PROPOSAL PROYEK DESAIN INOVASI DATA SCIENCE

Sistem Deteksi Penipuan pada Transaksi Digital Berbasis Data Science

Kelompok : 24

Anggota Kelompok:

1. M. Reza Faris Al Faqih – 255150207111071

2. Muhammad Iqbal Fahmi – 255150200111024

3. Faisya Anindya Shafah – 255150201111046

4. Naila Sakha Nabila Akbar – 255150207111082

5. Jogi Christian Siburian– 255150200111003

DEPARTEMEN TEKNIK INFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS BRAWIJAYA

2025

DAFTAR ISI

ABSTRAK

Perkembangan teknologi digital yang pesat telah mendorong pertumbuhan signifikan dalam jumlah dan kompleksitas transaksi daring. Namun, kemajuan tersebut juga diiringi oleh meningkatnya risiko penipuan digital yang dilakukan dengan metode semakin variatif dan sulit dideteksi. Dalam konteks ini, *data science* berperan penting sebagai pendekatan ilmiah berbasis algoritma dan analisis data untuk mengidentifikasi pola-pola anomali yang berpotensi mengindikasikan aktivitas penipuan. Melalui penerapan berbagai teknik seperti *machine learning*, *deep learning*, serta analisis *big data*, sistem deteksi penipuan dapat dikembangkan menjadi lebih adaptif, responsif, dan mampu beroperasi secara *real-time* dalam mengenali transaksi mencurigakan.

Penelitian ini mengkaji bagaimana penerapan *data science* dapat meningkatkan efektivitas sistem deteksi penipuan pada transaksi digital, khususnya dengan membandingkan kinerja beberapa metode klasifikasi seperti *Random Forest*, *Decision Tree*, dan *Neural Networks*. Setiap metode memiliki karakteristik berbeda dalam menangani data yang tidak seimbang (*imbalanced data*), mengekstraksi fitur penting, dan menyesuaikan model terhadap perubahan pola perilaku pelaku penipuan. Selain itu, penelitian ini juga menyoroti pentingnya tahapan *feature engineering* dan pemrosesan data yang tepat agar sistem mampu mencapai tingkat akurasi tinggi tanpa mengorbankan efisiensi waktu komputasi.

Hasil kajian menunjukkan bahwa integrasi *data science* dalam sistem deteksi penipuan mampu meningkatkan kecepatan, akurasi, serta skalabilitas proses identifikasi anomali transaksi. Pendekatan ini tidak hanya memperkuat perlindungan bagi pengguna dan institusi keuangan, tetapi juga berkontribusi terhadap pengembangan ekosistem transaksi digital yang lebih aman dan terpercaya di tengah meningkatnya ancaman kejahatan siber.

BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era digital saat ini, transaksi keuangan daring telah menjadi bagian tak terpisahkan dari aktivitas ekonomi global. Kemudahan akses, efisiensi waktu, serta kemajuan teknologi finansial (fintech) telah mendorong peningkatan signifikan pada volume dan frekuensi transaksi digital. Namun, di balik kemudahan tersebut muncul tantangan serius berupa meningkatnya risiko kejahatan siber, terutama dalam bentuk penipuan digital yang menimbulkan kerugian finansial dan menurunkan tingkat kepercayaan pengguna terhadap sistem keuangan daring. Menurut laporan Kaspersky (2025), kerugian akibat penipuan digital terus mengalami peningkatan di berbagai sektor, menandakan kebutuhan mendesak akan sistem deteksi penipuan yang lebih adaptif, cerdas, dan efisien dalam menghadapi dinamika ancaman yang terus berkembang.

