

PENGEMBANGAN SISTEM E-COMMERCE JAGOANGKAT.ID DI PT ELHIFA GROUP DENGAN IMPLEMENTASI HTTPS DAN JWT AUTHENTICATION

Muhammad Daniel Ilyasa^{1*}, Himmatul Miftah², Uus Firdaus³

^{1,2,3}Universitas Djuanda, Indonesia

¹muhammaddanielilyasa@gmail.com.

²himmatul.miftah@unida.ac.id, ³uus.firdaus@unida.ac.id

*Corresponding Author

Informasi Artikel

Pengajuan : 28-08-2026
Peninjauan : 03-09-2026
Revisi : 10-09-2026
Diterima : 12-09-2026
Diterbitkan : 17-09-2026

Kata Kunci:

E-Commerce, HTTPS, JWT Authentication, Keamanan Sistem, Waterfall

Abstrak

Penelitian ini bertujuan untuk mengembangkan sistem e-commerce Jagoangkat.id di PT Elhifa Group guna mengotomatisasi proses transaksi serta meningkatkan keamanan komunikasi data dan autentikasi pengguna melalui penerapan HTTPS dan JSON Web Token (JWT). Metode penelitian yang digunakan adalah penelitian terapan dengan model pengembangan Waterfall yang meliputi tahapan analisis kebutuhan, perancangan, implementasi, pengujian, dan pemeliharaan. Pengumpulan data dilakukan melalui observasi, wawancara, dan studi pustaka. Pengujian sistem menggunakan Black Box Testing dengan bantuan Playwright serta User Acceptance Testing (UAT) menggunakan kuesioner skala Likert terhadap 5 administrator dan 20 pelanggan. Hasil penelitian menunjukkan bahwa seluruh 15 skenario pengujian fungsional berhasil dijalankan sesuai dengan hasil yang diharapkan. Penerapan HTTPS mendukung pengamanan komunikasi antara klien dan server, sedangkan autentikasi JWT dengan masa berlaku token selama 24 jam dan middleware autentikasi mendukung validasi identitas serta pembatasan akses pengguna. Hasil UAT memperoleh nilai rata-rata 4,72 dari administrator dan 4,65 dari pelanggan, yang keduanya termasuk kategori sangat baik. Simpulan penelitian ini adalah bahwa sistem e-commerce Jagoangkat.id berhasil dikembangkan dengan mengintegrasikan pengelolaan produk, keranjang belanja, checkout, pembayaran, dan pengelolaan pesanan serta menerapkan mekanisme keamanan komunikasi dan autentikasi pengguna untuk mendukung transaksi digital yang lebih terintegrasi dan aman.

Cara Mengutip : Ilyasa, M. D., Miftah, H., & Firdaus, U. (2026). Pengembangan sistem e-commerce Jagoangkat.id di PT Elhifa Group dengan implementasi HTTPS dan JWT authentication. Journal of Computer Science and Information Technology (JCSIT), 3(4), 605–613. <https://doi.org/10.70248/jcsit.v3i4.4756>

DOI : <https://doi.org/10.70248/jcsit.v3i4.4756>

This is an open access article under <https://creativecommons.org/licenses/by/4.0/>

Copyright© 2026 by Author. Published by Yayasan Nuraini Ibrahim Mandiri



PENDAHULUAN

Jagoangkat.id merupakan salah satu platform bisnis e-commerce milik PT Elhifa Group yang bergerak di bidang fabrikasi alat angkat, sling sintetis, wire rope, dan aksesoris rigging. Platform ini pada mulanya dibangun menggunakan WordPress dengan template e-commerce standar, sementara proses checkout masih dilakukan secara semi-manual melalui percakapan WhatsApp untuk konfirmasi transaksi. Pendekatan tersebut menyebabkan proses pencatatan transaksi, verifikasi pengguna, dan pelaporan belum terintegrasi secara optimal (Bawamohiddin et al., 2024). Penelitian ini menunjukkan bahwa digitalisasi proses pencatatan dapat mendukung otomatisasi dan mengurangi ketergantungan terhadap proses manual. Sejalan dengan perkembangan perdagangan digital, pemanfaatan platform e-commerce juga dapat mendukung proses transaksi yang lebih terintegrasi serta meningkatkan efisiensi aktivitas perdagangan (Adhitya et al., 2024). Hasil observasi awal terhadap alur transaksi Jagoangkat.id menunjukkan bahwa konfirmasi pemesanan dan pembayaran

