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

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

Keamanan E-business (Kelebihan dan Kekurangan E-business)

Endri Dores, Anggy Anggrainy ; Audyana Azzahra; Dwika Prasetyo[3]
Email: anggyanggrainy994@gmail.com[1]; Audyanazzahra@gmail.com[2]; dwikaprasetyo213@gmail.com[3]

Abstrak

Perkembangan e-business yang semakin luas telah meningkatkan efisiensi operasional serta memberikan fleksibilitas bagi pelaku usaha dalam mengelola transaksi digital. Namun, berbagai literatur menunjukkan bahwa keamanan menjadi aspek paling krusial sekaligus tantangan terbesar dalam implementasi e-business. Permasalahan utama yang sering muncul mencakup risiko serangan siber, kebocoran data, dan rendahnya kesadaran pengguna terhadap praktik keamanan digital. Penelitian ini menggunakan metode studi pustaka dengan menelaah jurnal nasional dan internasional terbitan lima tahun terakhir untuk mengidentifikasi kelebihan dan kekurangan e-business dari perspektif keamanan. Hasil temuan menunjukkan bahwa e-business menawarkan sejumlah keunggulan, seperti efisiensi biaya, peningkatan jangkauan pasar, integrasi teknologi yang mudah, serta kemampuan analitik yang mendukung pengambilan keputusan. Namun demikian, e-business juga menghadapi kekurangan signifikan, seperti ancaman peretasan, ketergantungan pada infrastruktur digital, potensi penyalahgunaan data, dan lemahnya sistem proteksi keamanan di beberapa platform. Kesimpulan penelitian menegaskan bahwa keamanan merupakan faktor penentu keberhasilan e-business, sehingga diperlukan strategi penguatan sistem dan peningkatan literasi keamanan bagi pengguna maupun pelaku usaha.

Kata Kunci: *e-business; keamanan digital; efisiensi; risiko siber; data*

Abstract

The rapid expansion of e-business has increased operational efficiency and provided flexibility for organizations in managing digital transactions. However, existing literature highlights that security remains the most critical and challenging aspect of e-business implementation. Key problems frequently addressed include cybersecurity risks, data breaches, and low user awareness of digital security practices. This study employs a literature review method by examining national and international journals published within the last five years to analyze the advantages and disadvantages of e-business from a security perspective. The findings reveal that e-business offers several advantages, including cost efficiency, broader market reach, seamless technological integration, and enhanced analytical capabilities for decision-making. Nevertheless, e-business also faces major drawbacks such as hacking threats,

dependency on digital infrastructure, potential data misuse, and insufficient security protection on certain platforms. The study concludes that security is a fundamental determinant of e-business success; therefore, comprehensive system strengthening and improved security literacy for both users and businesses are essential.

Keywords: *e-business; digital security; efficiency; cyber risk; data*

A. PENDAHULUAN

Perkembangan teknologi digital dalam lima tahun terakhir telah mendorong perubahan signifikan dalam aktivitas bisnis global, termasuk percepatan penerapan e-business sebagai model operasional utama. Digitalisasi proses bisnis memungkinkan perusahaan meningkatkan efisiensi, memperluas jangkauan pasar, dan mengoptimalkan layanan kepada pelanggan. Menurut Kumar, Gupta, dan Singh (2022), percepatan transformasi digital pascapandemi telah menjadikan e-business sebagai kebutuhan strategis bagi berbagai sektor usaha. E-business memungkinkan integrasi antara data, transaksi, dan layanan pelanggan secara real-time sehingga menciptakan fleksibilitas dan efektivitas dalam pengelolaan bisnis modern.

Meskipun menawarkan banyak manfaat, perkembangan e-business juga disertai risiko keamanan digital yang semakin kompleks. Studi oleh Pappas et al. (2020) menemukan bahwa serangan siber pada platform bisnis digital meningkat pesat akibat celah sistem, kurangnya proteksi data, serta meningkatnya aktivitas kejahatan online. Risiko kebocoran data, pencurian identitas, dan manipulasi transaksi menjadi tantangan utama yang berdampak langsung pada kepercayaan konsumen. Sari dan Pratama (2022) juga menegaskan bahwa ketidakamanan data merupakan faktor yang paling memengaruhi keputusan konsumen untuk menggunakan layanan e-business. Selain itu, penelitian oleh Fernando (2024) menunjukkan bahwa tingkat kompetisi yang tinggi dalam pasar digital mendorong pelaku usaha untuk mempercepat digitalisasi, tetapi sering kali tidak diimbangi dengan kesiapan infrastruktur dan manajemen keamanan yang memadai.

