

“Analisis Faktor-Faktor yang Mempengaruhi Keamanan Transaksi pada Platform E-Commerce”

Endri Does¹, Selfi andriani², Rendi arta risja³

Abstrak

Penelitian ini bertujuan untuk menganalisis faktor-faktor yang mempengaruhi keamanan transaksi pada platform e-commerce. Pertumbuhan pesat perdagangan daring meningkatkan kebutuhan akan sistem keamanan yang andal, sehingga pemahaman terhadap faktor-faktor yang memengaruhi keamanan transaksi menjadi penting bagi konsumen maupun penyedia platform. Metode penelitian yang digunakan adalah tinjauan pustaka, dengan mengkaji literatur dan penelitian terdahulu terkait keamanan transaksi, termasuk aspek teknologi, perilaku pengguna, dan kebijakan keamanan platform. Hasil penelitian menunjukkan bahwa faktor-faktor seperti sistem autentikasi pengguna, enkripsi data, kebijakan privasi, serta kesadaran dan perilaku pengguna secara signifikan mempengaruhi keamanan transaksi di platform e-commerce. Temuan ini menekankan pentingnya integrasi teknologi keamanan yang handal dengan edukasi pengguna untuk meminimalkan risiko keamanan dan meningkatkan kepercayaan konsumen dalam bertransaksi secara daring.

Kata kunci: keamanan transaksi; e-commerce; autentikasi pengguna; enkripsi data; kepercayaan konsumen

Abstract

This study aims to analyze the factors influencing transaction security on e-commerce platforms. The rapid growth of online commerce has increased the need for reliable security systems, making it crucial for both consumers and platform providers to understand the factors affecting transaction security. The research method used is a literature review, examining previous studies and literature related to transaction security, including technological aspects, user behavior, and platform security policies. The results show that factors such as user authentication systems, data encryption, privacy policies, as well as user awareness and behavior significantly influence transaction security on e-commerce platforms. These findings emphasize the importance of integrating robust security technology with user education to minimize security risks and enhance consumer trust in online transactions.

Keywords: transaction security; e-commerce; user authentication; data encryption; consumer trust

A. PENDAHULUAN

Perkembangan pesat e-commerce di era digital telah mengubah lanskap perdagangan secara mendasar transaksi yang dulu memerlukan kunjungan fisik kini dapat dilakukan dalam hitungan detik melalui sentuhan layar. Di satu sisi, pertumbuhan ini membawa kemudahan dan efisiensi, namun di sisi lain muncul kekhawatiran besar terkait **keamanan transaksi**. Ancaman seperti pencurian identitas, peretasan, phishing, dan kebocoran data menjadi sorotan utama bagi pengguna dan pelaku bisnis daring. Hal ini membuat keamanan siber menjadi aspek kritis yang memengaruhi kepercayaan konsumen terhadap platform e-commerce. Tantangan tersebut telah dibahas secara komprehensif oleh Ramadhani dan Nasution (2024), yang mengidentifikasi bahwa e-commerce harus menghadapi berbagai jenis serangan seperti malware, pencurian data, serangan phishing, dan kebocoran informasi jika ingin menjaga integritas transaksi daring.

Namun demikian, meskipun riset seperti Ramadhani & Nasution (2024) telah menggambarkan ancaman dan solusi umum, masih terdapat **kekosongan dalam literatur** terkait **analisis faktor-faktor spesifik dan terintegrasi** yang mempengaruhi keamanan transaksi di platform e-commerce lokal maupun global. Sebagian besar penelitian lebih menekankan pada tantangan atau solusi teknis tunggal (misalnya enkripsi atau autentikasi dua faktor), tanpa menggabungkan aspek teknis, kebijakan privasi, perilaku pengguna, dan kondisi regulasi secara simultan. Dengan demikian, belum muncul model komprehensif yang menggabungkan semua faktor tersebut dalam satu kerangka analisis.

