ZERO TRUST ARCHITECTURE: SOLUSI KEAMANAN DAN PRIVASI UNTUK INSTITUSI PENDIDIKAN, *SYSTEMATIC LITERATURE REVIEW*

Muhamad Mukhlisin [1], Rico Agung Firmansyah [2]
[1] Program Studi Program Profesi Insinyur
Fakultas Teknologi Industri Universitas Negeri Makassar,
[2] Fakultas Teknologi Industri, Magsiter Teknik Informatika Universitas Islam Indonesia
src.hbarkah@gmail.com

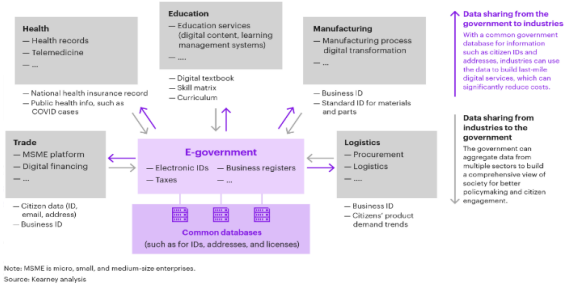
ABSTRAK

Keamanan jaringan di institusi pendidikan sangat penting untuk melindungi data sensitif. *Zero Trust Architecture* (ZTA) dapat meningkatkan keamanan dengan tidak memberikan kepercayaan implisit pada perangkat dan pengguna. Namun, penerapan ZTA di institusi pendidikan menghadapi tantangan besar, seperti keterbatasan sumber daya, keahlian teknis yang rendah, dan kurangnya kesadaran tentang pentingnya keamanan. Tujuan penelitian ini adalah untuk mengeksplorasi dan memberikan rekomendasi terkait implementasi ZTA dalam keamanan jaringan di institusi pendidikan, dengan fokus pada tantangan dan solusi yang relevan. Penelitian ini diharapkan memberikan wawasan praktis bagi institusi pendidikan dalam mengadopsi ZTA secara lebih efektif. Metode penelitian ini menggunakan *Systematic Literature Review* (SLR) karena pengumpulan dan analisis data yang terstruktur serta memberikan gambaran komprehensif dalam mengidentifikasi aspek maupun variabel penelitian sehingga menghasilkan temuan penelitian yang relevan, akurat. Proses SLR pada penelitian ini menghasilkan 1034 artikel pencarian, 130 artikel lolos filtering berdasarkan kata kunci, inklusi dan eksklusi, serta 61 artikel ilmiah yang dianalisa berdasarkan konteks penerapan ZTA pada organisasi. Hasil penelitian menunjukkan bahwa ZTA dapat meningkatkan keamanan data dan memenuhi kepatuhan privasi di institusi pendidikan. Namun, penerapannya terhambat oleh keterbatasan sumber daya dan keahlian teknis. Penelitian ini menyarankan agar institusi pendidikan memperkuat kesadaran keamanan dan memberikan pelatihan yang tepat untuk implementasi ZTA yang lebih efektif.

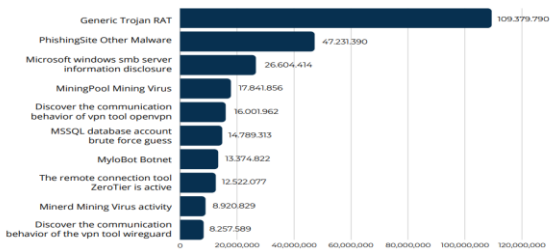
Kata kunci: *Zero Trust Architecture, Keamanan Jaringan, Institusi Pendidikan, Privasi Data, Cyber Security, Perlindungan Data, Keamanan Informasi*

1. PENDAHULUAN

Transformasi digital di Indonesia dan berbagai negara memberikan manfaat signifikan, seperti peningkatan layanan publik melalui *e-government* dan sistem elektronik lainnya [1]. Laporan BSSN mencatat 403,9 juta serangan pada 2023, menunjukkan pentingnya kesiapan keamanan data [2,3].



Gambar 1. *Digital transformation landscape* [4].



Gambar 2. Data 10 Jenis serangan keamanan siber di indonesia tahun 2023 [5]

Keamanan jaringan data dan informasi sangat penting tidak hanya di sektor swasta dan pemerintahan, tetapi juga di dunia pendidikan, termasuk sekolah yang semakin bergantung pada teknologi untuk pembelajaran, administrasi, komunikasi, dan integrasi layanan eksternal. Peningkatan penggunaan teknologi ini meningkatkan risiko serangan siber yang mengancam data sensitif, proses pembelajaran, dan reputasi sekolah [6]. Sekolah menengah menghadapi tantangan seperti keterbatasan anggaran dan kurangnya kesadaran tentang keamanan, membuat jaringan sekolah rentan terhadap serangan seperti hacking, peretasan akun, malware, phishing, dan DoS [7]. Untuk itu, pemerintah Indonesia mengatur keamanan sistem informasi melalui UU ITE dan peraturan terkait, yang mewajibkan perlindungan data pribadi di organisasi [8,9]. Zero Trust Architecture (ZTA) menawarkan solusi untuk memenuhi persyaratan pengamanan dengan memverifikasi eksplisit setiap akses data dalam organisasi [10]. Peran ZTA untuk lembaga pendidikan sangat penting dalam memastikan apakah mereka membutuhkan ZTA adalah pertanyaan mendasar yang dapat dijawab dengan menganalisa beberapa faktor perlu dipertimbangkan, yaitu :

a. Tingkat sensitivitas data yang disimpan dan dikelola oleh sekolah;
b. Tingkat risiko serangan siber yang dihadapi sekolah;

c. Kompleksitas infrastruktur jaringan sekolah;
d. Ketersediaan sumber daya untuk implementasi dan pengelolaan ZTA.

