Published by: Asosiasi Dosen Akuntansi Indonesia
https://journal.adaiindonesia.or.id/index.php/sintamai

SINTAMA: Jurnal Sistem Informasi, Akuntansi dan Manajemen
journal homepage: https://jurnal.adai.or.id/index.php/sintamai

Analisis Pola Tren Transaksi Mencurigakan Pada Aplikasi Dana Sebagai Indikator Fraud Digital Tahun 2020-2024

Ingga Floreancita Tarigan
Program Studi Akuntansi, Fakultas Ekonomi, Universitas Negeri Medan,
Penulis Korespondensi: Ingga Floreancita Tarigan
e-mail : inggatarigan@gmail.com

ARTIKEL INFO

Artikel History:
Menerima 30 Mei 2025
Diterima 31 Mei 2025
Tersedia Online: 31 Mei 2025

Kata kunci :
Penipuan Digital, E-wallet, Transaksi Mencurigakan, Deteksi Dini, Analisis Forensik Digital.

ABSTRAK

Penelitian ini bertujuan untuk menganalisis pola transaksi mencurigakan pada aplikasi dompet digital DANA sebagai indikator awal terjadinya fraud digital. Dengan menggunakan pendekatan deskriptif kuantitatif berbasis data sekunder, studi ini mengumpulkan dan merekonstruksi kasus-kasus penipuan dari berbagai sumber terpercaya seperti jurnal ilmiah, laporan media daring nasional, dan publikasi resmi dari platform DANA. Hasil analisis menunjukkan bahwa pola fraud digital pada DANA umumnya melibatkan teknik rekayasa sosial, phishing, penyalahgunaan OTP, hingga penggunaan akun palsu dan malware. Karakteristik transaksi mencurigakan meliputi aktivitas login dari perangkat tidak dikenal, pengajuan refund tanpa dasar, serta transaksi abnormal dalam frekuensi dan nominal. Pola ini menunjukkan adanya kecenderungan yang dapat dijadikan indikator fraud dan berkontribusi pada pembangunan sistem deteksi dini berbasis perilaku pengguna. Penelitian ini menegaskan pentingnya perlindungan data konsumen, edukasi digital, serta penguatan sistem keamanan berbasis analitik sebagai langkah pencegahan terhadap kejahatan digital yang semakin kompleks.

ARTICLE INFO

Artikel History:
Received 30 May 2025
Accepted 31 May 2025
Available Online:31 May 2025

Keywords :
Digital Fraud, E-wallet, Suspicious Transactions, Early Detection, Digital Forensic Analysis.

ABSTRACT

This study aims to analyze suspicious transaction patterns on the DANA digital wallet application as early indicators of digital fraud. Using a descriptive quantitative approach based on secondary data, the research collects and reconstructs fraud cases from various credible sources, including academic journals, national online media reports, and official publications from the DANA platform. The analysis reveals that digital fraud patterns on DANA commonly involve social engineering, phishing, OTP misuse, fake accounts, and malware. Suspicious transaction characteristics include logins from unknown devices, unjustified refund requests, and abnormal transaction frequencies or amounts. These patterns indicate trends that can serve as early fraud indicators and contribute to the development of user behavior-based detection systems. This study emphasizes the importance of consumer data protection, digital literacy, and the enhancement of security systems based on analytical methods as preventive measures against increasingly sophisticated digital crimes.

1. PENDAHULUAN

Di abad ke-21 ini, sudah semakin luas pengetahuan kita tentang teknologi yang telah memfasilitasi kita kemudahan untuk melakukan kegiatan di bidang pendidikan, bisnis, perbankan,

pemerintahan, industri, dan lainnya. Bersamaan dengan perkembangan teknologi yang semakin luas dan beragam, dampaknya semakin terlihat dalam cara masyarakat menjalani hidup serta mengubah pola sistem pembayaran di lingkungan mereka. Dampak ini pada umumnya membawa sejumlah keuntungan positif bagi masyarakat, salah satunya adalah kemudahan dalam melakukan transaksi melalui metode pembayaran baru, seperti uang elektronik.

