

Tinjauan Sistem Keamanan Data Pelanggan di *E-Commerce*: Studi Kasus Platform Shopee

Yayi Naulia Silalahi¹, Muhammad Irwan Padli Nasution²

¹ Sistem Informasi, Universitas Islam Negeri Sumatera Utara, Medan

² Sistem Informasi, Universitas Islam Negeri Sumatera Utara, Medan

¹yayinauliasilalahi@gmail.com, ²irwannst@uinsu.ac.id

INTISARI

Keamanan data pelanggan merupakan hal penting dalam e-commerce untuk melindungi informasi pribadi pelanggan dari berbagai ancaman siber yang semakin pesat. Artikel ini meneliti sistem keamanan data pelanggan Shopee dengan fokus pada kinerja perlindungan data dan solusi terhadap masalah keamanan. Penelitian ini menggunakan pendekatan deskriptif kualitatif berbasis studi literatur untuk menganalisis berbagai teknik keamanan Shopee, termasuk enkripsi, autentikasi dua faktor, dan pemantauan ancaman. Meskipun Shopee masih menghadapi tantangan seperti serangan siber dan kebocoran data, hasil penelitian menunjukkan bahwa perusahaan telah menerapkan kebijakan keamanan dan privasi yang komprehensif. Artikel ini memberi rekomendasi terhadap Shopee agar terus memperbarui teknologi keamanan dan memberi tahu pengguna tentang pentingnya menjaga data pribadi. Hasil penelitian ini diharapkan dapat meningkatkan pemahaman tentang metode untuk melindungi data di platform e-commerce.

Kata kunci: Keamanan Data, E-Commerce, Shopee, Enkripsi, Autentikasi Dua Faktor

ABSTRACT

Customer data security is an essential in e-commerce to protect customer's personal information from various rapidly growing cyber threats. This article examines Shopee's customer data security system with a focus on data protection performance and solutions to security issues. This research uses a descriptive qualitative approach based on literature studies to analyze various security techniques of Shopee, including encryption, two-factor authentication, and threat monitoring. Although Shopee still faces challenges such as cyberattacks and data breaches, the research results indicate that the company has implemented comprehensive security and privacy policies. This article recommends that Shopee continue to update security technology and inform users about the importance of protecting personal data. The results of this research are expected to enhance understanding of methods for protecting data on e-commerce platforms.

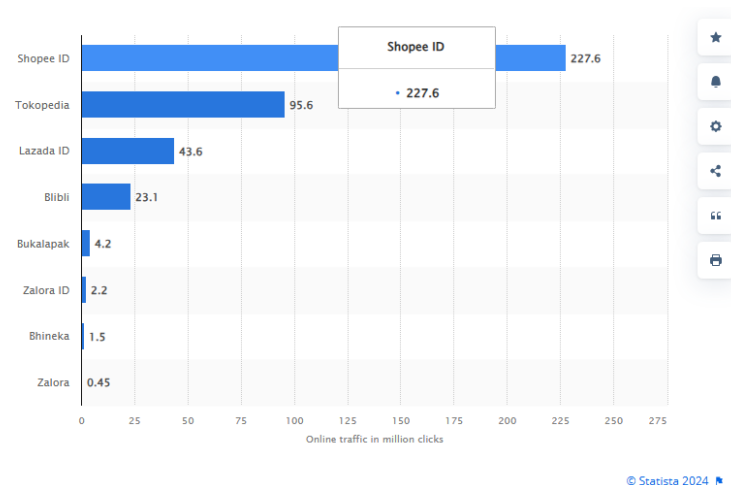
Keywords: Data Security, E-Commerce, Shopee, Encryption, Two-Factor Authentication

1. PENDAHULUAN

Perkembangan teknologi digital yang sangat pesat telah mendorong pertumbuhan industri *e-commerce* dan memungkinkan pelanggan dapat melakukan transaksi dan berbelanja secara online dengan lebih mudah. Namun, kemudahan ini juga diiringi dengan masalah besar seperti, ancaman yang semakin kompleks terhadap data

pribadi pelanggan. Dalam dunia modern, data pelanggan merupakan asset berharga yang sangat penting bagi bisnis. Namun, aka nada pihak-pihak yang tidak bertanggung jawab dapat menyalahgunakan hal tersebut. Perusahaan *e-commerce* harus memperhatikan keamanan data pelanggan jika mereka ingin membangun kepercayaan dan menjaga loyalitas pelanggan.