Artikel review ini menggunakan metode *Systematic Literature Review* (SLR) yang sistematis dan komprehensif, mengikuti prinsip-prinsip yang diuraikan dalam penelitian [1], untuk mengeksplorasi potensi implementasi ZTA dalam mengamankan jaringan sekolah menengah, menganalisis peningkatan keamanan, kepatuhan privasi data, dan optimalisasi performa jaringan, serta mengidentifikasi best practices, tantangan, dan peluang terkait. Dua pertanyaan penelitian utama yang akan dijawab dalam artikel ini adalah:

a. Bagaimana cara organisasi, khususnya sekolah menengah, memastikan bahwa mereka membutuhkan implementasi ZTA?
b. Bagaimana cara menerapkan ZTA secara efektif di lingkungan sekolah menengah?

2. TINJAUAN PUSTAKA

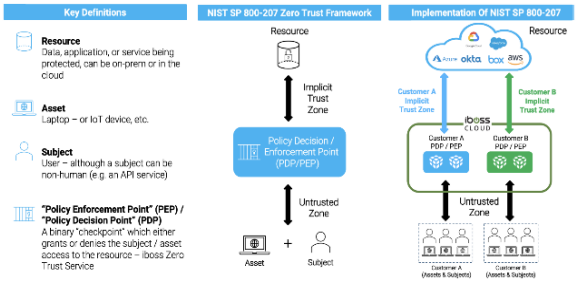
2.1. Zero Trust (ZTA) dan Urgensi penerapannya

Di era digital saat ini, data dan informasi merupakan aset berharga bagi setiap organisasi, termasuk sekolah menengah. Kehilangan atau kompromi data dapat menyebabkan kerugian finansial, kerusakan reputasi, dan pelanggaran hukum, sehingga pengamanan data menjadi krusial untuk kelangsungan dan keberhasilan organisasi. Beberapa alasan mengapa organisasi perlu menerapkan keamanan data dan informasi meliputi:

a. Perlindungan Aset: Data dan informasi merupakan aset yang berharga dan harus dilindungi dari pencurian, kerusakan, atau penyalahgunaan.
b. Kepatuhan Regulasi: Banyak peraturan privasi data yang mengharuskan organisasi untuk melindungi data pribadi individu. Pelanggaran terhadap peraturan ini dapat mengakibatkan denda yang besar dan tindakan hukum lainnya.
c. Keberlangsungan Bisnis: Kehilangan data dapat mengganggu operasional organisasi dan bahkan menyebabkan kebangkrutan.
d. Reputasi: Pelanggaran data dapat merusak reputasi organisasi dan mengurangi kepercayaan pelanggan.

Penerapan ZTA di institusi pendidikan sangat penting untuk melindungi data sensitif seperti informasi siswa, catatan keuangan, dan data penelitian dari ancaman siber. ZTA memastikan bahwa langkah-langkah keamanan berkembang sesuai dengan kompleksitas ancaman siber yang terus meningkat. Komponen utama ZTA meliputi segmentasi mikro, Multi-Factor Authentication (MFA), pemantauan, serta kebijakan kontrol akses seperti Role-Based Access Control (RBAC) dan Attribute-Based Access Control (ABAC). ZTA adalah kerangka kerja yang menghapus kepercayaan implisit dan menerapkan verifikasi ketat untuk semua akses dan pertukaran data, dengan prinsip bahwa tidak ada pengguna atau perangkat yang otomatis dipercaya, baik di dalam maupun di luar jaringan [10]. Pendekatan ini melindungi data dari ancaman internal dan eksternal dengan terus mengautentikasi akses ke sumber daya. ZTA semakin relevan karena model keamanan berbasis perimeter tradisional tidak cukup untuk melindungi data sensitif. Beberapa standar yang relevan untuk implementasi ZTA antara lain::

a. ISO 27001: Standar internasional untuk Sistem Manajemen Keamanan Informasi [11].
b. NIST *Cybersecurity Framework: Framework* yang dikembangkan oleh National Institute of Standards and Technology (NIST) untuk membantu organisasi meningkatkan postur keamanan siber sekaligus menyediakan panduan tentang identifikasi, perlindungan, deteksi, respons, dan pemulihan dari serangan siber [12].
c. CIS *Controls*: Daftar kontrol keamanan yang direkomendasikan oleh *Center for Internet Security* (CIS) untuk mengurangi risiko serangan siber yang meliputi manajemen aset, kontrol akses, dan manajemen kerentanan [13].
d. *General Data Protection Regulation* (GDPR): Regulasi Uni Eropa tentang perlindungan data pribadi. Regulasi ini menetapkan persyaratan ketat tentang bagaimana organisasi harus mengumpulkan, menggunakan, dan melindungi data pribadi [14].
e. UU PDP (Undang-Undang Perlindungan Data Pribadi): Undang-undang di Indonesia tentang perlindungan data pribadi. Undang-undang ini menetapkan hak-hak pemilik data pribadi dan kewajiban organisasi yang mengelola data pribadi [9].
f. NIST SP 800-207 *(Zero Trust Architecture)*: Publikasi dari NIST yang menjelaskan prinsip-prinsip dan komponen-komponen ZTA sekaligus panduan untuk merancang dan mengimplementasikan ZTA [16].
g. Zero Trust Maturity Model (ZTMM): Model yang dikembangkan oleh CISA untuk membantu organisasi mengukur dan meningkatkan kematangan implementasi ZTA mereka [17].



Gambar 2. Contoh Konsep Implementasi NIST Special Publication 800-207 pada organisasi.

Dengan mengacu pada standar dan framework ini, organisasi pendidikan dapat memastikan bahwa implementasi ZTA dilakukan secara efektif dan

efisien, serta sesuai dengan best practices dan memenuhi persyaratan kepatuhan terhadap regulasi yang berlaku.

