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

https://jurnal.almaidah.or.id/index.php/AMANAH/en

Evaluasi Aspek Keamanan pada e-Commerce serta Dampaknya terhadap Manfaat dan Risiko

Nur Azizah, Hendra, Amelia Puspitasari

Abstrak

Penelitian ini bertujuan untuk menganalisis keamanan e-Commerce dan implikasinya terhadap kelebihan dan kekurangan penggunaan platform e-Commerce. Peningkatan transaksi digital dan pertumbuhan pengguna e-Commerce menuntut pemahaman mendalam mengenai aspek keamanan agar dapat meminimalkan risiko sekaligus memaksimalkan manfaat platform. Metode penelitian yang digunakan adalah tinjauan pustaka, dengan mengkaji literatur dan penelitian terdahulu mengenai keamanan data, metode enkripsi, risiko penipuan online, perlindungan konsumen, serta dampaknya terhadap kelebihan dan kekurangan e-Commerce. Hasil penelitian menunjukkan bahwa penerapan sistem keamanan yang baik, seperti autentikasi ganda, enkripsi data, dan kebijakan privasi yang transparan, secara signifikan mempengaruhi kepercayaan pengguna, efisiensi transaksi, serta mengurangi potensi kerugian. Temuan ini menegaskan pentingnya integrasi aspek keamanan dalam pengembangan e-Commerce untuk memperkuat keunggulan platform, meminimalkan kelemahan, dan mendukung pengalaman transaksi digital yang aman dan optimal.

Kata kunci: *e-Commerce; keamanan digital; risiko transaksi; kelebihan dan kekurangan; perlindungan konsumen*

Abstract

This study aims to analyze e-Commerce security and its implications on the advantages and disadvantages of using e-Commerce platforms. The increasing number of digital transactions and the growth of e-Commerce users require a thorough understanding of security aspects to minimize risks while maximizing platform benefits. The research method used is a literature review, examining previous studies and literature on data security, encryption methods, online fraud risks, consumer protection, and their impact on the advantages and disadvantages of e-Commerce. The results indicate that the implementation of robust security systems, such as two-factor authentication, data encryption, and transparent privacy policies, significantly influences user trust, transaction efficiency, and reduces potential losses. These findings emphasize the importance of integrating security aspects into e-Commerce development to strengthen platform advantages, minimize weaknesses, and support a safe and optimal digital transaction experience.

Keywords: *e-Commerce; digital security; transaction risks; advantages and disadvantages; consumer protection*

A. PENDAHULUAN

Perkembangan teknologi informasi telah mendorong pertumbuhan e-Commerce sebagai salah satu metode transaksi yang tidak hanya efisien tetapi juga mudah diakses oleh masyarakat luas. Transformasi digital yang pesat, didorong oleh penetrasi internet yang semakin tinggi dan kemudahan akses melalui perangkat mobile, menjadikan e-Commerce sebagai platform utama bagi konsumen untuk membeli produk maupun jasa tanpa batasan lokasi dan waktu (Santoso, 2023). Kondisi ini memungkinkan pelaku usaha, baik skala mikro maupun besar, untuk menjangkau pasar yang lebih luas, mempercepat proses transaksi, serta mengefisiensikan operasional bisnis mereka. Keunggulan-keunggulan ini menjadikan e-Commerce tidak sekadar sebagai alternatif perdagangan tradisional, tetapi sebagai ekosistem digital yang mampu mendorong pertumbuhan ekonomi, terutama di era ekonomi berbasis digital (Wijaya & Prasetyo, 2022).

Selain kemudahan akses dan efisiensi, e-Commerce juga menawarkan keuntungan strategis bagi pelaku usaha. Dengan adanya platform digital, pedagang dapat memanfaatkan data konsumen untuk melakukan segmentasi pasar, mengembangkan strategi pemasaran yang lebih tepat sasaran, dan meningkatkan loyalitas pelanggan melalui layanan yang lebih personal. Di sisi konsumen, e-Commerce memberikan fleksibilitas untuk membandingkan produk, memanfaatkan diskon, dan melakukan pembelian secara instan. Kelebihan-kelebihan ini menjadikan e-Commerce sebagai pilihan utama dalam berbagai aktivitas perdagangan modern, sekaligus membuka peluang bagi inovasi layanan dan pengembangan teknologi digital yang lebih canggih.

