Digital Transformation Technology (Digitech) | e-ISSN: 2807-9000
Volume 4, **Number** 2, September 2024
https://doi.org/10.47709/digitech.v4i2.4969

Algoritma Autentikasi Multi Factor Sebagai Solusi Untuk Meningkatkan Keamanan Sistem Pembayaran E-Commerce

Ismi Melyana[1], M.Satria Darmawan[2], Syufiulloh syukur[3], M.Ikram Abib Syah[4], Fenny Purwani[5]
[1,2,3,4,5]Sistem Informasi, Fakultas Sains dan Teknologi, UIN Raden Fatah, Palembang, Indonesia
[1]melyanaismi22@gmail.com, [2]satriario1404@gmail.com, [3]syufiullohsyukur@gmail.com, [4]m.ikram0325@gmail.com, [5]fennypurwani_uin@radenfatah.ac.id

open access
Histori Artikel:
Diajukan: 17 November 2024
Disetujui: 15 Desember 2024
Dipublikasi: 30 Desember 2024
Kata Kunci:
Metode autentikasi, E-commerce, Keamanan, transaksi risiko,Ancaman Siber, Fraud Detection Systems
Digital Transformation Technology (Digitech) *is an Creative Commons License This work is licensed under a Creative Commons Attribution-NonCommercial 4.0 International (CC BY-NC 4.0).*

Abstrak
E-commerce dikenal sebagai pasar online, adalah aktivitas membeli barang dan jasa melalui internet dengan menggunakan perangkat elektronik. E-commerce menjadi semakin populer karena mudahnya dan menghemat waktu, memungkinkan transaksi tanpa pertemuan langsung antara penjual dan pembeli. Namun, risiko keamanan meningkat seiring dengan perubahan ini, terutama berkaitan dengan akses ilegal dan perlindungan data konsumen. Artikel ini membahas autentikasi multi faktor (AMF) dan peran teknologi ini dalam melindungi e-commerce dari ancaman keamanan yang semakin kompleks. Autentikasi multi faktor menggabungkan berbagai lapisan verifikasi untuk memperkuat sistem keamanan e-commerce, khususnya dalam hal transaksi pembayaran online. AMF diharapkan dapat meningkatkan kepercayaan konsumen dalam bertransaksi secara daring, menjaga kerahasiaan data, dan mengurangi risiko akses ilegal. Autentifikasi Multi-Faktor (AMF) merupakan solusi krisis yang efektif untuk masalah keamanan dalam e-commerce yang menggabungkan berbagai lapisan verifikasi untuk melindungi sistem pembayaran online, mengurangi risiko akses ilegal, dan meningkatkan kepercayaan konsumen. Artikel ini membahas manfaat autentikasi multi-faktor (AMF) dalam e-commerce, metode autentikasi yang digunakan, serta cara teknologi ini menghadapi ancaman keamanan yang terus berkembang.

PENDAHULUAN

E-commerce dikenal sebagai pasar online, adalah aktivitas membeli barang dan jasa melalui internet dengan menggunakan perangkat elektronik. E-commerce menjadi semakin populer karena mudahnya dan menghemat waktu, memungkinkan transaksi tanpa pertemuan langsung antara penjual dan pembeli (Raihan, 2023). Selain itu, Dengan kemajuan teknologi, e-commerce menjadi lebih mudah diakses oleh banyak orang. Sehingga, menjadi pilihan utama untuk menjalankan bisnis di era modern. E-commerce membawa risiko keamanan. Meskipun menawarkan kemudahan dan kenyamanan, Keamanan sendiri berarti melindungi atau melindungi sumber fisik dan konseptual dari ancaman dari manusia atau dunia luar. Sumber konseptual termasuk data dan informasi. Problem utama dalam industri e-commerce saat ini adalah privasi dan keamanan data pribadi (Nafi'ah, 2020).

