Seminar Nasional
FMI 2026 Surabaya
Prosiding

FMI Jawa Timur XVIII 2026

e-ISSN: 3026-4499
Vol. 4
20-22 Oktober 2026

Evaluasi Kritis Efektivitas Fitur Keamanan E-Commerce dalam Mencegah Pencurian Identitas Konsumen

Dyah Aldillah Armin, Auliah Alwi & Muhammad Ghifari

Universitas Muslim Indonesia, Makassar

Email: dyah.aldillah@umi.ac.id

Abstract

The growth of e-commerce has increased transaction convenience while also expanding the use of consumers' personal data, making identity theft and account takeover increasingly critical concerns. This study aims to critically evaluate the effectiveness of various e-commerce security features in preventing consumer identity theft. This study employed a Systematic Literature Review (SLR) approach and analyzed 10 scholarly articles published between 2021 and 2025. The literature was analyzed thematically, focusing on identity authentication and verification, behavior- and access-environment-based detection, the use of machine learning for fraud detection, and the interplay among security, privacy, risk, and consumer trust. The findings indicate that authentication methods, such as One-Time Passwords (OTPs) and phone number verification, have limitations when the underlying credentials or verification channels are compromised. Research suggests that leveraging device characteristics, IP addresses, transaction patterns, and user behavior can help identify activities that deviate from an account owner's established norms. Machine learning also shows promise in identifying fraud patterns, though its performance depends on data characteristics, specific features, the chosen model, and the application context. Furthermore, technical security measures must be integrated with robust privacy protection and consumer risk management. The synthesis concludes that safeguarding consumer identity cannot rely on a single security feature; rather, it requires a multi-layered security approach that combines authentication, behavioral analysis, fraud detection, and comprehensive data protection and management mechanisms.

Keywords e-commerce, identity theft, digital security, authentication, fraud detection.

1. Pendahuluan

Saat ini, *e-commerce* telah menjadi bagian utama dari aktivitas konsumsi digital masyarakat. Platform ini memudahkan konsumen untuk mencari produk, melakukan pembayaran, menyimpan alamat pengiriman, dan berkomunikasi dengan penjual tanpa harus bertemu langsung. Perubahan ini membuat pertukaran data pribadi menjadi syarat penting agar transaksi berjalan lancar. Namun, semakin banyak data yang dikumpulkan dan diproses oleh platform, semakin besar juga bahayanya jika data tersebut jatuh ke tangan pihak yang tidak bertanggung jawab. Penelitian terkait privasi *ecommerce* menunjukkan bahwa pengumpulan, penyimpanan, dan penggunaan data pribadi telah meningkatkan kekhawatiran privasi di kalangan pengguna (Maseeh et al., 2021).

Dalam *e-commerce*, pencurian identitas (*identity theft*) tidak hanya berarti pencurian nomor kartu kredit atau kerugian uang. Identitas digital konsumen kini terdiri dari gabungan alamat email, kata sandi, nomor telepon, riwayat transaksi, hingga kebiasaan pengguna, yang bisa

FMI Jawa Timur XVIII 2026
e-ISSN: 3026-4499
Vol. 4
20-22 Oktober 2026

dimanfaatkan pelaku untuk menyamar sebagai pemilik akun. Ketika data ini bocor melalui peretasan (*data breach*), *phishing*, rekayasa sosial, atau *malware*, pelaku kejahatan bisa menggunakan identitas korban untuk melakukan transaksi palsu, mengambil alih akun, atau menyambungkannya dengan kejahatan siber lainnya. Liu et al. (2022) membahas berbagai ancaman keamanan siber yang dapat menyebabkan kompromi data dan identitas dalam lingkungan *e-commerce*.

Masalah utamanya adalah ketersediaan fitur keamanan di sebuah platform tidak selalu menjamin pencurian identitas berhasil dicegah. Evaluasi terhadap sistem pencegahan penipuan (*fraud*) pada *e-commerce* menunjukkan bahwa sebuah perusahaan mungkin memiliki aturan perlindungan informasi yang ketat di atas kertas, tetapi belum tentu punya langkah taktis untuk menangkal pencurian identitas secara menyeluruh. Hal ini penting karena menunjukkan adanya perbedaan nyata antara sekadar memagari sistem secara teknis, dengan kemampuan perusahaan dalam mendeteksi penyalahgunaan akun setelah data pengguna telanjur berpindah tangan.

Bagi konsumen, kebocoran data juga membawa dampak buruk yang lebih luas dari sekadar kerugian teknis. Strzelecki & Rizun (2022), dalam penelitiannya terhadap konsumen yang mengalami kebocoran data di sebuah toko *online*, menemukan adanya penurunan kepercayaan yang drastis terhadap toko tersebut. Selain itu, Park et al. (2024) juga menemukan efek menular (*spillover effect*), di mana rasa khawatir konsumen terhadap risiko privasi ikut meningkat pada perusahaan lain, meskipun insiden kebocoran hanya terjadi pada satu toko. Ini menunjukkan bahwa efektivitas fitur keamanan tidak hanya dinilai dari kemampuannya menahan serangan peretas, tetapi juga dari kemampuannya merawat rasa aman konsumen.

Untuk menghadapi ancaman yang terus berkembang ini, fitur keamanan *e-commerce* juga ikut beradaptasi. Selain mengandalkan kata sandi dan enkripsi, platform saat ini juga menerapkan *MultiFactor Authentication* (MFA), sensor biometrik, pendeteksi aktivitas mencurigakan, hingga tokenisasi pembayaran. Fokus pengamanan juga mulai bergeser pada metode yang lebih tangguh terhadap *phishing*. Berdasarkan panduan NIST (2025), pengelolaan identitas digital kini secara tegas membedakan antara sistem keamanan yang kebal *phishing* dengan sistem lama yang masih rentan diretas melalui pencurian kode verifikasi (NIST, 2025).

