Zero Trust Network Architecture Design For Mid-Scale Organizations

Nurul Kamila[1)], Makhsun[2)], Sudarno[3)]

[1)2)3)]Teknik Informatika S-2, Program Pascasarjana, Universitas Pamulang
***)Correspondence author:** Nurul Kamila, nurulkamila1899@gmail.com, Tangerang Selatan, Indonesia
DOI : https://doi.org/10.37012/jtik.v12i1.3292

Abstract

The development of information technology, the adoption of cloud-based services, and the implementation of remote work patterns increase network security risks in medium-sized organizations. Traditional network security approaches that focus on the perimeter are considered no longer adequate in facing increasingly complex cyber threats. This study presents the design of a Zero Trust Network (ZTN) architectural blueprint specifically designed for medium-sized organizations. The research method used is a conceptual approach through literature review, network security requirements analysis, and the design of the ZTN logical architecture. The research results are a Zero Trust Network architectural blueprint that emphasizes continuous verification, identity-based access control, and the application of the principles of least privilege and micro-segmentation. The architectural design is arranged in a modular and phased manner and is aligned with the NIST SP 800-207 framework, so it remains realistic for adoption without requiring drastic infrastructure changes. The resulting ZTN architectural blueprint can be used as an initial reference for medium-sized organizations in designing a Zero Trust-based network security strategy. This research is conceptual in nature and does not include the implementation stage or empirical testing in a real operational environment. It is hoped that the results of this study can serve as an initial reference for medium-sized organizations in designing a more adaptive and sustainable network security strategy.

Keywords: *Zero Trust Network, Network Security, Network Architecture, Medium-Scale Organizations*

Abstrak

Perkembangan teknologi informasi, adopsi layanan berbasis cloud, serta penerapan pola kerja jarak jauh meningkatkan risiko keamanan jaringan pada organisasi skala menengah. Pendekatan keamanan jaringan tradisional yang berfokus pada perimeter dinilai tidak lagi memadai dalam menghadapi ancaman siber yang semakin kompleks. Penelitian ini menyajikan perancangan sebuah blueprint arsitektur Zero Trust Network (ZTN) yang dirancang khusus untuk organisasi skala menengah. Metode penelitian yang digunakan adalah pendekatan konseptual melalui studi literatur, analisis kebutuhan keamanan jaringan, serta perancangan arsitektur logis ZTN. Hasil penelitian berupa blueprint arsitektur Zero Trust Network yang menekankan verifikasi berkelanjutan, kontrol akses berbasis identitas, serta penerapan prinsip least privilege dan micro-segmentation. Rancangan arsitektur disusun secara modular dan bertahap serta diselaraskan dengan kerangka kerja NIST SP 800-207, sehingga tetap realistis untuk diadopsi tanpa memerlukan perubahan infrastruktur secara drastis. Blueprint arsitektur ZTN yang dihasilkan dapat digunakan sebagai referensi awal bagi organisasi skala menengah dalam merancang strategi keamanan jaringan berbasis Zero Trust. Penelitian ini bersifat konseptual dan belum mencakup tahap implementasi maupun pengujian empiris di lingkungan operasional nyata. Diharapkan hasil penelitian ini dapat menjadi referensi awal bagi organisasi skala menengah dalam merancang strategi keamanan jaringan yang lebih adaptif dan berkelanjutan.

Kata Kunci : Zero Trust Network, Keamanan Jaringan, Arsitektur Jaringan, Organisasi Skala Menengah

PENDAHULUAN

Perkembangan teknologi informasi yang pesat, adopsi layanan berbasis cloud, serta penerapan pola kerja jarak jauh telah meningkatkan kompleksitas dan risiko keamanan jaringan pada organisasi skala menengah (Ahmadi, 2024; Lund et al., 2024). Model keamanan jaringan tradisional yang berfokus pada pertahanan perimeter tidak lagi mampu memberikan perlindungan yang memadai terhadap ancaman siber modern (Gambo & Almulhem, 2025; Lund et al., 2024), terutama ketika akses terhadap sistem dan data dilakukan dari berbagai lokasi dan perangkat.

Pendekatan keamanan konvensional umumnya mengasumsikan bahwa entitas yang berada di dalam jaringan internal dapat dipercaya, sementara ancaman dianggap berasal dari luar jaringan (Lund et al., 2024). Asumsi ini menjadi tidak relevan dalam kondisi lingkungan kerja saat ini, di mana batas antara jaringan internal dan eksternal semakin kabur. Serangan siber seperti pencurian kredensial, pergerakan lateral penyerang, serta kebocoran data menunjukkan bahwa kepercayaan implisit dalam jaringan internal dapat menjadi celah keamanan yang serius (Kipkoech Denzel, 2025).

