Jurnal Riset Sistem Informasi Dan Teknik Informatika (JURASIK)
Volume 11, Nomor 1, Februari 2026, pp 44-52
Terakreditasi Nomor 204/E/KPT/2022 | ISSN: 2527-5771/EISSN: 2549-7839
https://tunasbangsa.ac.id/ejurnal/index.php/jurasik

Kajian Literatur tentang Model Investigasi Forensik dalam Mendeteksi Penipuan Transaksi pada Sistem E-Commerce

Mikael Arvito Kurnia Adi[1]*, Susanto[2]
[1,2]Program Studi Sistem Informasi, Fakultas Teknologi Informasi dan Komunikasi, Universitas Semarang, Indonesia
Email: michaelarvito@gmail.com[1], susanto@usm.ac.id[2]

Abstract

This study aims to systematically review various digital forensic investigation models used to detect transaction fraud in e-commerce systems, based on relevant scientific literature. This study was conducted to analyze the approaches, stages, and techniques applied in each forensic investigation model, while also revealing their advantages and limitations in handling transaction fraud cases. Furthermore, this study aims to compare the effectiveness of these models in supporting the process of fraud detection, analysis, and proof in e-commerce environments. This study uses a systematic literature review methodology to collect, analyze, and integrate various studies related to forensic investigation models for identifying transaction fraud in e-commerce systems. We used keywords such as "digital forensic investigation models," "e-commerce fraud detection," "cyber forensics," and "transaction fraud" to search for articles in scientific databases including Google Scholar, IEEE Xplore, Scopus, ScienceDirect, and SpringerLink. The results demonstrate various ways to build a safer and more reliable e-commerce ecosystem for all stakeholders, requiring the integration of these three elements: early prevention in the transaction flow, ML-based detection for risk tagging, and digital forensics for evidence.

Keywords: *Forensic investigation model, transaction fraud, e-commerce, online*

Abstrak

Penelitian ini bertujuan untuk mengkaji secara sistematis berbagai model investigasi forensik digital yang digunakan dalam mendeteksi penipuan transaksi pada sistem e-commerce berdasarkan literatur ilmiah yang relevan. Kajian ini dilakukan untuk menganalisis pendekatan, tahapan, serta teknik yang diterapkan dalam setiap model investigasi forensik, sekaligus mengidentifikasi kelebihan dan keterbatasannya dalam menangani kasus penipuan transaksi. Selain itu, penelitian ini bertujuan membandingkan efektivitas model-model tersebut dalam mendukung proses deteksi, analisis, dan pembuktian penipuan pada lingkungan e-commerce. Penelitian ini menggunakan metodologi tinjauan pustaka sistematis untuk mengumpulkan, menganalisis, dan mengintegrasikan beragam penelitian terkait model investigasi forensik untuk mengidentifikasi penipuan transaksi dalam sistem e-commerce. Kami menggunakan kata kunci seperti "model investigasi forensik digital", "deteksi penipuan e-commerce", "forensik siber", dan "penipuan transaksi" untuk mencari artikel dalam basis data ilmiah termasuk Google Scholar, IEEE Xplore, Scopus, ScienceDirect, dan SpringerLink. Hasil penelitian menunjukan adanya berbagai cara membangun ekosistem e-commerce yang lebih aman dan andal bagi semua pemangku kepentingan membutuhkan integrasi ketiga elemen ini: pencegahan sejak dini dalam alur transaksi, deteksi berbasis ML untuk penandaan risiko, dan forensik digital untuk bukti.

Kata kunci*: Model investigasi forensik, penipuan transaksi, e-commerce, sistem online*