Berdasarkan kondisi tersebut, diperlukan sebuah kajian yang tidak hanya sekadar mendata keberadaan fitur-fitur keamanan tersebut, tetapi juga menilai seberapa jauh efektivitasnya dalam mencegah pencurian identitas di dunia nyata. Oleh karena itu, artikel tinjauan literatur ini disusun untuk menelusuri fitur keamanan apa saja yang paling sering dikaji dalam literatur *e-commerce* selama lima tahun terakhir. Selanjutnya, evaluasi akan diarahkan untuk melihat bagaimana bukti-bukti penelitian yang ada menggambarkan keampuhan fitur-fitur ini dalam menekan risiko pengambilalihan akun. Selain itu, kajian ini juga akan mengidentifikasi kelemahan-kelemahan yang membuat sebuah fitur keamanan menjadi tidak maksimal jika hanya dibiarkan bekerja sendirian. Tujuan akhirnya adalah memberikan pemahaman yang utuh mengenai urgensi penerapan sistem keamanan yang berlapis dalam ekosistem *e-commerce*.

FMI Jawa Timur XVIII 2026
e-ISSN: 3026-4499
Vol. 4
20-22 Oktober 2026

2. Tinjauan Literatur

Fenomena kejahatan di dunia maya, termasuk pencurian identitas, pada dasarnya dapat dijelaskan melalui kacamata Teori Aktivitas Rutin (*Routine Activity Theory*). Teori ini mengemukakan bahwa sebuah kejahatan akan terjadi jika tiga kondisi ini bertemu: adanya pelaku yang termotivasi, ketersediaan target yang menarik (seperti data pribadi dan finansial konsumen), serta lemahnya pengawasan atau sistem keamanan. Dalam lingkungan *e-commerce*, pencurian identitas adalah bentuk penyalahgunaan data pribadi ini oleh pihak yang tidak berhak. Bentuknya bisa bermacam-macam, mulai dari pengambilalihan akun, pemakaian kata sandi yang bocor, hingga memakai identitas orang lain untuk membuat transaksi palsu. Soomro et al. (2021) menjelaskan bahwa penipuan identitas

(*identity fraud*) harus dibedakan dari keamanan informasi pada umumnya. Mencegah pencurian identitas membutuhkan aturan dan proses khusus untuk menangani penyalahgunaan akun meskipun pelaku sudah berhasil melewati halaman *login*.

Untuk menutup celah pengawasan tersebut, perancangan fitur keamanan *e-commerce* selalu berakar pada satu konsep utama, yaitu Segitiga Keamanan Informasi atau *CIA Triad* (Kerahasiaan, Keutuhan, dan Ketersediaan). Keamanan platform mencakup serangkaian langkah teknis untuk memastikan bahwa data pengguna tetap rahasia (*Confidentiality*), tidak diubah oleh pihak luar (*Integrity*), dan sistemnya selalu bisa diakses saat dibutuhkan (*Availability*). Di sisi lain, konsep keamanan ini sangat erat kaitannya dengan privasi, yang lebih fokus pada hak pengguna untuk tahu bagaimana data mereka dikumpulkan dan dibagikan. Maseeh et al. (2021) menunjukkan bahwa rasa khawatir pengguna *e-commerce* sering kali muncul akibat proses pembagian data pribadi yang kurang transparan. Oleh karena itu, penjagaan teknis (*CIA Triad*) dan kebijakan privasi harus berjalan beriringan dalam membangun kepercayaan konsumen.

Dalam penerapannya, menjaga ketiga unsur keamanan tersebut tidak bisa mengandalkan satu alat saja, melainkan membutuhkan prinsip Pertahanan Berlapis (*Defense in Depth*). Sebagai garda terdepan dari lapisan ini, platform menggunakan sistem autentikasi untuk memastikan bahwa pihak yang mencoba masuk ke akun benar-benar pemilik aslinya. Karena kata sandi biasa sangat rentan ditebak atau dicuri, penggunaan *Multi-Factor Authentication* (MFA) memberikan lapisan tambahan sehingga satu kata sandi yang bocor tidak akan langsung membuka akses akun. Namun, tidak semua MFA sama kuatnya. NIST (2025) menjelaskan bahwa sistem yang kebal *phishing* harus mampu mengikat proses *login* secara langsung dengan perangkat atau jalur yang dituju, sehingga kode akses yang disadap oleh peretas akan hangus dan tidak bisa digunakan di tempat lain.

Sebagai pelengkap di lapisan berikutnya, prinsip kerahasiaan (*Confidentiality*) dijaga melalui enkripsi. Enkripsi berfungsi mengacak informasi sehingga data tidak bisa dibaca tanpa kunci pembuka yang sah. Dalam *e-commerce*, pengamanan jalur komunikasi (seperti TLS) membantu mencegah penyadapan saat data sedang diantarkan melalui jaringan internet. Namun, enkripsi jaringan ini tidak secara otomatis melindungi data yang sudah menetap di *server* perusahaan, atau saat pengguna tanpa sadar memberikan sendiri kata sandinya ke situs penipu (*phishing*).

FMI Jawa Timur XVIII 2026
e-ISSN: 3026-4499
Vol. 4
20-22 Oktober 2026

Karena itu, enkripsi tetap harus diposisikan sebagai salah satu lapisan pengamanan saja, bukan solusi tunggal yang kebal dari segala celah.

Ketika pertahanan autentikasi dan enkripsi berhasil dilewati oleh peretas, platform membutuhkan lapisan pengawasan akhir, yaitu sistem deteksi aktivitas mencurigakan (*fraud detection*). Sistem ini bertugas mengenali transaksi atau aktivitas *login* yang melenceng dari kebiasaan normal pengguna. Pendekatannya bervariasi, mulai dari melacak kejanggalan lokasi, jenis perangkat yang dipakai, pola transaksi, hingga kecepatan interaksi di layar. Penelitian Vaithyasubramanian et al. (2021) menunjukkan bahwa informasi mengenai karakteristik pengguna dan transaksi dapat dimanfaatkan untuk mengenali penyusup yang sedang menyamar. Meski begitu, sistem ini punya kelemahan karena terkadang bisa salah mengenali pemilik asli sebagai ancaman (*false positive*), dan pemantauan aktivitas pengguna yang terlalu ketat justru bisa memicu masalah pelanggaran privasi baru.

