Banking Cybersecurity ML System

Network Intrusion Detection & Log Anomaly Detection

Estudiantes: Inmaculada Concepción Rondon & Iván Darío Amarillo Lozada
Clase: IA en Finanzas | Profesores: Andrés Mauricio Alzate Virviescas & Oscar Fernández
Grupo 9 | Fecha: 18 de Septiembre de 2025

1. El Problema

Las instituciones financieras enfrentan amenazas crecientes en ciberseguridad:
- Intrusiones en redes que comprometen transacciones bancarias.
- Anomalías en logs de servidores que pueden indicar ataques internos, fraudes o campañas avanzadas (APT).
- Nuevas amenazas (zero-day exploits) que no siguen patrones previos.

En un ecosistema financiero globalizado, con transacciones en tiempo real, la detección temprana y precisa es clave para pr

2. Justificación del Enfoque

El enfoque adoptado responde a las limitaciones de los sistemas convencionales de ciberseguridad:
- Reglas estáticas y firmas conocidas no detectan ataques sofisticados.
- Volumen masivo de datos financieros supera las capacidades humanas de análisis.
- Necesidad de cumplimiento normativo (GDPR, PCI-DSS, leyes financieras locales).

Nuestro modelo aprovecha Machine Learning e Inteligencia Artificial para:
- Detectar anomalías en patrones de red y registros de actividad.
- Anticipar amenazas emergentes con algoritmos que aprenden en tiempo real.
- Ofrecer explicabilidad y trazabilidad, cruciales para regulaciones legales y sociales.

3. Solución con IA

El sistema se implementó como un pipeline integral en Google Colab, estructurado en tres fases principales.

Modelos utilizados:
1. Network Intrusion Detection: Random Forest + XGBoost (ensemble).
2. Log Anomaly Detection: Isolation Forest + LSTM híbrido.

Objetivos del proyecto:
- Construir un sistema modular, reproducible y escalable para entornos financieros.
- Simular escenarios de ataque en transacciones y registros.
- Validar desempeño con métricas sólidas (precisión, recall, AUC).

4. Resultados y Descubrimientos

El sistema alcanzó resultados competitivos:
- Alta precisión (>95%) en intrusión de red.
- Capacidad de detección de anomalías en tiempo real.
- Escalabilidad para procesar grandes volúmenes de datos.

Ventajas del modelo:
- Combina enfoques supervisados y no supervisados.
- Reproducibilidad asegurada en Colab con documentación y código limpio.
- Diseño modular que permite añadir nuevos algoritmos.
- Se adapta a cambios económicos y de políticas mediante reentrenamiento.

5. Importancia de la Vigilancia Humana y Actualización

Aunque el sistema es robusto, la supervisión humana en tiempo real es esencial:
- Analistas de seguridad interpretan alertas y confirman amenazas.
- La IA debe alimentarse con nuevos datos: cambios en economía, variaciones culturales, políticas de stakeholders.

Esto garantiza que el modelo evolucione dinámicamente frente a nuevas amenazas.

6. Consideraciones Legales, Éticas y Sociales

El sistema debe adherirse a políticas internacionales de ciberseguridad:
- Reglas gubernamentales: GDPR, PCI-DSS, FFIEC.
- Principios éticos: explicabilidad, transparencia y no discriminación algorítmica.
- Aspectos sociales y psicológicos: garantizar confianza y evitar sesgos.

En caso legal, el sistema debe proveer trazabilidad completa: cómo se tomaron decisiones, bajo qué datos y qué políticas se

7. Comparación con Proyectos Similares

Otros proyectos en banca y finanzas han utilizado enfoques similares:
- KDD Cup Intrusion Detection Datasets: algoritmos básicos supervisados.
- Sistemas antifraude bancario: centrados en transacciones, no en logs.
- Modelos en FinTech recientes: detección de fraude en pagos digitales.

Nuestro aporte diferencial:
- Integramos detección de intrusión de red + anomalías en logs en un solo sistema.
- Usamos ensemble híbrido con Random Forest, XGBoost, Isolation Forest y LSTM.
- Diseñamos un pipeline explicable, reproducible y regulado, pensado en bancos reales.

8. Conclusión

El proyecto Banking Cybersecurity ML System demuestra la viabilidad de un enfoque IA-driven para la protección bancaria.

- Ofrece precisión y escalabilidad superiores.
- Introduce combinación de modelos híbridos en un mismo framework.
- Mantiene el foco en cumplimiento normativo, ética y vigilancia humana.
- Aporta innovación al sector financiero al unir detección de intrusión y monitoreo de logs en tiempo real.

Este sistema no solo es un ejercicio académico, sino una propuesta sólida que puede contribuir a la evolución de la ciberseg