PT Jurnal Cendekia Indonesia
Journal of Information Systems and Business Technology
Homepage: https://journal.jci.co.id/jisbt
Vol. 1 No. 4 (2025) Page : 73-77
E-ISSN: 3109-8886

Keamanan Jaringan komputer Dalam Bisnis E-Commerce (Studi Kasus: Kebocoran Data Tokopedia 2020)

[1]**Dhifa Dharma Rafadhani,** [2]**Dinda Pratiwi,** [3]**Nabila Sayidina**

[123]Sistem Informasi, Ilmu Komputer, Universitas Pamulang, Kota Tangerang Selatan, Indonesia

rafadhanidhifa@gmail.com, dp93720@gmail.com, nabilasayidina473@gmail.com

Abstract

The rapid development of digital activities in the modern era demands a way for humans to carry out various digital activities. Under these conditions, cloud computing has emerged as a paradigmatic solution that supports digital transformation by providing data storage services, application processing, and online collaboration. This study is to analyze the use of cloud computing in supporting various dimensions of digital activities and identify its strategic benefits and challenges. In addition, this digital technology is equipped with advanced security, multi-factor authentication, and role-based access management that can minimize data security risks. This study applies a systematic literature review with a qualitative approach that focuses on scientific publications and the latest industry reports (2019–2024). This study shows that cloud computing significantly supports digital activities through increased infrastructure scalability, accessibility of services from anywhere, efficiency of operational costs based on pay-per-use, and acceleration of innovation with ready-to-use services (such as AI and Big Data). However, challenges remain in the aspects of cybersecurity, the complexity of multi-cloud management, and dependence on service providers. This study confirms that cloud computing not only functions as a technology enabler, but also as a strategic pillar in building digital competitiveness in the modern era. The implications suggest that organizations need to formulate a robust cloud strategy, strengthen governance, and address security challenges to maximize its value and benefits.

Keyword: *Cloud Computing, Digital Transformation, Digital Productivity, Data Security, Real-time Access*

Abstrak

Perkembangan pesat bisnis e-commerce menjadikan jaringan komputer sebagai infrastruktur utama dalam pengelolaan transaksi dan data pengguna. Namun, meningkatnya ketergantungan terhadap sistem jaringan juga memperbesar risiko ancaman keamanan siber, seperti kebocoran data dan serangan jaringan. Insiden kebocoran data Tokopedia pada tahun 2020 menunjukkan pentingnya penerapan keamanan jaringan komputer yang efektif dalam bisnis e-commerce. Penelitian ini bertujuan untuk menganalisis keamanan jaringan komputer dalam bisnis e-commerce dengan studi kasus kebocoran data Tokopedia. Metode penelitian yang digunakan adalah studi literatur dan analisis deskriptif terhadap insiden keamanan jaringan, mekanisme perlindungan data, serta dampaknya terhadap operasional e-commerce. Hasil penelitian menunjukkan bahwa kelemahan dalam sistem keamanan jaringan dapat menyebabkan kebocoran data pengguna dan menurunkan tingkat kepercayaan pelanggan. Penerapan teknologi keamanan jaringan seperti firewall, enkripsi data, dan intrusion detection system terbukti berperan penting dalam meningkatkan perlindungan sistem e-commerce. Penelitian ini menyimpulkan bahwa keamanan jaringan komputer merupakan faktor krusial dalam menjaga kerahasiaan, integritas, dan ketersediaan data pada bisnis e-commerce serta mendukung keberlanjutan dan reputasi perusahaan.