Penelitian-penelitian sebelumnya telah mengkaji aspek e-business dari berbagai sudut pandang, seperti peningkatan performa bisnis (Tjandrawinata, 2021), perilaku konsumen digital (Putri & Maulana, 2023), dan kesiapan infrastruktur teknologi (Kim & Peterson, 2020). Namun, sebagian besar penelitian tersebut lebih menekankan manfaat fungsional e-business tanpa menguraikan secara mendalam bagaimana aspek keamanan digital berperan dalam menentukan keberhasilan suatu platform. Selain itu, masih terbatas penelitian yang secara komprehensif menganalisis kelebihan dan kekurangan e-business berdasarkan perspektif keamanan digital dengan memadukan temuan-temuan empiris terbaru lima tahun terakhir.

Kesenjangan penelitian (research gap) terletak pada kurangnya kajian yang menyoroti secara simultan manfaat e-business bagi pelaku usaha dan risiko keamanannya bagi pengguna dalam konteks perkembangan teknologi terkini. Oleh karena itu, penelitian ini dilakukan untuk menganalisis secara komprehensif kelebihan dan kekurangan e-business dengan fokus utama pada aspek keamanan digital sebagai faktor krusial dalam operasional bisnis modern. Tujuan penelitian ini adalah memberikan pemahaman yang lebih mendalam mengenai peluang dan

tantangan keamanan e-business serta memberikan dasar bagi pengembangan strategi mitigasi risiko yang dapat diterapkan oleh pelaku bisnis.

B. KAJIAN TEORI

Kajian teori pada penelitian ini berfungsi sebagai landasan konseptual untuk memahami kelebihan dan kekurangan e-business dalam perspektif keamanan digital. E-business secara umum didefinisikan sebagai seluruh aktivitas bisnis yang dilakukan menggunakan teknologi digital, mulai dari transaksi, komunikasi, hingga manajemen organisasi. Menurut Laudon dan Traver (2020), e-business tidak hanya berkaitan dengan proses jual beli, tetapi mencakup integrasi teknologi digital untuk mendukung seluruh fungsi bisnis agar lebih efisien dan responsif. Sejalan dengan itu, Chaffey (2019) menjelaskan bahwa e-business merupakan pemanfaatan teknologi informasi untuk meningkatkan efektivitas dan produktivitas organisasi melalui integrasi data, aplikasi digital, dan layanan online. Dalam konteks ini, e-business dianggap sebagai representasi modern dari inovasi bisnis yang menekankan kecepatan, fleksibilitas, dan akurasi dalam pemrosesan informasi.

Berbagai teori mengenai kelebihan e-business menegaskan bahwa digitalisasi memberikan efisiensi operasional bagi perusahaan. Porter dan Heppelmann (2020) menyatakan bahwa teknologi digital mampu mengotomatisasi proses kerja sehingga mengurangi biaya operasional dan meningkatkan produktivitas. Penelitian Kumar, Gupta, dan Singh (2022) menambahkan bahwa pemanfaatan platform e-business dapat memperluas jangkauan pasar secara global tanpa batasan geografis, sehingga pelaku usaha memiliki peluang yang lebih besar untuk mengembangkan bisnisnya. Selain itu, perusahaan yang menggunakan analitik berbasis big data memiliki kemampuan untuk memahami perilaku konsumen secara lebih mendalam. Setiawan dan Utami (2023) menemukan bahwa integrasi analitik digital pada e-business meningkatkan akurasi keputusan strategis serta mempermudah personalisasi layanan bagi pelanggan. Dengan demikian, teori-teori ini menunjukkan bahwa e-business memberikan sejumlah keuntungan signifikan bagi perkembangan bisnis modern.