Untuk memastikan keandalan dalam transaksi barang atau jasa jarak jauh, sistem e-commerce harus mengikuti aturan dari beberapa infrastruktur seperti sistem distribusi barang *(flow of goods)*, sistem pembayaran *(flow of money)*, dan sistem informasi *(flow of information)* (Karmawati E et al., 2019a). Aturan-aturan infrastruktur tersebut mencakup seluruh kebutuhan sistem e-commerce, terutama dalam menjaga kepercayaan konsumen. Salah satu langkah untuk memastikan kelancaran pemenuhan infrastruktur tersebut adalah dengan memperhatikan aspek keamanan (security) yang harus diberikan kepada pelanggan. Sistem keamanan e-commerce bertujuan untuk menjaga proses transaksi agar tetap aman dan nyaman. Oleh karena itu, penelitian ini mengembangkan sistem keamanan e-commerce dengan melindungi data transaksi langsung melalui script pada halaman web tanpa menggunakan protokol keamanan eksternal. Sistem ini memanfaatkan algoritma berbasis script, seperti encoding Base 64, enkripsi RC6, dan enkripsi RSA, untuk melindungi proses transaksi secara efektif (Putri et al., 2024). Keamanan adalah upaya perlindungan terhadap sumber daya fisik dan konseptual dari ancaman alam atau manusia. Perlindungan terhadap sumber konseptual mencakup data dan informasi. Salah satu masalah utama dalam e-commerce saat ini adalah privasi dan keamanan data pribadi seperti nama, alamat, nomor telepon, dan informasi keuangan, rentan terhadap pencurian atau penyalahgunaan oleh pihak yang tidak bertanggung jawab. Serangan malware, phishing, peretasan, dan pencurian identitas merupakan beberapa pelanggaran keamanan data pribadi pengguna e-commerce yang dapat menyebabkan kehilangan uang dan merusak reputasi pengguna di masyarakat (Nugraha et al., 2021).

Dengan menggunakan tiga kriteria pemilik, platform elektronik, dan pengguna, empat masalah keamanan utama yang dihadapi oleh industri e-commerce dapat diidentifikasi. (Kuruwitaarachchi et al., 2019). Sangat penting bagi pengguna e-commerce untuk memahami dan mengambil tindakan yang tepat untuk melindungi data pribadi mereka. Keempat masalah keamanan tersebut adalah keamanan transaksi, privasi, keamanan sistem perdagangan, dan kejahatan siber di e-commerce. Jurnal ini akan membahas tentang Penerapan Algoritma Autentikasi Multi factor sebagai Solusi untuk meningkatkan keamanan pada Sistem Pembayaran E-Commerce.

STUDI LITERATUR

Penelitian yang dilakukan oleh (Aji, 2023) mengungkapkan berbagai upaya yang telah diterapkan untuk meningkatkan keamanan e-commerce, terutama dalam menghadapi ancaman signifikan terhadap informasi pribadi pengguna. Dalam konteks ini, penekanan pada metode yang berpusat pada pengguna menjadi sangat penting. Metode ini tidak hanya bertujuan untuk memperkuat pertahanan terhadap serangan cyber tetapi juga untuk meningkatkan kesadaran pengguna mengenai pentingnya melindungi data pribadi mereka. Dengan menerapkan pendekatan yang lebih terarah kepada kebutuhan dan perilaku pengguna, langkah-langkah yang diambil dapat lebih efektif dalam mencegah kebocoran informasi dan menjaga privasi. Hal ini menunjukkan bahwa keamanan siber dalam e-commerce tidak bisa diabaikan, dan memerlukan kolaborasi antara teknologi dan kesadaran pengguna untuk menciptakan lingkungan yang aman bagi semua pihak terlibat.

Kemudian pada penelitian yang dilakukan oleh (Karmawati E et al., 2019) menunjukkan Model distribusi seperti Carrier Delivery dan Last Mile Delivery sangat efektif dalam meningkatkan layanan e-commerce dengan memastikan pengiriman yang efisien dan cepat. Carrier Delivery memanfaatkan berbagai jenis transportasi untuk mengantarkan produk dari pusat distribusi, sementara Last Mile Delivery fokus pada pengantaran akhir ke konsumen, yang merupakan tahap paling penting. Kedua model ini memenuhi harapan konsumen akan layanan yang cepat dan dapat diandalkan. Dengan mengintegrasikan teknologi modern seperti pelacakan real-time dan kendaraan ramah lingkungan, e-commerce tidak hanya meningkatkan pengalaman pelanggan, tetapi juga dapat mengurangi biaya operasional. Namun, peningkatan efisiensi ini juga membawa tantangan terhadap keamanan, karena informasi pribadi pengguna dalam proses pengiriman harus dilindungi secara ketat untuk mencegah kebocoran data dan ancaman cyber.