Perkembangan teknologi digital telah mendorong transformasi besar dalam sistem pembayaran di Indonesia. Salah satu bentuk inovasi yang paling signifikan adalah kehadiran dompet digital (e-wallet), yang memungkinkan masyarakat melakukan transaksi keuangan secara praktis dan cepat. DANA, sebagai salah satu aplikasi e-wallet terkemuka di Indonesia, mencatat pertumbuhan pengguna dan volume transaksi yang pesat dalam beberapa tahun terakhir. Berdasarkan data dari Bank Indonesia, nilai transaksi uang elektronik terus meningkat dari tahun ke tahun, mencerminkan pergeseran preferensi masyarakat dari pembayaran tunai ke nontunai.

Namun, kemajuan ini juga diiringi dengan tantangan meningkatnya potensi penyalahgunaan e-wallet. Laporan dari Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK) menunjukkan peningkatan transaksi mencurigakan terkait e-money selama periode pemilu lebih dari 100 %, sedangkan Satgas Pemberantasan Judi Online mencatat deposit judi online melalui e-wallet mencapai Rp34 triliun di 2023 dan Rp43 triliun pada kuartal III 2024. Di sisi pengguna, layanan seperti DANA telah memblokir lebih dari 30.000 akun dan merchant karena transaksi mencurigakan terkait judi online, sekaligus mencatat 50.000 pencarian per bulan di fitur “Scam Checker”

Dalam konteks ini, identifikasi pola transaksi mencurigakan menjadi sangat penting sebagai indikator dini fraud digital. Karakteristik seperti frekuensi transaksi tinggi dalam waktu singkat, jumlah nominal besar yang tidak wajar, atau aktivitas di luar jam operasional normal (misalnya transaksi malam hari) menjadi sinyal potensial fraud . Dengan penerapan metode forensik kuantitatif terhadap data sekunder, penelitian ini bertujuan untuk memetakan dan menganalisis pola transaksi mencurigakan di e-wallet DANA dari tahun 2020 hingga 2024.

Penelitian ini bertujuan untuk menganalisis pola transaksi mencurigakan pada aplikasi DANA dengan menggunakan data sekunder dari lembaga-lembaga resmi dan publikasi media. Penelitian ini dilakukan dengan pendekatan kuantitatif deskriptif menggunakan data sekunder dari dokumentasi publik yang relevan, tanpa melibatkan responden atau pengumpulan data primer.

2. STUDI LITERATUR

Keamanan dan Ancaman E-Wallet

Konsep keamanan dalam sistem pembayaran digital mengacu pada perlindungan data transaksi, autentikasi pengguna, dan integritas sistem. Dalam studi oleh Khaidir & Nasution (2024), dibahas bahwa meskipun e-wallet seperti DANA sudah dilengkapi teknologi enkripsi end-to-end, one-time password (OTP), hingga verifikasi biometrik, hal ini tidak menjamin sistem bebas dari risiko fraud. Hal ini disebabkan karena faktor manusia (human error) dan ancaman eksternal seperti social engineering dan phising yang menyasar pengguna e-wallet. Penelitian ini menegaskan pentingnya edukasi pengguna sebagai elemen penting dari sistem keamanan, bukan hanya ketergantungan pada teknologi. Studi sistematis oleh Dewi et al. (2024) juga mengidentifikasi berbagai ancaman yang membayangi sistem pembayaran digital, mulai dari malware yang menyusup ke aplikasi, hingga eksploitasi kelemahan dalam API (Application Programming Interface) penyedia e-wallet. Mereka menekankan bahwa sifat terdistribusi dari transaksi digital memperbesar kemungkinan pengguna menjadi target penipuan secara tersembunyi, serta menyulitkan pelacakan pelaku. Oleh karena itu, pengawasan transaksi dan deteksi dini menjadi kebutuhan mendesak.

Fraud Mitigation Melalui Digital Payment

Transaksi digital yang terdokumentasi secara otomatis diyakini mampu mengurangi celah fraud yang sering terjadi pada sistem tunai tradisional. Prasetya et al. (2021) memaparkan bahwa digitalisasi transaksi memberikan keunggulan dalam bentuk rekam jejak yang jelas, time-stamp akurat, dan integrasi audit trail, sehingga risiko manipulasi data dapat ditekan. Namun, riset ini juga menekankan bahwa sistem akan tetap rentan tanpa adanya sistem kontrol internal yang aktif dan real-time. Sementara itu, Mohamed & Shuhidan (2023) dalam studi kawasan Asia Tenggara menyoroti peran e-payment dalam meningkatkan transparansi dan akuntabilitas dalam rantai pembayaran, baik oleh individu maupun korporasi. Mereka mencatat bahwa digital payment lebih mudah dianalisis dengan tools analitik dan kecerdasan buatan (AI) dibanding metode tradisional, karena tersedianya data besar (big data) dan struktur metadata yang bisa diolah.