Secara keseluruhan, tarik-ulur antara ketatnya keamanan dan kebebasan privasi ini bisa dipahami melalui Teori Persepsi Risiko (*Perceived Risk Theory*). Teori ini menyebutkan bahwa konsumen selalu menimbang antara kenyamanan berbelanja dengan risiko tercurinya data mereka. Saeed (2023) menyebutkan bahwa sistem keamanan *e-commerce* tidak boleh hanya fokus pada kecanggihan teknologi, tetapi juga harus memperhatikan kenyamanan penggunanya. Jika sistem keamanan terlalu kaku, atau justru terbukti gagal menjaga data (Strzelecki & Rizun, 2022), hal itu tidak hanya merugikan secara finansial, tetapi juga menghancurkan rasa percaya konsumen. Titik keseimbangan antara kuatnya sistem keamanan, perlindungan privasi, dan terjaganya kepercayaan konsumen inilah yang selanjutnya akan menjadi acuan dasar dalam mengevaluasi efektivitas berbagai fitur keamanan *e-commerce*.

3. Metode Penelitian

Artikel ini menggunakan pendekatan *Systematic Literature Review* (SLR) untuk mengidentifikasi, menyeleksi, dan menganalisis secara kritis penelitian terdahulu mengenai efektivitas fitur keamanan *e-commerce* dalam mencegah pencurian identitas konsumen. Tinjauan literatur dilakukan melalui empat tahapan utama.

Langkah pertama adalah identifikasi sumber literatur. Penelusuran artikel dilakukan secara daring melalui basis data akademik seperti Scopus, IEEE Xplore, ScienceDirect, Web of Science, dan Sinta. Pencarian dilakukan menggunakan kombinasi kata kunci "*e-commerce security*", "*identity theft*", "*identity fraud*", "*account takeover*", "*authentication*", "*multi-factor authentication*", "*fraud detection*", dan "*data protection*". Kata kunci tersebut digunakan secara kombinatif untuk memperoleh penelitian yang berkaitan dengan keamanan transaksi, perlindungan identitas, serta pencegahan *fraud* pada lingkungan *e-commerce*.

Langkah kedua adalah penetapan kriteria inklusi dan eksklusi. Artikel yang dimasukkan dalam kajian adalah artikel jurnal atau prosiding ilmiah yang diterbitkan pada periode 2021–2025, menggunakan bahasa Indonesia atau Inggris, dapat diverifikasi melalui halaman penerbit, DOI, atau basis data akademik, serta memiliki keterkaitan dengan keamanan *e-commerce*, pencurian identitas, *account takeover*, autentikasi, deteksi *fraud*, perlindungan data, atau analisis perilaku

FMI Jawa Timur XVIII 2026
e-ISSN: 3026-4499
Vol. 4
20-22 Oktober 2026

pengguna. Artikel yang diterbitkan di luar periode tersebut, tidak berkaitan dengan konteks *e-commerce*, hanya membahas keamanan jaringan secara umum, berupa berita atau opini, serta tidak memiliki informasi publikasi yang dapat diverifikasi tidak dimasukkan dalam kajian.

Langkah ketiga adalah proses seleksi literatur. Seleksi dilakukan dengan memeriksa judul dan abstrak, kemudian dilanjutkan dengan pembacaan isi artikel untuk memastikan kesesuaian dengan fokus penelitian. Berdasarkan proses penelusuran dan verifikasi tersebut, dipilih 10 artikel final yang paling relevan dengan tujuan kajian. Artikel terpilih mencakup penelitian mengenai *identity theft* pada *online shopping*, kebijakan pencegahan *identity fraud*, deteksi *fraud* berbasis *machine learning*, verifikasi identitas, analisis perilaku pengguna, serta keamanan dan privasi konsumen dalam *ecommerce*.

Langkah keempat adalah ekstraksi dan analisis data. Informasi dari 10 artikel terpilih dianalisis menggunakan *coding* tematik dengan memperhatikan jenis fitur atau mekanisme keamanan yang dibahas, bentuk ancaman yang ditangani, bukti efektivitas, serta keterbatasan penerapannya. Hasil penelitian kemudian dikelompokkan ke dalam beberapa tema, yaitu autentikasi dan verifikasi identitas, deteksi aktivitas atau transaksi mencurigakan, analisis perilaku pengguna, perlindungan data dan privasi, serta penggunaan *machine learning* dalam pencegahan *fraud*. Analisis dilakukan secara kritis untuk melihat bahwa efektivitas suatu fitur keamanan tidak hanya ditentukan oleh keberadaan teknologi tersebut, tetapi juga oleh jenis ancaman yang dihadapi, cara implementasinya, serta kemungkinan adanya celah apabila fitur digunakan secara tunggal. Rangkuman literatur utama ini disajikan pada Tabel 1.

Tabel 1. Matriks Ekstraksi Literatur Utama

No.	Penulis (Tahun)	Judul	Fokus/Metode	Temuan Utama
1	Vaithyasubramanian et al. (2021)	Communal Fraud Detection Algorithm for Establishing Identity Thefts in Online Shopping	Deteksi identity theft pada online shopping menggunakan Communal Fraud Detection (CFD) dan white list.	Hasil eksperimen menunjukkan bahwa pendekatan white list lebih efektif dibandingkan onetime password (OTP) dalam mendeteksi identity theft.
2	Gao et al. (2024)	Detecting Compromised	Mendeteksi akun yang dikompromikan	Data Meituan berisi 32.388 akun compromised dan 91.575 akun