Namun, di balik kelebihan tersebut, e-Commerce juga menghadapi tantangan signifikan yang dapat memengaruhi pengalaman pengguna dan keberlangsungan platform itu sendiri. Salah satu tantangan yang paling krusial adalah **keamanan digital**. Setiap transaksi online melibatkan pertukaran data yang bersifat sensitif, termasuk informasi pribadi, nomor kartu kredit, dan detail finansial lainnya, sehingga potensi risiko seperti kebocoran data, penipuan, akses tidak sah, hingga peretasan menjadi ancaman nyata (Haryanto, 2021). Risiko-risiko ini tidak hanya dapat menurunkan kepercayaan konsumen, tetapi juga dapat merusak reputasi platform, bahkan memicu kerugian finansial bagi pelaku usaha dan konsumen. Fenomena ini menunjukkan bahwa keamanan bukan sekadar isu teknis, melainkan faktor strategis yang menentukan keberhasilan dan daya saing e-Commerce di pasar digital.

Perkembangan teknologi informasi telah mendorong pertumbuhan e-Commerce sebagai metode transaksi yang efisien dan mudah diakses oleh masyarakat luas. Peningkatan penggunaan internet dan perangkat digital menjadikan e-Commerce platform utama bagi konsumen untuk membeli produk maupun jasa, memungkinkan pelaku usaha menjangkau pasar yang lebih luas dan mempercepat proses transaksi (Santoso, 2023). Keunggulan tersebut termasuk kemudahan akses, penghematan waktu, serta potensi peningkatan volume penjualan bagi pelaku usaha, sekaligus memberikan fleksibilitas bagi konsumen dalam membandingkan produk dan melakukan pembelian secara instan (Wijaya & Prasetyo, 2022). Di sisi lain, e-Commerce menghadapi tantangan signifikan, khususnya terkait keamanan digital, karena setiap transaksi online melibatkan pertukaran data sensitif seperti informasi pribadi dan data keuangan, yang berisiko mengalami kebocoran, penipuan, atau akses tidak sah (Haryanto, 2021). Risiko-risiko ini dapat menurunkan kepercayaan konsumen, merusak reputasi platform,

dan menimbulkan kerugian finansial bagi pengguna dan pelaku usaha, sehingga keamanan menjadi faktor strategis yang menentukan keberhasilan platform. Penelitian sebelumnya menekankan aspek teknis keamanan, seperti enkripsi data, autentikasi ganda, dan kebijakan privasi transparan (Rahman, 2022; Lestari & Nugroho, 2021), namun fokus pada implikasi keamanan terhadap persepsi pengguna mengenai kelebihan dan kekurangan e-Commerce masih terbatas

Dalam hal ini, penelitian ini hadir untuk memberikan analisis yang lebih komprehensif mengenai keamanan e-Commerce dan implikasinya terhadap kelebihan dan kekurangan platform. Dengan memeriksa literatur terbaru, penelitian ini mencoba menggambarkan bagaimana strategi keamanan yang diterapkan dapat membentuk persepsi pengguna, meningkatkan kepercayaan, serta mengoptimalkan pengalaman transaksi digital. Hal ini juga menjadi dasar bagi pelaku usaha dan pengembang platform untuk merancang mekanisme keamanan yang lebih efektif dan sesuai kebutuhan pengguna.

Kontribusi penelitian ini terletak pada pemaparan hubungan antara praktik keamanan dan evaluasi kelebihan serta kekurangan e-Commerce secara terintegrasi. Temuan yang diperoleh diharapkan dapat memberikan rekomendasi strategis bagi pengelola platform dalam merancang sistem keamanan, sekaligus memperkaya literatur akademik mengenai manajemen risiko digital dan pengalaman konsumen di era e-Commerce. Dengan pendekatan ini, penelitian menawarkan perspektif yang lebih menyeluruh dibandingkan studi sebelumnya yang hanya berfokus pada aspek teknis atau aspek manfaat secara parsial.

B. KAJIAN TEORI

1. keamanan E-Commerce

Keamanan e-Commerce merupakan salah satu aspek paling krusial dalam pengelolaan transaksi digital, karena setiap aktivitas perdagangan daring melibatkan pertukaran informasi yang bersifat sensitif, termasuk data pribadi, informasi pembayaran, dan riwayat transaksi pengguna (Prasetya & Ramadhan, 2023). Risiko kebocoran data, peretasan, dan penyalahgunaan informasi dapat menurunkan kepercayaan konsumen sekaligus mengancam keberlangsungan platform. Oleh karena itu, penerapan mekanisme keamanan yang memadai menjadi kebutuhan utama bagi penyedia layanan e-Commerce. Secara konseptual, keamanan e-Commerce mencakup prinsip-prinsip dasar yang melindungi integritas, kerahasiaan, dan ketersediaan data (Setiawan, 2022). Integritas memastikan bahwa informasi yang disimpan dan dikirimkan melalui sistem tetap akurat dan tidak dimanipulasi, sementara kerahasiaan menjaga agar data hanya dapat diakses oleh pihak yang berwenang. Ketersediaan menjamin bahwa sistem tetap dapat digunakan oleh pengguna kapan saja tanpa gangguan signifikan akibat serangan atau kegagalan teknis.