2.2. Konseptual Implementasi ZTA

Implementasi *Zero Trust Architecture* (ZTA) di organisasi pendidikan memerlukan pemenuhan beberapa kriteria minimal yang menjadi syarat agar ZTA dapat diimplementasikan secara efektif. Berikut adalah kriteria minimal yang harus dipertimbangkan oleh organisasi pendidikan sebelum memutuskan untuk mengimplementasikan ZTA:

a. Tingkat Sensitivitas Data.
   Organisasi pendidikan yang menyimpan data sensitif, seperti data pribadi siswa, informasi akademik, data keuangan, dan catatan kesehatan, perlu mengimplementasikan ZTA. Jika data yang dikelola sangat sensitif dan perlindungan datanya menjadi hal yang sangat krusial, maka organisasi tersebut wajib menerapkan ZTA.
b. Peningkatan Risiko Keamanan Siber.
   Jika organisasi pendidikan mengalami peningkatan intensitas serangan siber, seperti *malware, ransomware, phishing*, dll maka implementasi ZTA menjadi keharusan.
c. Kepatuhan terhadap Regulasi Privasi Data.
   Organisasi pendidikan yang beroperasi di wilayah tertentu terikat pada regulasi seperti GDPR di Eropa atau UU-PDP di Indonesia, yang mewajibkan penerapan ZTA sebagai mekanisme kontrol lebih ketat terhadap siapa dan bagaimana data diakses dan digunakan.
d. Keterbatasan dalam Infrastruktur Keamanan.
   Jika organisasi pendidikan tidak memiliki sistem keamanan yang memadai untuk melindungi data dan informasi dari ancaman yang berkembang, maka ZTA harus dipertimbangkan. Organisasi yang memiliki sistem TI yang tidak dilengkapi dengan kontrol keamanan yang memadai perlu meningkatkan keamanan dengan menerapkan ZTA.
e. Sumber Daya dan Keahlian Teknologi yang Memadai.
   Untuk mengimplementasikan ZTA, organisasi pendidikan harus memiliki sumber daya manusia yang cukup dan memiliki keahlian teknis dalam bidang keamanan siber. Selain itu, harus ada anggaran yang memadai untuk investasi teknologi dan pelatihan. Jika organisasi tidak memiliki sumber daya untuk melakukan implementasi ZTA, maka mereka harus terlebih dahulu memastikan ketersediaan sumber daya ini sebelum mengadopsi ZTA.
f. Kompleksitas Infrastruktur Jaringan.
   Jika organisasi pendidikan memiliki infrastruktur jaringan yang kompleks, dengan banyak perangkat, pengguna, dan aplikasi yang harus diakses, ZTA menjadi solusi yang tepat. Infrastruktur yang besar dan tersebar membutuhkan pengelolaan akses yang lebih ketat dan terstruktur.
g. Kesiapan untuk Implementasi Bertahap.
   Mengingat bahwa implementasi ZTA bukanlah proses yang cepat, organisasi pendidikan perlu memiliki kesiapan untuk implementasi bertahap. Ini mencakup perencanaan jangka panjang untuk membangun sistem yang sesuai dengan framework ZTA, serta kesiapan untuk melibatkan seluruh staf dan pengguna dalam proses perubahan.

Dengan memenuhi kriteria minimal ini, organisasi pendidikan dapat menentukan apakah mereka siap untuk mengimplementasikan Zero Trust Architecture atau apakah ada faktor-faktor lain yang perlu dipertimbangkan sebelum mengambil langkah tersebut. Selain itu, Implementasi ZTA yang efektif harus mempertimbangkan integrasi dengan standar dan framework yang telah disebutkan, seperti diantaranya:

a. Mengimplementasikan kontrol akses berdasarkan prinsip least privilege sesuai dengan panduan dari CIS Controls dan ISO 27001.
b. Mengenkripsi data sensitif sesuai dengan standar ISO 27701 dan GDPR/UU PDP.
c. Menerapkan pemantauan keamanan yang komprehensif sesuai dengan panduan dari NIST Cybersecurity Framework dan ZTMM.
d. Memperkuat verifikasi identitas dengan menerapkan multi-factor authentication (MFA) sesuai dengan rekomendasi dari NIST dan standar industri lainnya.

Dengan mengintegrasikan standar dan framework yang relevan tersebut diatas, organisasi pendidikan dapat membangun ZTA yang terukur, memastikan data dan informasi mereka terlindungi dari ancaman siber. Implementasi ZTA bukanlah proses yang sederhana dan membutuhkan perencanaan yang matang serta eksekusi yang cermat. Berikut adalah gambaran singkat tentang langkah-langkah atau tahapan yang umumnya terlibat dalam implementasi ZTA:

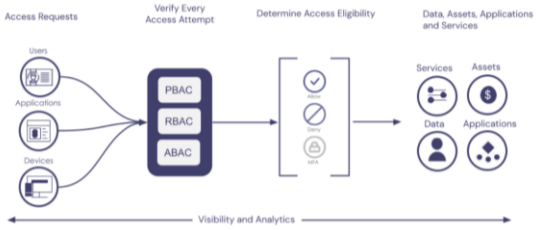
a. *Assessment*: Tahap awal ini melibatkan penilaian menyeluruh terhadap infrastruktur jaringan, sistem, dan aplikasi yang ada di organisasi. Tujuannya adalah untuk mengidentifikasi aset-aset kritikal, kerentanan keamanan, dan risiko yang mungkin timbul.
b. Perencanaan *(Planning)*: Berdasarkan hasil penilaian, organisasi perlu menyusun rencana implementasi ZTA yang komprehensif. Rencana ini harus mencakup tujuan yang jelas, ruang lingkup implementasi, anggaran yang tersedia, sumber daya yang dibutuhkan, dan jadwal waktu yang realistis.
c. Desain (Design): Tahap ini melibatkan perancangan arsitektur ZTA yang sesuai dengan kebutuhan dan karakteristik organisasi.

