KAMPUS AKADEMIK PUBLISING
Jurnal Sains Student Research (JSSR)
Vol.4, No.3 Juni 2026
e-ISSN: 3025-9851, p-ISSN : 3025-986X, Hal 623-633
DOI : https://doi.org/10.61722/jssr.v4i3.10532

Implementasi Zero Trust Architecture pada Infrastruktur Self-Hosted: Analisis Pengujian Keamanan Data Berdasarkan Prinsip CIA Triad

Arjuna Ragil Putera[1], Evy Nurmiati[2]

[1, 2] Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, UIN Syarif Hidayatullah Jakarta, Jl. Ir. H. Djuanda No. 95, Ciputat, Tangerang Selatan, Banten 15412, Indonesia
*Penulis Korespondensi: arjuna.ragil24@mhs.uinjkt.ac.id

Abstract. *The trend of self-hosting is increasingly favored by information technology practitioners; however, its implementation often relies on conventional perimeter-based security models that are vulnerable to exploitation and lateral movement. This study aims to mitigate these security gaps by designing, implementing, and evaluating the effectiveness of Zero Trust Architecture (ZTA) within a micro-scale self-hosted server infrastructure ecosystem. System reliability was evaluated using observational functional testing methods based on the CIA Triad security matrix (Confidentiality, Integrity, Availability). The testing environment was built using container technology integrated with an outbound tunnel service (Cloudflare Tunnels), a Single Sign-On system (Authentik), and a mesh VPN network (Tailscale). The test results confirm that the ZTA architecture successfully fulfills all three data security parameters optimally. Regarding confidentiality, the SSO gateway actively blocks anonymous access. In terms of integrity, end-to-end encryption based on TLS 1.3 and WireGuard protocols is proven to protect data transmission from Man-in-the-Middle threats. For availability, closing public physical ports successfully secures server resources from automated scanning without compromising the accessibility of legitimate users. This research proves that corporate-level cybersecurity can be efficiently applied to personal infrastructure while demonstrating compliance with professional ethics through simulation in a controlled environment.*.

Keywords: *Zero Trust Architecture, Self-Hosted, CIA Triad, Data Security, Cybersecurity*

Abstrak. Tren *self-hosting* banyak diminati oleh praktisi teknologi informasi, namun implementasinya sering kali masih mengandalkan model keamanan konvensional berbasis perimeter jaringan yang rentan terhadap eksploitasi. Penelitian ini bertujuan untuk memitigasi celah keamanan tersebut dengan merancang, mengimplementasikan, dan mengevaluasi efektivitas *Zero Trust Architecture* (ZTA) pada ekosistem infrastruktur server mandiri berskala kecil. Evaluasi keandalan sistem dilakukan menggunakan metode pengujian fungsional observasional berdasarkan matriks keamanan CIA Triad (*Confidentiality, Integrity, Availability*). Lingkungan pengujian dibangun menggunakan server lokal dengan linux ubuntu 24.04 yang diintegrasikan dengan layanan *outbound tunnel* (Cloudflare Tunnels), sistem *Single Sign-On* (Authentik), dan jaringan VPN (Tailscale). Hasil pengujian mengonfirmasi bahwa arsitektur ZTA berhasil memenuhi ketiga parameter keamanan data secara optimal. Pada aspek kerahasiaan, gerbang SSO secara aktif memblokir akses anonim. Pada aspek keutuhan, enkripsi ujung-ke-ujung berbasis protokol TLS 1.3 dan WireGuard terbukti melindungi transmisi data dari ancaman. Pada aspek ketersediaan, penutupan port fisik publik sukses mengamankan sumber daya server dari pemindaian otomatis tanpa mengorbankan aksesibilitas pengguna yang sah. Penelitian ini membuktikan bahwa keamanan siber tingkat korporat dapat diaplikasikan secara efisien pada infrastruktur personal, sekaligus mendemonstrasikan kepatuhan terhadap etika profesi melalui simulasi di lingkungan terkendali..

Kata kunci: *Zero Trust Architecture*, *Self-Hosted*, CIA Triad, Keamanan Data, Keamanan Siber

Naskah Masuk: 01 Juni 2026; Revisi: 02 Juni 2026; Diterima: 03 Juni 2026; ; Terbit: 04 Juni 2026.