Dalam praktiknya, berbagai teknologi dan mekanisme diterapkan untuk menjaga keamanan e-Commerce. Enkripsi data menjadi salah satu metode yang paling sering digunakan, di mana informasi sensitif dikodekan sehingga hanya pihak yang memiliki kunci dekripsi yang dapat membacanya (Santika & Utama, 2022). Selain itu, autentikasi ganda atau two-factor authentication (2FA) digunakan untuk memastikan bahwa pengguna yang mengakses akun adalah pemilik sahnya, sehingga mengurangi risiko akses tidak sah. Sistem firewall juga berperan dalam membatasi akses ke jaringan internal platform dan mencegah serangan siber dari pihak luar. Tidak kalah penting, kebijakan privasi yang transparan dan mudah dipahami oleh pengguna membantu membangun kepercayaan, karena

konsumen mengetahui bagaimana data mereka dikumpulkan, disimpan, dan digunakan (Hadi & Gunawan, 2023).

Keamanan digital yang kuat tidak hanya melindungi data, tetapi juga berperan dalam membentuk persepsi pengguna terhadap platform. Tingkat keamanan yang tinggi dapat meningkatkan kepercayaan dan loyalitas konsumen, sementara celah keamanan dapat memunculkan ketidakpuasan, persepsi negatif, dan bahkan berpindahnya pengguna ke platform lain yang lebih aman (Fauzi & Rahardjo, 2023). Dalam hal ini, keamanan e-Commerce menjadi faktor strategis yang memengaruhi keberhasilan dan keberlanjutan platform, karena aspek teknis dan manajerial saling berkaitan. Integrasi prinsip keamanan, teknologi, dan kebijakan operasional yang efektif memungkinkan e-Commerce untuk memaksimalkan kelebihan platform, sekaligus meminimalkan risiko dan kelemahan yang mungkin dirasakan pengguna.

2. Persepsi Pengguna Dan Kepercayaan Digital

Kepercayaan pengguna merupakan salah satu faktor penentu dalam kesuksesan e-Commerce karena transaksi daring sangat bergantung pada persepsi konsumen terhadap keamanan, kenyamanan, dan keandalan platform (Amelia & Putra, 2023). Teori persepsi pengguna dan kepercayaan digital menekankan bahwa tingkat keamanan yang dirasakan oleh pengguna secara langsung memengaruhi sikap mereka terhadap platform, termasuk keputusan untuk melakukan pembelian, frekuensi penggunaan, dan loyalitas jangka panjang. Persepsi keamanan bukan hanya ditentukan oleh teknologi yang diterapkan, tetapi juga oleh transparansi kebijakan, reputasi platform, dan pengalaman sebelumnya dalam bertransaksi secara online. Dengan kata lain, meskipun sistem keamanan teknis telah diterapkan secara optimal, jika pengguna merasa kurang aman atau tidak memahami kebijakan privasi, tingkat kepercayaan mereka tetap dapat menurun.

Selain keamanan teknis, interaksi pengguna dengan antarmuka dan pengalaman layanan juga memengaruhi persepsi kepercayaan. Proses transaksi yang mudah, responsif, dan bebas dari gangguan teknis memberikan rasa aman dan kenyamanan bagi pengguna, yang kemudian berdampak pada keputusan mereka untuk menggunakan platform secara berulang (Saputra & Handayani, 2022). Sebaliknya, kesalahan sistem, keterlambatan respons, atau insiden kebocoran data dapat merusak persepsi kepercayaan dan menimbulkan persepsi negatif terhadap kelebihan platform. Dengan demikian, hubungan antara keamanan, pengalaman pengguna, dan keputusan transaksi menjadi sangat penting untuk dipahami, karena aspek ini menjembatani dimensi teknis dan psikologis dari penggunaan e-Commerce.

Lebih lanjut, teori ini juga dapat digunakan untuk menjelaskan bagaimana aspek keamanan digital memengaruhi evaluasi pengguna terhadap kelebihan dan kekurangan e-Commerce. Misalnya, platform dengan tingkat keamanan tinggi cenderung dipersepsikan lebih unggul dalam hal keandalan dan kenyamanan, sementara platform yang memiliki celah keamanan sering dianggap memiliki kelemahan signifikan meski menawarkan kelebihan lain seperti harga murah atau variasi produk yang lengkap

3. Keunggulan dan Kelemahan E-Commerce

e-Commerce sebagai metode perdagangan digital menawarkan berbagai keunggulan yang menjadikannya pilihan utama bagi konsumen dan pelaku usaha di era modern. Salah satu kelebihan utama adalah efisiensi operasional, di mana

transaksi dapat dilakukan kapan saja dan di mana saja tanpa batasan geografis, sehingga menghemat waktu dan biaya bagi semua pihak yang terlibat (Rahmawati & Ardiansyah, 2023). Selain itu, e-Commerce menyediakan aksesibilitas yang lebih luas bagi konsumen, memungkinkan mereka untuk menjelajahi berbagai produk dan layanan dengan mudah melalui perangkat digital. Kelebihan lain yang signifikan adalah peningkatan jangkauan pasar bagi pelaku usaha, termasuk UMKM, karena platform digital memungkinkan mereka menembus pasar nasional maupun internasional tanpa harus memiliki toko fisik yang luas (Halim & Sari, 2022).