Arsitektur ini harus mencakup komponen-komponen ZTA yang relevan, seperti microsegmentation, multi-factor authentication (MFA), dan continuous monitoring.

d. Implementasi (Implementation): Tahap ini melibatkan penerapan komponen-komponen ZTA yang telah dirancang. Implementasi harus dilakukan secara bertahap dan terkoordinasi untuk meminimalkan gangguan terhadap operasional organisasi.
e. Pengujian (Testing): Setelah implementasi selesai, perlu dilakukan pengujian yang komprehensif untuk memastikan bahwa ZTA berfungsi sebagaimana mestinya dan efektif dalam melindungi aset-aset kritikal organisasi.
f. Pemantauan (Monitoring): ZTA harus dipantau secara terus-menerus untuk mendeteksi potensi ancaman dan kerentanan keamanany, mencakup analisis log, deteksi intrusi, dan penilaian kerentanan.
g. Pemeliharaan (Maintenance): ZTA perlu dipelihara secara teratur untuk memastikan bahwa sistem tetap aman dan efektif meliputi pembaruan perangkat lunak, konfigurasi keamanan, dan pelatihan pengguna.

Langkah-langkah ini bersifat umum dan dapat disesuaikan dengan kebutuhan setiap organisasi. Implementasi ZTA merupakan proses berkelanjutan yang membutuhkan komitmen dan investasi jangka panjang. Beberapa faktor kunci yang dapat mempengaruhi keberhasilan implementasi ZTA antara lain:

a. Dukungan Manajemen
b. Keterlibatan Pengguna.
c. Pelatihan dan Kesadaran pengguna.
d. Pemilihan Teknologi yang Tepat.
e. Pemantauan dan Evaluasi



Gambar 3. Konsep Implementasi ZTA

Komponen yang diperlukan untuk membangun ZTA di suatu organisasi:

a. *Access Requests* (Permintaan Akses), antara lain:
   - Users (Pengguna): Pengguna yang meminta akses ke sistem atau data.
   - Applications (Aplikasi): Aplikasi yang diakses oleh pengguna atau perangkat.
   - Devices (Perangkat): Perangkat yang digunakan oleh pengguna untuk mengakses aplikasi atau data.
b. *Verify Every Access Attempt* (Verifikasi Setiap *Permintaan* Akses), yaitu Setiap permintaan akses harus verifikasi terlebih dahulu, memastikan bahwa hanya akses yang sah yang diperbolehkan. Proses ini memastikan bahwa keamanan di tingkat akses sangat ketat.
c. *Determine Access Eligibility* (Menentukan *Kelayakan* Akses), yaitu: opsi kelayakan akses berdasarkan kebijakan PBAC *(Policy Based Access Control)*, RBAC *(Role-Based Access Control), dan* ABAC *(Attribute-Based Access Control)*, sistem menentukan apakah akses diberikan atau ditolak berdasarkan:
   - PBAC: Akses berdasarkan kebijakan yang ditetapkan oleh organisasi.
   - RBAC: Akses berdasarkan peran yang dimiliki pengguna dalam organisasi.
   - ABAC: Akses berdasarkan atribut yang lebih spesifik, seperti lokasi, waktu, atau atribut lainnya.
d. *MFA (Multi-Factor Authentication).*
e. *Data, Assets, Applications, and Services.*
   - *Data*: Informasi yang perlu dilindungi dalam organisasi.
   - *Assets*: Aset yang dapat mencakup perangkat keras dan perangkat lunak.
   - *Applications*: Aplikasi yang digunakan oleh organisasi untuk operasional.
   - *Services:* Layanan yang diakses oleh pengguna atau perangkat.
f. *Visibility and Analytics*.
   Untuk memastikan bahwa ZTA dapat dipantau dengan baik, sistem visibility dan analytics digunakan untuk memberikan wawasan yang jelas tentang aktivitas akses, keamanan, dan pengelolaan risiko dalam organisasi.

3. METODE PENELITIAN

Untuk menghasilkan artikel review yang komprehensif dan relevan, kami melakukan pencarian literatur sistematis menggunakan berbagai database akademik dan mesin pencari, seperti SINTA 1-6, Google Scholar, IEEE Xplore, ScienceDirect, dan Scopus. Strategi pencarian ini difokuskan pada studi mengenai implementasi Zero Trust Architecture (ZTA) dalam keamanan jaringan di institusi pendidikan, dengan kata kunci berdasarkan definisi PICOC (Population, Intervention, Comparison, Outcome, Context) yang telah disajikan pada tabel 1. Kombinasi kata kunci ini memperluas cakupan pencarian untuk memastikan identifikasi studi yang relevan. Selain itu, pencarian literatur juga mencakup pemeriksaan manual pada daftar referensi artikel yang relevan untuk menemukan studi tambahan yang mungkin terlewatkan dalam pencarian database.. Artikel yang dimasukkan (inklusi) harus memenuhi kriteria berikut:

a. Berfokus pada implementasi ZTA atau konsep terkait dalam konteks keamanan jaringan.

b. Membahas aplikasi ZTA di lingkungan pendidikan atau sekolah.
c. Ditulis dalam bahasa Inggris atau Indonesia.
d. Dipublikasikan dalam rentang waktu 7 tahun terakhir (2018-2025) untuk memastikan relevansi dengan perkembangan teknologi terkini.

Sedangkan Artikel yang dikeluarkan (eksklusi) meliputi kriteria antara lain:

a. Artikel yang tidak membahas ZTA atau konsep terkait lainnya.
b. Artikel yang berfokus pada aspek teknis ZTA tanpa membahas implementasi atau aplikasi praktis.
c. Artikel yang tidak relevan dengan konteks pendidikan atau sekolah.
d. Artikel yang tidak dapat diakses secara penuh.