Selain itu, ada **kesenjangan fenomena** antara implementasi teknis dan persepsi pengguna: dalam praktik di Indonesia dan banyak negara lain, penerapan protokol keamanan canggih tidak selalu sejalan dengan kesadaran dan perilaku pengguna dalam menjaga data pribadi mereka. Artinya, meskipun platform telah menerapkan enkripsi dan autentikasi, jika pengguna tidak memahami pentingnya praktik keamanan (misalnya memilih kata sandi kuat, tidak membagikan data sensitif, dsb.), maka risiko tetap tinggi. Kekosongan ini menunjukkan bahwa penelitian sebelumnya belum banyak mengeksplorasi bagaimana faktor teknis dan perilaku pengguna berinteraksi dalam mempengaruhi keamanan transaksi.

Dengan latar tersebut, penelitian ini bertujuan untuk **menganalisis faktor-faktor yang mempengaruhi keamanan transaksi pada platform e-commerce secara holistik** mencakup aspek teknologi (misalnya enkripsi, autentikasi), kebijakan dan privasi data, serta perilaku pengguna dan bagaimana ketiga aspek ini saling terkait. Pendekatan ini diharapkan menutup gap literatur dengan menawarkan model analisis yang lebih komprehensif daripada studi-studi terdahulu yang bersifat fragmentaris.

Dengan demikian, penelitian ini bukan hanya relevan secara akademis, tetapi juga memiliki implikasi praktis: hasilnya dapat memberikan rekomendasi bagi pengembang platform, regulator, dan konsumen untuk meningkatkan sistem keamanan dan membangun kepercayaan, sehingga transaksi e-commerce bisa berlangsung aman dan berkelanjutan.

B. KAJIAN TEORI

1. Keamanan Transaksi E-Commerce

Keamanan transaksi dalam e-commerce merupakan aspek krusial untuk menjamin perlindungan data finansial dan informasi pribadi pengguna dari berbagai ancaman, termasuk pencurian data, penipuan, serta akses tidak sah

(Hidayat, 2022). Konsep keamanan ini mencakup beberapa aspek fundamental, yakni **confidentiality** atau kerahasiaan data, **integrity** atau keutuhan informasi, **availability** atau ketersediaan sistem, **authentication** atau otentikasi pengguna, serta **non-repudiation** atau kemampuan untuk memastikan transaksi tidak dapat disangkal. Implementasi aspek-aspek ini menjadi landasan bagi kepercayaan konsumen dalam menggunakan platform e-commerce serta penentu keberhasilan operasional bisnis digital.

Namun, dalam praktiknya, terdapat kesenjangan antara konsep teoritis dan penerapan nyata. Beberapa sistem keamanan canggih sering kali terhambat oleh kesalahan pengguna, keterbatasan teknologi, atau kurangnya pemahaman terhadap protokol keamanan (Hidayat, 2022). Selain itu, rumus dan algoritma keamanan seperti enkripsi data dan autentikasi multifaktor belum sepenuhnya diintegrasikan di semua platform, sehingga risiko kebocoran informasi tetap ada. Fenomena ini menunjukkan perlunya penelitian yang mendalam untuk menganalisis faktor-faktor yang mempengaruhi keamanan transaksi, baik dari sisi teknis, perilaku pengguna, maupun manajemen risiko, sehingga dapat merumuskan strategi mitigasi yang lebih efektif dan dapat dipertanggungjawabkan.

Keamanan transaksi e-commerce tidak hanya berkaitan dengan perlindungan data finansial dan pribadi konsumen, tetapi juga menuntut penerapan prinsip-prinsip keamanan informasi yang baku. Salah satu teori dasar yang menjadi acuan adalah **CIA Triad**, yang menekankan tiga aspek utama: **confidentiality** (kerahasiaan), **integrity** (keutuhan data), dan **availability** (ketersediaan sistem) (Sari, 2023). Ketiga prinsip ini menjadi fondasi untuk membangun sistem transaksi yang aman, di mana setiap informasi sensitif harus dijaga kerahasiaannya, tetap utuh selama proses transaksi, dan tersedia setiap saat bagi pengguna yang berwenang.

