Analyzing the Impact of AI-Powered Attacks on Financial Stability in the UK

Ramya Raman , Agoba Abel

Sheffield Business School

Sheffield, United Kingdom

Submitted 3oth September 2025

Accepted 7th March , 2025

Published 7th March , 2025

Extended Abstract

In my dissertation, I investigated the multi-faceted consequences of AI-facilitated cyber-attacks on the financial stability of the UK banking sector. My research focused on four key areas: quantifying economic losses, evaluating regulatory frameworks, identifying vulnerabilities, and examining ethical considerations surrounding AI use in finance. To conduct this study, I utilized secondary data sources including financial reports, case studies, industry analyses, and academic literature. This approach allowed me to provide a comprehensive analysis of the current landscape and bridge critical knowledge gaps. Key Findings:

1. **Economic Impact**: the analysis revealed that AI-powered attacks have inflicted substantial economic losses on the UK banking sector. It is found that larger financial institutions suffered disproportionately more due to their complex interconnections. By synthesizing data from various sources, I was able to estimate both direct financial losses and indirect costs such as reputational damage. This quantification is crucial for developing evidence-based risk management strategies.
2. **Regulatory Frameworks**: After evaluating the effectiveness of existing UK regulatory frameworks in mitigating AI-powered attack risks. My research indicated that current regulations require continuous updating to address emerging AI threats effectively. There is a significant lag between the rapid evolution of AI technologies and the development of adequate regulatory responses. Based on the analysis of regulatory documents and

expert opinions, we need to make several improvements to enhance the adaptability and comprehensiveness of these frameworks.

3. **Vulnerabilities**: Through examination of technical reports and industry studies, we can identify the key vulnerabilities in UK financial systems that could be exploited by AI-powered attackers. In my research and findings, I have highlighted that outdated security measures and legacy systems pose significant risks. They have developed systematic approaches for vulnerability identification and mitigation, which can help financial institutions strengthen their security infrastructure.
4. **Ethical Considerations**: I have highlighted the ethical concerns surrounding the use of AI for both attack and defense in the UK financial sector. After examining issues such as transparency, accountability, and algorithmic bias. Based on my analysis of academic literature and policy papers, it is proposed that ethical frameworks for responsible AI development and deployment in financial security can be used in a more efficient way to provide ethical considerations.

Implications and Recommendations: My dissertation has significant implications for policymakers, financial institutions, and cybersecurity professionals. The findings underscore the urgent need for:

1. Adaptive regulatory approaches that can keep pace with rapidly evolving AI technologies.
2. Robust cybersecurity measures that specifically address AI-powered threats.
3. Ethical frameworks to guide the responsible development and deployment of AI in finance.

Based on my findings, it is recommended:

1. Regular updates to regulatory frameworks to address emerging AI threats.
2. Implementation of AI-driven defense systems to counter sophisticated attacks.
3. Continuous vulnerability assessments and updates to security measures.
4. Development of industry-wide ethical guidelines for AI use in financial security.
5. Enhanced collaboration between financial institutions, regulators, and cybersecurity experts to share threat intelligence and best practices.

In My dissertation I have observed the key contributions made to the field:

1. It provides a comprehensive, UK-specific analysis of the economic impact of AI-powered attacks on the financial sector.
2. It offers a critical evaluation of current regulatory frameworks and proposes evidence-based improvements.

3. It develops systematic approaches for identifying and mitigating vulnerabilities in financial systems.
4. It proposes ethical frameworks for responsible AI deployment in financial security.

By synthesizing existing knowledge and data, my study bridges the gap between theoretical understanding and real-world impacts of AI-based attacks on the UK financial sector. The findings offer critical insights for strengthening the stability and security of the UK financial system in an era of rapid technological advancement.

Future Research Directions: While my research provides valuable insights, it also highlights areas that require further investigation:

1. Long-term economic impacts of AI-powered attacks on the financial sector.
2. Effectiveness of proposed regulatory improvements in real-world scenarios.
3. Development of AI-driven defense systems that can anticipate and counter evolving threats.
4. Practical implementation of ethical frameworks in AI development for financial security.

In conclusion, my dissertation provides a comprehensive analysis of the impact of AI-powered attacks on UK financial stability. By addressing critical knowledge gaps and offering actionable recommendations, this research contributes significantly to enhancing the resilience of the UK financial sector against evolving AI-powered threats.

Reference list

MSc. Finance and Investment Dissertation Report Analyzing the Impact of AI-Powered Attacks on Financial Stability in the UK. (n.d.).