1. LATAR BELAKANG

Perkembangan teknologi bergerak dengan sangat cepat, saat ini terdapat teknologi seperti intranet, *artificial intelligence* dan *cloud* yang terus berkembang [1]. Teknologi-teknologi ini telah mengubah cara organisasi ataupun individu dalam mengelola infrastruktur IT mereka, baik dari sisi keamanan ataupun fungsionalitas [2]. Pada era saat ini, tren self-hosting atau pengelolaan server personal secara mandiri banyak dilakukan oleh berbagai macam kalangan. *Self-hosting* berbeda dengan standar industri saat ini, yaitu *cloud computing*. *Cloud computing* merupakan server *off-premise* yang disediakan oleh perusahaan pihak ketiga untuk dipakai pihak lain [3], sedangkan *self-hosting* adalah server personal & *on-premise* yang segala pengelolaan dilakukan secara mandiri dan dapat digunakan untuk hosting aplikasi ataupun AI lokal [4]. Tren self-hosting ini tidak hanya dilakukan oleh praktisi ataupun antusias IT, tetapi dilakukan juga oleh masyarakat yang sebelumnya tidak memiliki pengalaman dalam bidang IT. Tren ini muncul dan terus meningkat dikarenakan keinginan untuk memiliki kendali penuh terhadap kepemilikan data, mengurangi biaya, dan menjaga privasi data pribadi [5]. Dengan adanya *self-hosting*, data pribadi yang bersifat sensitif tidak tersebar dan dikendalikan oleh infrastruktur lokal sendiri, tidak dikelola oleh pihak ketiga yang dapat menyalahgunakan data tersebut [6]. Selain itu, modal dasar untuk melakukan *self-hosting* relative murah, yaitu perangkat bekas seperti laptop atau hp yang dapat diubah menjadi sebuah server lokal.

Meskipun tujuan dari *self-hosting* ini positif, namun ada dampak negatif apabila tidak dikonfigurasi dengan baik dan benar. Sebuah server lokal yang menggunakan hp ataupun laptop pada dasarnya memiliki keamanan standar bawaan dari OS yang dipakai. Tingkat keamanan ini sudah sangat cukup apabila ekosistem infrastruktur yang dibangun masih dalam satu jaringan. Namun, keamanan ini menganggap bahwa semua perangkat yang berada dalam satu jaringan itu aman dan dapat mengakses server lokal dengan password yang mudah dibuka secara paksa. Fenomena ini dapat dianalogikan dengan istilah *castle and moat*, dimana kerajaan dijaga ketat dari luar, namun tidak ada pertahanan dari serangan internal [7]. Selain itu, sebagian besar server lokal yang

dibangun memiliki tujuan, yaitu dapat diakses dari mana saja oleh pemilik. Didorong dengan tren WFH yang tersisa dari COVID-19, pengendalian dari segala tempat merupakan suatu fitur yang wajib untuk diadakan [8]. Hal ini menyebabkan server lokal harus dibuka ke publik, dimana keamanan bawaan OS dapat dengan mudah dieksploitasi dan menyebabkan kebocoran data. Pembukaan server ke publik tanpa pengamanan merupakan tindakan terburuk yang dapat dilakukan, ditambah perkembangan serangan siber yang semakin canggih dan banyak [9], [10]. Meskipun server dijaga password, seseorang dapat menggunakan teknologi *deepfake* untuk membohongi admin untuk memberikan password tersebut [11]. Hal terburuk yang dapat terjadi adalah keseluruhan ekosistem infrastruktur yang terhubung diserang semua, tidak hanya server lokalnya.

Maka dari itu, diperlukan sebuah paradigma baru yang tidak terikat pada satu jaringan dan aman dibuka ke publik. *Zero Trust Architecture* (ZTA) merupakan salah solusi arsitektur keamanan modern yang menggunakan prinsip "*Never Trust, Always Verify*" [12]. Dalam konsep ZTA, sebuah ekosistem arsitektur tidak pernah berasumsi bahwa semua alat yang berada dalam satu jaringan itu aman [13]. Semua perangkat yang berada dalam satu jaringan harus terdaftar dan tercatat oleh server untuk dapat berkomunikasi dalam ekosistem tersebut. Hal ini sesuai dengan standar keamanan IT, yaitu segala jenis permintaan dari suatu perangkat elektronik harus diverifikasi terlebih dahulu [14]. ZTA tidak hanya memberikan hak akses pada admin, ZTA juga mengelola bagian infrastruktur yang dapat diakses oleh publik secara terbuka dan memblokir segala bot yang mencoba untuk membuka. Selain itu, konsep ZTA memastikan bahwa aliran data terjadi secara *end-to-end*, menandakan bahwa segala jenis data itu tidak bisa diakses oleh siapapun dan terenkripsi kecuali untuk penerima dan pengirim [15].