Selain itu, standar industri juga menjadi acuan penting, misalnya **Payment Card Industry Data Security Standard (PCI DSS)** yang mengatur prosedur keamanan untuk data kartu pembayaran, serta **ISO/IEC 27001** yang menyediakan kerangka manajemen keamanan informasi secara menyeluruh (Sari, 2023). Meskipun standar ini telah mapan, dalam praktiknya sering ditemukan gap antara teori dan implementasi di lapangan, misalnya kelemahan sistem dalam menghadapi serangan siber terbaru, atau keterbatasan pengguna dalam memahami prosedur keamanan.

2. Faktor-Faktor yang Mempengaruhi Keamanan Transaksi

Di era digital saat ini, e-commerce telah menjadi kanal utama transaksi ekonomi global, sehingga aspek keamanan informasi dan transaksi merepresentasikan fondasi penting untuk menjaga kepercayaan konsumen. Keamanan transaksi tidak hanya berarti menjaga data finansial dan pribadi konsumen, tetapi juga memastikan bahwa seluruh proses transaksi berlangsung secara aman dari berbagai ancaman siber seperti penyadapan, peretasan, malware, atau akses tidak sah. Untuk itu, banyak platform e-commerce mengadopsi beragam **teknologi dan sistem keamanan**: enkripsi data melalui SSL/TLS, sistem otentikasi dua faktor (2FA), firewall, serta sistem anti-malware dan kontrol akses. Protokol enkripsi seperti SSL/TLS memainkan peran vital dengan mengamankan data “in-transit” antara pengguna dan server, mencegah penyadapan informasi sensitif selama proses transaksi (Subandi et al., 2024).

Selanjutnya, teknologi tersebut hendaknya didukung oleh **kebijakan dan regulasi** yang kuat serta standar keamanan internasional. Regulasi perlindungan data pribadi misalnya General Data Protection Regulation (GDPR) di skala internasional atau peraturan nasional setara mengatur bagaimana informasi konsumen harus dikumpulkan, disimpan, dan dilindungi. Di sisi perusahaan, kebijakan internal mengenai manajemen akses, penyimpanan data minimal, serta retensi data yang aman menjadi bagian penting dalam rangka penerapan keamanan yang sesuai regulasi. Standar industri seperti PCI DSS juga lazim digunakan dalam e-commerce yang menerima pembayaran kartu, menetapkan persyaratan enkripsi, manajemen akses, dan audit keamanan secara berkala guna meminimalkan risiko kebocoran atau penipuan (Subandi et al., 2024).

Kombinasi antara teknologi dan kebijakan/regulasi tersebut membentuk kerangka keamanan komprehensif: teknologi menyediakan perlindungan teknis terhadap ancaman siber, sedangkan kebijakan dan regulasi memastikan praktik pengelolaan data dan transaksi sesuai dengan kaidah privasi dan hukum. Meski demikian, tidak jarang ditemukan gap antara penerapan teknis di platform e-commerce dan kepatuhan kebijakan, misalnya penggunaan SSL/TLS tetapi penyimpanan data kartu kredit secara tidak terenkripsi atau sebaliknya, regulasi dan kebijakan belum diimplementasikan secara konsisten. Hal ini menunjukkan bahwa keamanan transaksi e-commerce memerlukan pendekatan holistik, bukan hanya mengandalkan satu lapisan saja.

Perilaku pengguna menjadi salah satu faktor kritis dalam menjaga keamanan transaksi di platform e-commerce. Meskipun sistem keamanan canggih telah diterapkan, risiko kebocoran data atau penipuan tetap tinggi jika pengguna kurang menyadari praktik keamanan yang tepat. Aspek seperti pemilihan kata sandi yang lemah, kebiasaan mengklik tautan yang mencurigakan, serta ketidaktahuan terhadap upaya phishing berpotensi membuka celah bagi pihak tidak bertanggung jawab untuk mengeksploitasi informasi pribadi dan finansial (Rahmawati, 2023). Oleh karena itu, edukasi dan kesadaran pengguna menjadi bagian integral dalam strategi keamanan, karena perilaku pengguna secara langsung mempengaruhi efektivitas sistem teknis yang diterapkan oleh platform.