Selanjutnya penelitian yang dilakukan oleh (Putri et al., 2024) diidentifikasi bahwa enkripsi dan verifikasi ganda memainkan peran krusial dalam menjaga keamanan data pelanggan. Enkripsi berfungsi untuk melindungi informasi sensitif dari akses yang tidak sah, sementara verifikasi ganda menambah lapisan keamanan tambahan dengan memastikan bahwa hanya pengguna yang terotorisasi yang dapat mengakses data tersebut. Kombinasi kedua metode ini tidak hanya meningkatkan kepercayaan pelanggan terhadap sistem, tetapi juga meminimalkan risiko kebocoran data yang dapat merugikan baik pelanggan maupun perusahaan.

Pada penelitian yang dilakukan oleh (Kehista et al., 2023) tentang pentingnya melindungi data pribadi dari ancaman malware dan phishing melalui pemanfaatan teknologi seperti One-Time Password (OTP). Teknologi OTP berfungsi sebagai lapisan tambahan dalam sistem keamanan, di mana setiap transaksi atau akses ke informasi sensitif memerlukan kode yang hanya berlaku untuk satu kali penggunaan. Dengan cara ini, meskipun informasi identitas seorang pengguna telah dicuri, penyerang tidak akan dapat mengakses data tersebut tanpa kode OTP yang valid. Implementasi teknologi ini semakin penting di tengah meningkatnya serangan siber, menawarkan solusi yang efektif untuk melindungi data pribadi dan meningkatkan keamanan online secara keseluruhan.

Pada penelitian selanjutnya dilakukan oleh (Pebiyanti et al., 2023) membahas mengenai kualitas informasi, persepsi keamanan, dan privasi merupakan faktor-faktor yang signifikan dalam memengaruhi kepercayaan pengguna saat berbelanja online. Pengguna cenderung merasa lebih aman dan percaya ketika mereka mendapatkan informasi yang akurat dan transparan tentang produk serta layanan yang ditawarkan. Selain itu, persepsi positif terhadap keamanan situs web dan pengelolaan privasi data pribadi juga berkontribusi terhadap peningkatan kepercayaan ini. Hasil penelitian menunjukkan bahwa implementasi autentikasi multi-faktor (AMF) sangat relevan dalam konteks ini, karena memberikan perlindungan tambahan yang dapat meningkatkan persepsi keamanan dan meminimalkan risiko kebocoran informasi, sehingga mendorong pengguna untuk lebih percaya dan aktif dalam berbelanja secara online.

METODE PENELITIAN

Metode kualitatif dalam penelitian ini digunakan untuk memahami pengalaman dan persepsi pengguna terhadap algoritma autentifikasi multi-faktor (AMF) dalam e-commerce. memanfaatkan studi literatur sebagai metode utama. Data sekunder dikumpulkan dari berbagai sumber, termasuk jurnal ilmiah, artikel konferensi, dan buku yang diterbitkan dalam lima tahun terakhir. Sementara itu, algoritma autentifikasi multi-faktor bekerja dengan menggabungkan dua atau lebih metode verifikasi identitas pengguna, seperti password, token atau SMS, dan biometrik. Sehingga meningkatkan keamanan secara signifikan dengan mengurangi risiko akses tidak sah,

terlepas dari kemungkinan kebocoran data password. Integrasi pendekatan kualitatif ini dengan algoritma (AMF) memungkinkan pengembang untuk merancang sistem yang lebih responsif terhadap kebutuhan dan kekhawatiran pengguna.



Gambar 1. Alur Penelitian

Penelitian ini berfokus pada kajian penerapan autentikasi multi-faktor (AMF) dalam meningkatkan keamanan pada sistem pembayaran e-commerce serta tantangan yang dihadapi.

Tahapan penelitian dilakukan melalui langkah-langkah berikut:

1) Pengumpulan Data Sekunder
   Mengidentifikasi sumber literatur relevan menggunakan database akademik seperti Google Scholar, IEEE Xplore, dan ScienceDirect. Literatur dipilih berdasarkan topik penerapan AMF, keamanan siber, dan e-commerce.
2) Evaluasi dan Seleksi Literatur
   Literatur yang terkumpul dievaluasi berdasarkan relevansi, keakuratan, dan kontribusi terhadap pemahaman penerapan teknologi AMF.
3) Analisis Data
   Data dianalisis untuk mengidentifikasi metode autentikasi terkini, seperti teknologi biometrik dan verifikasi berbasis perangkat seluler, serta efektivitas teknologi tersebut dalam menangani ancaman siber.
4) Penyusunan Rekomendasi
   Berdasarkan hasil analisis, rekomendasi disusun mengenai penerapan AMF dalam sistem pembayaran e-commerce, terutama dalam menghadapi krisis keamanan yang berkembang.