Kata kunci: Keamanan Jaringan, E-Commerce, Tokopedia, Kebocoran Data, Keamanan Informasi

A. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi yang pesat telah mengubah cara bisnis beroperasi, terutama melalui pertumbuhan perdagangan elektronik (e-commerce). E-commerce sangat bergantung pada jaringan komputer untuk memungkinkan transaksi online, mengelola data pelanggan, dan menjaga komunikasi real-time antara penjual dan pembeli. Di Indonesia, Tokopedia adalah salah satu platform e-commerce terbesar yang memainkan peran penting dalam ekonomi digital, dengan memungkinkan jutaan pengguna melakukan perdagangan secara daring. Dalam ekosistem perdagangan elektronik yang semakin luas, stabilitas jaringan sebagai fondasi utama

Diterima Redaksi: 01-12-2025 | Selesai Revisi: 14-12-2025 | Diterbitkan Online: 31-12-2025

dalam repuasi bisnis dimana keamanan bukan sekedar fitur, melainkan perlindungan terhadap aset igital pelanggan.

walaupun e-commerce menawarkan banyak kemudahan, penggunaan jaringan komputer yang luas juga menciptakan tantangan besar dalam hal keamanan. Platform e-commerce sering menjadi target serangan siber karena menyimpan banyak informasi sensitif, seperti data pribadi pengguna, kredensial login, dan riwayat transaksi. Ancaman keamanan jaringan yang umum di lingkungan e-commerce mencakup kebocoran data, serangan malware, phishing, serta serangan Distributed Denial of Service (DDoS). Ancaman-ancaman ini tidak hanya mengganggu ketersediaan sistem, tetapi juga membahayakan kerahasiaan dan keutuhan data, yang merupakan elemen dasar keamanan informasi.

Beberapa penelitian sebelumnya telah membahas pentingnya keamanan jaringan dalam sistem e-commerce. Penelitian oleh Stallings menekankan bahwa mekanisme keamanan seperti firewall, enkripsi, dan sistem deteksi intrusi (IDS) adalah komponen penting untuk melindungi infrastruktur digital dari ancaman siber. Selain itu, Laudon dan Traver menyatakan bahwa kepercayaan pengguna terhadap platform e-commerce sangat dipengaruhi oleh kemampuan platform tersebut dalam mengamankan data pengguna dan proses transaksi. Penelitian lain juga menunjukkan bahwa insiden keamanan siber dapat berdampak besar pada reputasi organisasi, loyalitas pelanggan, dan menyebabkan kerugian finansial yang signifikan.

Namun, meskipun kajian tentang keamanan jaringan dan e-commerce terus berkembang, masih ada keterbatasan penelitian yang secara spesifik menganalisis insiden keamanan nyata pada platform e-commerce besar di Indonesia. Salah satu kasus penting adalah kebocoran data Tokopedia pada tahun 2020, di mana jutaan data akun pengguna dilaporkan terungkap. walaupun kejadian ini mendapat perhatian besar dari masyarakat dan media, penelitian akademik yang membahas aspek keamanan jaringan dan pengaruh terhadap bisnis e-commerce masih sedikit. ini menunjukkan adanya celah dalam penelitian yang perlu dipelajari lebih mendalam.

Pentingnya penelitian ini terletak pada kontribusinya untuk memberikan pemahaman tentang bagaimana dampak kegagalan keamanan jaringan yang memengaruhi kelangsungan bisnis e-commerce. Dengan mempelajari kasus kebocoran data Tokopedia sebagai studi kasus, penelitian ini diharapkan dapat memberikan wawasan tentang betapa pentingnya menerapkan strategi keamanan jaringan yang kuat untuk melindungi data pengguna dan menjaga kepercayaan pelanggan. Hasil penelitian ini diharapkan dapat menjadi acuan bagi praktisi e-commerce, administrator sistem, serta peneliti dalam membangun infrastruktur jaringan yang lebih aman.

Oleh karena itu, tujuan penelitian ini adalah untuk menganalisis keamanan jaringan komputer dalam bisnis e-commerce dengan menggunakan studi kasus kebocoran data Tokopedia. Secara khusus, penelitian ini bertujuan untuk mengidentifikasi potensi kerentanan keamanan jaringan, mengevaluasi peran mekanisme keamanan jaringan dalam mencegah kebocoran data, serta menilai dampak insiden keamanan terhadap operasional e-commerce. Kontribusi penelitian ini adalah memberikan analisis yang praktis dan kontekstual tentang masalah keamanan jaringan dalam e-commerce, khususnya dalam lingkungan bisnis digital di Indonesia.
yang akan dilakukan.