1. PENDAHULUAN

Teknologi informasi telah berkembang pesat dalam waktu singkat, dan hal ini menyebabkan pertumbuhan pesat e-commerce di banyak negara, termasuk Indonesia. Platform e-commerce menjadi pilihan utama bagi mereka yang ingin

membeli dan menjual barang karena mudah digunakan, cepat, dan fleksibel. Namun, ekspansi ini juga meningkatkan risiko kejahatan siber, termasuk penipuan transaksi. Penipuan dalam sistem e-commerce dapat mencakup pengubahan data transaksi, penggunaan identitas palsu, pencurian akun, dan bahkan memanfaatkan celah keamanan untuk melakukan tindakan ilegal yang merugikan pelanggan dan penyedia layanan. E-commerce, atau perdagangan elektronik, adalah proses pembelian dan penjualan barang atau jasa secara daring. Revolusi digital model bisnis tradisional memungkinkan konsumen untuk menjelajahi dan memperoleh barang secara daring dari kenyamanan rumah mereka[1]. Ada beberapa manfaat menggunakan platform e-commerce, seperti pembelian yang lebih cepat, biaya yang lebih rendah, lebih banyak pilihan bagi pelanggan, kemampuan untuk membandingkan produk dan harga, respons yang lebih cepat terhadap permintaan pembeli dan pasar, serta lebih banyak pilihan pembayaran. Meskipun ada beberapa hal baik tentang e-commerce, hal ini sangat penting bagi perekonomian[2] dan bahkan lebih penting lagi selama pandemi, ketika pemerintah telah mengimbau masyarakat untuk tinggal di rumah dan menerapkan karantina wilayah untuk mencegah orang bepergian[3]. Karena itu, semakin banyak orang yang membeli barang-barang seperti makanan dan obat-obatan yang mereka butuhkan setiap hari secara daring. Sebuah studi yang baru-baru ini dilakukan di Prancis menemukan bahwa pesanan daring meningkat sebesar 35,4% selama karantina wilayah tahun 2020 dibandingkan dengan bulan yang sama pada tahun 2019[4]. eMarketer mengatakan bahwa penjualan e-commerce di seluruh dunia naik 27,6% pada tahun 2020 dan diprediksi akan naik 14,3% pada tahun 2021, mencapai sekitar $5 triliun.

Jumlah uang yang besar ini menarik para penipu, yang dapat merugikan banyak orang. Juniper Research2 baru-baru ini melakukan studi yang menyatakan bahwa penipuan akan meningkat dari $17,5 miliar pada tahun 2020 menjadi $20 miliar pada tahun 2021. Angka-angka ini menunjukkan betapa pentingnya bagi platform e-commerce dan perbankan untuk memiliki mekanisme guna menemukan dan menghentikan penipuan agar terhindar dari kerugian. Beberapa makalah penelitian saat ini sedang mengkaji beragam teknik untuk mengurangi penipuan dalam e-commerce[5]; [6]; [7]; [8]

Sistem deteksi penipuan seringkali bergantung pada analisis data konsumen, yang mencakup navigasi internet, aktivitas historis, dan pola perilaku. Metode-metode ini menggunakan rekayasa data dan penambangan data pada peristiwa mentah dari sistem yang sedang berjalan, seperti berkas log[7]. Strategi dalam bidang pembelajaran mesin (ML) menggunakan ekstraksi data dan analisis pola dalam teknik klasifikasi yang dirancang untuk mengantisipasi perilaku penipuan. Algoritma klasifikasi adalah bagian dari pembelajaran mesin (ML) yang mencoba menemukan kelompok observasi tertentu dengan mengamati set data pelatihan. Beberapa metode umum untuk mengklasifikasikan objek guna menemukan dan menghentikan penipuan adalah Hutan Acak[6], Regresi Logistik (Baesens dkk., 2021), dan Jaringan Syaraf Tiruan[8], Untuk mempelajari cara kerja penipuan, algoritma ini diberikan contoh kasus penipuan di masa lalu. Ketika mendapatkan informasi baru, seperti pelanggan baru di situs web, mereka dapat

mengelompokkan pelanggan baru tersebut berdasarkan kemiripannya dengan pelanggan sebelumnya. Ada berbagai cara untuk melakukan ini, tetapi membangun sistem yang dapat menemukan dan menghentikan penipuan membutuhkan analisis data yang cermat dan akses data yang lebih cepat. Algoritma dapat memproses log data dan mendeteksi risiko penipuan lebih awal dalam proses transaksi daring ketika data tersedia dengan cepat.