e-ISSN: 3026-4499
Vol. 4
20-22 Oktober 2026

		Accounts Caused by Phone Number Recycling on E-Commerce Platforms: Taking Meituan as an Example	akibat phone number recycling (PNR). Menggunakan pola temporal dan fitur statistik melalui model TSF.	normal. Model TSF menggabungkan temporal pattern encoder dan statistical feature encoder serta mengungguli beberapa baseline.
3	Tax et al. (2021)	Machine Learning for Fraud Detection in E-Commerce: A Research Agenda	Membahas penerapan machine learning dalam operasi antifraud dari perspektif organisasi.	Menghasilkan 6 topik penelitian, 12 tantangan praktis, dan 22 tantangan penelitian terbuka. Menekankan bahwa model ML harus terintegrasi dengan proses kerja tim anti-fraud, bukan berdiri sendiri.
4	Maseeh et al. (2021)	Privacy Concerns in E-Commerce: A Multilevel Meta-Analysis	Meta-analisis mengenai faktor yang memengaruhi privacy concerns konsumen e-commerce.	Menganalisis 184 artikel. Risk perceptions meningkatkan privacy concerns, sedangkan benefit perceptions, familiarity, reputation, privacy policy, dan trust dapat mengurangi privacy concerns.
5	Ye et al. (2022)	Modeling Access Environment and Behavior Sequence for Financial Identity Theft Detection in E-Commerce Services	Deteksi financial identity theft menggunakan lingkungan akses (device, IP, delivery address) dan urutan perilaku pengguna. Mengembangkan model EnvIT.	Menggunakan kasus nyata dari Meituan. EnvIT menggabungkan heterogeneous graph, urutan perilaku, dan attention mechanism. Model mencapai AUC 0,9210 dan mengungguli beberapa baseline.

FMI Jawa Timur XVIII 2026
e-ISSN: 3026-4499
Vol. 4
20-22 Oktober 2026

6	Golyeri et al. (2023)	Fraud Detection on E-Commerce Transactions Using Machine Learning Techniques	Membandingkan Decision Tree, Logistic Regression, Random Forest, dan XGBoost untuk mendeteksi fraud.	Dataset berasal dari aktivitas belanja selama 90 hari pada platform Boyner Group. Menggunakan precision, recall, dan F1 dengan 10-fold crossvalidation. Setelah fitur IsGuestOrder ditambahkan, Logistic Regression mencapai accuracy 0,93, precision 0,95, recall 0,89, dan F1 0,92.
7	Patil et al. (2024)	Enhancing Digital Security: How Identity Verification Mitigates E-Commerce Fraud	Membahas mobile identity verification, biometrik, MFA, AI/ML, tokenisasi, dan enkripsi.	Penelitian melaporkan fraud rate rata-rata turun dari 8,5% menjadi 2,7%, atau penurunan 68,87% setelah penerapan mobile identity verification. Mereka juga melaporkan peningkatan deteksi fraud pada penggunaan AI.
8	Handoyo (2024)	Purchasing in the Digital Age: A Meta-Analytical Perspective on Trust, Risk, Security, and e-	Meta-analisis mengenai trust, perceived risk, perceived security, dan e-WOM terhadap	Menganalisis 54 studi dengan total 32.658 responden. Trust, perceived risk, perceived security, dan e-WOM berhubungan dengan keputusan pembelian. Perceived risk
		WOM in ECommerce	keputusan pembelian e-commerce.	memiliki efek moderasi signifikan, sedangkan perceived security dan e-WOM tidak menunjukkan efek moderasi yang signifikan pada hubungan trust–purchase decision.

FMI Jawa Timur XVIII 2026
e-ISSN: 3026-4499
Vol. 4
20-22 Oktober 2026

9	Zhang et al. (2025)	Identifying E-Commerce Fraud Through User Behavior Data: Observations and Insights	Deteksi fraud menggunakan mouse trajectory, page-view sequence, dwell time, page ID, dan item price melalui MultiModal Behavioral Transformer (MMBT).	MMBT pada data industri nyata menghasilkan APR 66,09%, AUC 67,60%, dan Precision@Recall=0,1 sebesar 88,89%. Dibandingkan model terbaik berikutnya, peningkatan AUC 2,94% dan precision hingga 6,95%. Latensi online inference P99 < 500 ms.
10	Karim & Fahmi (2025)	Analisis Prediktif untuk Mendeteksi Penipuan E-Commerce Menggunakan Algoritma Pembelajaran Mesin	Membandingkan Deep Learning, Naïve Bayes, Logistic Regression, Decision Tree, dan Neural Network untuk deteksi fraud.	Menggunakan 1.472.952 transaksi sintetis dari Kaggle, dengan pembagian training/testing 80:20. Neural Network memperoleh accuracy 0,9555 dan F1 0,9770; Decision Tree accuracy 0,9547 dan F1 0,9767. Decision Tree memiliki sensitivity tertinggi 0,9992.

4. Hasil dan Pembahasan

Efektivitas Autentikasi dan Verifikasi Identitas. Hasil telaah menunjukkan bahwa autentikasi merupakan salah satu lapisan penting dalam perlindungan akun e-commerce, tetapi penggunaan satu metode autentikasi belum sepenuhnya mampu mengatasi berbagai bentuk pencurian identitas. Vaithyasubramanian et al. (2021) mengembangkan *Communal Fraud Detection* dengan pendekatan *white list* untuk mendeteksi pencurian identitas pada aktivitas belanja daring. Sistem tersebut menggunakan sejumlah informasi pengguna dan karakteristik transaksi untuk membentuk *white list*, kemudian dibandingkan dengan penggunaan *one-time password* (OTP). Hasil eksperimen dalam penelitian tersebut menunjukkan bahwa pendekatan *white list* memberikan hasil yang lebih efektif dibandingkan OTP dalam mendeteksi pencurian identitas pada skenario yang diuji. Temuan ini menunjukkan bahwa keberhasilan perlindungan identitas tidak hanya bergantung pada proses verifikasi ketika pengguna melakukan login, tetapi juga pada kemampuan sistem mengenali apakah aktivitas yang dilakukan sesuai dengan