Proses seleksi artikel dilakukan dalam dua tahap. Pertama, kami menyaring artikel berdasarkan judul dan abstrak untuk mengidentifikasi artikel yang berpotensi relevan. Kedua, kami membaca artikel secara penuh untuk memastikan bahwa artikel tersebut memenuhi kriteria inklusi dan eksklusi. Selain itu, agar pencarian lebih spesifik dan relevan, pencarian juga perlu memperhatikan pendefinisian PICOC, Identifikasi Kebutuhan Literature Review, serta Research Quuestion seperti yang disajikan tabel berikut.

Tabel 1. PICOC pada penelitian Zero Trust Architecture: Solusi Efektif untuk Keamanan Jaringan Sekolah Sebagai Peningkatan Performa dan Kepatuhan Keamanan Informasi

Item PICOC	**Aktualisasi PICOC dalam Penelitian**
Population	Organisasi Pendidikan dalam dan luar negeri, memiliki IT Asset
Intervention	SMKI, ISMS, ISO 27001, Zero Trust Architecture
Comparison	Organisasi pemerintahan, organisasi tanpa penerapan IT Governance, organisasi tanpa pengelolaan IT Asset
Outcomes	Penguatan keamanan data, Peningkatan respon insiden, Kepatuhan terhadap regulasi, Efisiensi operasional, Pengurangan biaya dan waktu yang diperlukan untuk pengamanan data/informasi
Context	Organisasi Pendidikan di Era Transformasi Digital yang memiliki tantangan pengelolaan keamanan data dan informasi

Tabel 2. Identifikasi Kebutuhan Literature Review

Item Identifikasi	**Penjelasan**
Topik Penelitian	Zero Trust Architecture: Solusi Efektif untuk Keamanan Jaringan Sekolah sebagai Peningkatan Performa dan Kepatuhan Keamanan Informasi
Poin utama landasan SLR	Analisa penerapan *Zero Trust Architecture sebagai Solusi Efektif untuk Peningkatan Performa dan Kepatuhan Keamanan Informasi di lingkungan Organisasi Sekolah*
PICOC	Terdefinisi pada tabel 1
Research Question	• Bagaimana cara organisasi, khususnya sekolah menengah, memastikan bahwa mereka membutuhkan implementasi ZTA? • Bagaimana cara menerapkan ZTA secara efektif di lingkungan sekolah menengah?
Article Databases	• SINTA 1-6: Journal Repository. • Google Scholar. • IEEE Xplore • ScienceDirect, Scopus Database
Key word pencarian	*"Zero Trust Architecture", "Keamanan Jaringan", "Sekolah Menengah", "Privasi Data", "Cyber Security"*
Year	2018-2025
Tier	Sinta1, S2, S3, S4, S5, S6 (Indonesia), Q1, Q2, Q3, Q4, (internasional, opsional)

Tabel 3. *Exclude keywords* pada PRISMA SLR

Kategori	***Exclude Key Words***
Health	*Public Health, Healthcare Technology, Mental Health, Chronic Diseases, Telemedicine, Preventive Medicine, Health Policy, Vaccination, etc*
Power Plant	*Renewable Energy, Nuclear Power, Thermal Power Plants, Hydroelectric Power, Power Generation Efficiency, Carbon Emissions, etc*
Transportation	*Sustainable Transport, Electric Vehicles, Urban Mobility, Smart Transportation Systems, Autonomous Vehicles, Public Transit Systems, Logistics, Road, , etc*
Flood, Water, Ocean	*Flood Risk Management, Hydrology, Coastal Erosion, Tsunami Monitoring, Ocean Currents, Climate Change Impact on Water, Water Quality, etc*
Finance, Bank	*Financial Technology, Digital Payments, Risk Management, Investment Strategies, Central Bank Policies, Cryptocurrencies, Banking Regulations, Microfinance, etc*
Nature	*Biodiversity Conservation, Wildlife Habitat, Ecological Restoration, Sustainable Forestry, Endangered Species, Nature-Based Solutions, etc*
Social, Culture	*Cultural Heritage, Social Inclusion, Multiculturalism, Identity and Diversity, Community Development, etc*

Kategori	***Exclude Key Words***
Religion	*Religious Tolerance, Comparative Religion, Faith and Spirituality, Interfaith Dialogue, Religious Rituals, Theology, Sacred Texts, Pilgrimage Studies, etc*
Parent- ing	*Child Development, Parenting Styles, Parental Involvement in Education, Attachment Theory, Positive Parenting, Parenting Challenges, etc*
Space, Atmosphere, Universe	*Space Exploration, Astrobiology, Exoplanets, Atmospheric Sciences, Space Weather, Black Holes, Cosmic Rays, Satellite Technology, etc*
Law	*Criminal Justice, International Law, Human Rights, Constitutional Law, Environmental Law, Corporate Law, , etc*
Arts	*Visual Arts, Performing Arts, Contemporary Art, Art History, Digital Art, Sculpture, Photography, Painting,etc*
Entertainment	*Film Production, Television Shows, Streaming Media, Video Games, Pop Culture, Music Industry, Animation, Celebrities, Entertainment Law, , etc*
Sports	*Sports Analytics, Physical Fitness, Professional Sports, Youth Sports, Sports Psychology, Athletic Training, , etc*