Penipuan pada transaksi digital kini dilakukan dengan metode yang semakin kompleks dan sulit dideteksi, seperti *social engineering*, pencurian identitas (*identity theft*), serta manipulasi data transaksi. Sistem deteksi tradisional berbasis aturan (*rule-based system*), yang bergantung pada pola tetap dan parameter statis, tidak lagi mampu mengidentifikasi variasi modus kejahatan baru. Pendekatan konvensional semacam ini memiliki keterbatasan dalam mengenali pola-pola baru karena tidak memiliki kemampuan pembelajaran dari data historis. Dalam konteks inilah, *data science* hadir sebagai solusi inovatif yang memanfaatkan kekuatan analisis *big data*, *machine learning*, dan *deep learning* untuk mendeteksi pola anomali secara lebih akurat dan *real-time*. Pendekatan ini memungkinkan sistem mengenali perilaku transaksi yang tidak wajar, sekaligus menyesuaikan model deteksi terhadap perubahan karakteristik penipuan seiring waktu.

Berbagai penelitian terdahulu menunjukkan bahwa algoritma seperti *Decision Tree*, *Random Forest*, dan *Neural Networks* memiliki efektivitas tinggi dalam membedakan antara transaksi normal dan mencurigakan (Setiawan et al., 2024). Model-model tersebut mampu mempelajari pola dari data historis dan mengidentifikasi potensi penipuan berdasarkan karakteristik tertentu. Selain pendekatan *supervised learning*, metode *unsupervised learning* seperti *clustering* dan *anomaly detection* juga terbukti efektif dalam menemukan perilaku transaksi yang menyimpang dari kebiasaan umum tanpa membutuhkan label data eksplisit. Kombinasi kedua pendekatan ini menjadikan sistem deteksi penipuan lebih fleksibel, adaptif, dan mampu menanggapi ancaman baru dengan cepat.

Dengan demikian, penerapan *data science* dalam sistem deteksi penipuan digital memiliki peran strategis dalam meningkatkan keamanan, akurasi, dan kemampuan adaptasi sistem terhadap pola kejahatan yang terus berevolusi. Penelitian ini berfokus pada analisis penerapan metode *data science* untuk mengembangkan sistem deteksi penipuan yang lebih efisien dan responsif terhadap dinamika transaksi digital. Melalui penelitian ini, diharapkan dapat dihasilkan kerangka kerja yang mendukung pengembangan sistem keamanan digital yang tidak hanya mampu mendeteksi penipuan secara cepat, tetapi juga mampu beradaptasi terhadap perubahan perilaku dan risiko dalam ekosistem keuangan digital yang terus berkembang.

1.2 Rumusan Masalah

- Bagaimana pendekatan data science dapat dimanfaatkan untuk merancang dan mengembangkan sistem deteksi penipuan dalam transaksi digital?
- Algoritma machine learning mana yang menunjukkan performa paling optimal dalam meningkatkan dan efisiensi sistem deteksi penipuan dalam transaksi digital?
- Bagaimana desain sistem deteksi penipuan digital berbasis data science dapat disusun agar mampu merespons secara cepat dan tangguh terhadap perubahan pola ancaman siber?

1.3 Tujuan

- Menganalisis dan meneliti pendekatan data science yang dapat dimanfaatkan untuk merancang dan mengembangkan sistem deteksi penipuan dalam transaksi digital.
- Mengidentifikasi algoritma machine learning mana yang dapat menunjukkan performa paling optimal dalam meningkatkan dan efisiensi sistem deteksi penipuan dalam transaksi digital.
- Menguji desain sistem deteksi penipuan digital berbasis data science dapat disusun agar mampu merespons secara cepat dan tangguh terhadap perubahan pola ancaman siber.