Gambar 1 E-Commerce

B. PELAKSAAAN DAN METODE

2.1 Pendekatan dan Jenis Penelitian

Penelitian ini menggunakan pendekatan kualitatif dengan metode studiliteratur(literaturereview). Pendekatan ini dipilih karena sesuai dengan tujuan penelitian untuk menganalisis dan mensintesis fenomena kebocoran data serta dampaknya terhadap kepercayaan konsumen secara mendalam dan kontekstual, tanpa melakukan pengukuran kuantitatif.Jenis penelitian ini adalah deskriptif-analitis, yang bertujuan untuk:

a.Mendeskripsikansecara sistematis kronologi, skala, dan respons dari kasus kebocoran data Tokopedia periode 2020-2023.

b.Menganalisishubungan sebab-akibat antara insiden kebocoran data dengan dinamika kepercayaan konsumen e-commercedi Indonesia berdasarkan bukti-bukti empiris yang telah dipublikasikan.

2.2 Sumber Data

Data yang digunakan dalam penelitian ini seluruhnya bersumber dari data sekunder. Pengumpulan data dilakukan dengan teknikstudi dokumenter, dengan mengumpulkan berbagai teks dan dokumen yang relevan. Sumber data diklasifikasikan sebagai berikut:

1. **Sumber Primer Data Kasus:**
   Sumber-sumber yang secara langsung melaporkan atau menganalisis detail teknis kebocoran data.
   a. Laporan investigasi dari firma keamanan siber (contoh:Kaspersky, Ethical Hat, BleepingComputer).

b. Pernyataan resmi dan publikasi dari pihak Tokopedia danotoritas yang berwenang (Kominfo).

2. **Sumber Sekunder Analisis Konteks dan Dampak**
   Sumber-sumber yang memberikan konteks, analisis, dan bukti tidak langsung mengenai dampak yang terjadi.
   a. **Artikel Media Massa Terpercaya:** Kompas, Katadata, CNBC Indonesia, yang meliputirespons publik, sentimen, dan perkembangan kasus.
   b. **Laporan Survei dan Data Statistik:** Data dari APJII (profil pengguna internet), serta laporan dari lembaga seperti Cisco atau IBMyang memberikan konteks global tentang tren kepercayaan dan keamanan siber.
   c. **Jurnal Akademis dan Prosiding Seminar:** Karya ilmiah yang membahas teori kepercayaan dalam e-commerce, dampak kebocoran data, dan perilaku konsumen digital.
   d. **Dokumen Regulasi:** Peraturan Pemerintah No. 71 Tahun 2019 dan Undang-Undang No. 27 Tahun 2022 tentang Perlindungan Data Pribadi.

2.3 Teknik Pengumpulan Data

Teknik pengumpulan data dilakukan dengan carapencatatan dan kajian dokumen(documentary review). Langkah-langkahnya adalah:

1. **Pencarian Literatur (Literature Searching)** Mengidentifikasi kata kunci pencarian seperti "Tokopedia databreach", "kebocoran data e-commerceIndonesia", "digital trust e-commerce", "dampak kebocoran data terhadap konsumen". Pencarian dilakukanpada database elektronik (Google Scholar, ScienceDirect),situs berita, dan situs resmi lembaga terkait.
2. **Seleksi dan Evaluasi Sumber** Memilih sumber-sumber yang kredibel dan relevan dengan periode waktu 2020-2023. Kriteria inklusi meliputi:
   a. sumber terbit dari institusi/media terpercaya,
   b. konten relevan dengan rumusan masalah, dan
   c. memiliki tanggal publikasi yang jelas.
3. **Ekstraksi Data** Menandai dan mencatat informasi-informasi kunci dari setiap sumber yang terpilih ke dalam matriks pengumpulan data. Informasi yang dicatat meliputi: temuan fakta, pernyataan opini, data statistik, dankesimpulan analitis yang terkait dengan variabel penelitian.