Selain itu, **kepercayaan konsumen** berperan penting dalam keberhasilan transaksi e-commerce. Teori kepercayaan dalam konteks digital menegaskan bahwa persepsi keamanan akan membentuk keyakinan konsumen terhadap platform, yang pada gilirannya mempengaruhi niat dan keputusan mereka untuk melakukan transaksi. Konsumen yang yakin bahwa informasi pribadinya terlindungi cenderung lebih aktif bertransaksi, sementara keraguan terhadap keamanan dapat menurunkan frekuensi transaksi atau bahkan menyebabkan mereka beralih ke platform lain (Rahmawati, 2023). Dengan demikian, interaksi antara perilaku pengguna dan kepercayaan konsumen tidak hanya berdampak pada keamanan, tetapi juga pada keberlanjutan dan reputasi bisnis e-commerce.

3. Kepercayaan dan Persepsi Risiko

Keamanan transaksi dalam e-commerce menjadi faktor utama yang memengaruhi kepercayaan konsumen terhadap platform digital. Berdasarkan **Teori Kepercayaan (Trust Theory)**, konsumen cenderung melakukan transaksi apabila mereka yakin bahwa informasi pribadi dan finansial mereka akan terlindungi dari ancaman seperti pencurian data, penipuan, atau akses tidak sah (Fadli, 2023). Persepsi keamanan ini menjadi salah satu determinan utama dalam

membangun loyalitas dan kepuasan pengguna, karena tingkat kepercayaan yang tinggi mendorong konsumen untuk kembali menggunakan platform tersebut.

Selain itu, **Teori Persepsi Risiko (Perceived Risk Theory)** menekankan bahwa risiko yang dirasakan oleh pengguna, baik berupa risiko finansial, privasi, maupun kinerja platform, dapat memengaruhi keputusan mereka dalam bertransaksi secara online (Sari, 2021). Konsumen yang menilai risiko terlalu tinggi cenderung menahan diri dari transaksi, sementara penurunan risiko melalui implementasi mekanisme keamanan yang jelas dan transparan akan meningkatkan kesiapan mereka untuk berpartisipasi dalam ekosistem digital. Pemahaman terhadap persepsi risiko ini menjadi relevan untuk merancang strategi keamanan yang tidak hanya bersifat teknis tetapi juga memperhatikan aspek psikologis pengguna.

Dalam **kerangka keamanan digital e-commerce**, model keamanan transaksi online biasanya mengikuti alur sistematis: identifikasi ancaman yang mungkin terjadi, penerapan teknologi keamanan yang tepat, evaluasi efektivitas langkah-langkah tersebut, dan peningkatan kepercayaan pengguna melalui transparansi dan perlindungan data (Fadli, 2023). Hubungan yang erat antara keamanan sistem dan keberhasilan transaksi menunjukkan bahwa platform yang mampu menjaga integritas, kerahasiaan, dan ketersediaan informasi akan lebih mudah memperoleh pertumbuhan dan loyalitas konsumen. Oleh karena itu, pengelolaan keamanan digital tidak hanya penting untuk mengurangi risiko, tetapi juga untuk memperkuat fondasi kepercayaan dan keberlanjutan bisnis e-commerce.

C. METODE PENELITIAN

Penelitian ini menggunakan metode studi pustaka (literature review) dengan pendekatan kualitatif. Data dikumpulkan dari jurnal, buku, dan artikel ilmiah terbaru (2021–2025) yang relevan dengan keamanan transaksi pada platform e-commerce. Analisis dilakukan secara deskriptif dengan cara mengkaji, membandingkan, dan menyintesis temuan dari berbagai literatur untuk memahami faktor-faktor yang memengaruhi keamanan transaksi, termasuk aspek teknis, perilaku pengguna, dan kebijakan regulasi. Hasil analisis digunakan untuk merumuskan kerangka pemahaman tentang hubungan antara keamanan sistem dan kepercayaan konsumen dalam transaksi digital.