Tabel 4. *Include* dalam proses *screening* SLR Artikel

Kategori	***Include Key Words***
General Keywords	*Zero Trust Architecture (ZTA), Keamanan Jaringan Sekolah, Keamanan Informasi, Performa Jaringan, Kepatuhan Keamanan, Solusi Keamanan Jaringan, Keamanan Data Sekolah, Manajemen Akses, Peningkatan Keamanan, Verifikasi Akses, Keamanan Perimeter, Teknologi Keamanan, Keamanan TI Pendidikan, Perlindungan Data Sekolah, Arsitektur Keamanan, Sistem Keamanan Zero Trust, Pengelolaan Risiko Keamanan, Keamanan Jaringan Pendidikan*

Proses seleksi menghasilkan 1034 artikel dari pencarian dalam dan luar negeri. Setelah dilakukan filtering berdasarkan kata kunci inklusi dan eksklusi, ditemukan 130 artikel relevan untuk tahap screening. Proses screening mengeliminasi artikel yang tidak relevan, menghasilkan 61 artikel ilmiah yang sangat relevan dengan topik penelitian. Artikel-artikel ini akan dianalisis lebih lanjut untuk memberikan dasar teori dan data dalam artikel review ini.

4. HASIL DAN PEMBAHASAN

Sesuai dengan penjelasan pada bab Metodologi diatas, bahwa Proses pencarian literatur awal menggunakan kata kunci menghasilkan 1034 artikel, kemudian hasil setelah dilakukan filtering inklusi dan eksklusi 130 artikel relevan, serta proses screening artikel sesuai substanasi menghasilkan 61 artikel ilmiah, maka peneliti melakukan ekstraksi dan penyajian data hasil analisa literatur tersebut sebagaimana tersaji pada tabel dan grafik berikut ini.

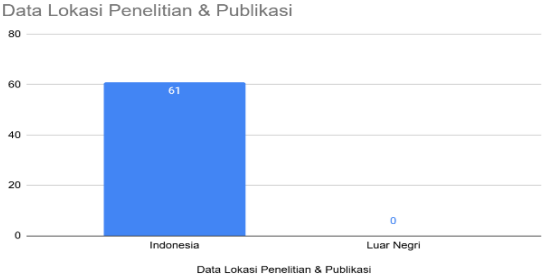
Tabel 5. Tabel hasil pencarian Artikel berdasarkan key word yang telah difilter dan screening berdasarkan parameter LR

No	Judul	*Author*	*Relevansi*
1	Pemberdayaan Media Cyber di Era Digital	Abdullah, S; Widyastuti, TAR; Suharyanto, CE; Januru, L	Tidak
2	Sistem Informasi Manajemen SDM Berbasis Cloud untuk UMKM: Desain, Etika & keamanan siber	Nugraha, Y; Kusumastuti, E; Putra, DDG; Munif, BA	Ya
3	Penafsiran Hukum Terhadap Objek Penguasaan Negara Tentang Sumber Daya Ekonomi Digital Di Indonesia	Rahmatullah, I	Tidak
4	Optimalisasi Keamanan Jaringan Di Era Digital menggunakan metode Zero Trust	Haeruddin, H; Prasetyo, SE	Ya
5	Implementasi Zero Trust Architecture untuk Meningkatkan Keamanan Jaringan: Pendekatan Berbasis Simulasi	Kusnanto, Y; Nugroho, MA	Ya
6	Fundamental Cyber Security dan Software Security	Muzawi, R	Ya
7	Pengembangan Perangkat Keras Komputer untuk AI	Kristiawan, H	Tidak
8	Internet of Things: Membangun Dunia yang Terkoneksi	Angellia, F; Judijanto, L; Sampebua, MR; Apriyanto,	Tidak
9	DASAR-DASAR JARINGAN KOMPUTER	Hartono, R; Manuhutu, MA; Wahyono, BT; Seta, HB	Tidak
10	Prinsip-Prinsip Desain Sistem Komputer	Munsyir, M; Mallisza, D; Hadi, H Setya; Wahyudi, E	Tidak
11	E-government di era artificial intelligence	Amrozi, ST Yusuf; MT, M	Ya
12	Pengantar Bisnis: Strategi Inovatif di Era Digital	Akbar, SS; Putri, DE; Chairoel, L; Sulistyowati, A	Tidak
13	Transformasi E-Government Berkelanjutan Dalam Proses Pelayanan publik pada pengelola ruang kendali pemerintah kota …	Rohaeti, Y	Tidak
14	Kecerdasan Buatan: Arah dan Eksplorasinya	Christia, A; Hadi, AS; Febriana, A; Budihardjo, A	Tidak