2.3 Teknik Analisis Data

Data yang telah terkumpul dianalisis menggunakan teknikanalisis isi kualitatif(qualitative content analysis). Teknik ini digunakan untuk mengidentifikasi pola, tema, dan makna dari teks-teks yang dikumpulkan. Proses analisis mengikuti tahapan berikut:

1. **Reduksi Data (Data Reduction)** Menyederhanakan dan memfokuskan data yang banyak dan beragam dengan cara memilih, memusatkan perhatian, dan menyaring intisari informasi yang paling relevan dengan fokus penelitian.
2. **Display Data (Data Display)** Menyajikan data yang telah direduksi dalam bentuk matriks, tabel, atau diagram (seperti diagram kerangka pemikiran pada Bab II) untuk mempermudah dalam melihat hubungan antar kategori dan menarik kesimpulan.
3. **Penarikan Kesimpulan dan Verifikasi (Conclusion Drawing/Verification)** Menarik makna dari data yang telah disajikan. Pada tahap ini, peneliti melakukan:
   a. **Analisis Tematik (Thematic Analysis)** Mengidentifikasi tema-tema utamayang muncul dari berbagai sumber, seperti: "krisis transparansi", "perilaku protektif konsumen", "efek spillover", dan "respons regulatif".
   b. Analisis Naratif (Narrative Analysis) Menyusun temuan-temuan tersebut menjadi sebuah narasi analitis yang koheren untuk menjawabrumusan masalah.
   c. Triangulasi Sumber Memastikan keabsahan temuan dengan membandingkan dan mengecek konsistensi informasi dari berbagai sumber data yang berbeda (contoh: membandingkan laporan firma keamanan dengan pemberitaan media).

2.4 Keabsahan Data

Untuk memastikan keabsahan data dan temuan dalam penelitian kualitatif ini, digunakan tekniktriangulasi. Triangulasi yang diterapkan adalahtriangulasi sumber, yaitu dengan membandingkan dan mengecek balik data yang diperoleh dari satu sumber dengan sumber lainnya. Misalnya, informasi mengenai skala kebocoran data dariBleepingComputerdicek dengan laporan dariKasperskydan pemberitaan media nasional. Hal ini dilakukan untuk meminimalisasi bias dan meningkatkan akurasi serta kredibilitas analisis.

C. HASIL DAN PEMBAHASAN

Bagian ini menjelaskan hasil pemeriksaan keamanan jaringan komputer di bisnis belanja online, dengan menggunakan contoh kasus kebocoran data di Tokopedia sebagai bahan studi. Penelitian ini didasarkan pada data tambahan yang dikumpulkan dari laporan kejadian, artikel tentang keamanan internet, dan penelitian ilmiah yang relevan. Pembahasannya akan fokus pada temuan penting tentang kelemahan keamanan jaringan, serta dampaknya terhadap kegiatan operasional bisnis dan kepercayaan pelanggan.

1. **Kerentanan Keamanan Jaringan sebagai Penyebab Kebocoran Data**
   Dari hasil analisis, kebocoran data di Tokopedia sangat terkait dengan kelemahan dalam sistem keamanan jaringan. Data yang bocor termasuk informasi akun pengguna, seperti alamat email dan kata sandi yang sudah dienkripsi. Ini menunjukkan ada celah dalam cara melindungi jaringan dan mengatur siapa yang bisa

mengaksesnya. Temuan ini menegaskan bahwa bisnis belanja online berskala besar punya banyak titik yang rentan diserang, jadi mereka butuh sistem keamanan jaringan yang bertingkat dan saling terhubung.

Temuan ini cocok dengan penelitian sebelumnya yang bilang kalau kelemahan di lapisan jaringan dan sistem deteksi bisa dimanfaatkan orang jahat untuk mengambil data penting. Studi dari Stallings menunjukkan bahwa tanpa pengawasan jaringan yang aktif dan sistem deteksi penyusupan yang cukup, serangan siber bisa berjalan lama tanpa ketahuan. Di Tokopedia, kejadian bocornya data menunjukkan bahwa kalau kapasitas sistem ditingkatkan, keamanan jaringan juga harus diperbaiki secara menyeluruh.