Penilaian keamanan sistem pada dasarnya dapat diukur melalui tiga parameter yang terdapat dalam CIA Triad, yaitu aspek Kerahasiaan (*Confidentiality*), Keutuhan (*Integrity*), dan Ketersediaan (*Availability*) data [16]. Penelitian mengenai ZTA berskala industri telah banyak dilakukan, namun ZTA untuk ekosistem berskala kecil, bahkan mikro masih sangat terbatas. Maka dari itu, penelitian ini dilakukan untuk merancang, mengimplementasikan, dan menguji efektivitas dari ZTA pada home server atau ekosistem berskala kecil. Hasil pengujian ini diharapkan dapat memberikan kontribusi

praktis dan panduan beretika bagi profesional IT ataupun kalangan lain yang berkeinginan untuk mengamankan data sensitif pada infrastruktur independen.

2. METODE PENELITIAN

Penelitian ini menggunakan pendekatan eksperimental terapan untuk merancang, mengimplementasikan, dan mengevaluasi keamanan ZTA pada lingkungan infrastruktur mandiri. Lingkungan pengujian dibangun di atas sebuah laptop bekas yang diubah menjadi sebuah server, menjalankan sistem operasi Linux Ubuntu. Untuk efisiensi alokasi sumber daya dan kemudahan manajemen layanan, sistem ini memanfaatkan teknologi virtualisasi berbasis *container* melalui Docker, dengan CasaOS yang berfungsi sebagai antarmuka manajemen terpusat. Pemilihan teknologi-teknologi ini secara akurat merepresentasikan arsitektur *self-hosted* modern yang hemat daya namun memiliki kapabilitas operasional dan kontrol penuh di sisi admin.

Implementasi *Zero Trust Architecture* (ZTA) dalam eksperimen ini dibagi menjadi tiga lapisan pertahanan utama yang saling terintegrasi. Lapisan pertama berfokus pada keamanan jaringan home server saat dibuka ke publik menggunakan layanan tunnelling dari Cloudflare. Mekanisme ini secara efektif menyembunyikan alamat IP publik asli server dan memastikan seluruh *port* pada *router* tetap tertutup dari paparan internet luar. Selain itu, suatu policy dari cloudflare ditambahkan untuk memperketat akses pada sistem [17]. Lapisan kedua menerapkan kontrol akses berbasis identitas menggunakan platform *Single Sign-On* (SSO) yang berperan sebagai sistem autentikasi sentral [18], dalam hal ini menggunakan Authentik. Authentik ini bertindak sebagai gerbang validasi. Setiap permintaan akses yang masuk wajib melewati proses autentikasi dan otorisasi yang ketat sebelum diizinkan menyentuh segala jenis layanan [19]. Lapisan ketiga melibatkan enkripsi jalur komunikasi antar perangkat yang terdaftar menggunakan jaringan VPN terenkripsi dari Tailscale. Jaringan VPN ini dibawahi protokol *WireGuard* yang berfungsi untuk memastikan data hanya mengalir pada perangkat yang telah terverifikasi dan segala jenis komunikasi terenkripsi [20].