masih bergantung pada komunikasi manual melalui *WhatsApp*. Kondisi tersebut dapat menyebabkan proses pencatatan pesanan dan status pembayaran membutuhkan verifikasi oleh admin sebelum transaksi dapat ditindaklanjuti. Selain itu, penggunaan platform yang belum mengintegrasikan seluruh proses transaksi menyebabkan pengelolaan data pesanan dan pelaporan belum dapat dilakukan secara terpusat. Permasalahan tersebut menunjukkan adanya kebutuhan terhadap sistem *e-commerce* yang mampu mengintegrasikan proses transaksi, pengelolaan data, dan autentikasi pengguna dalam satu platform.

Selain integrasi proses bisnis, keamanan komunikasi dan autentikasi merupakan aspek penting dalam pengembangan sistem *e-commerce*. Transaksi digital melibatkan pertukaran berbagai informasi antara pengguna dan server sehingga perlindungan terhadap data selama proses komunikasi diperlukan. Norian et al. (2020) menjelaskan bahwa keamanan dan privasi merupakan salah satu tantangan dalam penerapan *e-commerce*. Persepsi konsumen terhadap keamanan transaksi juga berkaitan dengan tingkat kepercayaan dalam menggunakan *marketplace* digital (Cece Cece, 2025). Oleh karena itu, sistem yang dikembangkan perlu menyediakan mekanisme untuk mengamankan komunikasi data serta melakukan validasi identitas pengguna sebelum pengguna memperoleh akses terhadap fitur tertentu.

Sejumlah penelitian telah menerapkan mekanisme keamanan melalui HTTPS dan JWT pada aplikasi berbasis web. Wakoli. (2024) membahas penggunaan HTTP dan SSL/TSL dalam pengamanan komunikasi pada *website e-commerce*, sedangkan Tamara et al. (2024) menjelaskan penerapan protokol keamanan dalam lingkungan *e-commerce*. Pada sisi autentikasi, Nashikhuddin et al. (2023) menerapkan JWT pada aplikasi *e-commerce* untuk mendukung autentikasi dan otorisasi pengguna. Prasetya & Suharjo. (2025) juga menerapkan JWT dalam perlindungan akses *backend API*. Sementara itu, Moshood & Jeffrey. (2025) membahas penggunaan JWT sebagai mekanisme autentikasi dengan memperhatikan pengelolaan masa berlaku token. Hasil penelitian terdahulu tersebut menjadi landasan dalam pemilihan HTTPS dan JWT sebagai mekanisme keamanan yang diterapkan pada sistem *Jagoangkat.id*. Pada penelitian ini, HTTPS diterapkan untuk mengamankan komunikasi antara *client* dan *server* melalui enkripsi pada jalur transmisi data. HTTPS menggunakan TLS untuk menyediakan koneksi terenkripsi sehingga informasi yang dikirimkan selama proses komunikasi terlindungi dari penyadapan pada jaringan (Parkash & Lal, 2018). Selanjutnya, JWT diterapkan sebagai mekanisme autentikasi dan otorisasi pengguna. JWT memungkinkan informasi identitas dan klaim pengguna dikemas dalam sebuah token yang dapat diverifikasi oleh sistem pada saat pengguna mengakses layanan yang memerlukan autentikasi (Nashikhuddin et al., 2023). Penerapan JWT juga perlu memperhatikan masa berlaku token dan pengelolaan kunci secara tepat untuk mengurangi risiko penyalahgunaan token (Moshood & Jeffrey, 2025).