Di sisi lain, literatur juga banyak membahas kekurangan e-business, terutama dalam aspek keamanan digital. Pappas et al. (2020) menjelaskan bahwa pertumbuhan transaksi digital turut meningkatkan risiko serangan siber, kebocoran data, dan manipulasi sistem. Kerentanan ini menjadi ancaman serius karena seluruh aktivitas e-business bergantung pada keamanan jaringan dan sistem elektronik. Sari dan Pratama (2022) mengungkapkan bahwa lemahnya proteksi data dapat mengurangi kepercayaan konsumen dan berdampak pada penurunan penggunaan layanan digital. Selain itu, Kim dan Peterson (2020) menegaskan bahwa ketergantungan pada infrastruktur digital dapat menghambat proses transaksi ketika sistem mengalami gangguan. Penelitian Hakim dan Nuraini (2021) juga menunjukkan bahwa masalah logistik dan kesalahan proses pengiriman sering menjadi kelemahan utama yang memengaruhi tingkat kepuasan pelanggan e-business. Teori kepercayaan konsumen dari Gefen, Karahanna, dan Straub (2021) menjelaskan bahwa kepercayaan merupakan faktor penting dalam transaksi digital, sehingga risiko keamanan yang tidak tertangani dapat menurunkan niat konsumen untuk berpartisipasi dalam e-business.

Berdasarkan teori-teori tersebut, dapat dirumuskan kerangka berpikir bahwa e-business memiliki dua sisi yang saling berkaitan. Pada satu sisi, e-business menawarkan berbagai kelebihan seperti efisiensi biaya, jangkauan pasar

luas, dan kemampuan analitik yang mendukung pengambilan keputusan. Namun pada sisi lain, keberhasilan e-business sangat dipengaruhi oleh tingkat keamanan digital yang diterapkan. Semakin kuat sistem keamanan yang dimiliki, semakin besar manfaat e-business yang dapat dirasakan oleh pelaku usaha dan konsumen. Sebaliknya, semakin rentan platform terhadap ancaman siber, semakin besar pula kelemahan yang muncul dalam layanan digital tersebut. Dengan demikian, keamanan digital menjadi variabel kunci yang menghubungkan kelebihan e-business dengan tantangan yang dihadapinya.

Dari kerangka berpikir tersebut, hipotesis konseptual yang dapat dirumuskan adalah bahwa e-business memiliki kelebihan signifikan dalam meningkatkan kinerja dan jangkauan pasar perusahaan, namun risiko keamanan digital berpengaruh langsung terhadap tingkat kepercayaan dan efektivitas penggunaannya. Selain itu, semakin baik sistem keamanan digital suatu platform, semakin besar peluang e-business untuk berfungsi secara optimal dan berkelanjutan. Hipotesis ini menegaskan bahwa keamanan digital bukan hanya faktor pendukung, tetapi merupakan fondasi yang menentukan keberhasilan e-business dalam lingkungan bisnis modern yang sangat bergantung pada teknologi.

C. METODE PENELITIAN

Penelitian ini menggunakan metode penelitian deskriptif kualitatif dengan pendekatan studi pustaka (library research), yang ditujukan untuk mengkaji secara mendalam kelebihan dan kekurangan e-business dari perspektif keamanan digital dengan merujuk pada hasil-hasil penelitian yang telah dipublikasikan dalam kurun waktu lima tahun terakhir. Desain penelitian ini dipilih karena sesuai untuk menggali pemahaman konseptual, menganalisis teori-teori yang mendasari fenomena, serta menelaah temuan-temuan ilmiah yang relevan tanpa melakukan intervensi langsung terhadap objek penelitian. Dalam konteks penelitian kualitatif, posisi peneliti menjadi instrumen utama yang bertanggung jawab mengumpulkan, mengolah, menganalisis, dan menginterpretasikan berbagai sumber literatur sehingga menghasilkan temuan yang terorganisasi secara sistematis. Kehadiran peneliti berperan aktif dalam keseluruhan proses, mulai dari penentuan sumber data, penilaian kualitas literatur, hingga penyusunan sintesis teoretis. Walaupun penelitian berbasis pustaka tidak melibatkan subjek manusia secara langsung, tetapi tetap memerlukan kehati-hatian dalam memilih sumber agar informasi yang dihasilkan valid, mutakhir, dan relevan.

Populasi penelitian ini mencakup seluruh sumber literatur ilmiah yang membahas e-business dan keamanan digital, termasuk jurnal nasional terindeks SINTA, jurnal internasional bereputasi, buku ilmiah, prosiding konferensi, laporan penelitian institusi, serta artikel akademik yang menjelaskan perkembangan teknologi digital dan sistem keamanan siber. Sampel penelitian ditentukan menggunakan teknik purposive sampling berdasarkan kriteria tertentu, yaitu sumber harus: (1) diterbitkan antara tahun 2019 hingga 2024; (2) relevan secara langsung dengan topik e-business, keamanan digital, risiko siber, dan transformasi digital; (3) berasal dari publikasi yang telah melewati proses peer-review; dan (4) memiliki kontribusi signifikan terhadap pemahaman teoritis maupun empiris mengenai variabel penelitian. Literatur yang tidak memenuhi standar akademik, tidak relevan, atau memiliki bias metodologis yang signifikan dieliminasi dari proses analisis.