Untuk mengevaluasi efektivitas keamanan dari arsitektur yang telah dibangun, metode pengujian yang digunakan adalah pengujian fungsional observasional. Pendekatan empiris ini dipilih untuk memvalidasi kemampuan sistem secara praktis berdasarkan tiga parameter utama dalam matriks CIA Triad tanpa pembuatan script yang

terlalu teknikal. Pada aspek kerahasiaan (*Confidentiality*), evaluasi dilakukan melalui observasi langsung terhadap percobaan akses ke URL dalam server loakl menggunakan web *incognito* dan perangkat yang tidak terdaftar dalam jaringan tailscale untuk menguji kedua tipe aplikasi, yaitu internal dan eksternal. Langkah ini bertujuan untuk memvalidasi secara visual bahwa sistem SSO dan Tailscale mampu secara aktif memblokir akses tanpa kredensial dan mengalihkan koneksi tersebut ke halaman autentikasi terpusat secara presisi. Pada aspek keutuhan (*Integrity*), pengujian difokuskan pada inspeksi sertifikat keamanan protokol secara langsung melalui fitur *developer tools* pada web. Validasi dilakukan dengan memeriksa parameter *Transport Layer Security* (TLS) pada koneksi yang terbentuk. Hal ini memastikan bahwa terowongan data (*tunnel*) benar-benar menerapkan enkripsi *end-to-end*, sehingga lalu lintas data dijamin kebal terhadap risiko manipulasi. Terakhir, pada aspek ketersediaan (*Availability*), pengujian dilakukan melalui metode pemindaian visibilitas *port* publik menggunakan instrumen pengecekan jaringan standar. Tujuannya adalah untuk membuktikan bahwa tunnelling yang telah dilakukan berhasil menutup semua port yang tidak terdaftar agar tidak dapat diakses publik.

3. HASIL DAN PEMBAHASAN

Hasil

Implementasi ZTA pada infrastrukur *self-hosted* telah berhasil dibangun dan dijalankan. Linux dengan distro Ubuntu 24 telah berhasil diinstall pada laptop. Dilanjutkan dengan proses instalasi CasaOS yang membantu dalam manajemen *container* ketiga aplikasi yang menjadi fondasi dari ZTA berskala kecil, yaitu cloudflare, authentik, dan tailscale. Integrasi antar ketiga teknologi tersebut berjalan sesuai dengan rencana awal. Tailscale berhasil dalam membuat sebuah jaringan VPN pribadi untuk komunikasi internal antar perangkat yang tidak terbuka kepada publik. Selain itu, cloudflare juga berhasil dalam membuka sebuah terowongan dari server ke publik tanpa harus mengekspos IP internal dari server. Terakhir, authentik yang berperan sebagai SSO untuk login, baik pada aplikasi internal maupun external berhasil untuk disambungkan. Semua aplikasi yang terdapat pada server harus melewati authentikasi pada authentik terlebih dahulu sebelum dapat diakses. Setelah semua persiapan sudah dilakukan, maka selanjutnya dilakukan pengujian berdasarkan aspek-aspek CIA Triad.

Pada pengujian aspek kerahasiaan (*confidentiality*), pengujian pertama dilakukan dengan laptop yang terdaftar pada jaringan tailscale home server, tetapi belum melakukan autentikasi pada SSO authentik. Hasil dari pengujian ini menghasilkan pengarahan dari halaman aplikasi menuju halaman login authentik dan mengharuskan autentikasi sebelum lanjut. Selain itu, pada pengujian kedua dilakukan dengan laptop yang mematikan jaringan tailscale (mensimulasikan perangkat yang tidak terdaftar pada jaringan tailscale home server). Hasil dari pengujian menunjukkan halaman error "*This site can't be reach*". Saat tailscale laptop tersebut dinyalakan, maka halaman error tersebut hilang dan digantikan dengan halaman login authentik.