Deteksi dan pencegahan penipuan mungkin tampak serupa, meskipun keduanya memiliki pengertian yang berbeda[9]. Pencegahan penipuan berarti mencari tahu tentang penipuan dan mencegahnya terjadi sejak awal. Di sisi lain, deteksi penipuan adalah ketika Anda mengetahui penipuan setelah penipuan terjadi. Dengan kata lain, setelah penipuan terjadi, penipuan tersebut tidak dapat dihentikan; satu-satunya cara untuk mengurangi dampaknya adalah dengan menemukannya. Gambar 1 menunjukkan cara kerja transaksi e-commerce daring, yang menunjukkan di mana pencegahan dan deteksi penipuan dapat digunakan. Secara khusus, pencegahan dapat dilakukan pada platform e-commerce dan keuangan sebelum bank memberikan persetujuannya. Setelah otorisasi perbankan diberikan, menghentikannya tidak lagi memungkinkan; satu-satunya metode untuk menemukannya adalah melalui deteksi.

Dalam situasi ini, forensik digital telah menjadi cara penting untuk menemukan, mempelajari, dan menyelidiki jejak digital yang dapat menunjukkan tanda-tanda penipuan. Model investigasi forensik telah diciptakan untuk membuat langkah-langkah pengumpulan, analisis, interpretasi, dan pelaporan bukti lebih terorganisir. Beberapa model yang paling populer adalah DFRWS, NIST, Abstract Digital Forensics Model (ADFM), dan lainnya. Namun, kita masih perlu mempelajari lebih lanjut tentang seberapa baik model-model ini bekerja di dunia e-commerce. Kerumitan transaksi digital, partisipasi berbagai pemangku kepentingan, dan sifat risiko keamanan siber yang terus berkembang menjadikan pemilihan model forensik yang tepat sebagai komponen penting dari proses investigasip[10]. Oleh karena itu, analisis literatur ini bertujuan untuk mengidentifikasi, menganalisis, dan menilai metode investigasi forensik yang digunakan untuk mendeteksi penipuan transaksi dalam sistem e-commerce. Hasilnya diharapkan dapat memberikan gambaran lengkap tentang model-model terpenting, kelebihan dan kekurangannya, serta saran bagi para profesional keamanan siber tentang cara menggunakan pendekatan investigasi yang efektif[11].

Menurut analisis terbaru oleh Juniper Research, kerugian terkait pembayaran online di platform e-commerce meningkat dengan laju yang mengejutkan sebesar 18 persen setiap tahunnya[12]. Hal ini menyoroti pentingnya mempelajari bidang ini untuk menginformasikan strategi deteksi atau pencegahan penipuan guna memperlambat tren peningkatan tersebut. Seringkali, strategi saat ini tidak mampu mengimbangi para penipu, yang terus beradaptasi dan mengubah metode mereka untuk mengeksploitasi platform[13]. Terlebih lagi, upaya penelitian dan pengembangan yang rendah dipicu oleh kurangnya data praktis dan kebutuhan bisnis untuk melindungi kerentanan platform mereka semakin memperburuk masalah ini. Misalnya, tidak masuk akal untuk menjelaskan metode

deteksi atau pencegahan penipuan secara terbuka karena hal itu akan mempersenjatai para penipu dengan pengetahuan yang mereka butuhkan untuk menghindari deteksi[14].

Dalam literatur, penanganan penipuan dalam bentuk apa pun dapat dilakukan dalam dua bentuk: (1) Pencegahan, yang mengacu pada langkah-langkah yang diambil untuk mencegah terjadinya tindakan tersebut sejak awal. Ini termasuk desain yang rumit, nomor identitas pribadi, keamanan internet untuk interaksi online dengan platform digital, dan kata sandi serta mekanisme otentikasi untuk komputer dan perangkat seluler[15]. Jenis penipuan ini paling umum terjadi di platform e-commerce dan telah ada sejak awal peralihan bisnis dari lokasi fisik ke online. Dengan menggunakan informasi keuangan atau pembayaran yang diperoleh melalui eksploitasi kerentanan yang disebutkan di atas, penipu sering melakukan transaksi yang tidak sah[2].