1.4 Manfaat

- Manfaat bagi Ilmu Pengetahuan
    1. Mendorong pengembangan model machine learning yang mampu mendeteksi pola pola dan karakteristik dari penipuan seiring waktu.
    2. Menciptakan kerangka kerja yang mendukung pengembangan sistem keamanan digital yang efisien.
- Manfaat bagi Masyarakat
    1. Membantu masyarakat dalam mendeteksi macam-macam penipuan berbasis digital
    2. Meningkatkan kepercayaan masyarakat dalam melakukan transaksi berbasis digital seperti jual beli online, transfer melalui m-banking, dan sebagainya

BAB II
TINJAUAN PUSTAKA

Tinjauan pustaka berisi ulasan dari penelitian-penelitian terdahulu yang relevan dengan topik penelitian. Sumber literatur yang digunakan mengacu pada:

1. **Teori atau Teknologi yang Digunakan**

1. Deteksi anomali dan paradigma pembelajaran

Sistem deteksi penipuan dalam transaksi digital didasarkan pada konsep deteksi anomali, yaitu mengidentifikasi perilaku transaksi yang tidak sesuai dengan pola biasa. Sistem ini juga menggunakan dua pendekatan utama dalam pembelajaran: supervised learning, yang memanfaatkan data yang sudah diberi label sebagai penipuan atau bukan penipuan, serta unsupervised atau semi-supervised learning, yang mendeteksi kemungkinan anomali tanpa perlu label. Kedua pendekatan ini biasanya digabungkan: unsupervised digunakan untuk pengelompokan awal atau mendeteksi jenis penipuan baru, sementara supervised digunakan untuk memberi skor dan mengambil keputusan akhir. Pendekatan gabungan ini membantu mendeteksi penipuan baru secara lebih sensitif sekaligus mempertahankan akurasi klasifikasi pada kasus yang sudah diketahui. (pdf: https://listwr.com/zS0Dit)

2. Algoritma utama dan karakteristiknya

- Decision Tree & Random Forest: mudah diaplikasikan, cukup mudah diartikan (tingkat fitur), dan kuat untuk data berbentuk tabel; sering dijadikan pilihan dasar yang solid dalam masalah penipuan.
- Gradient Boosting (XGBoost, LightGBM, CatBoost): lebih unggul pada data berbentuk tabel yang besar dan kelas yang tidak seimbang, banyak penelitian melaporkan performa yang bagus dalam mendeteksi penipuan.
- Neural Networks / Deep Learning (LSTM, Transformer, Autoencoder): berguna untuk mengenali pola urutan atau data time-series (misalnya urutan transaksi atau perilaku login) serta untuk merepresentasikan fitur yang kompleks; autoencoder sering digunakan untuk mendeteksi anomali tanpa perlu label.
- Isolation Forest & variasi algoritma unsupervised: efektif mendeteksi nilai-nilai yang tidak normal dalam skenario dengan kelas tidak seimbang.

Pemilihan algoritma tergantung pada trade-off antara akurasi, kemudahan diartikan, dan waktu komputasi. (*Albalawi & Dardouri, 2025*. jurnal: https://listwr.com/NtYtTD)

3. Infrastruktur & requirement real-time

Untuk merespons ancaman yang selalu berubah dengan cepat, sistem sebaiknya mendukung proses pengembangan fitur secara streaming, pelayanan model dengan latensi yang rendah, pemantauan kinerja model (deteksi pergeseran konsep), serta mekanisme pelatihan ulang secara otomatis atau semi-otomatis. Konsep deteksi pergeseran konsep dan pembelajaran online sangat penting untuk menjaga ketepatan model ketika pola transaksi mengalami perubahan.

2. **Proyek-Proyek Sejenis sebagai Pembanding**

1. Laporan industri — gambaran ancaman dan kebutuhan adaptif

Laporan dari para praktisi keamanan, seperti Kaspersky, menunjukkan bahwa para pelaku kejahatan siber semakin menggunakan teknik canggih berbasis AI dan stealth, serta meningkatkan metode phishing dan jumlah serangan yang dilancarkan. Hal ini menunjukkan bahwa diperlukan sistem deteksi yang mampu beradaptasi dan bekerja secara real-time. Temuan-temuan dari industri ini juga mendukung penelitian yang menekankan kemampuan adaptif dan kejelasan dalam sistem deteksi tersebut. (Kaspersky, 2025. https://listwr.com/Mqz5RE)

