Y., & Shyu, J. Z. (2024). A paradigm shift in crisis management: The nexus of AGI‑driven intelligence fusion networks and blockchain trustworthiness. *Journal of Contingencies and Crisis Management*, *32*(1). https://doi.org/10.1111/1468-5973.12541