Research Commons

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

By Joshi, S (Joshi, Satyadhar)

Source International Journal of Innovations in Science Engineering And Management
Page: 73-88
DOI: 10.69968/ijisem.2025v4i373-88

Published Jul 11 2025

Indexed 2025-08-04

Document Type Article

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.

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

+ See more data fields

Citation Network

In All Databases

0 Citations

25
Cited References

This record is from:

Research Commons

Suggest a correction
If you would like to improve the quality of the data in this record, please Suggest a correction