2. Implementasi akademik dan industrial

- Ensemble / stacking frameworks: beberapa studi terbaru (2023–2025) mengusulkan stacking/ensemble (XGBoost, LightGBM, CatBoost, RF) dengan teknik oversampling/SMOTE atau sampling heuristics untuk mengatasi imbalance, menghasilkan peningkatan metrik seperti F1 dan AUC.
- Autoencoder / deep anomaly pipelines: banyak proyek menggunakan autoencoder (dan variasinya) untuk mendeteksi anomali pada transaksi dan data akuntansi; studi menunjukkan autoencoder efektif sebagai lapisan deteksi awal.
- Drift-aware frameworks: penelitian tahun-terkini mengusulkan pipeline yang mengintegrasikan preprocessing adaptif dan drift detection untuk mempertahankan performa di lingkungan real-time.

3. **Literatur Akademik**

- **Efektivitas tree-based ensembles** — Banyak studi menunjukkan Random Forest dan gradient boosting (XGBoost/LightGBM) sering memberikan trade-off terbaik antara akurasi dan biaya komputasi pada dataset tabular transaksional; beberapa hasil empiris menemukan Random Forest atau boosting sebagai top-performer pada dataset kredit kartu. (*Albalawi & Dardouri, 2025*.https://listwr.com/cxkdsk)
- **Model sekuensial & temporal** — LSTM dan transformer-based architectures menunjukkan keunggulan mendeteksi anomali yang bersifat temporal (mis. pola transaksi berurutan), tetapi menuntut lebih banyak data, tuning, dan perhatian terhadap overfitting. (Darwish et al,2025. https://listwr.com/BlidjS)
- **Concept drift & adaptivity** — Studi 2024–2025 menekankan pentingnya deteksi dan adaptasi terhadap concept drift (perubahan distribusi fitur/perilaku), dengan pendekatan adaptive windowing, drift detectors, dan online retraining untuk lingkungan transaksi frekuensi tinggi. (https://listwr.com/5e2j8B)

BAB III
METODOLOGI DAN SOLUSI

3.1 Metodologi Perancangan

- Pendekatan penelitian yang digunakan dalam perancangan sistem deteksi penipuan digital ini adalah studi literatur dan simulasi eksperimental. Pendekatan studi literatur dilakukan untuk memahami teori, algoritma, serta metode yang relevan terkait penerapan *data science* dalam mendeteksi penipuan digital. Berbagai sumber ilmiah seperti jurnal penelitian, artikel akademik, dan laporan industri dijadikan dasar untuk merumuskan model konseptual dan menentukan algoritma yang paling sesuai.
- Tahapan Perancangan Sistem meliputi langkah-langkah berikut:

    1. Identifikasi Masalah dan Tujuan

        Menentukan permasalahan utama yaitu meningkatnya risiko penipuan digital akibat keterbatasan sistem deteksi tradisional berbasis aturan. Tujuannya adalah mengembangkan sistem deteksi yang adaptif dan cerdas melalui penerapan *data science*.

    2. Pengumpulan dan Analisis Data

        Data yang digunakan berupa data transaksi digital dengan atribut seperti waktu transaksi, nominal, jenis transaksi, dan status validasi. Data ini dapat bersumber dari dataset publik (misalnya *Credit Card Fraud Dataset* dari Kaggle) atau data sintetis yang menyerupai pola transaksi nyata.

    3. Pra-pemrosesan dan *Feature Engineering*

        Meliputi pembersihan data, normalisasi nilai, serta pembuatan fitur baru untuk memperkuat kemampuan model dalam mengenali pola anomali. Contohnya yaitu menghitung frekuensi transaksi pengguna dalam periode waktu tertentu, atau mendeteksi transaksi yang menyimpang dari kebiasaan pengguna.

    4. Evaluasi dan Validasi Model

        Hasil dari ketiga algoritma dibandingkan untuk menentukan model dengan kinerja paling optimal. Evaluasi ini bertujuan mengidentifikasi algoritma yang paling efisien dalam mendeteksi penipuan digital dengan tingkat kesalahan minimal.