Teknik pengumpulan data dilakukan melalui penelusuran mendalam pada berbagai database ilmiah, seperti Google Scholar, ScienceDirect, Scopus, Wiley

Online Library, ResearchGate, dan SpringerLink. Peneliti juga mengakses portal jurnal nasional seperti GARUDA dan SINTA untuk memperoleh literatur kontekstual terkait perkembangan e-business di Indonesia. Proses pencarian dilakukan menggunakan kata kunci seperti e-business, cybersecurity, data protection, digital transformation, trust in digital platforms, dan digital business risks. Untuk memastikan kelengkapan data, peneliti menggunakan strategi snowballing, yaitu menelusuri daftar pustaka pada artikel yang telah dipilih untuk menemukan literatur lain yang relevan. Setiap literatur kemudian dicatat menggunakan instrumen penelitian berupa lembar pencatatan literatur yang memuat identifikasi judul, penulis, metode penelitian, temuan utama, teori yang digunakan, serta tahun publikasi. Untuk menjaga konsistensi sitasi, peneliti menggunakan aplikasi pengelola referensi seperti Mendeley dan Zotero dengan format APA Edisi 6 sebagaimana dipersyaratkan dalam penulisan karya ilmiah.

Instrumen penelitian utama adalah peneliti sendiri, dibantu oleh perangkat digital seperti komputer, koneksi internet stabil, aplikasi manajemen referensi, serta perangkat lunak PDF reader untuk melakukan highlight dan anotasi pada setiap literatur. Dalam penelitian kualitatif seperti ini, kehadiran peneliti dipahami sebagai human instrument yang menentukan arah analisis dan interpretasi data. Meskipun penelitian ini berbasis literatur, konsep “lokasi penelitian” tetap merujuk pada tempat atau media di mana data dikumpulkan, yaitu database jurnal ilmiah dan repositori penelitian. Durasi penelitian berlangsung selama dua bulan, mencakup proses pengumpulan literatur, seleksi sumber, analisis data, verifikasi temuan, dan penyusunan laporan ilmiah.

Teknik analisis data menggunakan analisis isi (content analysis), yaitu metode yang digunakan untuk mengidentifikasi pola, tema, dan hubungan antar konsep dalam literatur. Proses analisis berlangsung melalui tiga tahap utama. Tahap pertama adalah reduksi data, yaitu proses penyaringan literatur berdasarkan kesesuaian topik, kualitas publikasi, dan kontribusi terhadap variabel penelitian. Tahap kedua adalah penyajian data, di mana literatur disusun ke dalam kategori seperti definisi e-business, teori kelebihan e-business, teori risiko keamanan digital, tantangan e-business dalam era transformasi digital, serta strategi penguatan keamanan. Tahap ketiga adalah penarikan kesimpulan, yaitu proses merangkum keseluruhan temuan literatur menjadi satu pemahaman komprehensif mengenai kelebihan dan kekurangan e-business dari perspektif keamanan digital.

Validitas temuan diperkuat menggunakan teknik triangulasi sumber, yaitu membandingkan konsistensi informasi dari berbagai literatur yang ditulis oleh peneliti berbeda dan menggunakan metodologi yang beragam. Selain triangulasi, peneliti juga melakukan peer debriefing dengan dosen pembimbing atau rekan akademik untuk memastikan bahwa interpretasi data tidak bias dan tetap konsisten dengan kaidah ilmiah. Dengan demikian, metode penelitian ini memberikan dasar analitis yang kuat untuk menghasilkan kesimpulan yang objektif, mendalam, dan relevan sebagai kontribusi teori mengenai keamanan e-business dalam era digitalisasi global.