Teknik Deteksi Fraud Digital

Deteksi terhadap aktivitas mencurigakan dalam sistem digital semakin berkembang berkat kemajuan teknologi analisis data. Pendekatan berbasis data mining dan machine learning menjadi standar dalam studi-studi internasional. Metode seperti unsupervised learning (clustering, outlier detection) dan supervised learning (decision tree, random forest) digunakan untuk membangun model yang mampu mengenali pola anomali dalam transaksi digital. Salah satu studi menyebutkan bahwa algoritma seperti XGBoost, SVM, dan neural network telah berhasil digunakan untuk memetakan pola transaksi mencurigakan dalam sistem blockchain dan fintech global. Teknik ini efektif karena dapat belajar dari riwayat transaksi sebelumnya dan mengklasifikasikan transaksi baru berdasarkan kemiripan pola.

Kajian E-Wallet dan Pencegahan Fraud

Di Indonesia, kajian mengenai pengawasan sistem dompet digital masih berkembang. Dewi et al. (2024) menunjukkan bahwa perlindungan konsumen sangat tergantung pada kejelasan regulasi dan keterlibatan lembaga pengawasan seperti OJK dan BI. Mereka mengkaji bagaimana UU ITE, Peraturan Bank Indonesia No. 22/23/PBI/2020, dan peran Satgas Anti Fraud menjadi pilar penting dalam ekosistem pembayaran digital. Studi ini menekankan perlunya audit terhadap aktivitas akun yang berisiko, serta transparansi dari penyedia e-wallet terhadap aktivitas yang mereka blokir atau laporkan ke pihak berwajib. Khaidir & Nasution (2024) juga menyampaikan bahwa tingginya kasus penipuan online di Indonesia menunjukkan kurangnya literasi digital masyarakat serta lemahnya sanksi hukum terhadap pelaku. Penelitian mereka menyoroti pentingnya keterlibatan komunitas, edukasi pengguna, dan peningkatan literasi keamanan digital sebagai strategi pelengkap dari sisi teknologi dan kebijakan.

Kasus Fraud dan Teknis Deteksi

Penelitian berbasis teknologi oleh Hasugian & Suharjito (2023) menampilkan implementasi deep learning (CNN dan LSTM) untuk mengenali pola transaksi mencurigakan dalam sistem digital banking. Mereka menggunakan data transaksi aktual dan mencapai akurasi tinggi dalam mendeteksi potensi fraud. Dalam jurnal JTIE (2024), dijelaskan bagaimana penerapan machine learning mampu mendeteksi scam digital dan perilaku mencurigakan di berbagai platform, termasuk e-commerce dan dompet digital. Dengan mengklasifikasikan data berdasarkan riwayat transaksi, waktu, dan pola pengguna, sistem dapat menandai potensi aktivitas penipuan secara otomatis. Kajian ini juga menyarankan integrasi sistem fraud alert dengan dashboard pengawasan internal lembaga keuangan.

Meskipun berbagai studi terdahulu menggunakan metode pembelajaran mesin atau data mining dalam mendeteksi fraud, penelitian ini tidak menerapkan teknik tersebut secara langsung,

melainkan mengadopsi hasil analisis mereka sebagai referensi pola yang digunakan untuk studi dokumentasi.

3. METODE RISET

Penelitian ini menggunakan pendekatan kuantitatif deskriptif berbasis studi dokumentasi, dengan tujuan untuk menganalisis pola transaksi mencurigakan pada aplikasi dompet digital DANA sebagai indikator terjadinya fraud digital. Pendekatan kuantitatif dalam penelitian ini tidak melibatkan pengumpulan data primer dari responden, kuesioner, atau wawancara, melainkan sepenuhnya mengandalkan data sekunder yang dikumpulkan melalui penelusuran sumber terpercaya di internet. Sumber data mencakup artikel jurnal ilmiah, laporan dari lembaga regulator seperti Bank Indonesia dan Otoritas Jasa Keuangan, pernyataan resmi dari pihak DANA, serta pemberitaan dari media massa nasional seperti Kompas, CNBC Indonesia, Katadata, dan Detik.com.