No	Judul	*Author*	*Relevansi*
15	Menuju Transformasi Digital Eksistensi Kewirausahaan Digital	Setyawati, A; Augustinah, F; Faradilla, C;	Tidak
16	Penerapan Technology Acceptance Model (TAM) Melalui Konsep Perceived Usefulness Pada Pemasaran Briguna Digital	Anuar, S	Tidak
17	Pengantar Ilmu Administrasi Negara	Almahdali, H; Sampe, F; Sulaiman, S; Puspita, M	Tidak
18	Teknologi Keamanan Siber (Cyber Security)	Santoso, JT	Ya
19	Kejahatan Siber dan Kebijakan Identitas Kependudukan Digital: Sebuah Studi Tentang Potensi Pencurian Data Online	Purba, YO; Mauluddin, A	Tidak
20	Analisis Pengaruh Peran Mediasi E-Satisfaction Dan E-Trust Terhadap E-Loyalty Pada Konsumen Belanja Daring Wanita	Putri, NK	Tidak
21	Analisis Faktor-Faktor Penerimaan Mobile Banking Di Indonesia Menggunakan Extended Tam	ANDHIKA, I	Tidak
22	Manajemen Proyek Sistem Informasi	Sinaga, IA	Tidak
23	Efektivitas E-Service Quality Aplikasi GoPay Pada Mahasiswa Fakultas Ekonomi dan Bisnis Universitas Pakuan Bogor	Rahmawati, I	Tidak
24	Manajemen Risiko Bisnis Era Digital	Anwar, A	Tidak
25	Manajemen Keuangan Menghadapi Industri 5.0	Agung, IGA; SE, MM; Subhan, MN; SE, MM; Putri,	Tidak
26	Keamanan Komputer'	Mahendra, GS; Wali, M; Idwan, H; Listartha,	Ya
27	e-Government Berbasis Information technology infrastructure	Antoni, DA Darius	Tidak
28	Pengaruh Penggunaan QRIS Pada Aplikasi Mobile Banking BSI Terhadap Kelancaran Dan Keamanan Bertransaksi Non Tunai Bagi Para Pelaku UMKM (Studi Kasus …	Dhea, MN	Ya
29	Analisis Continuance Use Intention Platform Perdagangan Cryptocurrency di Indonesia Menggunakan Expectation-Confirmation Model (Studi Kasus: PT. …	Damanik, RY	Tidak
30	Dinamika Kejahatan dan Pencegahannya: Potret Beberapa Kasus Kejahatan di Provinsi Riau	Rinaldi, SH Kasmanto; Dinilah, A; Prakoso, BY; Siddik, F	Tidak
31	faktor-faktor yang berpengaruh dalam kualitas penggunaan website pelayanan badan pusat statistik (bps) lampung …	PUTRA, AD	Tidak
32	Kebijakan satu data Indonesia	Amrynudin, ADK; Dharmaningtias, DS; Savira,	Tidak
33	Pengelolaan BUMDES di era RI 4.0	Sriyono, S	Tidak
34	Analisis pengaruh kualitas layanan terhadap kepuasan dan loyalitas pengguna menggunakan Metode ServQual dan Expectation Confirmation Model (ECM)	Larasati, I	Tidak
35	Keuangan sosial islam dan pemulihan ekonomi terdampak pandemi covid-19 pendekatan buluk sumur framework	Wardani, TU; Yuslin, H	Tidak
36	Model transformasi digital pada industri halal di era revolusi industri 4.0	Ramadinah, D; Mahendra, W	Tidak
37	Sharia e-wallet user's intention determinants: do islamic values and psychological aspects matter	Adam, M	Tidak
38	Implementasi manajemen bisnis syariah terhadap pelaku umkm menuju good corporate governance (studi kasus ud petis hsn …	Elina, R; Faizah, M; Almawaddah, A	Tidak
39	Perencanaan strategi sistem informasi rumah sakit dengan metoda ward and peppard-cassidy	Weningsih, IR	Tidak
40	Nonagon model kualitas pembelajaran jarak jauh pendidikan tinggi terhadap kepuasan mahasiswa saat pandemi covid-19	Leonnard, L	Tidak
41	Peran e-commerce dalam penguatan umkm di era pandemi covid-19 (studi pada umkm makanan halal di provinsi daerah istimewa yogyakarta)	Yusuf, MZ; Afifah, H	Tidak
42	Pengembangan konsep e-government untuk kota kecil	Antoni, D; Syahri, R; Kom, M; Akbar, M; Herdiansyah	Tidak
43	Demokratisasi dan Lingkungan Media yang Berubah di Korea Selatan: Handbook Komunikasi Politik	Semetko, HA; Scammell, M; Lamahu, GOR	Tidak
44	Menggagas model pembelajaran dari rumah (Learning from Home)	Zakir, S	Tidak
45	Evaluasi Tingkat Kematangan E-government Dan Partisipasi Masyarakat dalam Pelayanan Publik (Studi Kasus Kabupaten Sukoharjo)	Akbar, MM	Tidak
46	Analisis Perbandingan Penerimaan Nasabah Dalam Menggunakan Mobile Banking Bank Syariah dan Bank Konvensional	Novitasari, KM	Tidak

No	Judul	*Author*	*Relevansi*
47	Audit manajemen teknologi informasi smp dan sma islam terpadu ar-raihan menggunakan framework cobit 5	SARI, RI	Tidak
48	Analisis Kepuasan Mahasiswa Terhadap Penggunaan Internet Banking Referensi Dari Perguruan Tinggi (Studi Kasus: Perguruan Tinggi Di Kota Surabaya)	Salfira, DPL; Hariadi, S	Tidak
49	Analisis pengaruh kualitas website toko buku online terhadap kepuasan pengguna menggunakan metode webqual 4.0 dan System Usability Scale	Haidir, S	Tidak
50	Penerapan metode webqual 4.0 pada pengukuran kualitas website pencarian kerja (studi kasus: Jobstreet)	Alifiarga, H	Tidak
51	Faktor-faktor yang mempengaruhi kesiapan penerapan sistem single sign-on di Uin Syarif Hidayatullah Jakarta	Qadrya, HA	Tidak
52	Analisis Faktor-Faktor Yang Mempengaruhi Minat Beli Produk Digital Secara Online	Rusmawan, U	Tidak
53	Analisis Kualitas Layanan E-Government Dengan Menggunakan E-GovQual	JAMIANSYAH, H	Tidak
54	Risiko Siber	Tarumingkeng, RC	Tidak
55	Sistem keamanan penyimpanan data identitas nasional terintegrasi dengan teknologi blockchain	FATHIYANA, RZ	Ya
56	Blockchain berbasis key-value store untuk mendukung dynamic smart contract interaction pada sektor agro-maritim	SAPUTRA, I	Tidak
57	Information Technology Governance Profile of E-Government	Antoni, D; Herdiansyah, MI; Akbar, M	Tidak
58	Implementasi penggunaan teknologi cloud computing untuk kepentingan sektor industri serta pendidikan pada PT XYZ	Barokah, MU	Tidak
59	Pengaruh Location Based Service Dan Brand Awareness Terhadap Repurchase Intention Pada Umkm Shopeefood Dengan Mediasi Customer Satisfaction	Wandira, ID	Tidak
60	Analisis kualitas layanan aplikasi e-government Depok Single Window (DSW) menggunakan metode e-govqual dan Importance Performance Analysis (IPA)	Viandari, O	Tidak
61	Analisis continuance use intention pada pengguna aplikasi music streaming dengan menggunakan extended expectation-confirmation model	Salam, MIH	Tidak