Shopee adalah toko online berbasis web dan aplikasi yang sudah berdiri sejak tahun 2015. Shopee menjual segala macam kebutuhan, mulai dari kebutuhan rumah tangga, *fashion*, alat kesehatan, elektronik, *skincare*, dan lainnya (Ramadhan & Anggraeni, 2022). Berdasarkan hasil penelitian yang dilakukan oleh Statista pada Februari 2024, Shopee merupakan platform *e-commerce* yang paling banyak dikunjungi di Indonesia dengan jumlah 227,6 juta kali dikunjungi (Statista, 2024).



Gambar 1. Leading E-Commerce Traffic Berdasarkan Kunjungan Web

Sebagai salah satu platform *e-commerce* terpopuler di Indonesia, Shopee juga menghadapi berbagai ancaman siber yang dapat mengancam integritas keamanan data pelanggan. Shopee harus memastikan bahwa sistem keamanannya mampu melindungi data pribadi pelanggan dari ancaman-ancaman keamanan seperti, penyalahgunaan data pribadi, pencurian data, dan serangan siber lainnya. Meskipun Shopee telah menggunakan berbagai teknologi keamanan seperti enkripsi dan autentikasi dua faktor, masih ada tantangan untuk memastikan keamanan data yang konsisten di tengah serangan siber dan ancaman privasi yang meningkat.

Dalam konteks *e-commerce*, keamanan data bukan sekedar menjaga informasi privasi pelanggan dari ancaman akses yang tidak sah, tetapi juga melibatkan

pengelolaan data secara bertanggung jawab, seperti penggunaan data hanya untuk tujuan yang sah dan hanya pihak berwenang yang memiliki akses untuk mengelolanya. Untuk melindungi data pribadi pelanggan dari berbagai serangan siber, pelaku bisnis *e-commerce* harus dapat memastikan bahwa mereka memiliki kebijakan privasi yang bersifat transparan dan sistem keamanan yang kuat (Mose, 2024).

General Data Protection Regulation (GDPR) merupakan regulasi keamanan data yang diterapkan di Uni Eropa. Secara global, GDPR ini menjadi standar yang ketat terkait keamanan data dan dijadikan referensi oleh banyak perusahaan *e-commerce* untuk sistem keamanan data mereka. *General Data Protection Regulation* (GDPR) mencakup pemrosesan data pribadi dengan dua cara, yaitu:

- 1) Data pribadi diproses secara otomatis yang artinya informasi data disimpan secara elektronik.
- 2) Data pribadi juga diproses secara non-otomatis atau manual untuk informasi pengarsipan.

Saat ini, Indonesia hanya memiliki Rancangan Peraturan Pemerintah tentang *E-commerce* (RPP *E-commerce*) yang memuat perubahan atas Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik. Karena belum disahkan, maka peraturan perundang-undangan yang berkaitan dengan *e-commerce* masih mengacu pada UU No. 11 tahun 2008 yang membahas Informasi dan Elektronik (UU ITE) (Jaya & Dewi, 2022).

Kebijakan privasi adalah perjanjian antar penyedia platform digital dengan pengguna, yang dikenal juga sebagai pernyataan atau pemberitahuan privasi. Kebijakan privasi mengatur informasi apa saja yang dikumpulkan, bagaimana pengorganisasian, bagaimana informasi itu digunakan, kepada siapa saja informasi itu akan dibagikan, prosedur pengamanan yang diberikan, hingga bagaimana cara membatalkan informasi yang tidak akurat (Dhianty, 2022). Dalam dunia *e-commerce*, teknik enkripsi data merupakan metode umum yang digunakan untuk menjaga keamanan data pelanggan. Enkripsi adalah teknik yang digunakan untuk mengkodekan data sehingga keamanannya terjaga dan tidak dapat dibaca tanpa dideskripsikan terlebih dahulu. Enkripsi berasal dari bahasa Yunani yaitu *kryptos* yang artinya tersembunyi atau rahasia (Rahmadi & Yunita, 2020).