Meski demikian, e-Commerce juga menghadirkan sejumlah kelemahan yang tidak dapat diabaikan. Risiko keamanan, seperti kebocoran data, peretasan, dan penipuan transaksi online, menjadi salah satu kelemahan yang paling menonjol dan berpotensi mengurangi kepercayaan konsumen (Wijayanti & Fauzan, 2023). Selain itu, keterbatasan teknis, termasuk gangguan server, antarmuka yang tidak ramah pengguna, dan masalah kompatibilitas perangkat, dapat menghambat pengalaman transaksi dan menimbulkan frustrasi bagi pengguna. Hambatan-hambatan ini menunjukkan bahwa meskipun e-Commerce menawarkan berbagai manfaat, keberhasilan platform tetap sangat tergantung pada kemampuan pengelola untuk menjaga kualitas layanan dan keamanan digital.

Teori keunggulan dan kelemahan e-Commerce ini juga berperan dalam menghubungkan aspek teknis keamanan dengan persepsi pengguna terhadap platform. Pengguna cenderung menilai platform lebih unggul jika keamanan digital terjamin, transaksi lancar, dan layanan konsisten, sementara kelemahan teknis atau celah keamanan dapat menurunkan persepsi positif terhadap kelebihan platform. Dengan kata lain, evaluasi pengguna terhadap manfaat dan kekurangan e-Commerce tidak hanya didasarkan pada fitur atau variasi produk, tetapi juga pada sejauh mana platform mampu menjamin keamanan, kenyamanan, dan keandalan transaksi digital (Pratama & Kurniawan, 2022). Pemahaman ini memberikan dasar bagi pengembang dan pelaku usaha untuk mengintegrasikan strategi keamanan dan peningkatan layanan, sehingga keunggulan e-Commerce dapat dimaksimalkan dan kelemahannya diminimalkan.

C. METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan pendekatan **studi pustaka**, yaitu pengumpulan dan analisis informasi dari jurnal ilmiah, buku, dan publikasi akademik yang relevan dengan keamanan e-Commerce, persepsi pengguna, serta kelebihan dan kekurangan platform digital. Metode ini dipilih untuk memahami konsep secara mendalam melalui interpretasi teoritis dan analisis komprehensif terhadap literatur yang ada (Amir & Putri, 2023).

Proses penelitian meliputi beberapa tahap, yaitu: pertama, identifikasi topik dan fokus penelitian; kedua, pencarian literatur yang valid dan terkini melalui database akademik seperti Scopus, Google Scholar, dan perpustakaan digital universitas; ketiga, pengelompokan tema utama yang berkaitan dengan keamanan digital, persepsi pengguna, serta kelebihan dan kelemahan e-Commerce; keempat, analisis isi dan interpretasi teoritis terhadap temuan dalam literatur; dan kelima, sintesis teori untuk menarik kesimpulan mengenai hubungan antara keamanan e-Commerce dan persepsi pengguna terhadap kelebihan dan kekurangan platform digital (Hendrawan, 2022).

D. HASIL DAN PEMBAHASAN

1. Analisis Keamanan e-Commerce

Keamanan dalam e-Commerce merupakan aspek fundamental yang memengaruhi kepercayaan pengguna dan keberlangsungan platform digital. Setiap transaksi daring melibatkan pertukaran data yang bersifat sensitif, termasuk informasi pribadi, detail pembayaran, dan riwayat transaksi. Oleh karena itu, platform e-Commerce perlu menerapkan mekanisme dan teknologi keamanan yang komprehensif untuk meminimalkan risiko kebocoran data, peretasan, dan penipuan (Santoso & Farhan, 2023). Dalam praktiknya, berbagai teknologi telah diterapkan untuk menjaga keamanan sistem, di antaranya enkripsi data, autentikasi ganda, firewall, dan kebijakan privasi yang transparan.