Zero Trust Network (ZTN) hadir sebagai pendekatan keamanan alternatif yang menolak konsep kepercayaan bawaan dan menerapkan prinsip never trust, always verify (Rose et al., 2020; Senan Mahmod Attar Bashi & Senan, 2025). Dalam model Zero Trust, setiap permintaan akses harus melalui proses verifikasi yang ketat berdasarkan identitas pengguna, kondisi perangkat, serta konteks akses, tanpa bergantung pada lokasi jaringan. Pendekatan ini dinilai lebih adaptif dalam menghadapi dinamika ancaman siber modern.

Meskipun konsep Zero Trust telah banyak diadopsi oleh organisasi berskala besar, penerapannya pada organisasi skala menengah masih menghadapi berbagai tantangan, seperti keterbatasan anggaran, sumber daya manusia, dan infrastruktur teknologi (Abdelmagid & Diaz, 2025; Kumar, 2025). Oleh karena itu, diperlukan suatu rancangan arsitektur Zero Trust yang disesuaikan dengan kebutuhan dan kemampuan organisasi skala menengah, tanpa menghilangkan prinsip-prinsip inti keamanan.

Berbagai penelitian sebelumnya telah membahas implementasi Zero Trust Architecture pada organisasi berskala besar maupun lingkungan cloud enterprise. Namun,

sebagian besar penelitian tersebut berfokus pada aspek implementasi teknis atau kajian literatur sistematis, dan belum secara spesifik merancang blueprint arsitektur Zero Trust yang disesuaikan dengan karakteristik organisasi skala menengah yang memiliki keterbatasan sumber daya. Selain itu, pendekatan modular dan bertahap yang realistis untuk konteks organisasi menengah masih belum banyak dibahas secara konseptual. Oleh karena itu, penelitian ini berupaya mengisi kesenjangan tersebut melalui perancangan blueprint arsitektur Zero Trust Network yang adaptif dan aplikatif untuk organisasi skala menengah.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk merancang sebuah blueprint arsitektur Zero Trust Network yang relevan dan realistis untuk diterapkan pada organisasi skala menengah. Rancangan yang diusulkan disusun secara konseptual, modular, dan bertahap, serta diselaraskan dengan kerangka kerja Zero Trust yang direkomendasikan oleh NIST SP 800-207. Diharapkan hasil penelitian ini dapat menjadi referensi awal bagi organisasi skala menengah dalam merancang strategi keamanan jaringan yang lebih adaptif dan berkelanjutan.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan konseptual dengan tujuan merancang sebuah blueprint arsitektur Zero Trust Network (ZTN) yang sesuai untuk organisasi skala menengah. Metode penelitian difokuskan pada perancangan arsitektur dan analisis konseptual tanpa melakukan implementasi langsung pada lingkungan operasional.

Tahapan penelitian diawali dengan studi literatur terhadap konsep, prinsip, dan arsitektur Zero Trust Network dari berbagai sumber ilmiah dan standar keamanan jaringan, termasuk kerangka kerja NIST SP 800-207. Studi literatur ini bertujuan untuk mengidentifikasi prinsip-prinsip utama Zero Trust serta komponen arsitektur yang relevan untuk diterapkan pada organisasi skala menengah.