Tujuan dari penelitian ini adalah untuk mengidentifikasi metode dan praktik keamanan data yang digunakan Shopee, menilai seberapa efektif kebijakan privasi mereka, dan memberikan saran untuk meningkatkan perlindungan data pelanggan. Metode deskriptif kualitatif, berbasis studi literatur, digunakan untuk mengevaluasi dan menganalisis sistem keamanan data Shopee. Artikel ini diharapkan dapat memberikan pemahaman yang lebih baik tentang metode keamanan data *e-commerce* dan membantu pihak-pihak yang terkait dalam menerapkan metode terbaik untuk melindungi data pelanggan di platform digital.

2. METODOLOGI

Artikel ini menggunakan metode penelitian pendekatan deskriptif kualitatif dengan teknik kajian pustaka atau studi literatur. Penelitian ini bertujuan untuk memahami dan menganalisis sistem keamanan data pelanggan pada *e-commerce* dengan studi kasus pada platform Shopee.

Kajian pustaka ialah metode penelitian yang menggunakan analisis literatur dari berbagai sumber, seperti artikel jurnal, buku, laporan penelitian, artikel konferensi, dan publikasi industri. Tujuan utama metode ini adalah untuk mengumpulkan informasi yang relevan untuk memperoleh pemahaman yang lebih baik tentang hal yang diteliti dan untuk menemukan pola, tren, dan perbedaan dalam penelitian sebelumnya (Wekke & Dkk, 2019).

Penelitian ini dilakukan secara sistematis dengan langkah-langkah seperti berikut:

- 1) Penelusuran literatur yang dilakukan dengan menggunakan kata kunci seperti, keamanan data, *e-commerce*, Shopee, enkripsi, dan autentikasi dua faktor. Penelusuran literatur ini dapat dilakukan pada *database* akademik seperti Google Scholar, ScientDirect, Xplore, artikel-artikel berita resmi, serta jurnal nasional yang memuat penelitian terkait.
- 2) Seleksi literatur, setelah melakukan penelusuran literatur dan mengumpulkan artikel-artikel, dilakukan seleksi sesuai dengan kriteria penelitian. Hanya literatur yang relevan dengan fokus penelitian dan memuat informasi terkini dan terpercaya yang akan digunakan dalam artikel ini.

- 3) Klasifikasi tematik, setelah seleksi literatur, literatur yang terpilih disusun menurut topik utama, seperti keamanan data pelanggan Shopee, arsitektur atau infrastruktur keamanan Shopee, tantangan keamanan yang dihadapi Shopee serta solusi yang digunakan.
- 4) Analisis dan sintesis data, pada langkah ini, data yang dikumpulkan, dianalisis dan disintesis untuk mendapatkan pemahaman yang lengkap tentang subjek penelitian. Setiap topik yang dianalisis disusun secara sistematis dan dinarasikan untuk menunjukkan bagaimana sistem keamanan data pelanggan pada platform Shopee.



Gambar 2. Alur Penelitian

3. HASIL DAN PEMBAHASAN

3.1. Arsitektur dan Infrastruktur Keamanan Data Shopee

Berdasarkan website resmi Shopee, sistem keamanan data pada Shopee sudah menggunakan enkripsi data dengan protocol SSL/TLS, autentikasi dua faktor untuk verifikasi data yang dapat dilakukan melalui:

1. Verifikasi KTP
2. Link verifikasi
3. No. Handphone
4. Email
5. Password akun
6. Verifikasi wajah
7. Verifikasi Biometrik

Verifikasi KTP diperlukan untuk akses ShopeePay untuk memverifikasi data saat pertama kali login dan melakukan transaksi dalam Shopee. Verifikasi melalui link, no. handphone, e-mail dan password merupakan pengaturan keamanan akun yang hanya dapat dilakukan oleh pengguna. Sedangkan verifikasi wajah, biasanya digunakan saat mendaftar ShopeePay dan mendaftar ShopeePay Later.