    5. Implementasi dan Simulasi Sistem

        Model dengan performa terbaik kemudian diimplementasikan ke dalam sistem *prototype* berbasis *data science* untuk diuji secara simulatif. Sistem diuji dalam lingkungan yang menyerupai kondisi transaksi nyata untuk melihat kemampuan respons dan adaptasinya terhadap data baru.

- Tools / software / hardware yang digunakan untuk mendukung perancangan.

    Software: Python dengan pustaka *Scikit-learn*, *TensorFlow*, dan *Pandas* untuk pengolahan dan pemodelan data.

Hardware: Komputer dengan spesifikasi minimal prosesor multi-core dan RAM 16 GB, serta GPU opsional untuk pelatihan model *deep learning*.

Dataset: Dataset publik "Credit Card Fraud Detection" atau dataset simulasi yang menyerupai pola transaksi digital nyata.

3.2 Solusi

- **Solusi**

Solusi yang diusulkan adalah pengembangan sistem deteksi penipuan digital berbasis *data science* dengan memanfaatkan kombinasi algoritma *machine learning* dan *deep learning*. Sistem ini dirancang untuk menganalisis pola transaksi secara otomatis, mendeteksi aktivitas mencurigakan, dan memberikan peringatan (*alert system*) secara real-time. Penerapan algoritma seperti Random Forest dan Neural Networks diharapkan mampu meningkatkan kemampuan sistem dalam mengenali pola baru dari aktivitas penipuan yang terus berubah.

Gambaran keluaran sederhana sistem yang digunakan:

1 . Database (PostgreSQL) digunakan untuk menyimpan transaksi & hasil prediksi.

2. Model ML (LightGBM) digunakan untuk menghitung skor kemungkinan penipuan.

3. API (Flask) menjadi tempat sistem untuk bertransaksi dan mengirim data untuk menerima hasil deteksi.

4. Dashboard Sederhana (HTML/Chart.js) untuk menampilkan transaksi yang dicurigai sebagai penipuan.

- **Cara kerja solusi**

1. Setiap transaksi digital yang masuk akan diproses melalui tahap *data preprocessing* untuk memastikan format dan struktur data sesuai dengan kebutuhan model.
2. Fitur-fitur transaksi seperti nominal, waktu, lokasi, serta perilaku pengguna dianalisis oleh model yang telah dilatih untuk menentukan apakah transaksi tersebut tergolong normal atau mencurigakan.
3. Hasil prediksi model ditampilkan dalam bentuk klasifikasi (misalnya "normal" atau "fraud"), dan jika terdeteksi anomali, sistem akan mengirimkan notifikasi peringatan kepada pihak pengelola.
4. Data hasil deteksi kemudian disimpan kembali untuk melatih ulang model di masa mendatang agar sistem terus beradaptasi terhadap pola kejahatan baru.

- **Manfaat Solusi**

1. Bagi institusi keuangan: meningkatkan efektivitas dan kecepatan deteksi penipuan, mengurangi kerugian akibat transaksi ilegal, serta memperkuat sistem keamanan digital.

2. Bagi pengguna: memberikan perlindungan dan rasa aman dalam bertransaksi daring serta meningkatkan kepercayaan terhadap layanan keuangan digital.
3. Bagi dunia akademik: menjadi referensi penelitian lanjutan dalam penerapan *machine learning* untuk keamanan siber dan sistem keuangan.

- **Batasan solusi**

  Diperlukan sumber daya komputasi yang memadai, terutama ketika menggunakan arsitektur *deep learning* untuk data berskala besar.