Adanya latar belakang tersebut menjadikan penulis memutuskan untuk melakukan jurnal dengan judul Kajian Literatur tentang Model Investigasi Forensik dalam Mendeteksi Penipuan Transaksi pada Sistem E-Commerce. Penelitian ini bertujuan untuk mengkaji secara sistematis berbagai model investigasi forensik digital yang digunakan dalam mendeteksi penipuan transaksi pada sistem e-commerce berdasarkan literatur ilmiah yang relevan. Kajian ini dilakukan untuk menganalisis pendekatan, tahapan, serta teknik yang diterapkan dalam setiap model investigasi forensik, sekaligus mengidentifikasi kelebihan dan keterbatasannya dalam menangani kasus penipuan transaksi. Selain itu, penelitian ini bertujuan membandingkan efektivitas model-model tersebut dalam mendukung proses deteksi, analisis, dan pembuktian penipuan pada lingkungan e-commerce. Hasil kajian diharapkan dapat memberikan gambaran komprehensif mengenai karakteristik model investigasi forensik yang ada serta menjadi dasar rekomendasi bagi peneliti dan praktisi dalam memilih atau mengembangkan model investigasi forensik yang sesuai untuk diterapkan pada sistem e-commerce.

2. METODOLOGI PENELITIAN

Penelitian ini menggunakan metodologi tinjauan pustaka sistematis untuk mengumpulkan, menganalisis, dan mengintegrasikan beragam penelitian terkait model investigasi forensik untuk mengidentifikasi penipuan transaksi dalam sistem e-commerce. Kami menggunakan kata kunci seperti "model investigasi forensik digital", "deteksi penipuan e-commerce", "forensik siber", dan "penipuan transaksi" untuk mencari artikel dalam basis data ilmiah termasuk Google Scholar, IEEE Xplore, Scopus, ScienceDirect, dan SpringerLink. Literatur yang dipilih terdiri dari publikasi dalam bahasa Indonesia dan Inggris, yang diterbitkan dari tahun 2014 hingga 2024, dengan fokus pada model forensik digital dan deteksi penipuan dalam transaksi e-commerce, dengan mengecualikan sumber non-ilmiah atau penelitian yang tidak relevan.

Setelah literatur dikumpulkan, analisis dilakukan untuk menentukan model investigasi forensik yang digunakan, tahapan proses investigasi, dan relevansinya dengan penipuan transaksi. Analisis ini bersifat deskriptif dan komparatif untuk menilai kekuatan, keterbatasan, dan efektivitas masing-masing model. Selain itu,

hasil analisis dikonsolidasikan untuk memperoleh temuan penting mengenai model optimal yang digunakan dalam investigasi penipuan e-commerce dan kendala yang dihadapi dalam pelaksanaannya, sehingga memungkinkan penelitian ini menawarkan rekomendasi yang relevan untuk kemajuan metodologi forensik digital di masa mendatang.

3. HASIL DAN PEMBAHASAN

Seiring dengan meningkatnya e-commerce di Indonesia, penipuan transaksi online menjadi semakin umum. Para penjahat memanfaatkan kemajuan teknologi untuk menipu pelanggan dengan memanipulasi data dan menggunakan identitas palsu. Literasi digital yang rendah dan kelemahan dalam sistem keamanan platform seringkali dikaitkan dengan fenomena ini. Kesadaran pengguna yang rendah, pelanggaran data, daya tarik hadiah palsu, tingginya angka pengangguran, dan peraturan pemerintah yang longgar merupakan beberapa faktor penyebabnya[16].

Perkembangan teknologi informasi mengubah pola transaksi masyarakat menjadi digital, tetapi membuka celah bagi tindak pidana penipuan yang masif di platform e-commerce. Faktor pendorong mencakup kebocoran data seperti kasus Tokopedia, minimnya edukasi konsumen, dan motif ekonomi pelaku akibat kemiskinan. Kendala penegakan hukum meliputi sulitnya pembuktian dan pelacakan pelaku lintas wilayah, meski diatur dalam KUHP dan UU ITE.