Untuk melindungi proses login dan transaksi tertentu, Shopee juga menggunakan autentikasi multifaktor (MFA). Pengguna menggunakan autentikasi multifaktor untuk verifikasi data identitas dengan metode verifikasi tambahan seperti OTP (*One Time Password*) yang dapat dikirimkan melalui e-mail maupun no. handphone (Shopee, 2023).

Enkripsi adalah proses mengubah data atau informasi asli (*plaintext*) menjadi bentuk yang tidak dapat dibaca atau dipahami (*ciphertext*). Proses ini dilakukan dengan menggunakan algoritma dan kunci enkripsi khusus. Enkripsi data digunakan untuk melindungi informasi sensitif saat dikirim melalui jaringan dan memastikan bahwa hanya orang yang dituju yang dapat membaca dan memahami data tersebut. Protokol yang paling umum digunakan dalam enkripsi adalah *Secure Sockets Layer* (SSL) / *Transport Layer Security* (TLS).

Secure Sockets Layer (SSL) ialah protocol kriptografi untuk keamanan komunikasi jaringan. SSL banyak digunakan dalam layanan transaksi online seperti *e-commerce*, perbankan online dan layanan keuangan digital lainnya. SSL bekerja pada lapisan transportasi di atas protocol TCP (*Transmission Control Protocol*). SSL memiliki kerahasiaan, integritas, dan autentikasi data yang ditransfer antara klien dengan server. Sedangkan *Transport Layer Security* (TLS) adalah protokol keamanan yang digunakan untuk menjaga keamanan komunikasi antara klien dan server melalui jaringan. Dibuat untuk menjaga kerahasiaan, integritas, dan autentikasi data yang dikirimkan melalui jaringan, TLS telah menggantikan protokol *Secure Sockets Layer* (SSL) dan telah menjadi standar industri (Suliman, 2023).

3.2. Efektivitas Kebijakan Privasi dan Perlindungan Data

Shopee memiliki kebijakan privasi yang dirancang untuk membantu pengguna memahami bagaimana proses pengumpulan, penggunaan, dan pengolahan data pribadi

dan membantu membuat keputusan yang tepat sebelum memberikan data kepada Shopee. Kebijakan privasi berlaku bagi setiap pengguna baik pembeli maupun penjual.

Kebijakan privasi diberikan setiap saat Shopee mengumpulkan data pribadi seperti saat melakukan pendaftaran akun, saat melakukan transaksi, atau saat melakukan perjanjian dengan pihak yang ada di Shopee. Data yang dikumpulkan oleh Shopee antara lain seperti, nama, email, tanggal lahir, alamat tagihan, rekening bank dan informasi pembayaran, nomor telepon, serta informasi-informasi yang berkaitan dengan konten yang digunakan pengguna. Kebijakan privasi diberikan untuk memastikan apakah pengguna setuju atau tidak terhadap data-data yang akan diminta oleh Shopee. Jika pengguna setuju, maka Shopee akan melanjutkan layanan berikutnya (Shopee, 2020).

Menurut kebijakan privasi Shopee, platform tersebut berkomitmen untuk melindungi data pengguna. Platform tersebut akan mematuhi peraturan yang diatur oleh Undang-Undang Perlindungan Data Pribadi (UU PDP) dan Undang-Undang Informasi dan Transaksi Elektronik (UU ITE).

3.3. Studi Kasus Keamanan Data Shopee

Tidak sedikit laporan kebocoran data pribadi pengguna Shopee. Viva News melaporkan insiden keamanan data di mana data pelanggan Shopee dicuri dan diperjualbelikan di forum peretas BreachForums. Informasi pertama tentang insiden ini datang dari akun X @FalconFeedsio, yang membagikan tangkapan layar dari forum tersebut. Seorang pengguna bernama "X3N666C00N3" menulis dalam postingannya bahwa dia memiliki data sekitar 200.000 pengguna Shopee, termasuk nama, nomor kontak, kode pos, dan alamat.