Pengembangan sistem dilakukan menggunakan *Next.js* sebagai *framework* aplikasi, *Neon PostgreSQL* sebagai basis data, *Better Auth* untuk mendukung mekanisme autentikasi, serta *Midtrans API* sebagai layanan pembayaran. Model *Waterfall* digunakan sebagai pendekatan pengembangan sistem yang meliputi analisis kebutuhan, perancangan, implementasi, pengujian, dan pemeliharaan. Sistem yang dikembangkan mengintegrasikan proses registrasi dan autentikasi pengguna, pengelolaan katalog produk, *checkout*, pengelolaan pesanan, hingga pembayaran sehingga proses transaksi tidak lagi sepenuhnya bergantung pada konfirmasi manual melalui *WhatsApp*. Berdasarkan uraian tersebut, permasalahan penelitian dirumuskan sebagai berikut: (1) bagaimana mengembangkan sistem *e-commerce Jagoangkat.id*

untuk mengotomatisasi proses transaksi yang sebelumnya dilakukan secara semi-manual; (2) bagaimana menerapkan HTTPS untuk mengamankan komunikasi data antara *client* dan *server*; dan (3) bagaimana menerapkan JWT Authentication untuk melakukan autentikasi dan otorisasi pengguna pada sistem. Penelitian ini bertujuan untuk mengembangkan sistem *e-commerce Jagoangkat.id* yang terintegrasi, menerapkan HTTPS sebagai mekanisme pengamanan komunikasi data, serta menerapkan JWT Authentication untuk mendukung proses autentikasi dan pengelolaan akses pengguna. Dengan demikian, penelitian ini diharapkan dapat memberikan solusi terhadap permasalahan transaksi semi-manual sekaligus mendukung keamanan komunikasi dan akses pengguna pada platform *Jagoangkat.id*.

METODE PENELITIAN

Penelitian ini merupakan penelitian terapan (*applied research*) di bidang rekayasa perangkat lunak yang menggunakan model pengembangan *Waterfall*. Model ini dipilih karena sesuai untuk proyek dengan kebutuhan dan ruang lingkup yang telah terdefinisi secara jelas sejak awal pengembangan. Balaji, (2012) menegaskan bahwa dibandingkan *V-Model* maupun *Agile*, *Waterfall* lebih unggul dalam kemudahan pengendalian proyek dan dokumentasi pada proyek berskala kecil hingga menengah dengan requirement yang relatif stabil, sebagaimana karakteristik pengembangan sistem *e-commerce Jagoangkat.id* ini. Tahapan yang dilalui dalam penelitian ini meliputi analisis kebutuhan sistem, desain, implementasi (*code generation*), pengujian (*testing*), dan pemeliharaan (*support*). Pengembangan sistem dilakukan untuk mengotomatisasi proses transaksi yang sebelumnya dilakukan secara semi-manual melalui WhatsApp serta meningkatkan keamanan komunikasi dan akses pengguna melalui penerapan protokol *HTTPS* dan autentikasi berbasis JWT.

Penelitian berfokus pada pengembangan sistem berbasis website yang mencakup pengelolaan produk, keranjang belanja, *checkout*, transaksi pembayaran, autentikasi pengguna, dan pengelolaan pesanan oleh administrator. Ruang lingkup keamanan dalam penelitian dibatasi pada penerapan protokol *HTTPS* untuk mengamankan pertukaran data antara pengguna dan server serta penerapan autentikasi JWT untuk proses validasi identitas dan pengelolaan akses pengguna. Integrasi pembayaran dilakukan menggunakan *Midtrans API*. Sistem dikembangkan menggunakan *Next.js* sebagai *framework* utama, *Neon PostgreSQL* sebagai basis data, serta *Better Auth* untuk mendukung mekanisme autentikasi pengguna. Pengumpulan data dilakukan melalui tiga teknik. Observasi dilakukan untuk memahami alur kerja transaksi manual *Jagoangkat.id*, mulai dari pemesanan hingga konfirmasi pembayaran melalui *WhatsApp*. Wawancara dilakukan bersama kepala bagian logistik, tim pemasaran, dan sejumlah pengguna untuk menggali kebutuhan fungsional maupun non-fungsional serta permasalahan keamanan data yang dialami selama ini. Studi pustaka dilakukan terhadap jurnal internasional dan dokumentasi resmi yang relevan dengan keamanan transaksi, khususnya terkait penerapan *HTTPS* dan autentikasi *JWT*.