e-ISSN: 3026-4499
Vol. 4
20-22 Oktober 2026

karakteristik pengguna yang sah (Vaithyasubramanian et al., 2021). Keterbatasan autentikasi berbasis nomor telepon juga terlihat dalam penelitian Gao et al. (2024). Penelitian tersebut membahas kasus *phone number recycling* pada platform e-commerce, yaitu ketika nomor telepon yang sudah tidak digunakan oleh pemilik sebelumnya diberikan kembali kepada pengguna baru. Kondisi tersebut dapat menyebabkan pemilik baru memperoleh akses terhadap akun e-commerce yang masih terhubung dengan nomor tersebut. Penelitian menggunakan kasus akun yang mengalami kompromi akibat *phone number recycling* pada platform Meituan dan mengembangkan model TSF yang memanfaatkan informasi perangkat, alamat IP, lokasi, pola waktu, serta perilaku pembelian dan pembayaran. Hasil penelitian menunjukkan bahwa informasi lingkungan akses dan perilaku dapat digunakan untuk mendeteksi akun yang mengalami kompromi. Dengan demikian, kepemilikan nomor telepon saja tidak selalu cukup untuk memastikan bahwa orang yang mengakses akun benar-benar pemilik yang sah (Gao et al., 2024). Temuan tersebut sejalan dengan pembahasan Patil et al. (2024) mengenai penggunaan verifikasi identitas pada transaksi digital. Penelitian ini membahas kombinasi biometrik, *multi-factor authentication* (MFA), dan analitik berbasis AI sebagai bagian dari perlindungan terhadap *identity theft*, *account takeover*, dan *phishing*. Penulis juga menunjukkan bahwa penerapan teknologi verifikasi identitas masih menghadapi persoalan seperti kerentanan teknis, biaya penerapan, dan masalah kemudahan penggunaan. Artinya, penambahan lapisan autentikasi memang dapat memperkuat keamanan, tetapi penerapannya tetap perlu mempertimbangkan bagaimana teknologi tersebut digunakan dan bagaimana data identitas pengguna dikelola (Patil et al., 2024). Dari ketiga penelitian tersebut terlihat bahwa autentikasi lebih tepat dipahami sebagai salah satu lapisan awal dalam perlindungan identitas, bukan sebagai mekanisme tunggal yang dapat menghentikan seluruh bentuk pencurian identitas. OTP dan verifikasi nomor telepon dapat membantu memastikan akses, tetapi masih memiliki kelemahan ketika kredensial atau sarana verifikasi berhasil diambil alih. Oleh karena itu, karakteristik perangkat, lokasi, pola aktivitas, serta metode verifikasi tambahan dapat digunakan sebagai lapisan pemeriksaan berikutnya.

Deteksi Berdasarkan Perilaku dan Lingkungan Akses. Literatur yang ditelaah memperlihatkan adanya perkembangan dari pendekatan keamanan yang hanya memeriksa kredensial menuju pendekatan yang mengamati perilaku pengguna secara lebih berkelanjutan. Ye et al. (2022), misalnya, menemukan bahwa akun-akun yang melakukan pencurian identitas finansial dapat menunjukkan perbedaan lingkungan akses, seperti perangkat dan alamat IP. Penelitian tersebut juga menemukan adanya pengelompokan perangkat, alamat IP, dan alamat pengiriman pada kelompok akun yang melakukan aktivitas penipuan. Berdasarkan temuan tersebut, peneliti mengembangkan EnvIT yang menggabungkan informasi lingkungan akses dengan urutan perilaku akun melalui *heterogeneous graph* dan *behavior sequence*. Pada dataset dunia nyata dari Meituan, EnvIT memperoleh nilai AUC sebesar 0,9210 dan mengungguli beberapa metode pembanding yang digunakan dalam penelitian tersebut (Ye et al., 2022). Pendekatan yang serupa dikembangkan lebih lanjut oleh Gao et al. (2024). Perbedaannya, penelitian tersebut secara khusus melihat kompromi akun akibat penggunaan kembali nomor telepon. Model yang dikembangkan tidak hanya melihat apakah nomor telepon dapat digunakan untuk masuk ke

akun, tetapi memanfaatkan kombinasi karakteristik perangkat, IP, GPS, waktu, serta perilaku pembelian dan pembayaran. Hal ini memperlihatkan bahwa pemeriksaan keamanan dapat dilakukan berdasarkan konsistensi antara aktivitas saat ini dengan pola penggunaan akun sebelumnya (Gao et al., 2024). Zhang et al. (2025) memberikan perkembangan yang lebih jauh dengan menggunakan data perilaku pengguna dalam proses deteksi fraud. Penelitian tersebut menjelaskan bahwa metode tradisional yang mengandalkan hubungan antara perangkat, email, atau alamat dapat menghadapi masalah ketika pelaku fraud memanipulasi entitas tersebut. Sebagai alternatif, penelitian ini mengembangkan *Multi-Modal Behavioral Transformer* (MMBT) yang menggabungkan perilaku pada halaman, seperti *mouse trajectory*, dengan perilaku antarhalaman, seperti urutan halaman yang dilihat dan durasi kunjungan. Pada data industri nyata, pendekatan tersebut menunjukkan peningkatan AUC sebesar 2,94% dan peningkatan *precision@recall = 0,1* sebesar 6,95% dibandingkan model pembanding terbaik. Penelitian ini juga mengembangkan alur pemrosesan *online* yang memiliki *latency* persentil ke-99 di bawah 500 milidetik, sehingga hasil deteksi dapat digunakan untuk merespons aktivitas yang dicurigai secara cepat (Zhang et al., 2025). Jika dibandingkan, ketiga penelitian tersebut memperlihatkan pola yang cukup konsisten, yaitu keamanan identitas semakin diarahkan pada pemeriksaan apakah perilaku pengguna masuk akal bagi pemilik akun, bukan hanya apakah kredensial yang digunakan benar. Pendekatan ini menjadi penting karena pencuri identitas dapat memperoleh informasi login, sedangkan pola perilaku, lingkungan akses, dan karakteristik interaksi pengguna relatif lebih sulit ditiru secara konsisten. Namun, hasil penelitian tersebut tetap berada pada konteks dataset dan platform tertentu sehingga belum dapat langsung dianggap berlaku sama pada seluruh platform e-commerce.