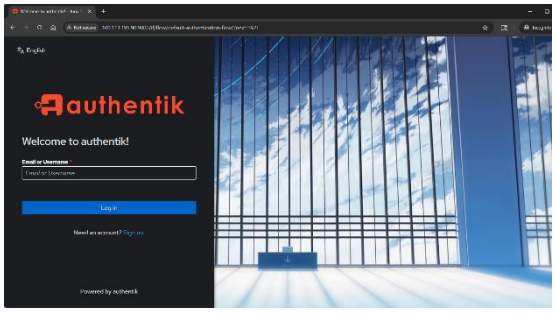

Figure 1. Halaman Login SSO

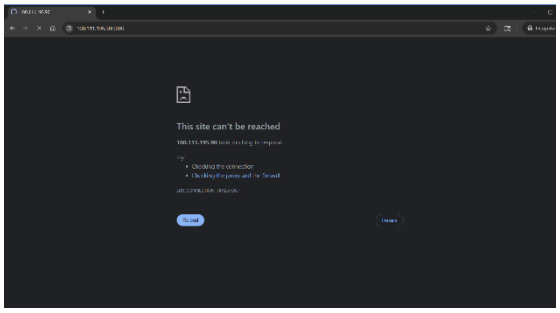

Figure 2. Halaman Error Tailscale

Pada pengujian aspek keutuhan (*integrity*), pengujian dilakukan dengan membuka salah satu aplikasi publik yang sudah diekspos melalui cloudflare tunnel dan melihat terdapatnya sertifikat TLS & HTTPS. Hasil dari pengujian ini menunjukkan bahwa terdapat sertifikat TLS & HTTPS pada web yang didapatkan melalui cloudflare. Hal ini menandakan bahwa semua data telah berhasil dienkripsi. Selain itu, untuk aplikasi internal keutuhannya dijaga oleh jaringan tailscale. Meskipun pada aplikasi internal tidak ada sertifikat TLS dan HTTPS, tailscale menggunakan metode lain bernama *WireGuard*. Metode ini berperan seperti sertifikat TLS dan HTTPS, namun metode ini tidak bergerak pada *layer* 7 (aplikasi), melainkan bergerak pada *layer* 3 (jaringan) yang pada umumnya tidak ditunjukkan kepada user melalui website.

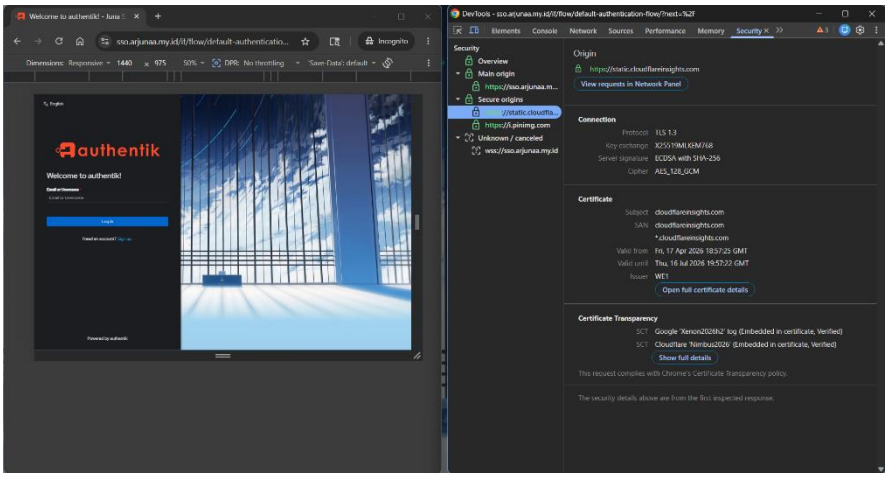

Figure 3. Sertifikat SSL & HTTPS

Pada pengujian aspek ketersediaan (*availability*), pengujian pertama dilakukan dengan mencoba membuka web internal dengan jaringan yang berbeda (mensimulasikan akses dari tempat lain), namun terhubung dengan jaringan tailscale yang sama. Hasil dari pengujian ini adalah aplikasi masih dapat dibuka meskipun jaringan yang digunakan berbeda. Pengujian kedua dilakukan dengan cara *scanning port-port* yang terbuka untuk menguji tunnelling cloudflare yang tidak mengekspos port yang tidak terpakai ke publik. Hasil dari pengujian ini menunjukkan bahwa *port* 80 yang rawan diserang tidak dapat dibaca oleh publik ataupun bot.

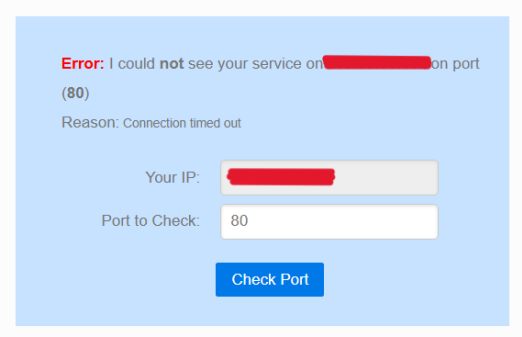

Figure 4. Hasil Pemeriksaan Port

Pembahasan

Hasil dari pengujian fungsional tersebut menunjukkan bahwa perubahan dari infrastruktur traditional menuju *Zero-trust Architecture* merupakan perubahan yang signifikan dalam menjaga keamanan sebuah infrastruktur. Pada arsitektur tradisional, keamanan yang harus diterapkan jauh lebih merepotkan. Salah satunya adalah *port*