Dampak dari temuan ini adalah pentingnya menerapkan keamanan jaringan yang nggak cuma fokus pada pencegahan, tapi juga pada mendeteksi dan merespons ancaman. Bagi para ahli di bisnis belanja online, hasil ini menekankan perlunya pemeriksaan keamanan jaringan secara rutin untuk menemukan celah potensial sebelum disalahgunakan oleh penyerang.

2. Dampak Kebocoran Data terhadap Kepercayaan Pengguna dan Operasional E-Commerce

Temuan penting kedua menunjukkan bahwa kebocoran data berdampak besar pada kepercayaan pengguna dan reputasi bisnis e-commerce. kejadian yang terjadi pada Tokopedia menimbulkan kekhawatiran pengguna terhadap keamanan data pribadi mereka, yang berpotensi memengaruhi tingkat loyalitas dan aktivitas transaksi. Dampak ini tidak hanya bersifat teknis, tetapi juga berdimensi bisnis dan sosial.

Hasil ini sesuai dengan penelitian sebelumnya yang menyatakan bahwa kepercayaan merupakan faktor kunci dalam keberhasilan e-commerce. Laudon dan Traver menegaskan bahwa keamanan itu jadi daar penting buat membangun hubungan jangka panjang dengan pelanggan. kalua ada terjadi kegagalan keamanan jaringan, perusahaan tidak hanya menghadapi risiko teknis, tetapi juga risiko penurunan citra dan kepercayaan publik.

Selain itu, hasil analisis ternyata penggunaan teknologi keamanan jaringan seperti firewall, enkripsi data, dan intrusion detection system sangat penting dalam mengurangi dampak dari kejadian keamanan. Dengan adanya mekanisme ini, sistem bisa lebih kuat melawan serangan dan proses penanganan insiden bisa lebih cepat. Temuan ini menunjukkan bahwa berinvestasi di keamanan jaringan adalah langkah strategis yang wajib dilakukan agar bisnis belanja online bisa terus berjalan lancar.

3. Limitations and Future Work

Penelitian ini punya beberapa batasan yang harus diperhatikan. Pertama, penelitian ini pakai data dari sumber luar, jadi analisisnya cuma berdasarkan info yang bisa diakses publik dan nggak bisa masuk ke detail teknis dalam sistem Tokopedia. Kedua, penelitian ini cuma deskriptif kualitatif, artinya nggak ada pengujian teknis langsung atau simulasi serangan jaringan. Batasan ini bisa bikin analisis tentang cara kerja keamanan jaringan kurang dalam.

Buat penelitian berikutnya, sebaiknya pakai cara yang lebih teknis, seperti mensimulasikan keamanan jaringan di platform belanja online atau melakukan analisis forensik digital terhadap kejadian keamanan. Penelitian selanjutnya juga bisa diperluas dengan membandingkan beberapa platform e-commerce biar dapat gambaran yang lebih lengkap tentang praktik keamanan jaringan di industri ini. Selain itu, pakai metode kuantitatif untuk mengukur seberapa besar dampak keamanan jaringan terhadap kepercayaan pengguna juga bisa jadi arah yang bagus.

Gambar 2 Hasil Penelitian Keamanan Jaringan Komputer

D. PENUTUP

Simpulan

Penelitian ini menyimpulkan bahwa keamanan jaringan komputer merupakan komponen fundamental dalam menjaga keberlanjutan bisnis e-commerce, khususnya pada platform berskala besar seperti Tokopedia. Berdasarkan hasil analisis studi kasus kebocoran data Tokopedia, penelitian ini menunjukkan bahwa kerentanan pada sistem keamanan jaringan dapat menyebabkan terjadinya kebocoran data pengguna yang berdampak signifikan terhadap kepercayaan pelanggan dan reputasi perusahaan. Temuan ini secara langsung menjawab tujuan penelitian dengan menegaskan bahwa penerapan mekanisme keamanan jaringan yang tidak memadai meningkatkan risiko pelanggaran data dan gangguan operasional e-commerce. Penelitian ini juga menyoroti peran penting teknologi keamanan jaringan, seperti firewall, enkripsi data, dan intrusion detection system, dalam melindungi kerahasiaan, integritas, dan ketersediaan data. Kontribusi utama penelitian ini terletak pada penyediaan analisis kontekstual terhadap insiden keamanan nyata pada industri e-commerce di Indonesia, yang masih