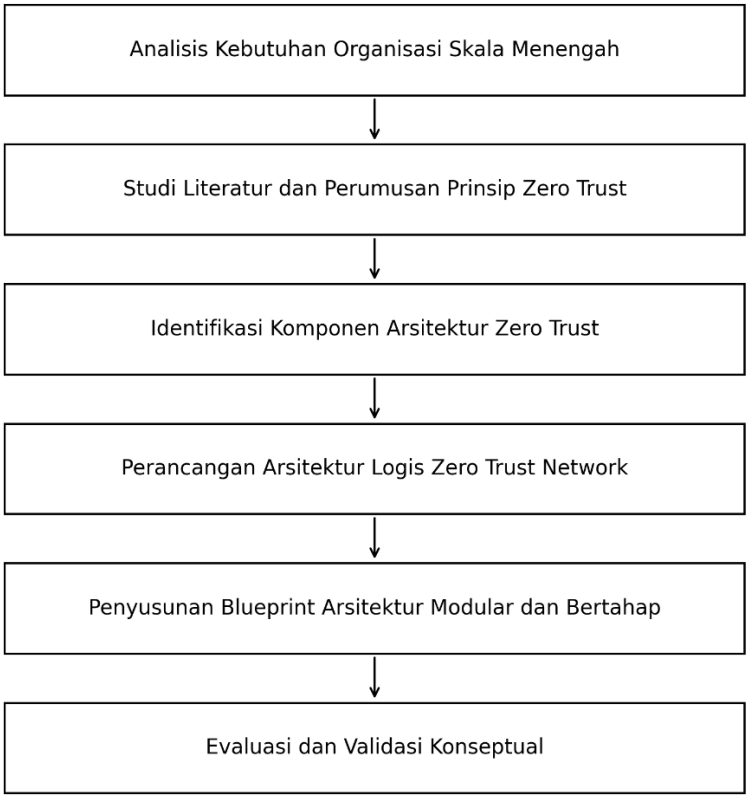
Selanjutnya dilakukan analisis kebutuhan keamanan jaringan organisasi skala menengah, dengan mempertimbangkan karakteristik umum organisasi, seperti keterbatasan anggaran, sumber daya manusia, serta kompleksitas infrastruktur teknologi informasi.

Analisis ini digunakan untuk menentukan komponen Zero Trust yang paling prioritas dan realistis untuk diadopsi.

Berdasarkan hasil studi literatur dan analisis kebutuhan, dilakukan perancangan arsitektur logis Zero Trust Network yang mencakup komponen utama seperti Identity and Access Management (IAM), Multi-Factor Authentication (MFA), Policy Decision Point (PDP), Policy Enforcement Point (PEP), micro-segmentation, serta mekanisme monitoring terpusat. Rancangan arsitektur disusun secara modular dan bertahap untuk memudahkan proses adopsi.

Tahap akhir penelitian adalah validasi konseptual, yaitu dengan membandingkan rancangan arsitektur yang diusulkan terhadap prinsip dan komponen Zero Trust yang direkomendasikan dalam NIST SP 800-207 serta temuan pada studi literatur terkait. Validasi ini bertujuan untuk memastikan bahwa blueprint arsitektur yang dirancang telah selaras dengan standar Zero Trust dan relevan untuk diterapkan pada organisasi skala menengah.

Untuk memperjelas proses validasi konseptual, penelitian ini menggunakan beberapa parameter evaluasi yang mengacu pada prinsip utama Zero Trust. Parameter tersebut meliputi: (1) penerapan verifikasi berkelanjutan pada setiap permintaan akses, (2) implementasi kontrol akses berbasis identitas dan prinsip least privilege, (3) penerapan micro-segmentation untuk membatasi pergerakan lateral, serta (4) integrasi monitoring dan logging terpusat. Blueprint arsitektur dinilai memenuhi validasi konseptual apabila seluruh parameter tersebut terakomodasi secara sistematis dalam rancangan yang diusulkan.



Gambar 1. Diagram Tahapan Penelitian

HASIL DAN PEMBAHASAN

Rancangan Blueprint Arsitektur Zero Trust Network

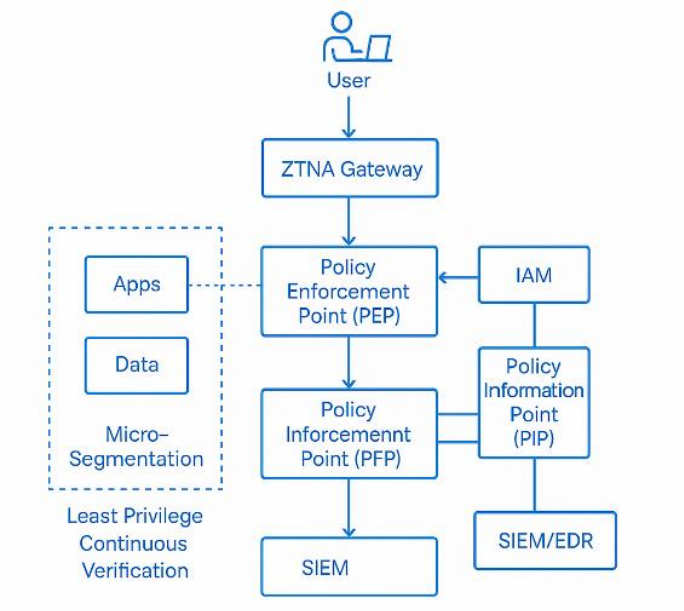
Hasil utama dari penelitian ini adalah sebuah blueprint arsitektur Zero Trust Network (ZTN) yang dirancang khusus untuk organisasi skala menengah. Rancangan arsitektur ini disusun berdasarkan prinsip dasar Zero Trust, yaitu tidak adanya kepercayaan bawaan terhadap pengguna maupun perangkat, serta penerapan proses verifikasi secara berkelanjutan pada setiap permintaan akses.

