Integrating RAG Pipelines, LLMs, GenAI, and ML in Finance and Cybersecurity: an overview of use cases

by Atsu Vovor[i]

Introduction

The convergence of Retrieval-Augmented Generation (RAG) pipelines, Large Language Models (LLMs), Generative AI (GenAI), and Machine Learning (ML) is transforming finance and cybersecurity. These technologies work in synergy to enhance decision-making, automate complex tasks, and improve security. From fraud detection and financial advisory to real-time threat response, this integration provides deeper insights, faster risk assessments, and more effective compliance management. This article explores key use cases across finance, cybersecurity, and their combined applications in financial cybersecurity.

Finance Use Cases

Use Case	RAG Pipeline	LLMs	GenAI	ML	Example Workflow
Fraud Detection & Prevention	Retrieves transaction patterns, historical fraud cases, and risk indicators.	Explains flagged transactions in human-readable language.	Generates Suspicious Activity Reports (SARs).	Predicts fraud likelihood using supervised models.	ML flags a transaction → RAG fetches similar cases → LLM explains the alert → GenAI generates an SAR.
Financial Advisory & Portfolio Optimization	Retrieves market data, company financials, and research reports.	Explains investment strategies in simple terms.	Summarizes earnings reports and generates market sentiment.	Predicts portfolio performance using historical data and macroeconomic factors.	Client requests portfolio advice → RAG retrieves data → LLM explains strategy → ML assesses risk and simulates performance.
Anti-Money Laundering (AML) Compliance	Retrieves customer information, transactions, and high-risk jurisdictions.	Identifies patterns in unstructured data (emails, contracts).	Generates compliance documentation and alerts.	Detects unusual transaction patterns using anomaly detection.	RAG retrieves flagged transactions → ML scores AML risk → LLM explains risks → GenAI creates compliance reports.

Cybersecurity Use Cases

Use Case	RAG Pipeline	LLMs	GenAI	ML	Example Workflow
Threat Detection & Response	Fetches threat intelligence from databases and logs.	Correlates incidents and explains threats in natural language.	Generates incident reports and remediation plans.	Identifies anomalies in user behavior, network traffic, or system activity.	ML detects unusual login behavior → RAG fetches similar attack patterns → LLM explains attack → GenAI produces a remediation report.
Vulnerability Management	Retrieves known vulnerabilities, patches, and system configurations.	Assesses impact and suggests mitigation steps.	Writes patch management policies and security advisories.	Prioritizes vulnerabilities based on risk and likelihood of exploitation.	RAG fetches CVEs → ML prioritizes risks → LLM explains vulnerability impact → GenAI drafts security advisories.
Real-Time Phishing Detection	Retrieves phishing database logs and recent email activity.	Analyzes email content for malicious intent.	Generates alerts and response templates.	Classifies emails as phishing or legitimate using NLP models.	Employee reports a phishing email → ML flags it → RAG fetches similar cases → LLM explains indicators → GenAI creates an alert.

Combined Use Case: Financial Cybersecurity

Use Case	RAG Pipeline	LLMs	GenAI	ML	Example Workflow
Real-Time Fraud & Threat Mitigation	Retrieves transaction histories, cybersecurity alerts, and threat intelligence.	Analyzes transactions for fraud and system logs for breaches.	Generates fraud summaries, incident reports, and notifications.	Flags unusual activity in transactions and system behavior using anomaly detection.	ML detects fraud and a data breach → RAG retrieves related fraud and cyber threats → LLM explains both → GenAI generates a coordinated response plan.

Conclusion

By combining RAG pipelines, LLMs, GenAI, and ML, organizations can streamline fraud detection, optimize financial strategies, and strengthen cybersecurity defenses. These AI-driven solutions not only improve operational efficiency but also enhance accuracy in risk management and compliance. As financial threats and cyber risks continue to evolve, leveraging these advanced technologies will be essential for maintaining security, trust, and competitive advantage in the digital economy.

---

[i] Atsu Vovor: Consultant, Data & Analytics Specialist | Machine Learning | Data science | Quantitative Analysis | French & English Bilingual | atsu.vovor@bell.net | https://github.com/atsuvovor/Pub_Data_Analytics_Project | https://public.tableau.com/app/profile/atsu.vovor8645/vizzes