Monitoreo en tiempo real de transacciones con Kafka

Nombre: Jonathan Vásquez

1. Objetivo del flujo

Implementar un sistema de monitoreo en tiempo real de las transacciones financieras de los clientes, con el fin de detectar patrones sospechosos y prevenir fraudes antes de que se produzcan pérdidas significativas.

2. Tipo de eventos a capturar

- Transacciones realizadas por los clientes: transferencias, pagos con tarjeta, depósitos y retiros.

- Eventos de inicio de sesión o cambios críticos en la cuenta (opcional, para detección de comportamiento sospechoso).

3. Qué se busca detectar o procesar en tiempo real

- Transacciones sospechosas según montos inusuales o frecuencia elevada.

- Patrones que podrían indicar fraude, como transferencias a cuentas no habituales o múltiples intentos fallidos.

- Generar alertas inmediatas al equipo de seguridad o bloqueo temporal de cuentas.

4. Herramienta principal

- **Apache Kafka**

Justificación: Kafka permite la ingesta de datos en tiempo real con alta escalabilidad y tolerancia a fallos, lo que lo hace ideal para sistemas financieros que requieren procesar grandes volúmenes de eventos de manera inmediata. Además, se integra fácilmente con plataformas de procesamiento como Flink o Spark Streaming para análisis en tiempo real.

5. Flujo general de ingesta

1. **Origen de datos:**
    - API de pagos de la fintech
    - Sistemas bancarios internos
    - App móvil de clientes
2. **Plataforma de mensajería:**
    - Kafka Topic: `transacciones_fintech`
    - Los productores (APIs y app móvil) envían eventos al topic en tiempo real.
3. **Procesamiento en tiempo real:**
    - Consumo de eventos desde Kafka mediante un consumidor (Flink o Spark Streaming conectado a Kafka).
    - Validaciones: verificar campos obligatorios (monto, cuenta origen/destino, timestamp).
    - Detección de patrones sospechosos mediante reglas predefinidas y algoritmos simples de análisis de comportamiento.
    - Limpieza y normalización de datos para análisis.
4. **Destino final:**
    - Sistema de alertas: notificaciones automáticas al equipo de seguridad o bloqueo de transacciones sospechosas.
    - Base de datos operativa: almacenamiento de transacciones procesadas para auditoría y análisis histórico.
    - Dashboard en tiempo real: visualización de métricas de fraude y transacciones en curso.

6. Beneficios de usar streaming frente a batch

1. **Detección inmediata de fraudes:** las alertas se generan en segundos, en lugar de esperar al procesamiento diario.

2. **Mayor eficiencia operativa:** permite reaccionar y tomar decisiones inmediatas, reduciendo riesgos y pérdidas financieras.

3. **Mejor experiencia de usuario:** se pueden bloquear o validar transacciones sospechosas antes de que afecten al cliente.