Unit analisis dalam penelitian ini adalah laporan-laporan transaksi digital mencurigakan dan insiden fraud yang dialami oleh konsumen aplikasi DANA pada kurun waktu 2022–2024. Data yang dikumpulkan meliputi kronologi kejadian, jenis fraud yang terjadi (seperti phishing, pencurian akun, dan manipulasi transaksi), serta indikator mencurigakan seperti frekuensi transaksi tinggi dalam waktu singkat, perubahan data akun mendadak, dan pelaporan saldo hilang. Informasi diklasifikasikan berdasarkan tema dan jumlah kasus yang dilaporkan, serta disusun ke dalam narasi dan rekap tabel manual yang memperlihatkan kecenderungan pola dan tren kasus fraud digital.

Teknik pengumpulan data dilakukan secara dokumentatif, yaitu dengan menghimpun data dan informasi tertulis dari berbagai sumber terbuka yang memenuhi kriteria kelayakan akademik dan aktualitas. Data diseleksi berdasarkan relevansi dengan fokus penelitian, kemudian dianalisis secara deskriptif kuantitatif melalui penghitungan manual atas jumlah kasus, jenis fraud, serta karakteristik transaksi mencurigakan yang diungkap dalam masing-masing sumber. Data disajikan dalam bentuk uraian naratif, tabel ringkas, dan statistik dasar yang dihitung secara manual (tanpa perangkat lunak statistik), seperti jumlah kasus per tahun, per jenis fraud, dan per indikator risiko.

Pendekatan ini memberikan gambaran faktual atas dinamika fraud digital yang terjadi dalam ekosistem e-wallet DANA berdasarkan informasi terbuka, serta mendukung pemetaan pola-pola transaksi yang dapat dijadikan indikator awal dalam pencegahan fraud. Validitas data diperoleh melalui triangulasi sumber, yaitu dengan membandingkan informasi yang sama dari beberapa sumber berbeda guna memastikan konsistensi dan keandalan data.

4. HASIL DAN PEMBAHASAN

Tren Kasus Fraud Digital pada Aplikasi DANA

dompet digital di Indonesia telah membawa kemudahan dalam bertransaksi, namun juga menghadirkan risiko baru berupa kejahatan siber, khususnya fraud digital. Salah satu platform yang sering menjadi sorotan dalam hal ini adalah aplikasi DANA. Berdasarkan data dokumentasi dari media dan lembaga resmi, berbagai kasus penipuan telah terjadi sejak tahun 2022 hingga 2024, mencakup jenis fraud yang beragam. Laporan Katadata (2022) menunjukkan bahwa sekitar 35% dari 26.000 aduan masyarakat kepada Kominfo terkait dengan layanan fintech dan e-wallet, termasuk DANA.

Salah satu tren yang mencolok adalah meningkatnya kasus penipuan berbasis social engineering, di mana pelaku menyamar sebagai petugas customer service resmi DANA. Dalam kasus yang dilaporkan DetikFinance (2023), seorang korban mengaku kehilangan saldo Rp12 juta setelah membagikan kode OTP karena mengira sedang berbicara dengan pihak DANA resmi.

Modus seperti ini sangat efektif karena memanfaatkan psikologis korban dan minim jejak digital yang bisa langsung dideteksi sistem keamanan aplikasi.

Selain itu, tren lain yang muncul adalah penyebaran link palsu yang menjanjikan top-up saldo gratis, refund palsu, dan program undian yang mengharuskan pengguna untuk memberikan data sensitif. Kasus semacam ini banyak ditemukan di media sosial seperti Instagram, TikTok, dan WhatsApp. Bahkan, menurut KompasTekno (2023), banyak pelaku menggunakan tautan palsu yang dibuat mirip dengan domain resmi DANA, untuk mengelabui korban.