forwarding, yaitu proses membuka sistem menjadi publik dengan cara mengekspos alamat IP server. Dampak negatif dari hal ini adalah menyebabkan alamat IP publik dan mudah diserang. Melalui penerapan ZTA, implementasi keamanan menjadi jauh lebih mudah dan aman. Pada ZTA, semua alamat IP, *port*, dan data tidak ada yang terekspos dan hanya ditunjukkan pada orang yang berhak. Arsitektur ini tidak hanya dapat diterapkan dalam arsitektur skala besar, bahkan skala kecil & mikro dapat menerapkannya juga.

Pada aspek kerahasiaan, sistem telah menunjukkan bahwa keamanan menggunakan SSO mampu memberikan proteksi akses yang sangat granular. Pada infrastruktur tradisional, apabila penyerang mengetahui alamat IP, maka mereka bisa dapat dengan mudah mengakses halaman login dari sistem tersebut dan membukanya secara paksa. Namun, adanya sebuah SSO memungkinkan semua sistem tertutup dan dijaga oleh suatu sistem autentikasi sentral yang tidak mudah diakses. Selain itu, SSO seperti authentik menyediakan *multi-factor authentication* (MFA) untuk keamanan yang lebih ketat. Pada sisi lain, kerahasiaan sistem terjaga aman oleh jaringan VPN tailscale. Meskipun IP address dari tailscale tersebar, perangkat yang tidak memiliki akses tidak akan dapat membuka IP address tersebut. Kedua hal ini menandakan bahwa sistem sudah mencukupi aspek kerahasiaan dengan cara menutupi semua sistem internal dan juga mengharuskan adanya autentikasi dengan MFA semisal penyerang berhasil mengakses perangkat yang memiliki akses ke jaringan VPN tailscale tersebut.

Pada aspek keutuhan, pengujian telah menunjukkan adanya sertifikat TLS dan HTTPS. Kedua hal ini merupakan syarat penting untuk menjaga integritas dari suatu data. Sertifikat tersebut menunjukkan bahwa data yang dikirim dan diterima telah dienkripsi terlebih dahulu sehingga tidak bisa terjadinya pencurian data pada alur data. Selain itu, untuk aplikasi internal yang hanya menggunakan jaringan VPN tailscale telah dijaga ketat oleh protokol dasar dari tailscale, yaitu *WireGuard*. *WireGuard* ini memastikan bahwa data yang dikirim dan diterima dienkripsi terlebih dahulu, disertakan pengiriman lewat jaringan internal yang tidak dapat diakses oleh perangkat yang tidak memiliki akses pada jaringan tailscale.

Pada aspek ketersediaan, sistem berhasil menunjukkan bahwa keamanan yang baik, tidak perlu mengorbankan kecepatan dan kenyamanan dalam mengaksesnya. Pengujian

telah berhasil untuk menunjukkan bahwa *tunnelling* yang dilakukan hanya mengekspos *port-port* yang memang ditujukan untuk publik. Selain itu, aplikasi internal yang bersifat rahasia dapat diakses dari berbagai tempat dan jaringan. Berbeda dengan infrastruktur tradisional yang mengharuskan semuanya dalam satu jaringan lokal yang terbatas.

Eksperimen keamanan pada infrastruktur *self-hosted* ini bukan sekadar pemenuhan hobi teknis, melainkan sebuah bentuk tanggung jawab moral dan kepatuhan terhadap kode etik professional, khususnya peran praktisi dalam mencegah terjadinya kebocoran data privasi [21]. Sesuai dengan prinsip standar etika profesi IT global (seperti standar *ACM* dan *IEEE*) yang sangat menekankan pada tanggung jawab sosial serta pencegahan bahaya [22], seorang calon atau praktisi IT memiliki kewajiban etis untuk menguji arsitektur baru di lingkungan yang terisolasi dan aman. Melakukan uji coba sistem pertahanan siber langsung pada server milik klien atau instansi publik yang menyimpan data masyarakat secara masif adalah tindakan yang tidak beretika dan melanggar prinsip kehati-hatian profesional. Kelalaian dalam merancang sistem ketersediaan data dan manajemen hak akses yang buruk berpotensi memicu dampak kerugian riil yang sangat besar di dunia nyata. Oleh karena itu, pemanfaatan infrastruktur personal sebagai media simulasi dan pengujian yang aman merupakan wujud nyata dari penerapan etika profesi demi menjamin kualitas dan keselamatan tata kelola data sebelum diimplementasikan pada skala industri.