Blueprint arsitektur yang diusulkan menempatkan Policy Enforcement Point (PEP) sebagai gerbang utama akses ke sumber daya organisasi. Setiap permintaan akses dari pengguna atau perangkat akan terlebih dahulu melalui PEP sebelum diteruskan ke sistem internal. Selanjutnya, Policy Decision Point (PDP) berperan dalam melakukan evaluasi

kebijakan akses berdasarkan informasi identitas, peran pengguna, kondisi perangkat, serta konteks akses yang diperoleh dari Policy Information Point (PIP).

Komponen Identity and Access Management (IAM) dan Multi-Factor Authentication (MFA) diintegrasikan untuk memastikan bahwa proses autentikasi dilakukan secara kuat dan tidak hanya bergantung pada kredensial tunggal. Selain itu, penerapan micro-segmentation membagi jaringan ke dalam beberapa segmen kecil, sehingga akses terhadap satu layanan tidak secara otomatis memberikan akses ke layanan lainnya. Pendekatan ini bertujuan untuk membatasi pergerakan lateral apabila terjadi kompromi pada salah satu komponen sistem.

Rancangan arsitektur Zero Trust Network yang diusulkan dalam penelitian ini ditunjukkan pada Gambar 1.



Gambar 2. Arsitektur Zero Trust Network

Secara teknis, relasi antar komponen dalam arsitektur yang diusulkan mengikuti prinsip kontrol akses terpusat. Setiap permintaan akses dari pengguna atau perangkat pertama kali melewati Policy Enforcement Point (PEP) yang berfungsi sebagai gerbang kontrol. PEP kemudian meneruskan permintaan tersebut ke Policy Decision Point (PDP) untuk dilakukan evaluasi kebijakan. PDP memperoleh informasi tambahan dari Policy Information Point (PIP), termasuk atribut identitas pengguna, status perangkat, serta konteks

akses. Keputusan akses yang dihasilkan oleh PDP dikirim kembali ke PEP untuk dieksekusi dalam bentuk pemberian akses terbatas atau penolakan akses. Mekanisme ini memastikan bahwa proses otorisasi tidak bergantung pada lokasi jaringan, melainkan pada verifikasi identitas dan kebijakan yang berlaku secara dinamis.

Integrasi antara IAM dan MFA memperkuat proses autentikasi sebelum keputusan akses diambil, sementara penerapan micro-segmentation membatasi komunikasi antar-segmen jaringan sehingga mencegah pergerakan lateral apabila terjadi kompromi. Monitoring terpusat melalui SIEM dan EDR memungkinkan deteksi aktivitas anomali secara berkelanjutan dan mendukung prinsip continuous verification dalam arsitektur Zero Trust.

Integrasi Komponen dan Alur Akses Zero Trust

Rancangan arsitektur Zero Trust Network yang diusulkan menekankan integrasi antar komponen keamanan secara terpusat dan terkoordinasi. Alur akses dimulai ketika pengguna melakukan permintaan terhadap aplikasi atau sumber daya tertentu. Permintaan tersebut tidak langsung diteruskan, melainkan diverifikasi melalui proses autentikasi dan otorisasi berbasis kebijakan.

Dalam proses ini, PDP melakukan pengambilan keputusan akses dengan mempertimbangkan berbagai parameter, seperti identitas pengguna, peran atau hak akses, status perangkat, serta kondisi lingkungan akses. Keputusan yang dihasilkan kemudian diterapkan oleh PEP dalam bentuk pemberian akses terbatas, penolakan akses, atau permintaan verifikasi tambahan. Dengan mekanisme ini, prinsip least privilege access dapat diterapkan secara konsisten pada seluruh sistem.

Selain kontrol akses, mekanisme monitoring terpusat melalui sistem Security Information and Event Management (SIEM) dan Endpoint Detection and Response (EDR) digunakan untuk memantau aktivitas pengguna dan perangkat secara berkelanjutan. Apabila terdeteksi aktivitas yang tidak normal, sistem dapat memberikan peringatan dini atau melakukan tindakan pembatasan akses secara otomatis.