Kasus ini menunjukkan kebingungan berkelanjutan tentang keamanan data di Indonesia, terutama di sektor *e-commerce*. Tren serupa telah terjadi pada perusahaan besar lainnya di Indonesia, seperti Tokopedia dan Bukalapak, sebelum kebocoran data ini. Situasi ini menunjukkan bahwa protokol keamanan siber yang lebih baik diperlukan untuk melindungi data pribadi pengguna dari ancaman digital yang semakin kompleks (Naufal, 2022).

3.4. Tantangan dan Upaya untuk Meningkatkan Keamanan Data

Meskipun Shopee telah mengambil berbagai tindakan keamanan, platform ini masih menghadapi masalah seperti serangan siber yang lebih kompleks dan kemungkinan kebocoran data. Untuk mengatasi tantangan ini, Shopee harus terus meningkatkan sistem keamanannya dan mendidik pengguna tentang pentingnya melindungi data mereka sendiri. Terdapat beberapa ancaman atau tantangan sistem keamanan data pada *e-commerce*, yaitu:

- 1) Penerobohan sistem, di mana seseorang yang tidak berhak dapat mengakses sistem komputer dan melakukan apa pun.
- 2) Penyalahgunaan wewenang, di mana seseorang yang berhak menyalahgunakan wewenang yang dimilikinya.
- 3) Penanaman, yang berarti melakukan penyerangan yang direncanakan, seperti memasukkan Trojan Horse dan melakukan penyerangan pada waktu yang telah ditentukan sebelumnya.
- 4) Pengawasan Komunikasi, yang berarti memantau semua informasi rahasia.
- 5) Tampering Komunikasi, yang berarti penyerang mengubah pesan di tengah-tengah proses transmisi data dan mengganti sistem server dengan sistem server yang palsu.
- 6) *Denial of Service* (DoS), yang berarti menolak layanan kepada klien yang berhak
- 7) *Reduption*, yang berarti menolak aktivitas transaksi karena kesalahan teknis atau kesalahan yang disengaja (Jaya & Dewi, 2022).

Upaya yang dapat dilakukan Shopee ialah melakukan audit keamanan secara rutin, mengembangkan sistem pemantauan ancaman yang lebih baik, dan memberikan notifikasi kepada pengguna mengenai perubahan status keamanan akun mereka.

Teknologi *Blockchain* dan *Smart Contract* dapat menjadi rekomendasi bagi Shopee untuk meningkatkan sistem keamanan datanya. Dengan sifat imutabilitas dan transparansi, *blockchain* dapat menjamin data atau informasi yang masuk dalam jaringan tidak akan dapat diubah oleh pihak-pihak yang tidak termasuk dalam jaringan tersebut (Hesananda, 2024). Sedangkan *Smart Contract* dapat digunakan ketika dilakukan perjanjian. *Smart Contract* merupakan perjanjian yang dilakukan secara otomatis menggunakan sistem komputer tanpa campur tangan pengadilan dan hanya

diketahui oleh pihak terkait, karena *Smart Contract* menggunakan kode untuk merahasiakan kontrak kesepakatan tersebut (Rizqi & Prasetya, 2022).

4. KESIMPULAN

Berdasarkan hasil penelitian Tinjauan Sistem Keamanan Data Pelanggan di *E-Commerce*: Studi Kasus Platform Shopee, dapat disimpulkan bahwa, sistem keamanan data pelanggan pada Shopee sudah mencapai standar yang canggih. Shopee menerapkan arsitektur atau infrastruktur keamanan enkripsi dengan teknik SSL/TLS yang berfungsi melindungi data selama proses transaksi di dalam jaringan. Selain itu, Shopee juga menyediakan fitur verifikasi autentikasi dua faktor, seperti verifikasi OTP, verifikasi wajah, hingga verifikasi biometrik sebagai verifikasi tambahan untuk memperkuat keamanan data.