Machine Learning dalam Deteksi Fraud E-Commerce. Penggunaan *machine learning* menjadi salah satu pendekatan yang banyak ditemukan dalam literatur untuk mengidentifikasi pola transaksi yang tidak wajar. Golyeri et al. (2023) menguji *Decision Tree*, *Logistic Regression*, *Random Forest*, dan *Extreme Gradient Boosting* menggunakan data aktivitas belanja dari situs dan aplikasi e-commerce Boyner Group. Fitur yang digunakan antara lain jumlah transaksi, jumlah barang, transaksi berhasil dan gagal, aktivitas pengembalian barang, serta metode pembayaran. Penelitian tersebut menggunakan dua versi dataset, dengan versi kedua menambahkan fitur *IsGuestOrder*. Penambahan fitur tersebut meningkatkan performa beberapa model. Pada dataset kedua, *Logistic Regression* memperoleh accuracy 0,93, precision 0,95, recall 0,89, dan F-measure 0,92. Hasil tersebut menunjukkan bahwa kualitas dan relevansi fitur yang digunakan ikut menentukan kemampuan model dalam mendeteksi aktivitas fraud (Golyeri et al., 2023). Hasil tersebut penting karena memperlihatkan bahwa pemilihan algoritma saja tidak dapat dipisahkan dari pemilihan karakteristik data. Pada penelitian Golyeri et al. (2023), penambahan *IsGuestOrder* menghasilkan peningkatan performa klasifikasi. Dengan demikian, efektivitas sistem deteksi tidak hanya ditentukan oleh model yang digunakan, tetapi juga oleh kemampuan sistem memperoleh fitur yang dapat membedakan aktivitas normal dan aktivitas yang mencurigakan. Karim & Fahmi (2025) juga membandingkan beberapa algoritma, yaitu *Deep Learning*, *Naïve Bayes*, *Logistic Regression*, *Decision Tree*, dan *Neural Network* untuk mendeteksi penipuan *ecommerce*. Penelitian tersebut menggunakan 1.472.952 transaksi dan

e-ISSN: 3026-4499
Vol. 4
20-22 Oktober 2026

mengevaluasi model berdasarkan *sensitivity*, *precision*, *accuracy*, dan F1-score. Hasil pengujian menunjukkan bahwa *Neural Network* memperoleh *accuracy* 0,9555 dan F1-score 0,9770, sedangkan *Decision Tree* memperoleh *sensitivity* tertinggi sebesar 0,9992. Temuan ini menunjukkan adanya perbedaan kemampuan antaralgoritma tergantung pada metrik yang digunakan, sehingga performa model sebaiknya tidak dinilai hanya berdasarkan satu ukuran saja (Karim & Fahmi, 2025). Akan tetapi, terdapat hal yang perlu diperhatikan dalam menginterpretasikan hasil Karim & Fahmi (2025), yaitu karakteristik dataset yang digunakan. Dataset penelitian tersebut berjumlah besar, tetapi berupa data transaksi sintetis. Oleh sebab itu, nilai performa yang tinggi tidak secara otomatis menunjukkan bahwa model akan menghasilkan tingkat performa yang sama ketika diterapkan pada data transaksi nyata dengan pola fraud yang lebih beragam. Keterbatasan ini berbeda dengan penelitian Golyeri et al. (2023), Ye et al. (2022), dan Zhang et al. (2025) yang menggunakan data aktivitas dari lingkungan e-commerce nyata. Sementara itu, Tax et al. (2021) memberikan perspektif yang berbeda. Penelitian tersebut tidak menguji satu algoritma tertentu untuk kemudian menyatakan algoritma tersebut paling efektif, melainkan membahas *machine learning* dalam konteks operasional organisasi anti-fraud. Penulis mengembangkan model operasional departemen anti-fraud dan mengidentifikasi enam topik penelitian, 12 tantangan praktis, serta 22 tantangan penelitian terbuka. Dengan demikian, penggunaan *machine learning* dalam e-commerce tidak seharusnya dipandang sebagai solusi yang berdiri sendiri. Model perlu ditempatkan dalam proses anti-fraud yang lebih luas, termasuk proses investigasi dan penanganan hasil deteksi (Tax et al., 2021). Temuan dari kelompok penelitian ini menunjukkan bahwa *machine learning* memiliki potensi besar untuk mendeteksi pola fraud, tetapi efektivitasnya sangat bergantung pada data, fitur, model, metrik evaluasi, dan konteks penerapan. Karena itu, hasil accuracy atau F1-score yang tinggi pada satu penelitian tidak dapat langsung digunakan untuk menyatakan bahwa algoritma tersebut paling efektif untuk seluruh sistem e-commerce.

Keamanan, Privasi, Risiko, dan Kepercayaan Konsumen. Perlindungan identitas konsumen tidak hanya berkaitan dengan kemampuan teknis sistem mendeteksi fraud. Aspek keamanan juga berkaitan dengan bagaimana konsumen memandang risiko dan penggunaan data pribadinya. Maseeh et al. (2021) melalui meta-analisis terhadap penelitian mengenai privasi dalam e-commerce menunjukkan bahwa persepsi risiko dapat memicu kekhawatiran privasi. Sebaliknya, manfaat yang dirasakan, familiaritas, reputasi, kebijakan privasi, dan kepercayaan dapat mengurangi kekhawatiran tersebut. Kekhawatiran privasi selanjutnya berhubungan dengan sikap dan penggunaan konsumen terhadap platform e-commerce. Penelitian ini juga menunjukkan adanya variasi hasil berdasarkan karakteristik metodologis dan konteks penelitian, sehingga hubungan antara privasi dan perilaku konsumen tidak dapat dipahami secara sederhana (Maseeh et al., 2021). Perspektif tersebut diperkuat oleh Handoyo (2024) melalui meta-analisis yang mencakup 54 studi dengan total 32.658 partisipan. Penelitian tersebut menunjukkan bahwa *trust*, *perceived risk*, *perceived security*, dan *electronic word-of-mouth* berhubungan dengan keputusan pembelian dalam ecommerce. *Perceived risk* juga memiliki peran moderasi pada hubungan antara kepercayaan dan keputusan pembelian. Namun, *perceived security* tidak menunjukkan efek moderasi yang sama pada hubungan tersebut.

