

Online Fraud Prediction - Kelompok 2, Machine Learning Projects

Johannes Simatupang, S.Kom., M.Kom

| | |
|--------------------------|------------|
| Jimmie Henderson Gunawan | 2602164685 |
| Mellisa angeline | 2602077862 |
| Tiara intan kusuma | 2602172220 |
| Angel eodia | 2602192140 |
| Benny strata wijaya | 2540128682 |

Membuat sistem deteksi kecurangan online (online fraud detection) adalah langkah yang penting dalam konteks keamanan transaksi keuangan dan perlindungan konsumen. Berikut adalah beberapa latar belakang mengapa pembuatan sistem ini sangat penting:

1. Ketidakamanan Transaksi Online: Dengan meningkatnya jumlah transaksi keuangan yang dilakukan secara online, risiko kecurangan dan penipuan juga meningkat. Penting bagi penyedia layanan keuangan untuk dapat mendeteksi transaksi yang mencurigakan secara real-time untuk mengurangi kerugian finansial.
2. Perlindungan Konsumen: Konsumen dan pengguna layanan keuangan membutuhkan perlindungan terhadap akses tidak sah ke akun mereka, pencurian identitas, dan kegiatan keuangan ilegal lainnya. Sistem deteksi kecurangan membantu dalam mengidentifikasi dan mencegah potensi penipuan sebelum kerugian yang signifikan terjadi.
3. Kepatuhan Regulasi: Banyak negara memiliki regulasi ketat terkait keamanan transaksi keuangan, seperti GDPR di Eropa dan regulasi PCI DSS untuk penyedia layanan pembayaran. Membangun sistem deteksi kecurangan membantu organisasi mematuhi standar keamanan ini dan menghindari sanksi serta dampak reputasi negatif.
4. Ketepatan Waktu: Deteksi kecurangan yang cepat dan efektif penting untuk mengurangi dampaknya terhadap organisasi dan konsumen. Sistem yang dapat mengidentifikasi pola dan perilaku transaksi yang mencurigakan secara otomatis memungkinkan tindakan preventif yang cepat.
5. Peningkatan Efisiensi Operasional: Dengan menggunakan teknologi seperti machine learning dan analisis data besar (big data analytics), sistem deteksi kecurangan dapat mengurangi jumlah transaksi yang perlu diperiksa manual, sehingga meningkatkan efisiensi operasional dan menghemat biaya.

Secara keseluruhan, pembangunan sistem deteksi kecurangan online bukan hanya tentang melindungi aset finansial, tetapi juga tentang memastikan kepercayaan dan keamanan dalam ekosistem transaksi keuangan global yang semakin terhubung dan kompleks.

Berikut adalah beberapa contoh umum dari kecurangan online yang sering terjadi:

1. **Phishing:** Penipuan phishing adalah usaha untuk memperoleh informasi pribadi seperti kata sandi, nomor kartu kredit, atau informasi keuangan lainnya dengan menyamar sebagai entitas tepercaya melalui email, pesan teks, atau situs web palsu. Penipu sering mengirimkan email palsu yang terlihat seperti berasal dari bank atau layanan keuangan untuk menipu korban agar mengungkapkan informasi sensitif mereka. Sumber: [Federal Trade Commission (FTC) - Phishing

Scams](<https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams>)

2. **Kartu Kredit dan Debit Skimming:** Penipu menggunakan perangkat ilegal untuk mencuri informasi dari kartu kredit atau debit saat digunakan untuk pembayaran. Skimming biasanya terjadi di mesin ATM, terminal pembayaran, atau bahkan di restoran dan toko ritel. Informasi yang dicuri kemudian digunakan untuk melakukan pembelian ilegal atau penarikan uang. Sumber: [NerdWallet - Credit Card

Skimming](<https://www.nerdwallet.com/article/credit-cards/what-is-credit-card-skimming>)

3. **Identitas Palsu dalam Transaksi Online:** Penipu menggunakan informasi identitas yang dicuri untuk membuat akun palsu atau melakukan transaksi online atas nama orang lain. Hal ini dapat mengarah pada pencurian identitas dan keuangan yang serius. Sumber: [Federal Trade Commission (FTC) - Identity Theft](<https://www.consumer.ftc.gov/articles/identity-theft>)

4. **Investasi dan Skema Ponzi:** Penipuan investasi melibatkan janji keuntungan tinggi dengan risiko rendah, tetapi sebenarnya adalah skema Ponzi di mana uang dari investor baru digunakan untuk membayar investor yang lebih lama. Skema ini berakhir ketika aliran uang baru berhenti, meninggalkan banyak investor dengan kerugian besar. Sumber: [U.S. Securities and Exchange Commission (SEC) - Ponzi

Schemes](<https://www.sec.gov/spotlight/enf-actions-ponzi-schemes.shtml>)

5. **Peretasan Akun:** Penipu mencuri akses ke akun online seseorang, seperti akun media sosial, email, atau layanan keuangan, untuk mencuri informasi pribadi atau melakukan tindakan merugikan atas nama pemilik akun. Sumber: [Norton - Hacked Accounts](<https://us.norton.com/internetsecurity-how-to-how-to-tell-if-your-account-has-been-hacked.html>)

Kecurangan online ini memiliki dampak finansial dan emosional yang signifikan pada korban, dan penting untuk mengenali tanda-tanda dan menerapkan langkah-langkah keamanan yang diperlukan untuk melindungi diri dari penipuan ini. Menjaga informasi pribadi tetap aman, waspada terhadap taktik penipuan baru, dan menggunakan teknologi keamanan yang tepat adalah langkah-langkah kunci untuk mengurangi risiko kecurangan online.

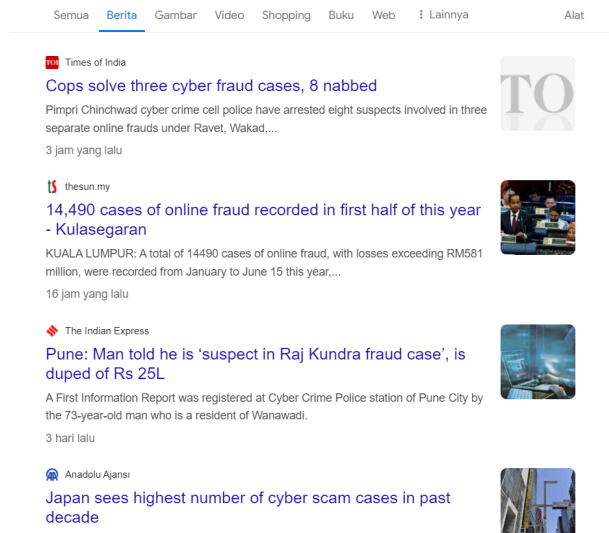


Fig.1. Online Fraud Cases