Penelitian dilaksanakan pada PT Elhifa Group yang berlokasi di Jl. Industri, Jl. Tengsaw, Tarikolot, Kecamatan Citeureup, Kabupaten Bogor, Jawa Barat 16811. Lokasi tersebut dipilih karena merupakan lingkungan operasional yang berkaitan dengan pengelolaan *Jagoangkat.id* dan menjadi objek pengamatan terhadap proses transaksi yang sedang berjalan. Penelitian dilaksanakan pada periode November 2025 sampai dengan Juni 2026. Kegiatan penelitian meliputi pengumpulan data, analisis kebutuhan, perancangan sistem, implementasi aplikasi, pengujian sistem, serta evaluasi hasil pengembangan. Pada tahap analisis kebutuhan, ditentukan fitur-fitur utama seperti

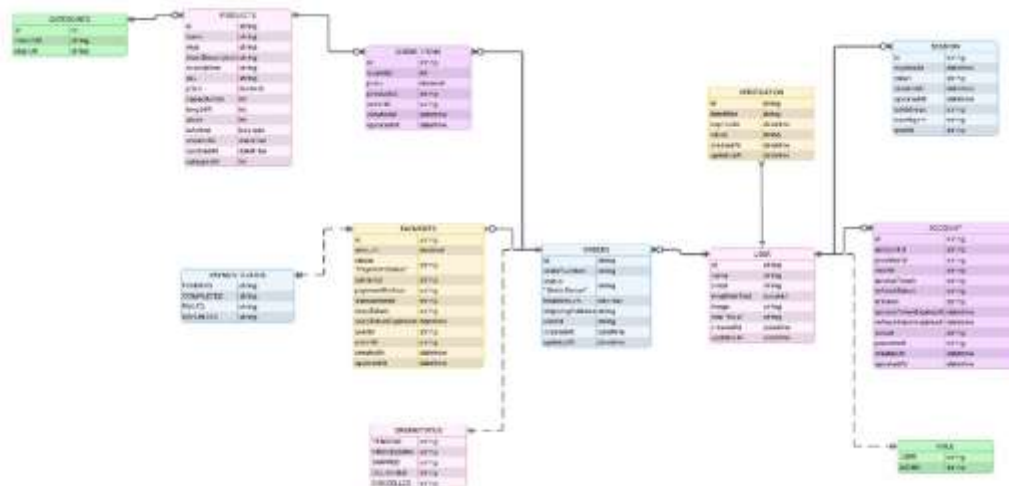
login dengan autentikasi, fitur *checkout*, *payment* dengan keamanan *SSL*, katalog produk, serta penerapan protokol *HTTPS*. Tahap desain mencakup perancangan *Entity Relationship Diagram (ERD)*, arsitektur perangkat lunak berlapis (*layered architecture*), *flowchart* proses bisnis, serta antarmuka pengguna untuk peran pengguna dan administrator. Tahap implementasi menggunakan *Next.js* dan *Prisma ORM* di atas basis data *Neon PostgreSQL*, dengan *Better Auth* untuk mengelola sesi berbasis *JWT* dan *Midtrans API* sebagai penyedia layanan pembayaran.

Pengujian sistem dilakukan dengan dua metode, yaitu *Black Box Testing* menggunakan *Playwright* untuk menguji fungsi login, proteksi halaman admin, katalog produk, keranjang belanja, dan proses *checkout* secara *end-to-end*, serta *User Acceptance Testing (UAT)* menggunakan kuesioner skala *Likert* (1–5) yang disebarakan kepada administrator dan pelanggan untuk mengukur tingkat penerimaan sistem. Penelitian dilaksanakan di lokasi operasional *PT Elhifa Group* di Citeureup, Kabupaten Bogor, Jawa Barat, dengan tahapan analisis kebutuhan hingga pengujian berlangsung selama kurang lebih delapan bulan. Penentuan responden *UAT* dilakukan menggunakan teknik *purposive sampling*. Lima responden administrator dipilih karena merupakan seluruh staf yang memiliki hak akses langsung terhadap panel admin dan terlibat penuh dalam pengelolaan produk, pesanan, dan pembayaran, sedangkan dua puluh responden pelanggan dipilih dari pengguna yang telah menyelesaikan transaksi uji coba pada sistem selama tahap *UAT* berlangsung. Pendekatan *purposive sampling* ini digunakan agar responden benar-benar memahami dan berinteraksi langsung dengan fitur inti sistem, sehingga penilaian pada skala *Likert* yang diberikan mencerminkan pengalaman penggunaan yang valid.