Enkripsi data menjadi metode utama dalam melindungi informasi sensitif. Proses enkripsi mengubah data asli menjadi kode yang hanya dapat dibaca oleh pihak yang memiliki kunci dekripsi. Dengan enkripsi, bahkan jika data berhasil diakses oleh pihak tidak sah, informasi tersebut tetap tidak dapat dimanfaatkan secara langsung. Teknologi ini dapat diterapkan pada berbagai lapisan, mulai dari penyimpanan data di server hingga transmisi data melalui jaringan internet (Herlina & Santika, 2022). Selain itu, algoritma enkripsi modern seperti AES (Advanced Encryption Standard) dan RSA memungkinkan tingkat keamanan tinggi sekaligus menjaga kecepatan transaksi, sehingga pengalaman pengguna tidak terganggu. Enkripsi bukan hanya mekanisme teknis, tetapi juga strategi untuk membangun kepercayaan pengguna, karena konsumen merasa data mereka dilindungi secara efektif.

Selain enkripsi, autentikasi ganda (two-factor authentication/2FA) menjadi lapisan tambahan yang penting. Autentikasi ini memastikan bahwa hanya pemilik sah akun yang dapat mengakses informasi atau melakukan transaksi. Biasanya, 2FA menggabungkan sesuatu yang diketahui pengguna (misal password) dengan sesuatu yang dimiliki pengguna (misal kode OTP melalui SMS atau aplikasi authenticator). Pendekatan ini secara signifikan mengurangi risiko akses tidak sah atau penyalahgunaan akun, terutama dalam kasus serangan phishing atau pencurian kredensial (Arifin & Wulandari, 2023). Penelitian sebelumnya menunjukkan bahwa platform e-Commerce yang menerapkan autentikasi ganda cenderung memiliki tingkat kepercayaan pengguna lebih tinggi dan tingkat insiden penipuan transaksi yang lebih rendah.

Firewall juga memainkan peran penting dalam menjaga integritas sistem e-Commerce. Fungsi utama firewall adalah memonitor dan membatasi lalu lintas jaringan yang masuk dan keluar, mencegah akses tidak sah dari pihak eksternal, serta melindungi server dari serangan siber seperti Distributed Denial of Service (DDoS). Firewall dapat dikombinasikan dengan sistem deteksi intrusi (Intrusion Detection System/IDS) untuk meningkatkan kemampuan platform dalam merespons potensi ancaman secara real-time. Dengan penerapan firewall yang tepat, risiko gangguan operasional dan peretasan dapat diminimalkan, sehingga platform dapat

terus melayani transaksi secara stabil dan aman (Putra & Handayani, 2022).

Selain aspek teknis, kebijakan privasi yang jelas dan transparan juga menjadi bagian penting dari strategi keamanan e-Commerce. Pengguna perlu mengetahui bagaimana data mereka dikumpulkan, disimpan, dan digunakan oleh platform. Transparansi ini tidak hanya meningkatkan kesadaran pengguna, tetapi juga membangun kepercayaan, karena konsumen merasa memiliki kendali terhadap informasi pribadi mereka. Beberapa penelitian menunjukkan bahwa ketidakjelasan dalam kebijakan privasi dapat menurunkan kepercayaan pengguna dan membuat mereka enggan melakukan transaksi daring, meskipun sistem teknis platform sudah aman (Rahardjo & Amelia, 2023).

Integrasi dari keempat mekanisme keamanan tersebut enkripsi, autentikasi ganda, firewall, dan kebijakan privasi menciptakan lingkungan transaksi digital yang lebih aman dan andal. Secara teori, pendekatan ini mencerminkan prinsip CIA (Confidentiality, Integrity, Availability) dalam keamanan informasi, di mana kerahasiaan, integritas, dan ketersediaan data dijaga secara simultan. Kerahasiaan dicapai melalui enkripsi dan kontrol akses, integritas melalui sistem monitoring dan autentikasi, sedangkan ketersediaan melalui perlindungan firewall dan pemeliharaan sistem yang optimal (Herlina & Santika, 2022). Dengan penerapan prinsip ini secara konsisten, platform e-Commerce dapat meminimalkan potensi kerugian bagi pengguna sekaligus menjaga reputasi dan keberlanjutan bisnis.

Lebih jauh, mekanisme keamanan ini tidak hanya berfungsi secara teknis tetapi juga memengaruhi persepsi pengguna terhadap platform. Pengguna yang merasakan keamanan dan perlindungan yang memadai cenderung menilai platform lebih unggul dan merasa nyaman untuk melakukan transaksi berulang. Sebaliknya, jika terdapat celah keamanan, persepsi negatif muncul dan dapat menurunkan loyalitas pengguna, meskipun platform tersebut memiliki keunggulan lain seperti harga bersaing atau variasi produk yang lengkap (Fauzan & Nugroho, 2023).