Tabel 1. Jenis bentuk penipuan

Bentuk Penipuan	**Deskripsi Modus Operandi**
Phishing	Pengiriman link palsu via email untuk mencuri data pribadi dengan iming-iming hadiah.
Pharming	Pengalihan situs resmi ke palsu agar korban masukkan data tanpa curiga.
Pretexting	Meminta data pribadi dengan dalih keperluan akses e-commerce.
Quid Pro Quo	Janji hadiah berupa uang/barang dengan syarat berikan data pribadi terlebih dahulu.
Penipuan Jual Beli	Tawarkan barang murah tapi tidak kirim setelah pembayaran, via media sosial/e-commerce.
Kontak Langsung	Telepon/WhatsApp berpura-pura dari e-commerce untuk minta nomor rekening.

a. Urgensi dan Dampak Kerugian

Penipuan transaksi e-commerce menargetkan nilai transaksi besar mencapai ratusan triliun rupiah, memicu kerugian masif hingga Rp4,6 triliun pada 2025 menurut data OJK, sehingga platform dan perbankan wajib terapkan mekanisme pengendalian ketat (Jalin, 2025). Transaksi bernilai tinggi menarik sindikat fraud terorganisir, dengan 42 ribu laporan penipuan yang menunjukkan risiko sistemik terhadap kepercayaan konsumen dan stabilitas ekonomi digital. Platform seperti marketplace dan perbankan perlu deteksi AI real-time, monitoring anomali, serta

audit berkala untuk cegah eskalasi. Tanpa ini, fraud berkembang pesat seiring digitalisasi, merusak loyalitas pelanggan dan operasi bisnis.

Penipuan transaksi e-commerce menimbulkan dampak utama berupa kerugian finansial konsumen yang mencapai miliaran rupiah per kasus melalui modus seperti phishing dan akun palsu, di mana korban kehilangan dana secara permanen akibat transfer ke rekening pelaku[17]. Platform mengalami beban operasional tinggi berupa biaya investigasi forensik digital, pengembalian dana klaim palsu, serta penurunan volume transaksi hingga 20-30% akibat hilangnya kepercayaan pengguna[18]. Secara reputasi, kebocoran data memicu boikot massal dan penurunan loyalitas pelanggan, sementara dampak sistemik mengganggu stabilitas perbankan nasional melalui fraud lintas wilayah yang memerlukan intervensi OJK seperti pemblokiran rekening ilegal.

b. Titik Intervensi pencehagan vs deteksi dalam jalur transaksi

Pra-otorisasi adalah fokus utama pencegahan, yang mencakup CAPTCHA anti-bot, penyaringan AI untuk pola transaksi mencurigakan guna memblokir transaksi secara otomatis sebelum konfirmasi pembayaran, dan validasi identitas penjual melalui kartu identitas digital. Verifikasi data pembeli-penjual oleh platform merupakan ambang batas kritis; karena bank belum menyelesaikan transfer, intervensi di sini menghentikan 70–80% penipuan. Dengan mencegah akses pelaku kejahatan sejak dini, mekanisme proaktif ini menurunkan kerugian[19].

Deteksi aktif setelah otorisasi bank, di mana transaksi sudah final dan tidak bisa dibatalkan secara instan, sehingga bergantung pada forensik digital untuk telusuri jejak seperti IP palsu atau rekening mule. Pasca-otorisasi, platform hanya bisa refund parsial via chargeback, tapi sering gagal jika dana dicuci. Urgensi prioritas pencegahan jelas karena deteksi reaktif hanya mitigasi kerugian, bukan cegah sepenuhnya[18].

c. Deteksi dini berbasis data dan machine learning

Dalam praktiknya, platform mengumpulkan berbagai fitur seperti frekuensi transaksi, nominal, perangkat yang digunakan, lokasi, pola login, hingga riwayat klaim sengketa untuk membedakan pola wajar dan pola menyimpang. Berdasarkan data tersebut, model machine learning mempelajari karakteristik transaksi yang sebelumnya terbukti fraud, lalu menggunakan pembelajaran itu untuk menandai transaksi baru yang memiliki kemiripan pola. Semakin kaya dan bersih data historis yang dianalisis, semakin akurat kemampuan sistem dalam mengantisipasi penipuan.

1. Random Forest: menggabungkan banyak pohon keputusan untuk “voting” apakah suatu transaksi termasuk aman atau mencurigakan, sehingga lebih tahan terhadap noise dan variasi data.
2. Regresi Logistik: memodelkan probabilitas sebuah transaksi menjadi fraud, sehingga hasilnya berupa skor risiko yang dapat dipakai sebagai dasar threshold (misalnya: di atas skor tertentu transaksi wajib diverifikasi).