HASIL PENELITIAN DAN PEMBAHASAN

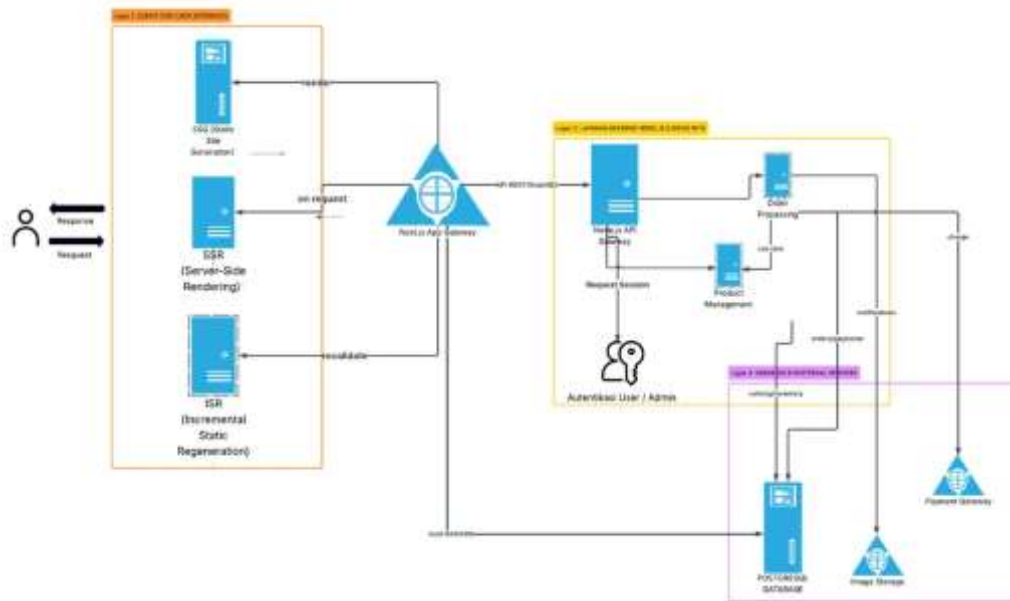
Analisis kebutuhan menghasilkan dua kategori kebutuhan sistem. Kebutuhan fungsional mencakup integrasi pihak ketiga (*payment gateway* dan autentikasi *JWT*), tampilan yang responsif pada perangkat mobile, pengelolaan atribut produk secara lengkap, serta alur pemesanan dan *checkout* yang terstruktur. Kebutuhan non-fungsional menitikberatkan pada aspek keamanan (*HTTPS* dan *JWT* dengan *role-based access control*), kinerja transaksi *real-time*, keandalan sistem terhadap kegagalan, kemudahan penggunaan, serta skalabilitas untuk menampung pertumbuhan pengguna.

Perancangan basis data dituangkan ke dalam *Entity Relationship Diagram (ERD)* yang terdiri atas entitas *User*, *Category*, *Product*, *Order*, *OrderItem*, dan *Payment* beserta relasinya, yang diimplementasikan menggunakan *Prisma ORM* di atas *PostgreSQL*. Arsitektur sistem dirancang secara berlapis (*layered architecture*) yang memisahkan sisi klien, *middleware/API gateway*, layanan *backend*, serta basis data dan layanan eksternal seperti *Midtrans* dan penyimpanan gambar, sehingga meningkatkan skalabilitas dan kemudahan pemeliharaan sistem.