2. Persepsi Pengguna terhadap Keamanan

Keamanan dalam platform e-Commerce memiliki pengaruh yang signifikan terhadap persepsi pengguna, yang selanjutnya membentuk tingkat kepercayaan dan loyalitas mereka. Persepsi pengguna terbentuk berdasarkan pengalaman mereka saat menggunakan platform, termasuk kemudahan transaksi, transparansi kebijakan privasi, serta penerapan mekanisme keamanan yang efektif (Hidayat & Larasati, 2023). Tingkat keamanan yang dirasakan tinggi dapat meningkatkan keyakinan pengguna bahwa informasi pribadi dan data finansial mereka terlindungi dengan baik. Kepercayaan ini tidak hanya menciptakan kenyamanan psikologis bagi pengguna, tetapi juga mendorong mereka untuk melakukan transaksi lebih sering, serta mempertahankan interaksi jangka panjang dengan platform (Saputra & Rizky, 2022).

Konsep ini selaras dengan teori Trust and Risk Perception in Digital Commerce, yang menyatakan bahwa persepsi risiko merupakan faktor utama yang memengaruhi keputusan pengguna dalam transaksi daring. Ketika risiko dianggap rendah karena mekanisme keamanan yang baik, pengguna cenderung memiliki kepercayaan lebih tinggi, sementara risiko yang tinggi akan menimbulkan kekhawatiran dan potensi penurunan loyalitas. Misalnya, pengguna yang menyadari bahwa platform menerapkan enkripsi data, autentikasi ganda, dan firewall yang efektif akan menilai platform tersebut aman, sehingga mereka lebih bersedia untuk melakukan pembelian berulang dan merekomendasikan platform kepada orang lain (Ardi & Fitriani, 2023).

Lebih lanjut, pengalaman transaksi yang aman berperan penting dalam membentuk loyalitas pengguna. Keamanan bukan hanya dimaknai sebagai perlindungan data, tetapi juga sebagai indikator profesionalisme dan kualitas layanan platform. Pengalaman transaksi yang lancar, tanpa gangguan teknis atau insiden keamanan, menciptakan rasa puas yang memperkuat loyalitas pengguna. Sebaliknya, insiden kebocoran data atau akses tidak sah dapat menimbulkan persepsi negatif, menurunkan kepercayaan, dan membuat pengguna beralih ke platform lain yang dianggap lebih aman. Hal ini menunjukkan bahwa keamanan e-Commerce memiliki peran strategis dalam menghubungkan aspek teknis dengan perilaku konsumen, khususnya dalam konteks loyalitas dan retensi pengguna (Wijaya & Haryanto, 2023).

Selain itu, hubungan antara keamanan dan pengalaman pengguna juga mencakup keputusan pengguna untuk tetap menggunakan platform dalam jangka panjang. Platform yang mampu menjaga keamanan transaksi secara konsisten dan transparan cenderung dipersepsikan lebih handal dan profesional. Keandalan ini mendorong pengguna untuk mempercayai platform dalam transaksi bernilai tinggi, termasuk pembelian produk dengan harga mahal atau penggunaan layanan berlangganan digital. Sebaliknya, celah keamanan yang berulang atau kurangnya transparansi dapat memicu ketidakpercayaan dan menurunkan tingkat retensi pengguna (Putri & Mahendra, 2022). Dengan kata lain, keamanan digital tidak hanya memengaruhi persepsi awal pengguna, tetapi juga membentuk pola keputusan mereka dalam jangka panjang, termasuk kesediaan untuk tetap menggunakan platform dan loyalitas terhadap layanan yang diberikan.

Lebih jauh lagi, literatur menunjukkan bahwa kepercayaan dan loyalitas pengguna berkorelasi erat dengan keuntungan kompetitif platform e-Commerce. Tingkat keamanan yang tinggi dapat menjadi pembeda utama di antara platform yang menawarkan produk serupa, karena pengguna cenderung memilih platform yang mereka anggap paling aman. Dengan demikian, keamanan digital tidak hanya merupakan elemen teknis, tetapi juga strategi bisnis yang memengaruhi persepsi nilai platform, kepuasan konsumen, dan kemampuan platform untuk mempertahankan pengguna dalam lingkungan persaingan yang ketat (Handayani & Prasetyo, 2023).

3. Implikasi Keamanan terhadap Kelebihan dan Kekurangan e-Commerce

Keamanan digital merupakan faktor kunci yang memengaruhi persepsi pengguna terhadap kelebihan dan kelemahan platform e-Commerce. Dari sisi kelebihan, mekanisme keamanan yang efektif berkontribusi pada peningkatan efisiensi, karena pengguna merasa transaksi dapat dilakukan dengan cepat dan aman tanpa harus memikirkan risiko kehilangan data atau penipuan. Efisiensi ini tercermin pada kelancaran proses pembayaran, konfirmasi pesanan, dan integrasi sistem yang memungkinkan transaksi dilakukan kapan saja dan di mana saja. Selain itu, keamanan yang kuat mendukung aksesibilitas platform, karena pengguna lebih percaya untuk mengakses layanan e-Commerce melalui berbagai perangkat digital, baik desktop maupun mobile, tanpa rasa khawatir terhadap potensi ancaman siber (Yuliana & Prasetyo, 2023). Keamanan juga meningkatkan jangkauan pasar, terutama bagi UMKM atau pelaku usaha kecil yang memanfaatkan platform digital untuk menembus pasar lebih luas, termasuk konsumen internasional. Pengguna yang merasakan keamanan yang memadai cenderung lebih percaya diri untuk melakukan transaksi lintas wilayah dan berinteraksi dengan berbagai fitur e-Commerce yang tersedia.