D. HASIL DAN PEMBAHASAN

Hasil penelitian ini diperoleh melalui analisis mendalam terhadap 32 literatur ilmiah yang terbit dalam rentang tahun 2019–2024. Literatur tersebut terdiri atas jurnal nasional terindeks SINTA, jurnal internasional bereputasi,

prosiding konferensi internasional, serta buku ilmiah yang relevan dengan tema e-business dan keamanan digital. Analisis literatur menunjukkan bahwa perkembangan e-business memberikan kontribusi signifikan terhadap efektivitas bisnis modern, khususnya dalam hal efisiensi operasional, perluasan pasar, dan kemampuan integrasi teknologi. Namun demikian, hasil kajian juga menegaskan bahwa keamanan digital tetap menjadi faktor penghambat terbesar dalam implementasi e-business, terutama terkait risiko serangan siber, kebocoran data, dan rendahnya literasi digital konsumen.

Untuk memberikan gambaran rinci mengenai hasil kajian, berikut disajikan tabel rangkuman temuan literatur:

Tabel 1
Ringkasan Temuan Penelitian Terkait Kelebihan dan Kekurangan E-Business

No	Peneliti & Tahun	Temuan Utama
1	Kumar et al. (2022)	E-Business memperluas jangkauan pasar dan mempercepat digitalisas pascapandemi
2	Porter & Heppelman (2020)	Digitalisasi meningkatkan efisiensi dan menurunkan biaya operasional
3	Setiawan & Utami (2023)	Big data meningkatkan kemampuan analitik e-business
4	Pappas et al. (2020)	E-Business rentan terhadap serangan siber dan kebocoran data
5	Sari & Pratama (2022)	Keamanan digital memengaruhi kepercayaan konsumen secara langsung
6	Kim & Peterson (2020)	Infranstruktur digital memengaruhi stabilitas dan keberhasilan e-business
7	Hakim & Nuraini (2021)	Logistic dan layanan pengiriman merupakan tantangan signifikan
8	Fernando (2024)	Persaingan e-business Asia Tenggara semakin ketat dan membutuhkan inovasi keamanan

Sumber: Data diolah (2022)

Hasil penelitian menunjukkan bahwa e-business memiliki empat kelebihan utama, yaitu efisiensi operasional, jangkauan pasar yang luas, kemampuan integrasi teknologi, dan penggunaan data analitik untuk pengambilan keputusan. Efisiensi operasional tercermin dari pengurangan biaya transaksi, percepatan proses bisnis, dan otomatisasi yang mengurangi beban kerja manual. Jangkauan pasar yang luas memungkinkan pelaku usaha memperluas target konsumen secara global. Kemampuan integrasi teknologi memungkinkan perusahaan mengadopsi berbagai sistem seperti payment gateway, artificial intelligence, dan cloud computing untuk meningkatkan kualitas layanan. Selain itu, kemampuan analitik berbasis big data membantu perusahaan memahami perilaku konsumen secara lebih mendalam.

Namun, hasil kajian juga mengidentifikasi empat kekurangan utama e-business, yaitu risiko keamanan digital, ketergantungan terhadap infrastruktur teknologi, masalah logistik, dan rendahnya literasi keamanan konsumen. Risiko keamanan digital menjadi isu sentral karena e-business bergantung pada data pengguna dan sistem transaksi online. Ketergantungan pada infrastruktur digital seperti jaringan internet dan server memengaruhi kualitas layanan. Masalah logistik muncul dalam bentuk keterlambatan pengiriman atau ketidaksesuaian barang. Literasi keamanan rendah membuat konsumen rentan terhadap penipuan online dan phishing.

Untuk mempermudah interpretasi, data hasil analisis disajikan pada tabel berikut.

Tabel 2
Kelebihan dan Kekurangan E-Business Berdasarkan Analisis Literatur

Aspek	**Kelebihan**	**Kekurangan**
Operasiona	Efisiensi biaya, otomatisasi proses	Ketergantungan pada sistem digital
Pasar	Jangkauan global, akses 24/7	Persaingan sangat tinggi antar platform
Teknologi	Integrasi AI, Cloud, payment system	Risiko error sistem, downtime server
Keamanan	Tersedia proteksi digital modern	Ancaman siber dan kebocoran data
Konsumen	Proses cepat dan mudah	Literasi keamanan rendah

Sumber: Data diolah (2022)

Pembahasan penelitian ini mengintegrasikan temuan kajian literatur dengan teori-teori yang telah dijelaskan pada bagian kajian teori, sehingga memberikan pemahaman komprehensif mengenai kelebihan dan kekurangan e-business dari perspektif keamanan digital. Hasil analisis terhadap 32 sumber literatur menunjukkan bahwa e-business telah mengalami perkembangan yang sangat pesat dalam lima tahun terakhir, terutama dipengaruhi oleh percepatan digitalisasi pascapandemi COVID-19 sebagaimana dijelaskan oleh Kumar et al. (2022). Percepatan tersebut mendorong organisasi untuk mengadopsi teknologi digital tidak hanya pada proses transaksi, tetapi juga dalam kegiatan operasional dan manajerial. Peningkatan adopsi ini sejalan dengan teori efisiensi digital oleh Porter dan Heppelmann (2020) yang menyatakan bahwa integrasi teknologi mampu mengurangi biaya operasional, mempercepat proses kerja, dan meningkatkan efektivitas layanan.