Gambar 1. Entity Relationship Diagram (ERD) Sistem

Pada sisi implementasi, autentikasi dikelola menggunakan *Better Auth* yang terintegrasi dengan *Next.js* dan *PostgreSQL* melalui *Prisma*. Sesi pengguna disimpan dalam bentuk token yang ditandatangani (JWT) dan dikelola melalui cookie aman, dengan masa berlaku token dibatasi selama 24 jam. Kebijakan pembatasan masa berlaku ini dirancang sebagai mekanisme mitigasi terhadap risiko pembajakan sesi (*session hijacking*): apabila token dicuri atau bocor, penyerang hanya dapat memanfaatkannya dalam rentang waktu terbatas sebelum token kedaluwarsa dan pengguna diwajibkan melakukan autentikasi ulang, sehingga jendela eksploitasi (*attack window*) menjadi jauh lebih sempit dibandingkan sesi tanpa batas waktu (Moshood & Jeffrey, 2025) . Namun demikian, pendekatan ini masih menyisakan celah selama periode aktif token apabila tidak dipadukan dengan mekanisme tambahan seperti *token rotation*, penyimpanan token pada cookie dengan atribut *HttpOnly* dan *Secure*, atau *device fingerprinting*, sehingga hal ini menjadi salah satu arah pengembangan lanjutan pada sistem ini. *Middleware* autentikasi diterapkan pada seluruh rute privat, termasuk halaman administrator dan halaman transaksi, sehingga hanya pengguna dengan sesi valid dan hak akses yang sesuai yang dapat mengaksesnya. Seluruh komunikasi antara klien dan server dienkripsi melalui protokol *HTTPS*, sehingga data sensitif seperti kredensial login dan detail pembayaran tidak dapat disadap oleh pihak yang tidak berwenang.



Gambar 2. Arsitektur Berlapis (Layered Architecture) Sistem

Pengujian fungsional dilakukan menggunakan metode *Black Box Testing* dengan bantuan *Playwright* untuk menyimulasikan interaksi pengguna secara end-to-end, mencakup proteksi halaman admin, proses login, katalog produk, keranjang belanja, hingga proses *checkout*. Ringkasan sebagian skenario pengujian disajikan pada Tabel 1.

Tabel 1.

Sebagian Skenario Black Box Testing

No	Skenario Pengujian	Hasil yang Diharapkan	Status
1	Akses halaman admin tanpa login	<i>Redirect</i> ke halaman login	Berhasil
2	Login dengan kredensial salah	Sistem menolak dan menampilkan pesan error	Berhasil
3	Login dengan kredensial benar	<i>Redirect</i> ke halaman utama	Berhasil
4	Menambahkan produk ke keranjang	Produk masuk ke keranjang dengan benar	Berhasil
5	Proses <i>checkout</i>	<i>Form checkout</i> dan alamat pengiriman tampil	Berhasil
6	Perhitungan total harga keranjang	Total harga sesuai jumlah produk	Berhasil
7	Akses rute admin tanpa autentikasi	<i>Redirect</i> ke halaman login (proteksi <i>middleware</i>)	Berhasil
8	Render dashboard admin	Halaman tampil tanpa server error	Berhasil

Seluruh 15 skenario pengujian *black box*, termasuk proteksi rute admin, validasi login, pengelolaan keranjang, hingga perhitungan total transaksi, dinyatakan berhasil sesuai hasil yang diharapkan. Hasil ini menunjukkan bahwa proteksi *middleware* autentikasi dan validasi sesi berbasis *JWT* berfungsi sebagaimana mestinya dalam mencegah akses tidak sah terhadap halaman dan data transaksi. Selain pengujian fungsional, dilakukan pula *User Acceptance Testing (UAT)* untuk mengetahui tingkat penerimaan sistem oleh pengguna akhir. Pengujian melibatkan 5 responden

administrator dan 20 responden pelanggan, menggunakan kuesioner skala *Likert* 1–5 yang dianalisis dengan metode rata-rata (*mean*).

Tabel 2.