Sebaliknya, dari sisi kelemahan, keamanan digital yang rendah atau tidak konsisten dapat memperbesar risiko yang dirasakan pengguna, seperti risiko kebocoran data, gangguan teknis, dan pengalaman transaksi yang buruk. Risiko ini menjadi salah satu faktor yang secara langsung memengaruhi persepsi pengguna terhadap kelemahan platform. Misalnya, meskipun platform menawarkan harga kompetitif, variasi produk yang lengkap, dan sistem navigasi yang mudah, jika terdapat celah keamanan yang menyebabkan kebocoran informasi atau penipuan, pengguna akan menilai platform sebagai tidak andal. Hal ini menunjukkan bahwa keamanan digital bukan sekadar aspek teknis, tetapi juga merupakan indikator kualitas layanan yang memengaruhi evaluasi pengguna secara keseluruhan (Rohman & Anggraini, 2022).

Hubungan antara aspek teknis keamanan dan persepsi keunggulan atau kelemahan platform dapat dijelaskan melalui konsep Information Security and Consumer Trust Framework. Kerahasiaan data yang dijaga melalui enkripsi, integritas yang terjaga melalui autentikasi ganda, dan ketersediaan layanan melalui firewall dan pemeliharaan sistem yang optimal, semuanya membentuk persepsi pengguna bahwa platform mampu memberikan layanan yang efisien, aman, dan handal. Sebaliknya, jika salah satu aspek ini tidak dijaga, misalnya kebijakan privasi tidak jelas atau autentikasi pengguna lemah, persepsi positif terhadap kelebihan platform dapat menurun, sementara kelemahan platform akan menjadi lebih nyata bagi pengguna (Santosa & Wirawan, 2023).

Lebih jauh, integrasi keamanan teknis dengan pengalaman pengguna secara langsung memengaruhi evaluasi pengguna terhadap nilai platform. Pengguna menilai keunggulan platform tidak hanya dari fitur dan

layanan yang ditawarkan, tetapi juga dari sejauh mana platform dapat menjamin keamanan transaksi dan data pribadi mereka. Dengan kata lain, keamanan digital berfungsi sebagai jembatan antara kelebihan teknis dan persepsi subjektif pengguna. Misalnya, platform yang aman memungkinkan pengguna untuk merasakan manfaat efisiensi dan aksesibilitas secara maksimal, sementara platform yang kurang aman akan menurunkan persepsi kelebihan sekaligus menonjolkan kelemahan yang ada.

Selain itu, keamanan digital juga memiliki efek jangka panjang terhadap loyalitas dan keputusan penggunaan platform. Platform yang berhasil mengintegrasikan aspek teknis keamanan dengan pengalaman pengguna yang positif cenderung memperoleh persepsi keunggulan yang konsisten dari pengguna, sehingga meningkatkan kemungkinan transaksi berulang dan loyalitas jangka panjang. Hal ini menunjukkan bahwa keamanan bukan hanya faktor mitigasi risiko, tetapi juga strategi untuk memperkuat posisi platform di pasar digital yang kompetitif (Putra & Fadilah, 2023).

E. KESIMPULAN

Keamanan e-Commerce memainkan peran sentral dalam membentuk persepsi, kepercayaan, dan loyalitas pengguna terhadap platform digital. Penerapan mekanisme keamanan seperti enkripsi data, autentikasi ganda, firewall, dan kebijakan privasi yang transparan tidak hanya melindungi informasi sensitif pengguna, tetapi juga meningkatkan efisiensi, aksesibilitas, dan jangkauan pasar platform. Tingkat keamanan yang tinggi memungkinkan pengguna merasa nyaman melakukan transaksi, meminimalkan risiko kebocoran data, gangguan teknis, atau pengalaman negatif, sekaligus memperkuat penilaian terhadap keunggulan platform. Sebaliknya, celah keamanan dapat menurunkan kepercayaan, menimbulkan persepsi kelemahan, dan memengaruhi loyalitas pengguna. Dengan demikian, keamanan digital berfungsi sebagai penghubung antara aspek teknis dan persepsi subjektif pengguna, memengaruhi keputusan penggunaan jangka panjang, sekaligus menjadi strategi penting dalam mempertahankan posisi kompetitif e-Commerce. Secara keseluruhan, integrasi keamanan teknis dengan pengalaman pengguna yang positif menjadi faktor kunci bagi keberhasilan dan keberlanjutan platform digital, mirip dengan bagaimana digital marketing dan strategi promosi online berperan dalam meningkatkan visibilitas serta memperluas jangkauan pasar bagi UMKM; keduanya menunjukkan bahwa pengelolaan strategis aspek inti baik keamanan maupun promosi mampu memperkuat keunggulan, membangun kepercayaan, dan mendorong pertumbuhan berkelanjutan di era digital modern.

