Nama : Mochammad Lintar Arya Dwiputra

NIM : 2024081032

Prodi : Sistem Informasi

Tgl : 25 Februari 2026

USE CASE AI DETEKSI TRANSAKSI MENCURIGAKAN PADA MOBILE BANKING

1. Masalah yang diselesaikan

   Bank perlu mendeteksi transaksi mencurigakan (misalnya transfer dalam jumlah besar, transaksi ke rekening yang tidak pernah digunakan, lokasi tidak wajar, atau jam transaksi tidak biasa) secara cepat untuk mencegah penipuan, pencurian saldo, dan penyalahgunaan akun. Tanpa sistem otomatis berbasis AI, pemantauan harus dilakukan secara manual dengan aturan statis, yang lambat, sulit mengikuti pola kejahatan baru, dan tidak mampu mengawasi jutaan transaksi real time.

2. Jenis Data yang digunakan
   - Data transaksi: waktu transaksi, nominal, jenis transaksi (transfer, top up, pembayaran), rekening tujuan, frekuensi transaksi, dan kanal yang digunakan (mobile, ATM, web).
   - Data perilaku pengguna: pola login harian, jenis perangkat (device ID), sistem operasi, lokasi (GPS/IP), jam aktif biasa, serta perubahan kebiasaan penggunaan aplikasi.
   - Data profil nasabah: jenis rekening (gaji, tabungan biasa, bisnis), pendapatan rata-rata, batas transaksi normal, riwayat transaksi sebelumnya, serta catatan jika pernah terlibat kasus fraud.
   - Data eksternal pendukung: daftar rekening blacklist, pola penipuan yang dilaporkan, dan informasi dari regulator atau jaringan antarbank.

3. Peran AI dalam Solusi
    - Menganalisis pola transaksi normal tiap nasabah menggunakan machine learning (misalnya anomaly detection) sehingga sistem bisa membedakan mana aktivitas wajar dan mana yang menyimpang.
    - Memberi skor risiko pada setiap transaksi berdasarkan berbagai fitur (nominal, lokasi, perangkat, waktu, tujuan) dan mengklasifikasikan transaksi menjadi risiko rendah, sedang, atau tinggi.
    - Memicu tindakan otomatis, seperti meminta verifikasi tambahan (OTP ekstra, challenge di aplikasi, verifikasi biometrik), menahan sementara transaksi berisiko tinggi, atau mengirim notifikasi ke tim fraud analyst.
    - Terus belajar dari data baru (feedback dari fraud analyst dan nasabah) sehingga model bisa beradaptasi dengan pola penipuan yang selalu berubah, seperti social engineering atau phishing yang model lama belum kenali.

4. Tantangan Penerapan
    - Risiko false positive yang tinggi, yaitu transaksi normal yang dianggap mencurigakan, dapat membuat nasabah terganggu karena transaksi tertahan atau diminta verifikasi berulang kali.
    - Kualitas, konsistensi, dan volume data menjadi krusial; data historis yang tidak lengkap, banyak noise, atau tidak terstandarisasi akan menyulitkan pelatihan model dan menurunkan akurasi deteksi.
    - Integrasi dengan sistem existing (core banking, mobile banking, sistem notifikasi) sering kompleks, karena banyak bank masih memakai sistem legacy yang tidak dirancang untuk AI real time.
    - Isu privasi dan keamanan data, karena sistem harus mengolah informasi sangat sensitif seperti lokasi, pola transaksi, dan identitas; perlu kepatuhan terhadap regulasi (misalnya aturan OJK/BI), enkripsi, dan kontrol akses yang ketat.
    - Kebutuhan sumber daya teknis dan SDM: bank harus punya infrastruktur komputasi yang memadai dan tim yang memahami baik sisi data science maupun regulasi keuangan, yang tidak selalu mudah dipenuhi.