Ringkasan Hasil User Acceptance Testing (UAT)

Kelompok Responden	Jumlah Responden	Rata-rata Skor	Kategori
Administrator	5	4,72	Sangat Baik
Pelanggan (User)	20	4,65	Sangat Baik

Nilai rata-rata keseluruhan sebesar 4,72 pada administrator dan 4,65 pada pelanggan menunjukkan tingkat penerimaan pada kategori Sangat Baik. Indikator dengan nilai tertinggi pada sisi pelanggan adalah rasa aman saat bertransaksi (4,75), yang mengindikasikan bahwa penerapan *HTTPS*, autentikasi *JWT*, dan integrasi *payment gateway* memberikan tingkat kepercayaan yang tinggi kepada pengguna [6], [15]. Temuan ini sejalan dengan penelitian yang menunjukkan bahwa transparansi mekanisme keamanan pada platform digital berkontribusi signifikan terhadap kepercayaan konsumen dalam bertransaksi secara online [6], [9]. Dibandingkan dengan sistem sebelumnya yang bergantung pada pencatatan manual melalui *WhatsApp*, sistem yang dikembangkan mampu mengotomatisasi seluruh alur transaksi secara *real-time* sekaligus menutup celah keamanan yang selama ini menjadi risiko utama bagi *Jagoangkat.id*. Nilai terendah pada aspek kecepatan website (4,55) diduga berkaitan dengan karakteristik arsitektur *serverless* yang digunakan pada lapisan basis data, di mana instans basis data dapat mengalami *cold start* ketika tidak menerima permintaan dalam rentang waktu tertentu, sehingga permintaan pertama setelah masa idle membutuhkan waktu respons lebih lama dibandingkan permintaan berikutnya. Selain itu, proses *server-side rendering* (*SSR*) pada *Next.js* turut memengaruhi waktu muat awal (*initial load*) karena data produk perlu diambil dan dirender di sisi server sebelum dikirimkan ke klien, terutama ketika turut memuat sejumlah gambar produk beresolusi tinggi dari layanan penyimpanan objek *cloud*. Kondisi ini membuka peluang optimasi lanjutan seperti penerapan strategi *caching*, penggunaan *Incremental Static Regeneration* (*ISR*) untuk halaman katalog yang jarang berubah, serta kompresi dan optimasi ukuran gambar sebelum disajikan kepada pengguna.

KESIMPULAN

Bahwa migrasi proses transaksi manual *Jagoangkat.id* ke platform berbasis website yang menerapkan protokol *HTTPS* dan autentikasi *stateless JWT* memberikan kontribusi praktis berupa otomatisasi alur bisnis serta penguatan lapisan keamanan terhadap risiko *Identification and Authentication Failures* yang sebelumnya melekat pada sistem berbasis *WordPress*. Secara metodologis, temuan ini memperkuat argumen bahwa arsitektur autentikasi *stateless* lebih adaptif diterapkan pada sistem *e-commerce* skala menengah dibandingkan pendekatan *session-based* konvensional, sekaligus menegaskan pentingnya integrasi keamanan sejak tahap perancangan (*security by design*) dalam siklus pengembangan perangkat lunak. Meskipun demikian, penelitian ini memiliki keterbatasan, antara lain arsitektur berbasis *Next.js* dan basis data *serverless* yang berpotensi mengalami kendala *cold start* pada beban akses rendah, ketergantungan pada satu penyedia *payment gateway*, serta belum diujinya sistem pada skenario beban transaksi tinggi (*high concurrency*) dalam jangka panjang. Berdasarkan keterbatasan tersebut, pengembangan lanjutan disarankan mengarah pada pengujian performa melalui *load testing* dan *stress testing*, penerapan *Multi-Factor*

Authentication, serta mekanisme *token rotation* untuk memperkuat mitigasi risiko pembajakan sesi pada arsitektur yang telah dibangun.

Pernyataan mengenai Penggunaan Kecerdasan Buatan (AI).

AI digunakan dalam penyusunan naskah ini. Penulis menggunakan perangkat kecerdasan buatan semata-mata untuk membantu perbaikan bahasa, pemeriksaan tata bahasa, serta penyuntingan demi kejelasan dan keterbacaan. Penulis tetap bertanggung jawab penuh atas akurasi, orisinalitas, integritas, dan konten akademis naskah tersebut. Seluruh konten yang dibantu oleh AI telah ditinjau dan diverifikasi oleh penulis sebelum naskah diserahkan

Konflik kepentingan

Penulis menyatakan tidak ada konflik kepentingan.