3. Jaringan Syaraf Tiruan (Neural Network): memanfaatkan banyak lapisan pemrosesan untuk menangkap pola non-linear dan kompleks, misalnya kombinasi perilaku login, device fingerprint, dan pola waktu transaksi yang sulit ditangkap metode klasik.

Agar deteksi dini benar-benar efektif, sistem membutuhkan tiga hal utama: kualitas data yang tinggi, proses analisis yang cermat, dan akses data yang sangat cepat. Data harus dibersihkan, di-label dengan benar (fraud vs non-fraud), dan diperbarui secara berkala karena modus penipuan terus berkembang; tanpa ini, model akan cepat usang dan akurasinya turun. Selain itu, infrastruktur harus memungkinkan pemrosesan hampir real-time, sehingga skor risiko dapat dihitung dalam hitungan milidetik dan keputusan (blokir, tunda, atau izinkan) bisa diambil sebelum transaksi berjalan terlalu jauh dalam alur system[20].

d. Forensik digitan dan model investigasi untuk membuktikan

Agar jejak digital penipuan seperti log transaksi, riwayat login, metadata perangkat, pesan dalam aplikasi, dan jejak pada dompet digital dan platform e-commerce dapat digunakan sebagai bukti yang sah di pengadilan, forensik digital digunakan untuk menemukan, mengamankan, dan menganalisis jejak-jejak ini secara terorganisir. Empat tahapan utama model forensik digital umumnya adalah pengumpulan, analisis, interpretasi, dan pelaporan. Tahap pengumpulan berfokus pada pencarian sumber bukti dan akuisisi data sambil menjaga integritas, tahap analisis dan interpretasi mengekstrak dan menghubungkan artefak yang relevan ke dalam garis waktu peristiwa, dan tahap pelaporan mengumpulkan temuan teknis dalam format yang dapat dijelaskan di pengadilan. DFRWS, yang menekankan alur identifikasi, pelestarian, pengumpulan, pemeriksaan, analisis, dan presentasi; kerangka kerja NIST, yang menekankan standardisasi prosedur dan validasi alat; dan berbagai model forensik adaptif, seperti ADFM, yang lebih iteratif dan memungkinkan penyelidik untuk kembali ke tahap sebelumnya ketika artefak baru ditemukan, adalah beberapa model yang sering dibandingkan dalam literatur. Model-model ini lebih sesuai dengan sifat dinamis dari insiden siber kontemporer[21].

Karena alur transaksi e-commerce seringkali kompleks dan melibatkan banyak pemangku kepentingan, termasuk pasar online, gerbang pembayaran, bank, dompet digital, dan regulator, pemilihan model investigasi sangat penting. Karena kemajuan teknik penipuan, penggunaan VPN, akun perantara, dan metode pengaburan lainnya, risiko siber juga berubah dengan cepat. Akibatnya, perusahaan sering menggunakan model seperti kerangka kerja NIST ketika dokumentasi ketat dan kepatuhan audit diperlukan, atau DFRWS untuk pelacakan menyeluruh alur transaksi dan aktivitas aplikasi. Untuk membuat seluruh proses investigasi penipuan e-commerce menjadi metodis dan fleksibel dalam menghadapi serangan siber yang dinamis, model yang lebih adaptif digunakan ketika investigasi perlu dilakukan dengan cepat dan responsive[22].

Deteksi penipuan berbasis machine learning berperan sebagai lapis awal untuk menandai risiko secara cepat, melakukan triase transaksi, dan membantu platform serta bank memutuskan apakah suatu transaksi perlu diblokir, ditunda,

atau diverifikasi lebih lanjut. Sistem ini fokus pada pemrosesan data volume besar secara hampir real-time, menghasilkan skor risiko atau label fraud yang sangat berguna untuk pencegahan dan respons dini di sepanjang alur transaksi[23]. Namun, ketika penipuan sudah terjadi atau dugaan fraud perlu dibuktikan secara hukum, forensik digital menjadi krusial untuk merekonstruksi kejadian secara rinci dan menguatkan pembuktian. Forensik digital menelusuri jejak teknis seperti log, artefak perangkat, dan alur dana, lalu menyusunnya dalam bentuk kronologi yang dapat dipertanggungjawabkan di pengadilan, sehingga melengkapi peran deteksi berbasis ML: ML untuk penandaan risiko dan triase cepat, forensik digital untuk pendalaman kasus dan kekuatan bukti formal[21].