FMI Jawa Timur XVIII 2026
e-ISSN: 3026-4499
Vol. 4
20-22 Oktober 2026

Temuan ini menunjukkan bahwa persepsi keamanan tetap memiliki hubungan dengan perilaku konsumen, tetapi pengaruhnya tidak sesederhana anggapan bahwa semakin tinggi persepsi keamanan maka semakin kuat pula seluruh hubungan antara kepercayaan dan keputusan pembelian (Handoyo, 2024). Jika dikaitkan dengan penelitian teknis sebelumnya, hasil tersebut menunjukkan bahwa keberadaan fitur keamanan saja belum tentu cukup untuk membentuk rasa aman konsumen. Sistem dapat memiliki MFA, deteksi fraud, atau mekanisme verifikasi identitas, tetapi konsumen tetap mempertimbangkan risiko penggunaan data, reputasi platform, kebijakan privasi, dan pengalaman mereka dalam menggunakan layanan. Dengan demikian, keamanan teknis dan persepsi konsumen merupakan dua aspek yang saling berkaitan tetapi tidak dapat disamakan.

Evaluasi Kritis terhadap Efektivitas Fitur Keamanan. Secara keseluruhan, sepuluh sumber yang ditelaah menunjukkan bahwa pencurian identitas dalam e-commerce memiliki bentuk dan jalur serangan yang beragam. Karena itu, tidak terdapat satu fitur keamanan yang dapat dipandang sebagai solusi tunggal untuk seluruh permasalahan. Penelitian Vaithyasubramanian et al. (2021) menunjukkan potensi penggunaan *white list* dan karakteristik pengguna untuk memperkuat deteksi identitas. Gao et al. (2024) memperlihatkan kelemahan autentikasi yang terlalu bergantung pada nomor telepon. Ye et al. (2022) dan Zhang et al. (2025) menunjukkan manfaat pemanfaatan lingkungan akses dan perilaku pengguna, sedangkan Golyeri et al. (2023) dan Karim & Fahmi (2025) memperlihatkan bahwa *machine learning* dapat digunakan untuk mengklasifikasikan pola transaksi yang mencurigakan. Pada saat yang sama, penelitian Patil et al. (2024) menunjukkan bahwa biometrik dan MFA juga mempunyai tantangan berupa kerentanan teknis, biaya, dan kemudahan penggunaan. Sementara itu, Maseeh et al. (2021) dan Handoyo (2024) memperlihatkan bahwa keamanan harus dilihat bersamaan dengan privasi, risiko, dan kepercayaan konsumen. Bahkan Tax et al. (2021) menekankan bahwa sistem *machine learning* perlu ditempatkan dalam keseluruhan proses operasional anti-fraud, bukan hanya digunakan sebagai model prediksi yang berdiri sendiri. Berdasarkan sintesis tersebut, efektivitas fitur keamanan lebih tepat dipahami berdasarkan fungsi dan posisi fitur dalam proses perlindungan, bukan dengan menentukan satu teknologi sebagai yang paling unggul. Autentikasi dan verifikasi berfungsi membatasi akses awal, sedangkan analisis perilaku dan lingkungan akses dapat digunakan untuk mengidentifikasi aktivitas yang tidak konsisten dengan pola pengguna. Selanjutnya, *machine learning* dapat membantu mengolah berbagai karakteristik tersebut untuk mendeteksi pola fraud, sementara mekanisme organisasi dan proses investigasi diperlukan untuk menindaklanjuti hasil deteksi. Pada sisi lain, kebijakan privasi dan pengelolaan data diperlukan agar penerapan keamanan tidak justru menimbulkan persoalan baru bagi pengguna. Dengan demikian, hasil *systematic literature review* ini mendukung pendekatan layered security atau *defense in depth* dalam perlindungan identitas konsumen e-commerce. Pendekatan tersebut bukan berarti seluruh teknologi harus selalu diterapkan secara bersamaan, tetapi menunjukkan bahwa perlindungan identitas perlu dibangun melalui beberapa lapisan yang memiliki fungsi berbeda. Autentikasi dapat menjadi lapisan pengendalian akses, analisis perilaku menjadi lapisan deteksi, *machine learning* menjadi pendukung pengenalan pola, sedangkan proses investigasi dan respons menjadi lapisan penanganan ketika indikasi

fraud ditemukan. Pola tersebut lebih sesuai dengan karakter pencurian identitas yang dapat terjadi melalui berbagai jalur, mulai dari kompromi kredensial hingga penyalahgunaan akun dan transaksi yang tidak sesuai dengan perilaku pemilik sebenarnya.

5. Kesimpulan

Berdasarkan hasil *Systematic Literature Review* terhadap 10 artikel yang diterbitkan pada periode 2021–2025, dapat disimpulkan bahwa efektivitas fitur keamanan *e-commerce* dalam mencegah pencurian identitas tidak dapat dilihat hanya dari keberadaan satu teknologi keamanan. Autentikasi dan verifikasi identitas menjadi lapisan penting dalam membatasi akses terhadap akun, tetapi beberapa penelitian menunjukkan adanya kelemahan pada metode yang bergantung pada OTP atau nomor telepon ketika sarana autentikasi tersebut berhasil dikompromikan. Pemanfaatan informasi tambahan seperti perangkat, alamat IP, lokasi, pola transaksi, dan karakteristik perilaku pengguna dapat membantu sistem mengenali aktivitas yang berbeda dari kebiasaan pemilik akun.

Penggunaan *machine learning* juga menunjukkan kemampuan dalam mendeteksi pola transaksi dan aktivitas yang mencurigakan. Namun, hasil evaluasi antarpenelitian tidak dapat dibandingkan secara langsung karena menggunakan dataset, fitur, algoritma, dan metrik yang berbeda. Selain itu, penggunaan data sintetis pada salah satu penelitian menunjukkan bahwa performa model yang tinggi belum tentu dapat langsung digeneralisasikan pada kondisi e-commerce nyata. Oleh karena itu, penerapan *machine learning* juga membutuhkan data yang sesuai serta integrasi dengan proses operasional anti-*fraud* dan tindak lanjut terhadap hasil deteksi.