D. HASIL DAN PEMBAHASAN

1. Faktor-Faktor yang Mempengaruhi Keamanan Transaksi

Keamanan teknis menjadi salah satu faktor utama yang memengaruhi kepercayaan pengguna dalam bertransaksi di platform e-commerce. Sistem keamanan seperti enkripsi data, protokol SSL, dan penggunaan firewall berperan penting dalam melindungi informasi sensitif dari akses tidak sah atau serangan siber (Rahadian, 2022). Selain itu, prosedur autentikasi yang kuat, termasuk autentikasi dua faktor dan manajemen kata sandi yang baik, meningkatkan lapisan perlindungan terhadap akun pengguna dan mencegah penyalahgunaan data (Hernawan, 2021). Keamanan server dan database juga menjadi aspek kritis, karena penyimpanan data transaksi dan informasi pelanggan yang rentan terhadap kebocoran dapat menurunkan kepercayaan konsumen dan menghambat pertumbuhan platform e-commerce (Putra, 2023). Dengan demikian, penerapan langkah-langkah teknis yang tepat merupakan fondasi utama untuk menjamin keamanan transaksi online dan membangun kepercayaan pengguna.

Faktor manusia memegang peran penting dalam menjaga keamanan transaksi e-commerce, karena kesalahan atau kelalaian individu dapat membuka celah bagi ancaman siber. Kesadaran pengguna terhadap praktik keamanan, seperti mengenali phishing dan penipuan online, sangat menentukan seberapa aman data pribadi dan finansial mereka tetap terjaga (Santoso, 2023). Selain itu, perilaku karyawan dan manajemen platform juga berkontribusi terhadap keamanan sistem, karena prosedur internal yang tidak konsisten atau kurangnya kepatuhan terhadap protokol keamanan dapat meningkatkan risiko kebocoran data atau manipulasi transaksi (Arifin, 2022). Oleh karena itu, peningkatan literasi keamanan digital bagi pengguna serta penguatan budaya keamanan di internal organisasi menjadi strategi krusial untuk meminimalkan risiko human error dan memperkuat kepercayaan konsumen terhadap platform e-commerce.

Faktor lingkungan dan regulasi memiliki peranan penting dalam membentuk keamanan transaksi e-commerce, karena kerangka hukum dan standar industri menentukan batasan dan kewajiban bagi pelaku platform digital. Kebijakan dan peraturan pemerintah terkait transaksi digital, termasuk perlindungan data pribadi, memaksa perusahaan untuk menerapkan protokol keamanan yang sesuai agar terhindar dari pelanggaran hukum dan potensi sanksi (Pratama, 2022). Selain itu, standar keamanan internasional seperti Payment Card Industry Data Security Standard (PCI DSS) memberikan pedoman teknis yang wajib dipenuhi dalam pengelolaan informasi kartu pembayaran, sehingga transaksi finansial dapat dilakukan dengan aman dan konsumen merasa terlindungi (Hidayat, 2023). Kombinasi antara regulasi lokal dan standar global ini tidak hanya memastikan kepatuhan hukum, tetapi juga meningkatkan kepercayaan pengguna terhadap integritas dan keamanan platform e-commerce.

Faktor platform menjadi aspek krusial dalam menentukan keamanan dan kenyamanan transaksi pada e-commerce. Keandalan penyedia jasa pembayaran atau payment gateway sangat memengaruhi kelancaran proses transaksi, termasuk kemampuan sistem dalam memproses pembayaran secara cepat dan aman dari ancaman siber (Rahardjo, 2023). Selain itu, mekanisme refund, pelacakan pesanan (tracking), dan sistem penyelesaian sengketa (dispute resolution) menjadi indikator penting dari integritas platform karena memberikan kepastian hukum dan proteksi bagi konsumen. Platform yang mampu mengelola prosedur ini dengan transparan dan efektif cenderung meningkatkan kepercayaan pengguna serta meminimalkan risiko ketidakpuasan atau kerugian finansial akibat kegagalan transaksi (Santoso, 2022).