Secara lebih rinci, temuan penelitian menunjukkan bahwa keuntungan utama e-business terletak pada kemampuannya menekan biaya operasional, memperluas jangkauan pasar, serta meningkatkan kualitas pengambilan keputusan melalui pemanfaatan data digital. Penelitian Setiawan dan Utami (2023) menegaskan bahwa big data analytics membantu perusahaan memahami pola belanja konsumen, menganalisis kebutuhan pasar, dan merancang strategi pemasaran yang lebih terarah. Ini memperkuat teori competitive advantage dari Barney (2019) yang memposisikan teknologi sebagai sumber keunggulan yang sulit ditiru oleh pesaing. Dengan demikian, e-business tidak hanya meningkatkan

efisiensi, tetapi juga berkontribusi pada diferensiasi layanan dan peningkatan nilai tambah bagi pelanggan.

Namun, pembahasan menjadi semakin kompleks ketika mencermati kekurangan e-business, terutama pada aspek keamanan digital. Sebagian besar literatur menekankan bahwa risiko keamanan merupakan hambatan terbesar dalam implementasi e-business yang efektif. Pappas et al. (2020) menyoroti meningkatnya ancaman seperti phishing, ransomware, dan serangan DDoS yang menyasar platform digital. Serangan-serangan ini tidak hanya berdampak pada kerugian finansial, tetapi juga mengganggu integritas data dan sistem. Kebocoran data menjadi salah satu isu paling serius, karena dapat mengurangi kepercayaan pelanggan. Sari dan Pratama (2022) menemukan bahwa konsumen cenderung menurunkan intensitas belanja online jika pernah mengalami atau mendengar insiden keamanan pada platform yang sama. Temuan ini sangat relevan dengan teori Consumer Trust (Gefen et al., 2021), yang menyatakan bahwa kepercayaan merupakan fondasi utama dalam transaksi digital. Tanpa keamanan, kepercayaan tidak dapat dibangun, sehingga e-business tidak akan mampu beroperasi secara optimal.

Pembahasan juga menyoroti bahwa risiko keamanan digital tidak berdiri sendiri, tetapi saling berkaitan dengan kualitas infrastruktur teknologi. Kim dan Peterson (2020) menjelaskan bahwa gangguan pada jaringan internet, server, atau sistem backend dapat menyebabkan kegagalan transaksi, penundaan layanan, dan kehilangan data. Ketergantungan pada teknologi inilah yang menjadi alasan mengapa e-business memerlukan infrastruktur digital yang kuat dan stabil. Ketika infrastruktur lemah, risiko kerentanan meningkat, sehingga keamanan platform turut terganggu. Temuan ini diperkuat oleh Fernando (2024) yang menunjukkan bahwa perusahaan e-business di Asia Tenggara mengalami tingkat persaingan yang sangat tinggi sehingga membutuhkan investasi besar dalam infrastruktur dan keamanan untuk mempertahankan keunggulan kompetitif.

Selain aspek teknis, pembahasan juga menunjukkan bahwa literasi digital pelanggan menjadi faktor penting dalam efektivitas penerapan e-business. Banyak konsumen belum memiliki kesadaran tinggi mengenai keamanan digital, seperti kemampuan mengenali email phishing, memahami keamanan kata sandi, atau menggunakan autentikasi dua faktor. Penelitian Yuliana (2021) menemukan bahwa sebagian besar insiden penipuan online terjadi karena kelalaian pengguna, bukan semata-mata karena kelemahan sistem. Kondisi ini memperjelas bahwa keamanan e-business bukan hanya tanggung jawab penyedia platform, tetapi juga pengguna. Keduanya perlu bekerja sama dalam menciptakan ekosistem digital yang aman dan terpercaya.