4. KESIMPULAN DAN SARAN

Berdasarkan hasil perancangan, implementasi, dan pengujian fungsional yang telah dilakukan, dapat disimpulkan bahwa penerapan *Zero Trust Architecture* (ZTA) terbukti sangat efektif dalam meningkatkan keamanan data pada infrastruktur *self-hosted* berskala kecil. Evaluasi komprehensif berdasarkan prinsip CIA Triad menunjukkan hasil yang optimal. Pada aspek kerahasiaan (*Confidentiality*), sistem SSO dan jaringan internal mampu memblokir akses anonim secara mutlak dan memastikan otorisasi granular. Pada aspek keutuhan (*Integrity*), pemanfaatan tunnelling dengan enkripsi end-to-end menjamin keamanan paket data dari risiko manipulasi eksternal. Pada aspek ketersediaan (*Availability*), penutupan seluruh *port* fisik dari internet publik sukses mengamankan server dari ancaman *bot scanning* maupun *brute-force*, tanpa mengorbankan aksesibilitas layanan bagi perangkat pengguna yang telah terautentikasi dan dapat diakses dari segala

tempat. Selain itu, pelaksanaan eksperimen ini juga mendemonstrasikan penerapan etika profesi teknologi informasi yang bertanggung jawab, di mana pengujian keamanan siber dilakukan di dalam lingkungan infrastuktur personal yang terkendali untuk berlatih dalam mencegah praktik buruk pada server produksi yang asli

DAFTAR REFERENSI

[1] N. Mokadem, J. Treur, and P. H. M. P. Roelofsma, "Enhancing cybersecurity through adaptive networks and AI-coaching: Organizational learning and risk management," *Cogn. Syst. Res.*, vol. 97, Jun. 2026, doi: 10.1016/j.cogsys.2026.101464.

[2] M. Xie and M. Zeng, "A multimodal reinforcement learning-based access control model for power systems under zero-trust architecture," *Alexandria Engineering Journal*, vol. 141, pp. 269–283, Apr. 2026, doi: 10.1016/j.aej.2026.03.017.

[3] M. Nadeem *et al.*, "Preventing Cloud Network from Spamming Attacks Using Cloudflare and KNN," *Computers, Materials and Continua*, vol. 74, no. 2, pp. 2641–2659, 2023, doi: 10.32604/cmc.2023.028796.

[4] M. A. Gopee, S. A. Prieto, and B. García de Soto, "Self-hosted multimodal large language models for speech-driven perception and navigation in construction robotics," *Autom. Constr.*, vol. 183, Mar. 2026, doi: 10.1016/j.autcon.2026.106805.

[5] C. Sharma, A. Kumar, and P. K. Tiwari, "Quality of service driven energy-efficient computing to enhance sustainable cloud," *Array*, vol. 30, Jul. 2026, doi: 10.1016/j.array.2026.100790.

[6] S. Cahyono, A. Gustomo, and A. Ghazali, "Integrating knowledge management with organizational culture transformation to enhance data security: A qualitative perspective," *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 12, no. 2, Jun. 2026, doi: 10.1016/j.joitmc.2026.100766.

[7] N. N. Hari, P. Krishnan, K. Jain, A. K. J. Saudagar, P. P., and R. C. Poonia, "A three-tier microsegmentation framework for enterprise networks under Zero Trust Architecture," *Alexandria Engineering Journal*, vol. 141, pp. 150–164, Apr. 2026, doi: 10.1016/j.aej.2026.03.014.