HASIL

Dampak dari Risiko terhadap ancaman keamanan data pribadi pengguna e-commerce dalam keamanan data pribadi e-commerce, mempunyai risiko termasuk kerusakan atau kehilangan data pelanggan serta kemungkinan akibat dampak buruk bagi perusahaan, seperti reputasi yang buruk, hukuman, atau kehilangan pelanggan. Selain itu, penulis berpendapat bahwa ancaman ini berdampak pada keamanan data pengguna e-commerce karena pengguna harus memastikan bahwa data mereka aman saat melakukan transaksi e-commerce. Pelanggaran data dapat berdampak negatif pada baik pengguna maupun perusahaan penyedia layanan e-commerce.Contoh kasus yang dibahas oleh (Raihan, 2023). terjadi pada Tokopedia, terdapat seorang hacker bernama “Why So Dank” berhasil mencuri data pengguna pada 17 April 2020. Berita tentang peretasan pertama kali dipublikasikan oleh akun Twitter @underthebreach, yang menyatakan bahwa 15 juta akun Tokopedia telah diretas. Namun, investigasi lebih lanjut menunjukkan bahwa jumlah akun yang diretas meningkat menjadi 7 juta akun penjual dan 91 juta pengguna, yang menunjukkan bahwa hampir semua akun Tokopedia terpapar dan data mereka dicuri. Kasus ini menunjukkan ancaman besar terhadap keamanan data pribadi karena e-commerce mengumpulkan dan menyimpan informasi pribadi pelanggan seperti data kartu kredit, alamat email, dan informasi lainnya. Relevansi antara ancaman dan keamanan data sangat penting karena menunjukkan betapa pentingnya mengambil tindakan proaktif untuk mengatasi ancaman dan menjaga privasi data. bahwa risiko memengaruhi niat beli, dengan keamanan yang buruk memengaruhi niat beli yang menurun. Dengan demikian, Jika tidak ditangani dengan baik, keamanan data pribadi e-commerce dapat terancam, yang dapat mengakibatkan kerugian finansial dan non-finansial serta kehilangan kepercayaan pelanggan.

Tabel 1. Risiko Keamanan Data dan Dampaknya terhadap Pengguna

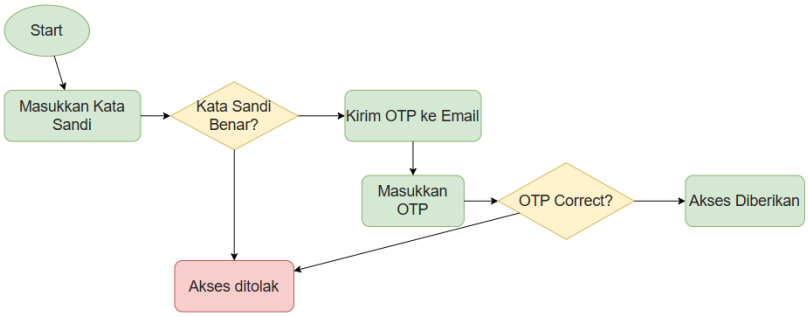
Jenis Ancaman	Dampak Terhadap Pengguna	Dampak Terhadap Perusahaan
Phishing	Pencurian kredensial pengguna	Penurunan kepercayaan pelanggan
Malware	Kehilangan data sensitif	Kerugian finansial

Pencurian Identitas	Penyalahgunaan data pribadi	Gugatan hukum dan denda
Peretasan (Hacking)	Akses tidak sah ke akun pengguna	Kehilangan pelanggan

Tabel 2. Tingkat Risiko Sebelum dan Sesudah Implementasi AMF (%)

Jenis Ancaman	Risiko Sebelum AMF (%)	Risiko Setelah AMF (%)
Phishing	80%	20%
Malware	70%	15%
Pencurian Identitas	60%	10%
Peretasan	75%	18%