Kajian ini juga menunjukkan bahwa keamanan teknis tidak dapat dipisahkan dari aspek privasi, persepsi risiko, dan kepercayaan konsumen. Fitur keamanan yang semakin kompleks perlu diterapkan dengan mempertimbangkan perlindungan data dan kemudahan penggunaan agar tidak menimbulkan persoalan baru bagi konsumen. Secara keseluruhan, hasil kajian mengarah pada pentingnya pendekatan *layered security* atau *defense in depth*, yaitu menggabungkan beberapa lapisan perlindungan dengan fungsi yang berbeda. Autentikasi dapat digunakan untuk mengendalikan akses, analisis perilaku dan lingkungan akses untuk mendeteksi kejanggalan, *machine learning* untuk membantu mengenali pola *fraud*, serta mekanisme investigasi, respons, dan perlindungan privasi untuk menangani risiko setelah indikasi ancaman ditemukan. Pendekatan berlapis tersebut memberikan kerangka yang lebih menyeluruh dalam menghadapi berbagai bentuk pencurian identitas pada lingkungan *e-commerce*.

Referensi

Gao, M., Chen, S., Gao, Y., Zhang, Z., Chen, Y., Li, Y., Ye, Q., Wang, X., & Chen, Y. (2024). Detecting Compromised Accounts Caused by Phone Number Recycling on E-Commerce Platforms: Taking Meituan as an Example. *Frontiers of Information Technology & Electronic Engineering*, *25*. https://doi.org/10.1631/FITEE.2300291

Golyeri, M., Bozyigit, F., Celik, S., & Kılınç, D. (2023). Fraud Detection on E-Commerce Transactions Using Machine Learning Techniques. *Artificial Intelligence Theory and*

Applications, *3*(1), 45–50. https://dergipark.org.tr/en/pub/aita/article/1273652

Handoyo, S. (2024). Purchasing in the digital age: A meta-analytical perspective on trust, risk, security, and e-WOM in e-commerce. *Heliyon*, *10*, e29714. https://doi.org/10.1016/j.heliyon.2024.e29714

Karim, A., & Fahmi, F. (2025). Analisis Prediktif untuk Mendeteksi Penipuan E-Commerce Menggunakan Algoritma Pembelajaran Mesin. *The Indonesian Journal of Computer Science*, *14*. https://doi.org/10.33022/ijcs.v14i2.4202

Liu, X., Ahmad, S. F., Anser, M. K., Ke, J., Irshad, M., Ul-Haq, J., & Abbas, S. (2022). Cyber security threats: A never-ending challenge for e-commerce. *Frontiers in Psychology*, *Volume 13-2022*. https://doi.org/10.3389/fpsyg.2022.927398

Maseeh, H., Jebarajakirthy, C., Pentecost, R., Arli, D., Weaven, S., & Ashaduzzaman, M. (2021). Privacy concerns in e-commerce: A multilevel meta-analysis. *Psychology & Marketing*, *38*, 1779–1798. https://doi.org/10.1002/mar.21493

National Institute of Standards and Technology. (2025). NIST SP 800-63-4: Digital identity guidelines. https://doi.org/10.6028/NIST.SP.800-63-4

National Institute of Standards and Technology. (2025). NIST SP 800-63B-4: Digital identity guidelines: Authentication and authenticator management. https://doi.org/10.6028/NIST.SP.800-63b-4

Park, J., Shin, W., Kim, B., & Kim, M. (2024). Spillover effects of data breach on consumer perceptions: evidence from the E-commerce industry. *Internet Research*, *35*(1), 1–24. https://doi.org/10.1108/INTR-11-2022-0898

Patil, S., Dudhankar, V., & Shukla, P. (2024). Enhancing Digital Security: How Identity Verification Mitigates E-Commerce Fraud. *Journal of Current Science and Research Review*, *2*(2), 69–81.

Saeed, S. (2023). A Customer-Centric View of E-Commerce Security and Privacy. *Applied Sciences*, *13*, 1020. https://doi.org/10.3390/app13021020

Soomro, Z. A., Shah, M. H., & Thatcher, J. (2021). A framework for ID fraud prevention policies in E-tailing sector. *Computers & Security*, *109*, 102403. https://doi.org/10.1016/j.cose.2021.102403

Strzelecki, A., & Rizun, M. (2022). Consumers' Change in Trust and Security after a Personal Data Breach in Online Shopping. *Sustainability*, *14*, 5866. https://doi.org/10.3390/su14105866

Tax, N., Vries, K. J., Jong, M., Dosoula, N., Akker, B., Smith, J., Thuong, O., & Bernardi, L. (2021). *Machine Learning for Fraud Detection in E-Commerce: A Research Agenda*. https://doi.org/10.48550/arXiv.2107.01979

Vaithyasubramanian, S., Saravanan, D., & Kirubhashankar, K. C. (2021). Communal Fraud Detection Algorithm for Establishing Identity Thefts in Online Shopping. *International Journal*

FMI Jawa Timur XVIII 2026
e-ISSN: 3026-4499
Vol. 4
20-22 Oktober 2026

of E-Collaboration (IJeC), *17*(3), 75–84. https://doi.org/10.4018/IJeC.2021070105

Ye, Q., Gao, Y., Zhang, Z., Chen, Y., Li, Y., Gao, M., Chen, S., Wang, X., & Chen, Y. (2022). Modeling Access Environment and Behavior Sequence for Financial Identity Theft Detection in E-Commerce Services. *2022 International Joint Conference on Neural Networks (IJCNN)*, 1–8. https://doi.org/10.1109/IJCNN55064.2022.9892383

Zhang, Z., Yin, H., Rao, S. X., Yan, X., Wang, Z., Liang, W., Zhao, Y., Shan, Y., Zhang, R., Lin, Y., & Jiang, J. (2025). Identifying E-Commerce Fraud Through User Behavior Data: Observations and Insights. *Data Science and Engineering*, *10*(1), 24–39. https://doi.org/10.1007/s41019024-00275-6

Copyrights

Copyright for this article is retained by the author(s), with first publication rights granted to the journal.

This is an open-access article distributed under the terms and conditions of the Creative Commons Attribution license (http://creativecommons.org/licenses/by/4.0/)