Pembahasan juga menegaskan relevansi antara hasil yang ditemukan dengan hipotesis konseptual penelitian. Hipotesis pertama yang menyatakan bahwa e-business memiliki kelebihan signifikan dalam meningkatkan efektisiensi dan jangkauan pasar terbukti melalui temuan Kumar et al. (2022), Setiawan dan Utami (2023), serta Porter dan Heppelmann (2020). Hipotesis kedua yang menyatakan bahwa risiko keamanan digital berpengaruh langsung terhadap kepercayaan pengguna juga terbukti berdasarkan penelitian Pappas et al. (2020), Gefen et al. (2021), dan Sari dan Pratama (2022). Demikian pula hipotesis ketiga yang menyebutkan bahwa keamanan digital yang kuat memperkuat kelebihan e-business, terlihat pada literatur Fernando (2024) yang menekankan bahwa platform dengan proteksi keamanan yang lebih baik cenderung lebih dipercaya oleh konsumen dan lebih kompetitif di pasar digital.

Dengan demikian, pembahasan ini menunjukkan bahwa e-business merupakan inovasi bisnis yang memiliki potensi besar, namun keberhasilannya sangat bergantung pada bagaimana pelaku usaha mengelola aspek keamanan digital. Semakin tinggi tingkat keamanan yang diterapkan, semakin besar kemungkinan e-business memberikan manfaat optimal bagi pelaku bisnis dan konsumen. Sebaliknya, jika keamanan diabaikan, risiko kerugian finansial, kehilangan data, dan hilangnya kepercayaan konsumen akan menjadi hambatan utama yang menghambat pertumbuhan bisnis digital. Oleh karena itu, pembahasan ini menegaskan pentingnya strategi perlindungan data, investasi pada infrastruktur, edukasi keamanan kepada pengguna, serta penerapan teknologi keamanan modern sebagai upaya untuk memaksimalkan keuntungan e-business sekaligus meminimalkan kelemahannya.

E. KESIMPULAN

Penelitian ini menyimpulkan bahwa e-business memiliki potensi strategis dalam meningkatkan efektivitas dan efisiensi operasional bisnis modern, terutama melalui kemampuan memperluas jangkauan pasar, mengoptimalkan proses internal, serta memanfaatkan data digital untuk pengambilan keputusan yang lebih akurat. Temuan kajian literatur menunjukkan bahwa keunggulan tersebut hanya dapat tercapai apabila aspek keamanan digital dikelola dengan baik, karena keamanan terbukti menjadi faktor penentu yang memengaruhi kepercayaan pengguna, stabilitas layanan, dan keberlanjutan operasional. Risiko seperti serangan siber, kebocoran data, hingga kelemahan infrastruktur digital terbukti memiliki dampak signifikan terhadap performa e-business, sehingga keamanan tidak dapat dipandang sebagai elemen pendukung semata, tetapi merupakan fondasi utama keberhasilan e-business. Dengan demikian, penelitian ini menegaskan bahwa optimalisasi kelebihan e-business membutuhkan penerapan keamanan digital yang kuat, adaptif, dan berkelanjutan, sehingga e-business dapat berjalan dengan efektif dan mampu bersaing di tengah dinamika transformasi digital yang semakin kompleks.

F. SARAN

Berdasarkan temuan penelitian, terdapat beberapa saran yang dapat diberikan untuk pengembangan e-business agar mampu beroperasi secara optimal di tengah semakin kompleksnya dinamika digital. Secara praktis, pelaku usaha perlu memberikan perhatian lebih besar pada penguatan keamanan digital melalui penerapan sistem perlindungan berlapis seperti enkripsi data, autentikasi multifaktor, firewall adaptif, serta pemantauan ancaman secara real-time. Upaya tersebut harus diimbangi dengan peningkatan literasi keamanan bagi pengguna, mengingat rendahnya kesadaran konsumen terhadap praktik keamanan digital masih menjadi salah satu penyebab utama kerentanan transaksi online. Edukasi mengenai pengelolaan password, kewaspadaan terhadap phishing, serta pentingnya memverifikasi identitas platform perlu dilakukan secara berkelanjutan sehingga kepercayaan konsumen dapat terjaga. Dari sisi organisasi, perusahaan juga perlu berinvestasi pada infrastruktur digital yang stabil dan berkualitas, karena keberhasilan layanan e-business sangat dipengaruhi oleh keandalan jaringan dan sistem teknologi yang digunakan.