Tahapan Implementasi

Untuk menyesuaikan dengan keterbatasan sumber daya organisasi skala menengah, blueprint arsitektur Zero Trust Network dirancang untuk dapat diimplementasikan secara bertahap. Tahap awal difokuskan pada penguatan identitas dan autentikasi melalui penerapan IAM dan MFA. Tahap selanjutnya mencakup penerapan kontrol akses berbasis kebijakan melalui PEP dan PDP, serta pembagian jaringan menggunakan micro-segmentation. Tahap akhir diarahkan pada optimalisasi monitoring dan respons insiden melalui integrasi SIEM dan EDR.

Pendekatan bertahap ini memungkinkan organisasi untuk mengadopsi konsep Zero Trust tanpa harus melakukan perubahan infrastruktur secara drastis dalam satu waktu. Dengan demikian, implementasi Zero Trust Network dapat dilakukan secara lebih realistis, terukur, dan sesuai dengan kapasitas organisasi skala menengah. Perbandingan antara model keamanan tradisional dan Zero Trust Network ditunjukkan pada Tabel 1.

Tabel 1. Perbandingan Keamanan Tradisional dan ZTN

Aspek	Keamanan Tradisional	Zero Trust Network
Model Kepercayaan	Trust berdasarkan lokasi jaringan	Tidak ada kepercayaan bawaan
Autentikasi	Username dan password	*MFA* dan *IAM* berbasis identitas
Segmentasi Jaringan	Jaringan bersifat flat	*Micro-segmentation*
Kontrol Akses	Akses luas setelah login	*Least privilege access*
Monitoring	Terbatas dan pasif	Berkelanjutan dan terpusat

Beberapa penelitian sebelumnya telah membahas implementasi Zero Trust Architecture pada berbagai konteks organisasi, baik melalui pendekatan implementasi teknis maupun kajian literatur sistematis. Namun, sebagian besar penelitian tersebut berfokus pada organisasi berskala besar atau lingkungan cloud enterprise, serta belum secara spesifik merancang blueprint arsitektur yang disesuaikan dengan karakteristik organisasi skala menengah.

Dibandingkan dengan penelitian oleh Abdelmagid dan Diaz (2025) yang menitikberatkan pada analisis risiko pada small–medium enterprises, penelitian ini berfokus pada perancangan blueprint arsitektur secara modular dan bertahap. Sementara itu,

penelitian oleh Gambo dan Almulhem (2025) merupakan kajian literatur sistematis yang mengidentifikasi tantangan implementasi Zero Trust, namun belum menyajikan rancangan arsitektur logis yang terstruktur. Dengan demikian, kontribusi penelitian ini terletak pada penyusunan blueprint arsitektur Zero Trust Network yang aplikatif dan realistis untuk organisasi skala menengah dengan mempertimbangkan keterbatasan sumber daya dan kompleksitas infrastruktur.

Kelebihan dan Keterbatasan Rancangan Arsitektur

Rancangan blueprint arsitektur Zero Trust Network yang diusulkan dalam penelitian ini memiliki beberapa kelebihan. Pertama, arsitektur dirancang secara modular dan bertahap sehingga memungkinkan organisasi skala menengah untuk mengadopsinya sesuai dengan kapasitas sumber daya yang dimiliki. Kedua, blueprint menekankan integrasi kontrol akses berbasis identitas, penerapan prinsip least privilege, serta micro-segmentation yang mampu membatasi pergerakan lateral dalam jaringan. Ketiga, rancangan ini diselaraskan dengan kerangka kerja NIST SP 800-207 sehingga tetap relevan dengan standar keamanan yang diakui secara internasional.

Namun demikian, terdapat beberapa keterbatasan dalam penelitian ini. Blueprint yang diusulkan masih bersifat konseptual dan belum diuji melalui implementasi empiris pada lingkungan operasional nyata. Selain itu, efektivitas penerapan arsitektur sangat bergantung pada kesiapan infrastruktur identitas serta kemampuan organisasi dalam melakukan monitoring dan respons insiden secara berkelanjutan. Oleh karena itu, penelitian lanjutan yang mencakup tahap implementasi dan pengujian kinerja arsitektur diperlukan untuk mengukur efektivitasnya secara kuantitatif.