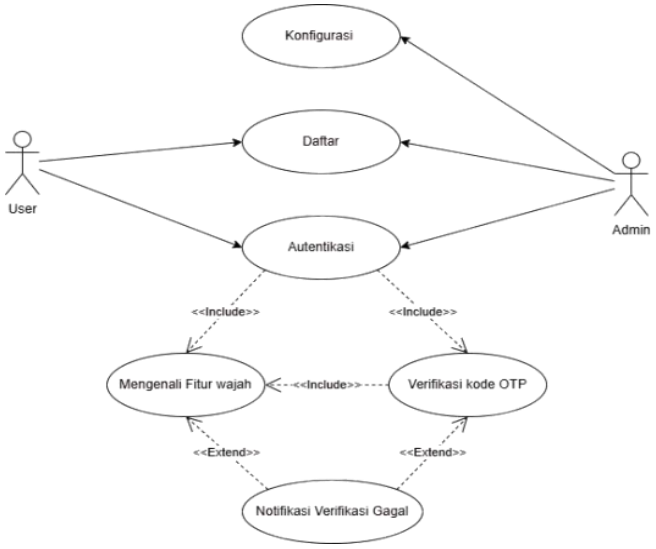
Alur Proses Autentikasi Multi-Faktor pada Sistem Pembayaran



Gambar 2. Proses Autentikasi Multi-Faktor pada Sistem Pembayaran

PEMBAHASAN

Dampak ancaman keamanan data pribadi pada pengguna e-commerce dalam konteks e-commerce ancaman terhadap keamanan data pribadi pengguna merupakan serangan digital atau kejahatan yang mengancam privasi dan keamanan pengguna. Hal ini, merupakan ancaman yang paling signifikan bagi sistem keamanan e-commerce yang melibatkan pelaku bisnis dan konsumen). E-commerce adalah jenis perdagangan online di mana untuk melakukan transaksi, pelanggan harus memberikan informasi pribadi seperti nama, alamat, nomor telepon, dan nomor kartu kredit. Jika informasi ini jatuh ke tangan orang yang salah, pelanggan berpotensi kehilangan uang atau ditipu oleh orang yang tidak bertanggung jawab

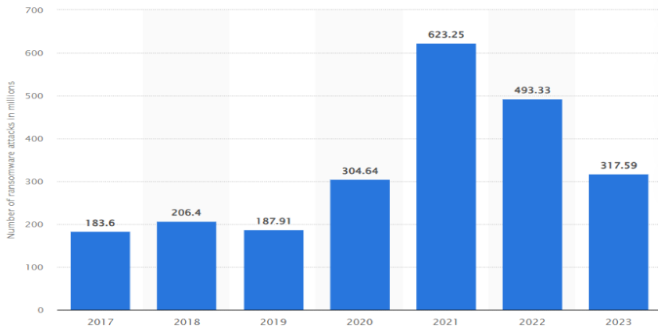


Gambar 3. Skema Interaksi Aktor dalam Autentifikasi Multi Faktor

Dalam sistem pembayaran e-commerce, *Customer* dan *Admin* berperan penting dalam proses autentikasi multi-faktor. *Customer* login untuk mengakses akun sebagai langkah awal autentikasi. Sistem kemudian meminta autentikasi tambahan, seperti kode OTP atau verifikasi biometrik, sebagai lapisan keamanan ekstra. Proses ini melibatkan *Verifikasi Email/OTP* atau *Verifikasi ID* untuk memastikan bahwa pengguna yang mengakses adalah sah. *Admin* bertugas mengelola sistem autentikasi dan memantau verifikasi ini agar transaksi terlindungi dari akses yang tidak sah. Dengan alur autentikasi berlapis ini, algoritma autentikasi multi-faktor dapat meningkatkan keamanan dan mencegah penyalahgunaan dalam transaksi e-commerce.
Berikut merupakan Langkah Langkah Penerapan Autentifikasi Multi Factor yang bisa diterapkan pada E-commerce sebagai berikut.

1. Identifikasi Kebutuhan Keamanan dalam e-commerce untuk perangkat yang mendukung seperti kombinasi kata sandi dan OTP atau biometrik untuk mendukung dalam meningkatkan keamanan. Menggunakan OTP yang dikirimkan melalui SMS atau Email untuk mencegah akses anomali.
2. Konfigurasi Sistem AMF ketika user mencoba login dari perangkat baru atau lokasi berbeda mereka diminta memverifikasi identitasnya
3. Uji Implementasi seperti menguji apakah pelanggan dapat menerima OTP atau kode autentifikasi secara cepat dan akurat
4. Sosialisasi dan Pelatihan Pengguna memberikan edukasi mengenai sistem keamanan AMF di platform e-commerce dan bagaimana AMF melindungi user dari resiko penipuan

Pemantauan dan Pemeliharaan pada tahap ini memantau aktifitas login, autentifikasi dan transaksi untuk medeteksi upaya login yang anomali dan mencurigakan. Selain itu, mengatur sistem dan memastikan apakah sistem mengirim peringatan jika ada upaya login yang mencurigakan pada akun pengguna dan melalukan keamanan secara rutin untuk memastikan keamanan tetap terjaga



Gambar 4. Grafik Upaya Dan Tindakan Ransomware 2017-2023

Sumber gambar : https://www.statista.com/statistics/494947/ransomware-attempts-per-year-worldwide/

Diagram di atas menunjukkan data ransomware global dari tahun 2017 hingga 2023 mencakup semua tindakan atau upaya yang dapat membahayakan keselamatan orang lain.