Dari perspektif teoritis, penelitian ini membuka peluang untuk pengembangan konsep keamanan digital yang lebih terintegrasi dengan perilaku konsumen dan strategi bisnis. Kajian selanjutnya dapat mengembangkan model teoretis yang menjelaskan hubungan antara persepsi keamanan, kepercayaan konsumen, dan keputusan pembelian pada platform e-business. Penelitian lanjutan juga disarankan untuk mengkaji variabel-variabel baru seperti peran kecerdasan buatan dalam mitigasi risiko siber, integrasi blockchain dalam perlindungan data, serta pengaruh regulasi pemerintah terhadap tingkat keamanan platform digital. Selain itu, pendekatan empiris dengan melibatkan pelaku usaha dan konsumen secara langsung diperlukan untuk menghasilkan temuan yang lebih aplikatif dan kontekstual. Dengan demikian, saran-saran ini diharapkan dapat memberikan kontribusi baik bagi praktik industri maupun pengembangan pengetahuan ilmiah mengenai keamanan e-business di masa mendatang..

G. DAFTAR PUSTAKA

Buku

Barney, J. B. (2019). Gaining and sustaining competitive advantage (5th ed.). Pearson.

Chaffey, D. (2019). Digital business and e-commerce management. Pearson Education.

Kotler, P., & Keller, K. L. (2020). Marketing management (15th ed.). Pearson.

Laudon, K. C., & Traver, C. G. (2020). E-commerce: Business, technology, society (16th ed.). Pearson.

Westerman, G., Bonnet, D., & McAfee, A. (2019). Leading digital: Turning technology into business transformation. Harvard Business Review Press

Jurnal Nasional & Internasional

Fernando, L. (2024). Competitive dynamics in Southeast Asian e-business markets. Asian Journal of E-Business, 12(2), 88–101.

Gefen, D., Karahanna, E., & Straub, D. W. (2021). Trust and TAM in online transactions: An integrated model. Journal of Management Information Systems, 38(4), 123–158.

Hakim, R., & Nuraini, L. (2021). Pengaruh kualitas logistik terhadap kepuasan pelanggan e-commerce di Indonesia. Jurnal Ilmu Manajemen, 9(2), 145–156.

Hidayat, M. (2022). Pengaruh kualitas layanan digital terhadap loyalitas pelanggan e-commerce. Jurnal Manajemen Pemasaran, 10(2), 134–148.

Kumar, S., Gupta, A., & Singh, R. (2022). Digital acceleration and global commerce transformation post-pandemic. International Journal of Electronic Commerce, 26(3), 210–228.

Kim, J., & Peterson, R. A. (2020). Infrastructure readiness and its impact on e-business adoption. Electronic Markets, 30(2), 341–356.

Nugroho, F., & Ardiansyah, M. (2019). E-commerce readiness in developing countries. Journal of Digital Innovation, 4(1), 23–36.

Pappas, N., Patelis, T., & Gritzalis, D. (2020). Understanding cybersecurity threats in e-business. Computers & Security, 92, 101–119.

Porter, M. E., & Heppelmann, J. (2020). How smart, connected products are transforming competition. Harvard Business Review, 98(4), 112–131.

Pradana, M. (2021). Adaptasi strategi pemasaran digital pada era transformasi bisnis. Jurnal Ekonomi & Bisnis Indonesia, 6(1), 33–47.

Putri, A., & Maulana, T. (2023). Transformasi perilaku konsumen pascapandemi melalui e-business. Journal of Business and Digital Marketing, 5(1), 77–90.

Rahmawati, S. (2021). Dampak e-business terhadap pertumbuhan UMKM di Indonesia. Jurnal Manajemen dan Bisnis, 8(3), 211–220.

Sari, D., & Pratama, H. (2022). Keamanan siber dalam transaksi e-business: Tantangan dan peluang. Jurnal Teknologi Informasi, 14(1), 55–68.

Setiawan, A., & Utami, D. (2023). Peran big data dalam strategi pemasaran digital. Jurnal Teknologi dan Sistem Informasi, 7(2), 101–115.

Tjandrawinata, R. (2021). Digitalisasi dan daya saing UMKM di Indonesia. Jurnal Ekonomi Terapan, 15(2), 67–79.

Wijaya, L., & Santoso, H. (2020). Perubahan perilaku konsumen dalam penggunaan e-business. Jurnal Riset Ekonomi dan Bisnis, 13(2), 98–108.

Yuliana, E. (2021). Faktor kepercayaan konsumen dalam transaksi digital. Jurnal Ekonomi Digital, 2(1), 12–25.