4. SIMPULAN

Dengan memproses log dan pola perilaku dalam skala besar serta menghasilkan skor atau label risiko untuk mendukung pengambilan keputusan secara real-time, deteksi dini berbasis data dan pembelajaran mesin bertindak sebagai lapisan penyaringan cepat untuk mengidentifikasi transaksi berisiko. Sementara itu, setelah penipuan terjadi, forensik digital dan model investigasi terstruktur seperti DFRWS, NIST, atau model adaptif sangat penting karena dapat merekonstruksi peristiwa, melacak jejak digital secara metodis, dan memberikan bukti yang meyakinkan secara hukum. Membangun ekosistem e-commerce yang lebih aman dan andal bagi semua pemangku kepentingan membutuhkan integrasi ketiga elemen ini: pencegahan sejak dini dalam alur transaksi, deteksi berbasis ML untuk penandaan risiko, dan forensik digital untuk bukti.

DAFTAR PUSTAKA

[1] C. A. Cholik, "Perkembangan teknologi informasi komunikasi/ICT dalam berbagai bidang," *J. Fak. Tek. UNISA Kuningan*, vol. 2, no. 2, hal. 39–46, 2021, doi: https://doi.org/10.35957/mdp-sc.v4i1.11297.

[2] S. Suwandi dan A. Wahyu, "Perancangan dan Implementasi Sistem Informasi Kepegawaian pada PT Anugerah Sukses Kharisma," *J. Indones. Sos. Teknol.*, vol. 4, no. 3, hal. 290–298, 2023, doi: 10.59141/jist.v4i3.591.

[3] A. Ardi, A. Fenty, dan L. Lathifah, "Sistem Informasi Pengajuan Cuti Pegawai Menggunakan Metode Pengujian Iso 25010 (Study Kasus : Pt Mutiara Ferindo Internusa)," *J. Inform. dan Rekayasa Perangkat Lunak*, vol. 4, no. 3, hal. 326–334, Sep 2023, doi: 10.33365/jatika.v4i3.3721.

[4] A. Gunawan *et al.*, "Pengaruh Reward dan Punishment Terhadap Kinerja Karyawan PT. Bintang Toedjoe Cikarang," *J. Manaj.*, vol. 11, no. 1, hal. 1–9, 2023, doi: https://doi.org/10.36546/jm.v11i1.862.

[5] S. Suhari, A. Faqih, dan F. M. Basysyar, "Sistem Informasi Kepegawaian Mengunakan Metode Agile Development di CV. Angkasa Raya," *J. Teknol. dan Inf.*, vol. 12, no. 1, hal. 30–45, Mar 2022, doi: 10.34010/jati.v12i1.6622.

[6] C. F. Irwanto dan D. P. Kesuma, "Rancang Bangun Sistem Informasi Kepegawaian pada PT Ginting Jaya Energi," *J. Teknol. Sist. Inf.*, vol. 4, no. 2, hal. 406–420, 2023, doi: https://doi.org/10.35957/jtsi.v4i2.6012.

[7] A. Dumyati dan A. Farisi, "Penerapan Metode RUP dalam Pengembangan Sistem Kepegawaian di Perusahaan Media Massa Palembang," in *MDP Student Conference*, 2025, hal. 547–555. doi: https://doi.org/10.35957/mdp-sc.v4i1.11297.

[8] Rian Aji Febriansyah dan Lisa Amelia Franse, "Perancangan Sistem Informasi Kepegawaian Menggunakan Metode RUP pada PT BCD," *J. Multimed. dan Teknol. Inf.*, vol. 7, no. 01, hal. 185–196, Apr 2025, doi: 10.54209/jatilima.v7i01.1223.

[9] N. Anderiansyah dan T. Elizabeth, "Sistem Informasi Kepegawaian Berbasis Website Pada PT. Cahaya Sanubari Sakti Dengan Metode RUP," *J. Rekayasa Sist. Inf. dan Teknol.*, vol. 2, no. 3, hal. 1007–1018, 2025, doi: https://doi.org/10.70248/jrsit.v2i3.1850.