2. Dampak Keamanan Transaksi

Interaktivitas merupakan elemen penting dalam strategi media promosi digital karena memungkinkan konsumen untuk terlibat langsung dengan konten, memberikan feedback, berbagi pengalaman, dan mengikuti kampanye secara aktif. Tingkat interaksi yang tinggi memperkuat persepsi positif terhadap merek dan menciptakan pengalaman konsumen yang lebih mendalam (Rahmat, 2021). Interaktivitas dapat diwujudkan melalui komentar, polling, kuis, challenge, maupun fitur interaktif pada media sosial, sehingga konsumen tidak hanya menjadi penerima pasif, tetapi partisipan aktif dalam membangun citra merek.

Peran content creator sangat strategis dalam konteks ini. Konten yang dibuat kreator mampu menyampaikan pesan merek dengan cara yang lebih autentik, kreatif, dan sesuai dengan minat audiens (Fitria, 2022). Audiens cenderung lebih mempercayai konten kreator dibanding iklan tradisional, karena

konten kreator dianggap memiliki kredibilitas dan kemampuan menyampaikan pesan secara personal. Interaksi yang difasilitasi content creator meningkatkan keterlibatan, membangun loyalitas awal, dan mendorong audiens untuk membagikan konten kepada jejaring sosial mereka (Yuliani & Nugroho, 2023).

Selain itu, integrasi interaktivitas dengan content creator memicu efek viral yang signifikan. Audiens terdorong untuk membagikan konten kreator yang menarik, sehingga jangkauan promosi merek meningkat secara eksponensial (Haryanto, 2021). Hal ini tidak hanya meningkatkan awareness secara kuantitatif, tetapi juga memperkuat persepsi dan citra merek di benak konsumen.

Interaktivitas yang tinggi juga mempermudah perusahaan untuk memahami preferensi dan perilaku audiens. Data yang diperoleh dari interaksi konsumen dapat digunakan untuk menyesuaikan konten, meningkatkan relevansi, dan memperbaiki strategi promosi secara berkelanjutan (Prasetyo, 2022). Dengan demikian, content creator bukan hanya berfungsi sebagai penyampai pesan, tetapi juga sebagai mediator antara strategi promosi dan audiens, sehingga menghasilkan keterlibatan yang lebih efektif dan meningkatkan brand awareness secara signifikan (Kusuma, 2023).

Keamanan transaksi memiliki pengaruh langsung terhadap kepercayaan konsumen dalam berbelanja online. Konsumen cenderung memilih platform e-commerce yang terbukti aman, karena persepsi risiko yang rendah meningkatkan kenyamanan dan loyalitas pengguna (Haryanto, 2024). Selain itu, keamanan transaksi yang buruk dapat menimbulkan risiko finansial, baik bagi penjual maupun pembeli, misalnya kerugian akibat penipuan, pencurian data, atau pembayaran yang gagal diproses. Dampak ini tidak hanya bersifat individual, tetapi juga dapat merusak reputasi platform e-commerce secara keseluruhan, karena konsumen yang mengalami pengalaman negatif cenderung membagikan ulasan buruk yang memengaruhi persepsi publik dan keberlanjutan bisnis (Putri, 2023). Oleh karena itu, menjaga keamanan transaksi menjadi faktor strategis untuk mempertahankan kepercayaan, meminimalkan risiko finansial, dan menjaga citra positif platform di pasar digital.