KESIMPULAN

Autentikasi Multi-Faktor (AMF) meningkatkan keamanan sistem pembayaran e-commerce. AMF dapat mencegah akses ilegal dan ancaman keamanan lainnya dengan menggabungkan berbagai faktor verifikasi untuk melindungi informasi pribadi dan transaksi finansial pengguna. Pada akhirnya, implementasi AMF dapat mengurangi kekhawatiran konsumen tentang keamanan data pribadi mereka, meningkatkan kepercayaan dan kenyamanan dalam bertransaksi secara online. Untuk melindungi AMF dari ancaman keamanan yang terus berkembang di dunia e-commerce, langkah-langkah seperti konfigurasi sistem yang tepat, instruksi pengguna dan pemantauan dan pemeliharaan rutin diperlukan.

REFERENSI

Aji, M. P. (2023). Sistem Keamanan Siber dan Kedaulatan Data di Indonesia dalam Perspektif Ekonomi Politik (Studi Kasus Perlindungan Data Pribadi) [Cyber Security System and Data Sovereignty in Indonesia in Political Economic Perspective]. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri Dan Hubungan Internasional*, *13*(2), 222–238. https://doi.org/10.22212/jp.v13i2.3299

Karmawati E, D.S Efendi, & P. Wahid. (2019a). Potensi Peluang dan Kendala Pengembangan Agroindustri tanaman obat. *Prosiding Forum Konsultasi Strategi Dan Koordinasi Pengembangan Agroindustri Tanaman*

Obat, *3*(1), 23–37.

Karmawati E, D.S Efendi, & P. Wahid. (2019b). Potensi Peluang dan Kendala Pengembangan Agroindustri tanaman obat. *Prosiding Forum Konsultasi Strategi Dan Koordinasi Pengembangan Agroindustri Tanaman Obat*, *3*(1), 23–37.

Kehista, A. P., Fauzi, A., Tamara, A., Putri, I., Fauziah, N. A., Klarissa, S., & Damayanti, V. B. (2023). Analisis Keamanan Data Pribadi pada Pengguna E-Commerce: Ancaman, Risiko, Strategi Kemanan (Literature Review). *Jurnal Ilmu Manajemen Terapan*, *4*(5), 625–632.

Nafi'ah, R. (2020). Pelanggaran Data Dan Pencurian Identitas Pada E-Commerce. *Cyber Security Dan Forensik Digital*, *3*(1), 7–13. https://doi.org/10.14421/csecurity.2020.3.1.1980

Nugraha, M. A., Arisandi, D., & Perdana, N. J. (2021). Pengamanan Website E-Commerce Menggunakan Multi-Factor Authentication. *Jurnal Ilmu Komputer Dan Sistem Informasi*, *9*(1), 158. https://doi.org/10.24912/jiksi.v9i1.11588

Pebiyanti, E., Fauzi, A., Husniyyah, T., Intan Tasia, S., Sutendi, Z., & Elsa Vitri, A. (2023). Pengaruh Kualitas Informasi, Persepsi Keamanan, dan Persepsi Privasi Terhadap Kepercayaan Pengguna Belanja Online (Literature Review). *Jurnal Ekonomi Manajemen Sistem Informasi*, *4*(5), 850–858. https://doi.org/10.31933/jemsi.v4i5.1548

Putri, N. C. R., Fauzi, A., Ali, M. K., & ... (2024). Strategi Peningkatan Keamanan Data Pelanggan dalam Penjualan Online di Tokopedia. *Jurnal Siber Multi …*, *2*(1), 54–67.

Raihan, M. (2023). Perlindungan Data Diri Konsumen Dan Tanggungjawab Marketplace Terhadap Data Diri Konsumen (Studi Kasus: Kebocoran Data 91 Juta Akun Tokopedia). *Jurnal Inovasi Penelitian*, *3*(10), 7849–7850.