[8] A. Vinueza-Cabezas, J. J. Samaniego-Frixone, and M. Bourgeat-Salazar, "How personal and professional characteristics shape the link between work engagement and work–home interactions during the COVID-19 transition: Evidence from Ecuador," *Acta Psychol. (Amst).*, vol. 265, p. 106671, May 2026, doi: 10.1016/j.actpsy.2026.106671.

[9] S. Hasan, I. Amundson, and D. Hardin, "Zero-trust design and assurance patterns for cyber–physical systems," *Journal of Systems Architecture*, vol. 155, Oct. 2024, doi: 10.1016/j.sysarc.2024.103261.

[10] M. K. Islam, C. Ya, M. N. Islam, S. Sultana, and M. Das, “A bibliometric analysis of governmental cybersecurity policies: Trends, challenges, and future directions,” Jun. 01, 2026, *Elsevier B.V.* doi: 10.1016/j.jeconc.2026.100215.

[11] S. Singh and A. Dhumane, “Unmasking digital deceptions: An integrative review of deepfake detection, multimedia forensics, and cybersecurity challenges,” Dec. 01, 2025, *Elsevier B.V.* doi: 10.1016/j.mex.2025.103632.

[12] M. A. Mohamed, B. M. Chaudhry, J. Chakraborty, and K. J. O’sullivan, “Bridging the Zero Trust Gap: A Knowledge Management Approach to Business Data Protection,” *Procedia Comput. Sci.*, vol. 278, pp. 590–597, 2026, [Online]. Available: www.sciencedirect.com

[13] Y. Liu, “Construction of network access Layer security protection System based on zero trust architecture,” in *Procedia Computer Science*, Elsevier B.V., 2024, pp. 1013–1022. doi: 10.1016/j.procs.2024.09.121.

[14] T. Wan, B. Shi, and H. Wang, “A continuous authentication scheme for zero-trust architecture in industrial internet of things,” *Alexandria Engineering Journal*, vol. 122, pp. 555–563, May 2025, doi: 10.1016/j.aej.2025.03.012.

[15] F. Tang, C. Ma, and K. Cheng, “Privacy-preserving authentication scheme based on zero trust architecture,” *Digital Communications and Networks*, vol. 10, no. 5, pp. 1211–1220, Oct. 2024, doi: 10.1016/j.dcan.2023.01.021.

[16] S. A. Alanazi and F. Ahmad, “Future-Proofing CIA Triad with Authentication for Healthcare: Integrating Hybrid Architecture of ML & DL with IDPS for Robust IoMT Security,” *Computers, Materials and Continua*, vol. 85, no. 1, pp. 769–800, 2025, doi: 10.32604/cmc.2025.066753.

[17] C. Z. Oroni and F. Xianping, “Evaluating the influence of cybersecurity policies and cybersecurity behavior on institutional security performance in remote learning: the moderating role of technological readiness,” *Sustainable Futures*, vol. 10, Dec. 2025, doi: 10.1016/j.sftr.2025.101554.

[18] A. Zineddine, Y. Belfaik, A. Rehaimi, Y. Sadqi, and S. Safi, “Single Sign-On Security and Privacy: A Systematic Literature Review,” 2025, *Tech Science Press*. doi: 10.32604/cmc.2025.066139.

[19] S. Ahmadi, “Autonomous identity-based threat segmentation for zero trust architecture,” *Cyber Security and Applications*, vol. 3, Dec. 2025, doi: 10.1016/j.csa.2025.100106.

[20] Y. S. Razooqi and A. Pekar, “A flow-level dataset of WireGuard tunnel traffic with matched encrypted-side features and application labels,” *Data Brief*, vol. 66, Jun. 2026, doi: 10.1016/j.dib.2026.112696.

[21] A. S. S. Andari and E. Nurmianti, “Peran dan Tanggung Jawab Etis Profesional TI dalam Mencegah Kebocoran Data Privasi,” *Jejak digital: Jurnal Ilmiah Multidisiplin*, vol. 2, no. 3, pp. 3856–3863, 2026, doi: 10.63822/kpy62w91.

[22] R. A. Rahman, E. Nurmiati, and R. A. Diterima, “Tinjauan Etika Profesi TI pada Standar ACM-IEEE dan SKKNI: Systematic Literature Review,” *Jurnal Ilmiah Sistem Informasi*, vol. 2, no. 2, pp. 164–172, 2026.