relatif terbatas dalam kajian akademik. Secara teoretis, penelitian ini memperkuat pemahaman bahwa keamanan jaringan tidak hanya berfungsi sebagai lapisan teknis, tetapi juga sebagai faktor strategis dalam membangun kepercayaan dan loyalitas pengguna. Dari sisi praktis, hasil penelitian ini memberikan implikasi bagi pelaku bisnis e-commerce dan pengelola sistem informasi untuk menjadikan keamanan jaringan sebagai prioritas utama melalui evaluasi keamanan secara berkala dan penerapan sistem pengamanan yang berlapis. Meskipun penelitian ini memiliki keterbatasan pada penggunaan data sekunder dan pendekatan deskriptif, temuan yang dihasilkan tetap memberikan gambaran yang relevan mengenai tantangan dan kebutuhan keamanan jaringan dalam e-commerce. Oleh karena itu, penelitian ini diharapkan dapat menjadi referensi awal bagi penelitian selanjutnya yang berfokus pada pendekatan teknis atau komparatif dalam meningkatkan ketahanan keamanan jaringan pada platform e-commerce.

Saran

Saran disusun berdasarkan analisis terhadap kelebihan dan kekurangan, hal-hal yang sudah dan belum tercapai dalam kegiatan, serta mempertimbangkan kelangsungan atau keberlanjutan kegiatan tersebut.

E. DAFTAR PUSTAKA

[1] A. Kadir, *Pengenalan Sistem Informasi*. Yogyakarta: Andi Offset, 2018.

[2] R. Abdulloh, *Keamanan Sistem Informasi*. Bandung: Informatika, 2017.

[3] M. S. Wahyudi dan A. Nugroho, "Analisis Keamanan Sistem Informasi pada Aplikasi E-Commerce," *Jurnal Teknologi Informasi dan Ilmu Komputer (JTIIK)*, vol. 8, no. 2, pp. 215–222, 2021.

[4] S. R. Putra dan D. M. Khairina, "Evaluasi Keamanan Jaringan Menggunakan Firewall dan Intrusion Detection System," *Jurnal Ilmiah Teknologi Informasi*, vol. 6, no. 1, pp. 45–53, 2020.

[5] R. A. Prasetyo, "Keamanan Data dan Privasi Pengguna dalam Sistem E-Commerce," *Jurnal Sistem Informasi*, vol. 15, no. 2, pp. 89–98, 2019.

[6] Y. H. Wibowo dan A. F. Ramadhan, "Analisis Risiko Keamanan Informasi pada Platform E-Commerce di Indonesia," *Jurnal RESTI (Rekayasa Sistem dan Teknologi Informasi)*, vol. 5, no. 4, pp. 642–649, 2021.

[7] Kominfo Republik Indonesia, *Keamanan Siber dan Perlindungan Data Pribadi di Indonesia*. Jakarta: Kementerian Komunikasi dan Informatika, 2020.

[8] Badan Siber dan Sandi Negara (BSSN), *Laporan Tahunan Keamanan Siber Indonesia*. Jakarta: BSSN, 2020.

[9] Tokopedia, "Pernyataan Resmi Terkait Isu Keamanan Data Pengguna," Tokopedia Official Blog, 2020.

[10] A. Hidayat dan N. Sari, "Pengaruh Keamanan Sistem terhadap Kepercayaan Pengguna E-Commerce," *Jurnal Manajemen Informatika*, vol. 9, no. 1, pp. 33–41, 2020.