Fenomena ini menunjukkan bahwa peningkatan volume pengguna e-wallet tidak diiringi dengan literasi digital yang memadai. Akibatnya, pelaku fraud dapat mengeksploitasi celah perilaku pengguna, bukan hanya sistem aplikasi. Oleh karena itu, perlu adanya pembenahan dalam sistem pengawasan fraud digital, baik melalui peningkatan edukasi konsumen maupun pemanfaatan big data untuk mendeteksi aktivitas abnormal secara lebih dini.

Pola Transaksi Mencurigakan yang Umum Terjadi

Hasil analisis dokumentasi dari berbagai kasus yang dilaporkan di media menunjukkan pola-pola yang konsisten dalam terjadinya transaksi mencurigakan pada aplikasi DANA. Pola ini penting untuk diidentifikasi karena dapat dijadikan indikator awal dalam sistem deteksi fraud. Berdasarkan rekap data dan studi media seperti KompasTekno (2023), CNN Indonesia (2024), dan laporan keamanan dari DANA sendiri, terdapat beberapa ciri umum yang muncul dalam transaksi-transaksi mencurigakan tersebut.

Pertama, transaksi dalam jumlah kecil namun dilakukan secara berulang dalam waktu singkat. Pola ini sering digunakan pelaku untuk menguji validitas akun atau kartu yang terhubung dengan akun DANA korban sebelum melakukan pencurian dalam jumlah besar. Kedua, adanya aktivitas login dari perangkat yang berbeda dalam waktu yang hampir bersamaan. Misalnya, korban sedang tidak menggunakan akun, tetapi sistem mencatat login dari IP address luar negeri atau perangkat yang tidak dikenali. Ketiga, akun yang terlibat dalam fraud umumnya baru dibuat dan tidak memiliki riwayat transaksi yang normal. Ini menunjukkan bahwa pelaku sering menggunakan akun sementara atau hasil peretasan untuk melakukan penipuan. Keempat, adanya perubahan data akun secara tiba-tiba seperti penggantian nomor ponsel, email, atau PIN. Hal ini menjadi indikator kuat bahwa akun sudah diambil alih oleh pihak ketiga.

Transaksi mencurigakan ini kerap kali tidak langsung ditandai oleh sistem, khususnya jika masih berada di bawah batas transaksi wajar harian. Oleh karena itu, perlu adanya integrasi antara perilaku transaksi dan riwayat akun sebagai indikator tambahan. Sistem yang hanya mengandalkan nilai transaksi tidak akan cukup untuk mencegah fraud digital yang semakin canggih dan terstruktur. Penelitian ini memperkuat temuan sebelumnya bahwa identifikasi pola transaksi perlu dikombinasikan dengan aspek behavioristik untuk mendeteksi fraud secara lebih akurat dan cepat.

Respons Platform dan Celah Pengawasan

Pihak DANA, sebagai penyedia layanan e-wallet, telah menerapkan berbagai fitur keamanan untuk melindungi penggunanya, termasuk PIN transaksi, kode OTP, verifikasi dua langkah, hingga fitur pelaporan cepat untuk akun yang disusupi. Namun, meskipun fitur-fitur ini sudah diterapkan, kenyataannya masih banyak kasus fraud yang lolos dan menyebabkan kerugian finansial signifikan bagi pengguna. Hal ini menandakan bahwa sistem keamanan teknis saja tidak cukup tanpa disertai dengan kesadaran pengguna dan pengawasan yang adaptif terhadap pola baru penipuan. DANA menyatakan bahwa mereka tidak pernah meminta kode OTP ataupun informasi pribadi melalui telepon, WhatsApp, atau email. Namun, modus social engineering yang digunakan pelaku sering kali sangat meyakinkan, bahkan meniru logo, nada bicara, hingga format percakapan

layanan resmi. CNN Indonesia (2024) menyoroti bagaimana pelaku mampu menipu korban dengan teknik manipulatif yang menyerupai call center resmi DANA.

Di sisi lain, pengawasan dari regulator seperti OJK dan Bank Indonesia juga menghadapi tantangan dalam mengontrol ekosistem digital yang sangat cepat berkembang. Laporan tahunan OJK (2023) mencatat bahwa kasus pengaduan di sektor fintech meningkat hampir dua kali lipat dalam dua tahun terakhir. Bank Indonesia juga menyoroti perlunya sistem real-time monitoring terhadap transaksi digital yang mencurigakan. Sayangnya, hingga saat ini belum ada sistem terpadu antara penyedia platform dan otoritas yang memungkinkan deteksi dan penanganan cepat terhadap kasus fraud. Sering kali, pengguna hanya bergantung pada respons internal DANA dan membutuhkan waktu lama untuk penyelesaian, bahkan jika kerugian yang ditanggung cukup besar. Ini menunjukkan adanya celah koordinasi antara platform dan institusi pengawas yang perlu dibenahi.