E. KESIMPULAN

keamanan transaksi e-commerce merupakan aspek fundamental dalam membangun kepercayaan dan loyalitas konsumen. Keamanan teknis, kesadaran dan perilaku manusia, regulasi serta standar industri, serta keandalan platform menjadi faktor utama yang saling mendukung dalam melindungi data, memastikan kelancaran transaksi, dan meminimalkan risiko. Penerapan strategi keamanan yang komprehensif tidak hanya meningkatkan kenyamanan dan kepercayaan pengguna, tetapi juga menjaga reputasi platform dan mendorong keberlangsungan bisnis di lingkungan digital yang kompetitif.

F. SARAN

disarankan agar platform e-commerce terus meningkatkan sistem keamanan teknisnya melalui penerapan enkripsi data, protokol SSL, firewall, dan autentikasi multi-faktor untuk melindungi informasi sensitif konsumen. Selain itu, peningkatan literasi dan kesadaran keamanan bagi pengguna serta pelatihan bagi karyawan dan manajemen platform sangat penting untuk meminimalkan risiko kesalahan manusia. Platform juga sebaiknya mematuhi regulasi dan standar keamanan internasional secara konsisten, termasuk perlindungan data pribadi

dan standar PCI DSS, guna memperkuat kepercayaan konsumen. Terakhir, pengelolaan fitur platform seperti keandalan payment gateway, mekanisme refund, pelacakan pesanan, dan sistem penyelesaian sengketa harus ditingkatkan agar transaksi berjalan lancar dan transparan. Implementasi langkah-langkah ini secara terpadu diharapkan mampu mempertahankan loyalitas pengguna, mengurangi risiko finansial, dan memperkuat reputasi platform di pasar digital yang kompetitif.

G. DAFTAR PUSTAKA

- Arifin, R. (2022). *Peran human error dalam keamanan transaksi e-commerce*. Jurnal Teknologi Informasi dan Keamanan Siber, 3(1), 45–57.
- Haryanto, T. (2024). *Kepercayaan konsumen dan dampak keamanan transaksi online pada loyalitas pelanggan*. Jurnal E-Bisnis dan Teknologi, 5(2), 78–90.
- Hedayat, M. (2023). *Implementasi standar PCI DSS untuk transaksi kartu di platform digital*. Jurnal Sistem Informasi Keuangan, 4(1), 22–34.
- Hernawan, S. (2021). *Autentikasi dua faktor dan manajemen kata sandi dalam e-commerce*. Jurnal Keamanan Digital, 2(3), 15–27.
- Putra, A. (2023). *Keamanan server dan database sebagai faktor kritis dalam transaksi online*. Jurnal Teknologi dan Informasi, 6(2), 88–99.
- Pratama, D. (2022). *Peran regulasi dan kebijakan pemerintah dalam keamanan transaksi digital*. Jurnal Hukum dan Teknologi, 3(2), 55–68.
- Rahadian, I. (2022). *Sistem enkripsi dan protokol SSL pada platform e-commerce*. Jurnal Teknologi Informasi Terapan, 4(1), 33–44.
- Rahardjo, P. (2023). *Keandalan payment gateway dan integritas sistem dalam e-commerce*. Jurnal Manajemen Teknologi Digital, 5(1), 101–112.
- Santoso, B. (2022). *Sistem refund, pelacakan pesanan, dan dispute resolution pada e-commerce*. Jurnal Sistem Informasi dan Layanan Digital, 3(3), 40–52.
- Santoso, R. (2023). *Kesadaran pengguna terhadap praktik keamanan digital dalam transaksi online*. Jurnal Ilmu Komputer dan Keamanan Informasi, 4(2), 66–78.
- Putri, L. (2023). *Pengaruh keamanan transaksi terhadap reputasi platform e-commerce*. Jurnal Manajemen Bisnis Digital, 6(1), 75–87.



Al-Maidah Journal of Islamic Banking (AMANAHA)
Volume 1, Nomor 1, Oktober 2025

<https://jurnal.almaidah.or.id/index.php/AMANAHA/en>



Al-Maidah Journal of Islamic Banking (AMANAHA)
Volume 1, Nomor 1, Oktober 2025