Gen AI in Financial Cybersecurity: A Comprehensive Review of Architectures, Algorithms, and Regulatory Challenges

Satyadhar Joshi[1]

[1]Independent Researcher Alumnus, International MBA, Bar-Ilan University, Israel Alumnus, Touro College MSIT, NY, USA.

Abstract

This paper provides a comprehensive review of the intersection of cybersecurity, generative AI, and risk within the financial sector. We explore how AI is being leveraged for both defensive and offensive purposes, the emerging threats posed by GenAI, and the critical need for robust risk management frameworks and regulatory guidance. This paper reviews the intersection of cybersecurity, generative artificial intelligence (AI), and risk management in the financial sector. We examine the dual role of AI as both a tool for enhancing cybersecurity defenses and a vector for sophisticated cyber threats. The paper analyzes regulatory responses, emerging best practices, and the evolving threat landscape, with particular attention to generative AI's impact on financial institutions' risk profiles. We synthesize insights from recent industry reports, regulatory guidance, and academic literature to provide a comprehensive overview of current challenges and future directions in this critical domain. This paper presents a comprehensive review of AI-driven cybersecurity framework designed for financial institutions, integrating data analysis, risk assessment, and decision-making processes. The frameworks reviewed are structured around the DIKW (Data, Information, Knowledge, Wisdom) pyramid, which transforms raw data into actionable insights through natural language processing (NLP) and thematic extraction. Key components include a modular system architecture that processes data from multiple sources (e.g., transaction logs, threat feeds) using AI models, a risk engine for scoring threats, and a decision tree for implementing mitigation strategies. Anomaly detection is achieved through Isolation Forest and auto encoder models, with thresholds ($\tau = 0.6$ and $\tau = 0.5$, respectively) calibrated to balance sensitivity and specificity. The decision logic incorporates rules such as automatic blocking for high-risk transactions (scores > 0.95) and multi-factor authentication (MFA) for non-whitelisted locations. Visualizations demonstrate the system's effectiveness in identifying and responding to threats while maintaining regulatory compliance.

Keywords; *Cybersecurity, Generative AI, Artificial Intelligence, Financial Sector, Risk Management, Financial Institutions, AI Governance, Regulatory Compliance, Cyber Threats.*

INTRODUCTION

The financial sector's digital transformation has accelerated with the adoption of artificial intelligence (AI), particularly generative AI technologies [1]. While these innovations offer unprecedented opportunities for efficiency, customer service, and risk management, they also introduce complex cybersecurity challenges [2]. Financial institutions now operate in an environment where AI serves both as a defensive tool against cyber threats and as an offensive weapon in the hands of malicious actors [3].

Recent regulatory guidance, such as the New York Department of Financial Services (NYDFS) October 2024 letter on AI-related cybersecurity risks, highlights the growing concern among policymakers [4], [5]. This paper examines three critical dimensions: (1) AI-enhanced cybersecurity threats facing financial institutions, (2) AI-driven risk management solutions, and (3) the evolving regulatory landscape for AI in finance.

The integration of artificial intelligence (AI), especially generative models, is reshaping the cybersecurity landscape in financial services.