Penelitian ini merekomendasikan agar sistem pengawasan transaksi mencurigakan di DANA tidak hanya bersifat reaktif tetapi juga proaktif, misalnya melalui penerapan machine learning berbasis data pola perilaku pengguna, tanpa melanggar privasi. Selain itu, edukasi berkelanjutan melalui media sosial, in-app notification, dan kerja sama dengan Kementerian Kominfo harus ditingkatkan secara sistematis.

Penelitian ini menemukan bahwa pola fraud digital pada aplikasi DANA memiliki karakteristik yang berulang dan dapat dikenali. Hal ini menunjukkan bahwa meskipun metode yang digunakan oleh pelaku terus berkembang, terdapat pola dasar yang dapat dijadikan indikator awal untuk mencegah dan mengantisipasi tindak kejahatan serupa. Misalnya, penggunaan akun baru tanpa riwayat transaksi atau perubahan data akun secara mendadak adalah tanda-tanda yang hampir selalu muncul dalam kasus penipuan.

Temuan ini konsisten dengan teori dan studi sebelumnya, yang menyatakan bahwa fraud digital tidak terjadi secara acak, tetapi mengikuti strategi tertentu yang bisa dikenali jika sistem keamanan dan pengawasan bekerja secara adaptif (Bank Indonesia, 2023; OJK, 2023). Maka dari itu, penyedia layanan seperti DANA perlu mengembangkan sistem pemantauan transaksi yang tidak hanya bergantung pada nilai transaksi, tetapi juga pada pola perilaku pengguna yang tidak lazim. Implikasi lain dari penelitian ini adalah pentingnya meningkatkan kesadaran pengguna sebagai lini pertahanan pertama terhadap penipuan. Banyak kasus terjadi bukan karena lemahnya sistem aplikasi, melainkan karena pengguna secara tidak sadar membocorkan informasi penting.

Oleh karena itu, kampanye literasi digital harus dilakukan secara masif dan berkelanjutan, dengan pendekatan yang sesuai dengan kebiasaan digital masyarakat Indonesia, misalnya melalui media sosial, konten video, dan aplikasi edukatif. Dengan mengidentifikasi indikator awal dari pola transaksi mencurigakan, hasil penelitian ini diharapkan dapat menjadi dasar dalam pengembangan sistem deteksi dini, serta memperkuat kerja sama antara platform, regulator, dan masyarakat dalam menciptakan ekosistem transaksi digital yang aman dan terpercaya.

Berdasarkan penelusuran data sekunder dari media daring nasional selama periode 2022–2024, ditemukan sejumlah kasus fraud digital pada aplikasi DANA yang menunjukkan pola dan modus berulang. Tabel berikut menyajikan dokumentasi dari beberapa kasus yang dilaporkan:

Tabel 1. Kasus Fraud Digital pada Aplikasi DANA (2022-2024)

Tahun	Jenis Fraud	Modus Operandi	Estimasi Kerugian	Sumber Berita
2023	Phishing	Korban klik link palsu mirip situs DANA dan mengisi data login & OTP	Rp12 juta	DetikFinance, 2023 https://finance.detik.com
2022	Social Engineering	Pelaku menyamar jadi CS DANA via WA, minta OTP untuk "verifikasi akun"	Tidak disebutkan	KompasTekno, 2022 https://tekno.kompas.com
2023	Penipuan Top-Up Palsu	Tautan promo palsu mengaku beri saldo gratis, korban tertipu isi data pribadi	Tidak disebutkan	CNN Indonesia, 2023 https://cnnindonesia.com
2024	Akun Duplikat & Refund	Akun palsu meminta refund via aplikasi dengan dokumen palsu	Rp2 juta	Katadata, 2024 https://katadata.co.id
2022	Rekayasa Login	Login akun dari lokasi berbeda, akun berpindah tangan tanpa izin pengguna	Rp3,5 juta	KompasTekno, 2022 https://tekno.kompas.com
2023	Penipuan Jual Beli	Pelaku meminta pembayaran DANA lalu menghilang, jual beli fiktif	Rp800 ribu	Liputan6.com, 2023 https://liputan6.com
2024	Spam OTP	Korban menerima OTP berulang, akun berhasil dibobol setelah pelaku masukkan OTP	Tidak disebutkan	DANA Help Center (resmi) https://dana.id/help-center
2023	Malware & Keylogger	Korban pasang APK palsu, data dicuri dan akun dibobol	Rp5 juta	KompasTekno, 2023 https://tekno.kompas.com