F. SARAN

Platform e-Commerce disarankan untuk terus memperkuat mekanisme keamanan digital, termasuk enkripsi data, autentikasi ganda, firewall, dan kebijakan privasi yang transparan. Peningkatan kapasitas teknis dan evaluasi rutin terhadap sistem keamanan perlu dilakukan agar perlindungan terhadap data pengguna selalu optimal. Dengan penerapan keamanan yang lebih terintegrasi dan konsisten, platform dapat meningkatkan kepercayaan, memperkuat loyalitas pengguna, serta memaksimalkan keunggulan platform sekaligus meminimalkan kelemahan yang berpotensi mengganggu pengalaman transaksi.

G. DAFTAR PUSTAKA

Amir, F., & Putri, S. (2023). *Digital security and consumer perception in e-commerce platforms*. Jakarta: Pustaka Ilmu Digital.

Ardi, R., & Fitriani, L. (2023). Trust and risk perception in digital commerce platforms. *Journal of E-Commerce Studies, 8*(2), 33–51.

Amelia, R., & Putra, Y. (2023). *User trust and perception in digital commerce platforms*. Surabaya: Graha Ilmu Digital.

Fauzi, R., & Rahardjo, B. (2023). *Consumer trust and digital security in online commerce*. Bandung: Pustaka Digital.

Halim, A., & Sari, D. (2022). *Market expansion and accessibility in online retail platforms*. Jakarta: Media Ilmu Digital.

Handayani, F., & Prasetyo, H. (2023). The role of security in building user loyalty in online transactions. *International Journal of Digital Business Security, 6*(1), 20–38.

Hadi, S., & Gunawan, T. (2023). Privacy policies and user trust in e-commerce platforms. *Journal of Digital Business Security, 6*(1), 15–28.

Hidayat, T., & Larasati, R. (2023). User perception and trust in e-commerce: A literature review. *Journal of Online Consumer Behavior, 7*(1), 15–32.

Hendrawan, R. (2022). Methods of literature review in information systems research. *Journal of Research Methodology in Digital Economy, 5*(2), 22–38.

Nurhadi, A. (2023). Conceptual framework of e-commerce security and user trust. *Indonesian Journal of E-Business Studies, 9*(1), 15–29.

Prasetya, D., & Ramadhan, A. (2023). E-commerce security: Principles and implementation strategies. *Indonesian Journal of Information Technology, 12*(2), 45–60.

Pratama, R., & Kurniawan, B. (2022). User evaluation of e-commerce advantages and limitations. *Journal of Online Business Studies, 7*(1), 28–44.

Putra, R., & Fadilah, S. (2023). The impact of digital security on perceived platform advantages and disadvantages. *Journal of E-Commerce and Digital Services, 6*(2), 33–52.

Rahmawati, L., & Ardiansyah, T. (2023). Efficiency and operational benefits in digital commerce. *Indonesian Journal of E-Business Research, 8*(2), 55–70.

Rohman, A., & Anggraini, L. (2022). User evaluation of e-commerce platforms: Security as a determinant factor. *Indonesian Journal of Online Business Studies, 7*(3), 45–63.

Santika, P., & Utama, L. (2022). Data encryption and access control in online retail systems. *International Journal of Cybersecurity Studies, 4*(3), 33–49.

Santosa, D., & Wirawan, T. (2023). Integrating information security and user perception in digital commerce. *Journal of Information Security Research, 5*(1), 21–40.

Setiawan, F. (2022). Core principles of information security in digital commerce. *Journal of E-Business Research, 9*(2), 22–37.

Wijaya, H., & Haryanto, B. (2023). Consumer loyalty and security in online retail platforms. *Journal of E-Business and Digital Economy, 9*(1), 10–28.

Wijayanti, N., & Fauzan, M. (2023). Risks and limitations in online retail transactions. *Journal of Information Systems and Digital Economy, 6*(3), 40–58.

Yuliana, F., & Prasetyo, H. (2023). Digital security and market reach in e-commerce: A conceptual review. *International Journal of Digital Commerce Research, 4*(2), 27–46.