[10] D. Sulistiawati, A. Rachmayanti, P. S. Rahayu, P. Anggraeni, dan Q. Hidayat, "Implementasi sistem informasi manajemen pegawai," *Refresh Manjemen Pendidik. Islam*, vol. 2, no. 1, hal. 1–7, 2024, doi: https://doi.org/10.59064/rmpi.v2i1.36.

[11] M. Prabowo, *Metodologi pengembangan sistem informasi*. LP2M Press IAIN Salatiga, 2020.

[12] H. Meileni, S. Oktapriandi, dan D. Apriyanti, "Analisis PIECES Pada Aplikasi WebGIS Pemetaan Ekonomi Kreatif (Ekraf)," *Teknika*, vol. 9, no. 2, hal. 138–145, 2020, doi: 10.34148/teknika.v9i2.293.

[13] T. A. I. Alvayet dan E. V. Barrichelo, "Perancangan Sistem Informasi Pengolahan Data Laporan Pajak Bulanan Berbasis Web Pada Depo Unilever Padang," *J. Sains Inform. Terap.*, vol. 2, no. 3, hal. 108–113, 2023, doi: https://doi.org/10.62357/jsit.v2i3.202.

[14] T. Saputra, A. D. Angga.S, S. M. Maulidin, F. Alfaridz, dan M. R. Fadilah, "Perancangan Sistem Aplikasi Pembelian di Tiktok Shop dengan Menggunakan Software 'Star Uml' Use Case Diagram" Activity Diagram" Class Diagran" Normalisasi File" Ms. Access," *JEBI J. Ekon. dan Bisnis*, vol. 2, no. 7, hal. 802–8011, 2024, [Daring]. Tersedia pada: https://j-economics.my.id/index.php/home/article/view/195

[15] H. Amirullah dan A. Eviyanti, "Android File Security Application with AES Encryption and Fingerprint Authentication: Aplikasi Keamanan Berkas dengan Enkripsi AES dan Biometrik Sidik Jari Berbasis Android," *SMATIKA STIKI Inform. J.*, vol. 14, no. 1, hal. 23–32, Jan 2024, doi: 10.21070/ups.3769.

[16] B. C. Utomo dan A. A. Rahman, "Analisis Kesadaran Keamanan Data Pribadi pada Pengguna E-Wallet DANA," *JRST (Jurnal Ris. Sains dan Teknol.*, vol. 8, no. 2, hal. 155–166, Okt 2024, doi: 10.30595/jrst.v8i2.21162.

[17] A. A. Djunarjanto, A. Purwati, dan L. Marina, "Transformasi Modus Kejahatan Ekonomi Transnasional di Era Digital: Analisis Hukum Pidana dan Teknik Forensik Siber," *SENTRI J. Ris. Ilm.*, vol. 4, no. 8, hal. 1346–1360, Agu 2025, doi: 10.55681/sentri.v4i8.4448.

[18] J. A. R. Simanungkalit, R. Hertadi, dan A. ul Hosnah, "Analisis Tindak Pidana Penipuan Online dalam Konteks Hukum Pidana Cara Menanggulangi dan Pencegahannya," *Akad. J. Mhs. Humanis*, vol. 4, no. 2, hal. 281–294, Mei 2024, doi: 10.37481/jmh.v4i2.754.

[19] A. A. Q. A. Dalimunthe dan M. Azhari, "Analisis Forensik Digital Terhadap Perdagangan Data Pribadi Di Dark Web Menggunakan Osint & Threat Intelligence," *J. Komput. Teknol. Inf. Sist. Inf.*, vol. 4, no. 1, hal. 254–268, Jun 2025, doi: 10.62712/juktisi.v4i1.400.

[20] S. Utami, C. Carudin, dan A. Ridha, "Analisis Live Forensic pada Whatsapp Web untuk Pembuktian Kasus Penipuan Transaksi Elektronik," *Cyber Secur. dan Forensik Digit.*, vol. 4, no. 1, hal. 24–32, Jun 2021, doi: 10.14421/csecurity.2021.4.1.2416.