BAB IV
HIPOTESIS HASIL

4.1 Prediksi Keluaran Utama

Berdasarkan metodologi dan solusi yang telah dirancang, penelitian ini diperkirakan akan menghasilkan sebuah sistem prototype deteksi penipuan digital yang mampu mengklasifikasikan transaksi secara otomatis menjadi kategori "normal" atau "fraud" dengan tingkat akurasi tinggi. Sistem ini akan dibangun menggunakan kombinasi algoritma machine learning, yaitu Random Forest dan Neural Networks, yang memiliki karakteristik unggul dalam menangani data transaksi yang kompleks dan tidak seimbang. Random Forest diperkirakan akan menunjukkan keunggulan dalam hal kemudahan interpretasi dan kecepatan komputasi dengan akurasi tinggi, sejalan dengan penelitian yang menunjukkan bahwa Decision Tree dan Random Forest mudah diaplikasikan, cukup mudah diartikan pada tingkat fitur, dan kuat untuk data berbentuk tabel, sering dijadikan pilihan dasar yang solid dalam masalah penipuan. Sementara itu, Neural Networks diharapkan mampu mendeteksi pola penipuan yang lebih kompleks dan tersembunyi, terutama pada kasus yang melibatkan interaksi fitur rumit dan pola temporal, sebagaimana dijelaskan bahwa algoritma ini berguna untuk mengenali pola urutan atau data time-series serta untuk merepresentasikan fitur yang kompleks.

Dengan penerapan mekanisme retraining berkala menggunakan data baru, sistem diperkirakan akan mampu beradaptasi terhadap perubahan pola penipuan atau concept drift dan mempertahankan performa deteksi yang konsisten seiring waktu. Hal ini sangat penting mengingat pelaku penipuan terus mengembangkan metode baru untuk menghindari deteksi, sebagaimana ditunjukkan oleh Kaspersky (2025) yang melaporkan bahwa pelaku kejahatan siber semakin menggunakan teknik canggih berbasis AI dan stealth, serta meningkatkan metode phishing dan jumlah serangan yang dilancarkan.

4.2 Pencapaian Tujuan

Tujuan pertama penelitian ini adalah menganalisis dan meneliti pendekatan data science untuk merancang sistem deteksi penipuan dalam transaksi digital. Tujuan ini diperkirakan akan tercapai melalui kajian komprehensif terhadap berbagai pendekatan, termasuk konsep deteksi anomali yang mengidentifikasi perilaku transaksi menyimpang dari pola normal. Penelitian ini akan menghasilkan analisis mendalam mengenai paradigma

pembelajaran yang menggabungkan supervised learning untuk klasifikasi transaksi berlabel dan unsupervised learning untuk mendeteksi pola penipuan baru.

Tujuan kedua adalah mengidentifikasi algoritma machine learning yang menunjukkan performa paling optimal dalam meningkatkan akurasi dan efisiensi sistem deteksi penipuan. Tujuan ini diperkirakan akan tercapai melalui evaluasi komparatif sistematis antara Random Forest dan Neural Networks. Random Forest diperkirakan akan menunjukkan performa solid dengan keunggulan pada kemudahan interpretasi, kecepatan training, dan kemampuan memberikan informasi feature importance yang berguna untuk memahami faktor-faktor kunci dalam deteksi penipuan.

Tujuan ketiga adalah menguji desain sistem agar mampu merespons secara cepat dan tangguh terhadap perubahan pola ancaman siber. Tujuan ini diperkirakan akan tercapai melalui simulasi sistem dalam berbagai kondisi yang mencerminkan tantangan nyata dalam lingkungan transaksi digital. Sistem akan diuji kemampuannya dalam hal responsivitas real-time dengan latensi rendah, memastikan deteksi dapat dilakukan dalam hitungan milidetik hingga beberapa detik, sejalan dengan requirement bahwa sistem sebaiknya mendukung proses pengembangan fitur secara streaming, pelayanan model dengan latensi yang rendah, pemantauan kinerja model, serta mekanisme pelatihan ulang secara otomatis atau semi-otomatis.