KESIMPULAN DAN REKOMENDASI

Penelitian ini menghasilkan sebuah blueprint arsitektur Zero Trust Network (ZTN) yang dirancang untuk menjawab tantangan keamanan jaringan pada organisasi skala menengah. Rancangan arsitektur yang diusulkan mengadopsi prinsip-prinsip utama Zero Trust, seperti verifikasi berkelanjutan, kontrol akses berbasis identitas, penerapan least

privilege, serta micro-segmentation, dengan mengintegrasikan komponen IAM, MFA, PDP, dan PEP. Blueprint disusun secara modular dan bertahap serta diselaraskan dengan kerangka kerja NIST SP 800-207, sehingga tetap relevan secara konseptual dan realistis untuk diadopsi tanpa menuntut perubahan infrastruktur secara drastis. Dengan demikian, hasil penelitian ini dapat digunakan sebagai referensi awal bagi pengembangan strategi keamanan jaringan berbasis Zero Trust pada organisasi skala menengah. Namun demikian, perlu ditegaskan bahwa penelitian ini bersifat konseptual dan belum mencakup tahap implementasi maupun pengujian empiris di lingkungan operasional nyata.

REFERENSI

Abdelmagid, A. M., & Diaz, R. (2025). Zero trust architecture as a risk countermeasure in small–medium enterprises and advanced technology systems. *Risk Analysis*. https://doi.org/10.1111/risa.70026

Ahmadi, S. (2024). Zero trust architecture in cloud networks: Application, challenges and future opportunities. *Journal of Engineering Research and Reports, 26*(2), 215–228. https://doi.org/10.9734/jerr/2024/v26i21083

Arora, S., & Hastings, J. (2024). Microsegmented cloud network architecture using open source tools for a zero trust foundation. https://doi.org/10.1109/SIN63213.2024.10871361

Bashi, Z. S. M. A., & Senan, S. (2025). A comprehensive review of zero trust network architecture (ZTNA) and deployment frameworks. *International Journal on Perceptive and Cognitive Computing, 11*(1), 148–153. https://doi.org/10.31436/ijpcc.v11i1.494

Cao, Y., Pokhrel, S. R., Zhu, Y., Doss, R., & Li, G. (2024). Automation and orchestration of zero trust architecture: Potential solutions and challenges. *Machine Intelligence Research, 21*(2), 294–317. https://doi.org/10.1007/s11633-023-1456-2

Cloud Computing Indonesia. (2024, November 24). UMKM dan organisasi besar kian rentan serangan ransomware.

Gambo, M. L., & Almulhem, A. (2025). Zero trust architecture: A systematic literature review. http://arxiv.org/abs/2503.11659

Godwin Nzeako, & Shittu, R. A. (2024). Implementing zero trust security models in cloud computing environments. *World Journal of Advanced Research and Reviews, 24*(3), 1647–1660. https://doi.org/10.30574/wjarr.2024.24.3.3500

Kipkoech, D. (2025). A survey of security in zero trust network architectures. *GSC Advanced Research and Reviews, 22*(2), 182–214. https://doi.org/10.30574/gscarr.2025.22.2.0036

Kumar, P. (2025). Zero trust architecture for SME cybersecurity: Enhancing resilience in the digital transformation era. *Journal of Progressive Research in Engineering Management and Science, 5*, 2791–2819.

Lund, B. D., Lee, T.-H., Wang, Z., Wang, T., & Mannuru, N. R. (2024). Zero trust cybersecurity: Procedures and considerations in context. *Encyclopedia, 4*(4), 1520–1533. https://doi.org/10.3390/encyclopedia4040099

Mukhlisin, M., & Firmansyah, R. A. (2025). Zero trust architecture: Solusi keamanan dan privasi untuk institusi pendidikan, systematic literature review. *Jurnal Mahasiswa Teknik Informatika, 9*(4).

Nusantara. (2024). Jaminan informasi dan keamanan yang lebih baik: Studi kasus BPJS Kesehatan.

Rahman, A., Indrajit, E., Unggul, A., & Dazki, E. (2024). Implementation of zero trust security in MSME enterprise architecture: Challenges and solutions. *Jurnal dan Penelitian Teknik Informatika, 8*(3). https://doi.org/10.33395/sinkron.v8i3.13949

Rahman, R., Rahman, A. F., & Artikel, S. (2024). Penerapan zero trust network access (ZTNA) dengan penggunaan captcha pada website umum. *Technology Sciences Insights Journal*.