Shopee menggunakan berbagai teknologi ini untuk menunjukkan komitmennya yang kuat untuk menjaga privasi dan keamanan data pelanggannya. Selain itu, mereka memastikan bahwa setiap layer keamanan telah dirancang khusus untuk menghadapi berbagai ancaman siber yang mungkin mengancam platform e-commerce tersebut.

5. DAFTAR PUSTAKA

- Dhianty, R. (2022). Kebijakan Privasi (Privacy Policy) dan Peraturan Perundang-Undangan Sektor Digital vis a vis Kebocoran Data Pribadi. *Jurnal Kebijakan Publik dan Hukum*, 2(1). <https://journal.puskapum.org/index.php/scripta/article/view/16%0A>
- Hesananda, R. (2024). *Buku Ajar Finansial Teknologi* (M. Nasrudin (ed.)). PT Nasya Expanding Management.
- Jaya, I. K. N. A., & Dewi, I. A. U. (2022). *Regulasi Keamanan Data Pribadi Pelanggan pada E-commerce di Indonesia*. http://repo.unhi.ac.id/jspui/bitstream/123456789/2046/1/Keamanan_data_informasi_ecommerce.pdf
- Mose, A. (2024). *E-Commerce: Strategi Menghadapi Tantangan Perdagangan Online* (T. Yuwanda (ed.)). Takaza Innovatix Labs. https://www.google.co.id/books/edition/E_commerce/_WgnEQAAQBAJ?hl=id&gbpv=1&dq=keamanan+data+pelanggan+di+ecommerce&pg=PA122&printsec=fro ntcover
- Naufal, M. (2022). Data Shopee Diduga Bocor dan Diobral di Forum Hacker. *Viva News*. <https://www.viva.co.id/digital/startup/1525921-data-shopee-diduga-bocor-dan-diobral-di-forum-hacker>

- Rahmadi, P., & Yunita, H. D. (2020). Implementasi Pengamanan Basis Data dengan Teknik Enkripsi (Studi Kasus: PT. Sugar Group Companies). *Jurnal Cendikia*, 19(1). <https://jurnal.dcc.ac.id/index.php/JC/article/view/331>
- Ramadhan, I. C., & Anggraeni, T. C. (2022). Pengaruh Promosi, Keamanan dan Kualitas Pelayanan Terhadap Kepuasan Pelanggan Shopee. *Jurnal Ilmiah Disiplin*, 1(1). <https://doi.org/https://doi.org/10.56127/jukim.v1i1.121>
- Rizqi, L. A. M., & Prasetya, D. F. (2022). Urgensi Penggunaan Smart Contract Dalam Transaksi Jual Beli Di E-Commerce. *Jurnal Hukum Lex Generalis*, 3(4), 330–331.
- Shopee. (2020). *Kebijakan Privasi Shopee*. help.shopee.co.id. <https://help.shopee.co.id/portal/4/article/71188-Kebijakan-Privasi-Shopee>
- Shopee. (2023). *Tentang Keamanan Akun*. seller.shopee.co.id. <https://seller.shopee.co.id/edu/article/10801>
- Statista. (2024). *Leading e-commerce sites in Indonesia in February 2024, by monthly traffic (in million web visits)*. Statista. <https://www.statista.com/statistics/869700/indonesia-top-10-e-commerce-sites/>
- Suliman, A. H. (2023). *Analisis Keamanan Protokol Kriptografi SSL/TLS dengan Algoritma ECC pada Layanan Transaksi Online pada E-Commerce*. [https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2022-2023/Makalah2023/Makalah-KriptoKoding-2023 \(21\).pdf](https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi-dan-Koding/2022-2023/Makalah2023/Makalah-KriptoKoding-2023 (21).pdf)
- Wekke, I. S., & Dkk. (2019). *Metode Penelitian Ekonomi Syariah*. CV. Adi Karya Mandiri.