4.3 Kesesuaian dengan Kajian Pustaka

Hipotesis hasil yang dirumuskan dalam penelitian ini memiliki kesesuaian yang sangat kuat dengan kajian pustaka pada Bab II, baik dari aspek teoretis maupun implementasi praktis. Pendekatan deteksi anomali yang menjadi fondasi sistem ini sejalan dengan teori yang dikaji, yaitu mengidentifikasi perilaku transaksi yang menyimpang dari pola normal melalui kombinasi supervised dan unsupervised learning. Sebagaimana dijelaskan dalam kajian pustaka, sistem deteksi penipuan menggunakan dua pendekatan utama yang biasanya digabungkan, dengan unsupervised learning untuk pengelompokan awal atau mendeteksi jenis penipuan baru, sementara supervised learning untuk memberi skor dan mengambil keputusan akhir.

Desain sistem yang menekankan kemampuan real-time dan adaptif memiliki relevansi tinggi dengan temuan industri dan akademik yang dibahas dalam kajian pustaka. Laporan Kaspersky (2025) menunjukkan bahwa pelaku kejahatan siber semakin menggunakan teknik canggih berbasis AI dan stealth, yang menegaskan kebutuhan mendesak akan sistem deteksi yang mampu beradaptasi dan bekerja secara real-time. Kajian pustaka menyebutkan bahwa sistem sebaiknya mendukung pengembangan fitur secara streaming, pelayanan model dengan latensi rendah, pemantauan kinerja model, serta mekanisme pelatihan ulang otomatis atau semi-otomatis.

DAFTAR PUSTAKA

Kaspersky. (2025, Mei 7). *Kaspersky state of ransomware report-2025: Global and regional insights for international anti-ransomwae day*. Kaspersky. https://www.kaspersky.com/about/press-releases/kaspersky-state-of-ransomware-report-2025-global-and-regional-insights-for-international-anti-ransomware-day

Ardhitha, R., Anugerah, R. & Sutabri, T. (2025). *Analisis penerapan machine learning dan algoritma anomali untuk deteksi penipuan pada transaksi digital*. Jurnal Volume 3(1), Januari 2025. Diakses dari https://share.google/7xLPeiq1DNOuNCcqp

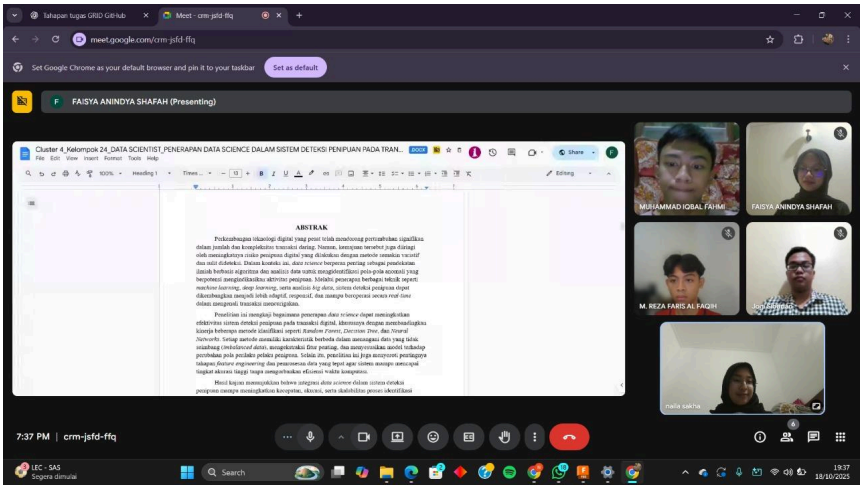
Albalawi, T. & Dardouri, S. (2025). *Enhancing credit card fraud detection using traditional and deep learning models with class imbalance mitigation*, *Frontiers in Artificial Intelligence*, 8, 1643292. Diakses dari https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2025.1643292