Sumber: Detik Finance, Kompas Tekno, CNN Indonesia, Katadata, Liputan6, DANA.

5. KESIMPULAN

Penelitian ini menemukan bahwa pola transaksi mencurigakan pada aplikasi DANA dapat diidentifikasi melalui indikator-indikator spesifik seperti transaksi berulang dalam waktu singkat, perubahan data akun secara tiba-tiba, aktivitas login dari perangkat asing, serta penggunaan akun baru tanpa histori transaksi yang wajar. Temuan ini menegaskan bahwa fraud digital pada dompet digital tidak semata terjadi karena kelemahan sistem teknologi, melainkan juga karena celah perilaku pengguna yang berhasil dimanfaatkan oleh pelaku. Oleh karena itu, pola tersebut dapat dimanfaatkan sebagai indikator awal dalam sistem peringatan dini untuk mendeteksi dan mencegah penipuan digital secara lebih akurat. Penelitian ini menunjukkan urgensi penguatan sistem keamanan berbasis analitik perilaku pengguna, serta pentingnya kolaborasi antara penyedia aplikasi, regulator, dan edukasi publik yang berkelanjutan. Gagasan selanjutnya dari penelitian ini adalah pengembangan kerangka deteksi fraud berbasis machine learning yang terintegrasi dengan data historis transaksi dan metadata akun, guna membentuk sistem pengawasan otomatis yang adaptif terhadap pola baru kejahatan digital.

DAFTAR PUSTAKA

CNN Indonesia. (2023, Februari 14). *Waspada penipuan e-wallet, begini cara pelaku curi saldo dompet digital*. https://www.cnnindonesia.com/ekonomi/20230214153415-78-914510/waspada-penipuan-e-wallet-begini-cara-pelaku-curi-saldo-dompet-digital

Dana Help Center. (2024). *Kenali dan hindari modus penipuan digital*. https://www.dana.id/help-center

Dewi, A.C., Erik Iman Heri Ujianto, & Rianto, R. (2024). Electronic Payment Threats and Security: A Systematic Literature Review. Jurnal Nasional Pendidikan Teknik Informatika: JANAPATI, 13(2), 301–315. https://doi.org/10.23887/janapati.v13i2.76635

Hasugian, L.S. & Suharjito, S. (2023). Fraud Detection for Online Interbank Transaction Using Deep Learning, Syntax Literate: Jurnal Ilmiah Indonesia, 8(6), 4263-4275. https://doi.org/10.36418/syntax-literate.v8i6.12627

Khaidir, K.N.L, Nasution, M. I. P. (2024)Analisis keamanan data terhadap penggunaan e-wallet sebagai alat transaksi digital untuk mencegah penipuan online. *Journal Sains Student Research*, 2(4), 108-116. https://doi.org/10.61722/jssr.v2i4.1955

Mohamed, I. S., & Shuhidan, S. M. (2023). Digital Payment in Mitigating Traditional Cash Payment Fraud Risk: A Systematic Literature Review. In J. Said, D. Daud, N. Erum, N. B. Zakaria, S. Zolkaflil, & N. Yahya (Eds.), Building a Sustainable Future: Fostering Synergy Between Technology, Business and Humanity, vol 131. European Proceedings of Social and Behavioural Sciences (pp. 723-738). *European Publisher*. https://doi.org/10.15405/epsbs.2023.11.61

Prasetya, M. E., dkk. (2021). Mitigating Fraud Risk in Cash-Based Payment System via E-Payment Implementation: Case of Indonesia. *Atlantis Press*, 558, 679-684. DOI:10.2991/assehr.k.210531.085