Kontribusi penulis

Konseptualisasi, Muhammad Daniel Ilyasa; pengumpulan data, Muhammad Daniel Ilyasa analisis formal, Muhammad Daniel Ilyasa pengembangan sistem dan pengujian, Muhammad Daniel Ilyasa; validasi data, Himmatul Miftah dan Uus Firdaus; penulisan— penyusunan draf awal, Muhammad Daniel Ilyasa penulisan, peninjauan dan penyuntingan, Himmatul Miftah dan Uus Firdaus membuat visualisasi, Muhammad Daniel Ilyasa; supervisi, Himmatul Miftah (pembimbing 1) dan Uus Firdaus (pembimbing 2). Seluruh penulis telah membaca dan menyetujui versi akhir naskah ini

Ucapan terima kasih

Penulis mengucapkan terima kasih kepada PT Elhifa Group atas izin, akses data, dan dukungan operasional selama penelitian berlangsung, serta kepada Universitas Djuanda atas dukungan dan bimbingan akademik yang diberikan dalam penyelesaian penelitian ini.

DAFTAR PUSTAKA

- Adhitya, W. R., Teviana, T., Sienny, S., Hidayat, A., & Khaira, I. (2024). Implementasi digital marketing menggunakan platform e-commerce dan media sosial terhadap masyarakat dalam melakukan pembelian. *TIN: Terapan Informatika Nusantara*, 5(1), 63–72. <https://doi.org/10.47065/tin.v5i1.5293>
- Balaji, S. (2012). Waterfall vs V-model vs Agile: A comparative study on SDLC. *International Journal of Information Technology and Business Management*, 2(1).
- Bawamohiddin, A. B., Mohamad, H., & Muhamad, 'Afifah Nailah. (2024). Digitize the eCommerce bookkeeping – An automation bookkeeping prototype development. *Malaysian Journal of Information and Communication Technology (MyJICT)*. <https://doi.org/10.53840/myjict8-2-100>
- Cece, C. (2025). Consumer perceptions of transaction security in digital marketplaces. *Digital Innovation: International Journal of Management*, 2(3), 12–20. <https://doi.org/10.61132/digitalinnovation.v2i3.386>
- Moshood, A. I., & Jeffrey, Z. (2025). An in-depth approach to strengthening security in open-access libraries utilizing JSON Web Tokens (JWT). *International Journal of Recent Technology and Engineering (IJRTE)*, 13(5), 14–19. <https://doi.org/10.35940/ijrte.E8181.13050125>

- Nashikhuddin, A. Y., Karaman, J., & Litanianda, Y. (2023). Implementasi API RESTful dengan JSON Web Token (JWT) pada aplikasi e-commerce Thrifty Shop untuk otentikasi dan otorisasi pengguna. *Methomika: Jurnal Manajemen Informatika dan Komputerisasi Akuntansi*, 7(2). <https://doi.org/10.46880/jmika.vol7no2.pp239-246>
- Norian, J. H., Jama, A. M., Eltaieb, M. H., & Adam, A. A. (2020). Data-driven e-commerce techniques and challenges in the era of the Fourth Industrial Revolution. *Scientific Journal of Informatics*, 7(2).
- Parkash, & Lal. (2018). [Judul artikel dan informasi publikasi perlu dilengkapi berdasarkan sumber asli.]
- Prasetya, A. B., & Suharjo, I. (2025). Backend API data protection menggunakan JWT token dan algoritma AES 256-bit dengan bahasa pemrograman Golang. *Jurnal Informatika dan Teknik Elektro Terapan*, 13(1). <https://doi.org/10.23960/jitet.v13i1.5699>
- Tamara, R., Lyudmyla, K., Vadym, P., Artem, M., & Volodymyr, B. (2024). Analysis of authentication methods for full-stack applications and implementation of a web application with an integrated authentication system. *Innovative Technologies and Scientific Solutions for Industries*, 2024(3), 76–90. <https://doi.org/10.30837/2522-9818.2024.3.076>
- Wakoli, L. W. (2024). Secure Sockets Layer/Transport Layer Security for e-commerce. *International Journal of Scientific Research and Management (IJSRM)*, 12(12), 8047–8052. <https://doi.org/10.18535/ijsrm/v12i12.em03>