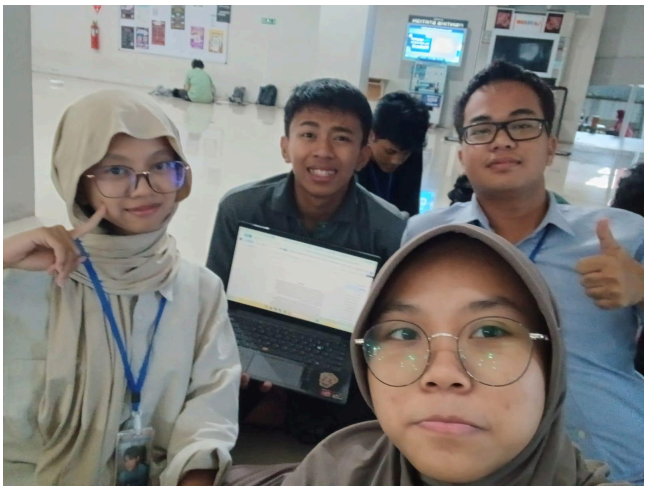
Kaspersky, 2025. *Phishing evolves with AI and stealth: Kaspersky highlights biometric and signature risks*. Diakses dari: https://www.kaspersky.com/about/press-releases/phishing-evolves-with-ai-and-stealth-kaspersky-highlights-biometric-and-signature-risks

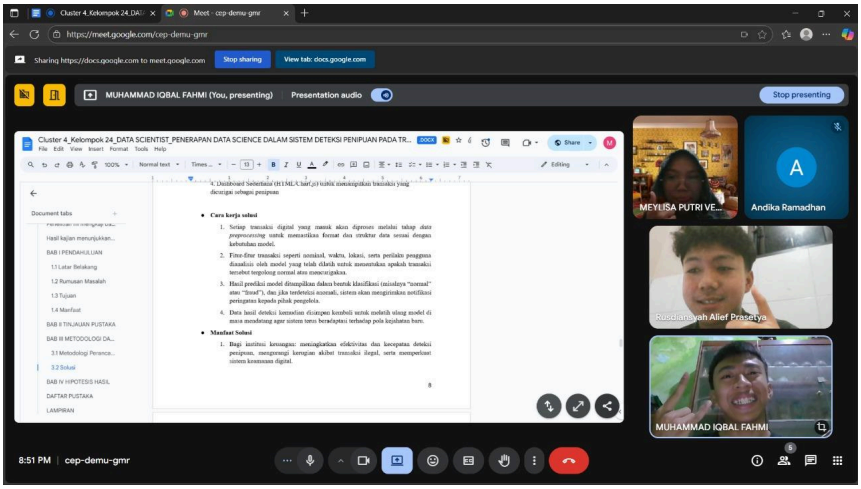
Darwish, S.M., Salama, A.I. & Elzoghabi, A.A., 2025. *Intelligent approach to detecting online fraudulent trading with solution for imbalanced data in fintech forensics*. *Scientific Reports*, 15, Article number: 17983. Diakses dari: https://www.nature.com/articles/s41598-025-01223-8

Al Lawati, H.M.R., Zainal, A., Al-rimy, B.A.S., Al-Azawi, M.A.N., Kassim, M.N. & Almalki, S.A.A., 2025. *An Integrated Preprocessing and Drift Detection Approach With Adaptive Windowing For Fraud Detection In Payment Systems*. IEEE Access. Diakses dari: https://www.researchgate.net/publication/391719384_An_Integrated_Preprocessing_and_Drift_Detection_Approach_With_Adaptive_Windowing_For_Fraud_Detection_In_Payment_Systems_February_2025

LAMPIRAN


FAISYA ANINDYA SHAFAH (Presenting)
MUHAMMAD IQBAL FAHMI
FAISYA ANINDYA SHAFAH
M. REZA FARIS AL FAQIH
7:37 PM | crm-jsfd-ffq




MUHAMMAD IQBAL FAHMI (You, presenting)
Presentation audio
Stop presenting
MEYLISA PUTRI VE...
Andika Ramadhan
Rusdiansyah Alief Prasetya
MUHAMMAD IQBAL FAHMI
8:51 PM | cep-demu-gmr