Gambar 4. Grafik Distribusi Artikel Berdasarkan Tahun Publikasi



Gambar 5. Data Distribusi Lokasi Penelitian

Tabel 6. Distribusi metode penelitian yang digunakan

Metode Penelitian	**Jumlah**
Kualitatif	24
Kuantitatif	25
Eksperimen kasus studi	2
Pengembangan model	2
Analisis literatur & evaluasi model	2
Sistematik Literatur Review (SLR)	1
Kualitatif dg desain framework	1
Kualitatif dg prototipe	1
Pendekatan konseptual	1
Survei dan wawancara	1
Wawancara semi-terstruktur	1

Gambar 6. Grafik Distribusi Relevansi Artikel yang dianalisa Berdasarkan Tema ZTA

Gambar 7. Grafik Distribusi Artikel yang dianalisa Berdasarkan Research area Institusi Pendidikan

Resume data dari analisa artikel literatur review tersebut diatas antara lain:

a. Artikel terjaring : 61
b. Trend penelitian : meningkat sejak 7 tahun terahir
c. Metode Penelitian : Kuantitatif (25), Kualitatif (24)
d. Lokasi Penelitian / Publikasi: 100% Indnesia
e. Relevansi Tema ZTA: 14,8%
f. Relevansi Area Institusi Pendidikan: 3,3%

5. KESIMPULAN DAN SARAN

Berdasarkan analisis literatur review, proses SLR menghasilkan 61 artikel terjaring dengan data 14,8% pembahasan penerapan ZTA di institusi pendidikan relevan. Metode penelitian dengan pendekatan kuantitatif (25 artikel) dan kualitatif (24 artikel) menunjukkan bahwa ZTA dapat meningkatkan keamanan data dan memenuhi kepatuhan privasi di institusi pendidikan namun penerapannya terhambat oleh keterbatasan sumber daya dan keahlian teknis

Data penelitian dapat menjawab RQ-1, yaitu "Bagaimana cara institusi pendidikan memastikan bahwa mereka membutuhkan implementasi ZTA?", dapat dijawab Bahwa ZTA diperlukan ketika data yang dikelola sangat sensitif, regulasi privasi data mengharuskan perlindungan yang lebih ketat, dan ancaman keamanan siber yang tinggi. Sedangkan RQ-2, "Bagaimana cara menerapkan ZTA secara efektif di lingkungan pendidikan?", dapat dijawab dengan menunjukkan bahwa implementasi ZTA harus melalui tahapan penilaian, perencanaan, desain, dan pengujian, serta pemantauan berkelanjutan untuk memastikan efektivitasnya.

Penelitian di masa depan berpotensi mengembangkan framework implementasi ZTA yang lebih spesifik untuk institusi pendidikan dengan sumber daya terbatas. Selain itu, studi kasus yang lebih mendalam tentang tantangan dan solusi praktis dalam penerapan ZTA di dunia pendidikan akan sangat berguna untuk memperkuat keamanan data dan kepatuhan privasi.

DAFTAR PUSTAKA

[1] Firmansyah, R. A., Prayudi, Y., & Luthfi, A. (2025). Integrasi digital forensic readiness dan information security management system pada organisasi pemerintahan: Systematic literature review. JATI (Jurnal Mahasiswa Teknik Informatika), 9(2), 13126. https://doi.org/10.36040/jati.v9i2.13126

[2] Saputra, P. N., Sudirman, A., Sinaga, O., Wardhana, W., & Hayana, N. (2019). Addressing Indonesia's Cyber Security through Public-Private Partnership (PPP). Central European Journal of International and Security Studies, 13(4), 104–120. https://doi.org/10.2478/cejiss-2019-0045

[3] Badan Siber dan Sandi Negara. (2023). Laporan Kinerja Badan Siber dan Sandi Negara Tahun 2023. https://www.bssn.go.id/laporan-kinerja-badan-siber-dan-sandi-negara-tahun-2023/

[4] https://www.kearney.com/industry/public-sector/article/-/insights/transforming-indonesia-s-e-government-landscape, diakses 24/12/2024

[5] https://www.bssn.go.id/wp-content/uploads/2024/03/Lanskap-Keamanan-Siber-Indonesia-2023.pdf , diakses 24/12/2024

[6] Herdiansyah, A., Suryani, N., & Pratama, D. (2021). Peningkatan penggunaan teknologi digital dalam pendidikan dan dampaknya terhadap keamanan data serta reputasi institusi. Jurnal Teknologi dan Keamanan Pendidikan, 16(2), 123–134. https://doi.org/10.12928/jati.v16i2.4591

[7] Prayudi, A., & Wahyuni, S. (2017). Faktor-faktor yang mempengaruhi penggunaan layanan mobile banking. J@ti Undip: Jurnal Teknik Industri, 12(2), 149–158. https://doi.org/10.12928/jati.v12i2.649:contentReference[oaicite:1]{index=1}

[8] Kominfo. (2018). Peraturan Menteri Komunikasi dan Informatika Nomor 4 Tahun 2016 tentang Sistem Manajemen Pengamanan Informasi. Kementerian Komunikasi dan Informatika Republik Indonesia. https://www.kominfo.go.id.

[9] Dewan Perwakilan Rakyat Republik Indonesia. (2022). Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi. https://jdih.setkab.go.id/PUUdoc/176837/Salinan_UU_Nomor_27_Tahun_2022.pdf:contentReference[oaicite:0]{index=0}

[10] Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). Zero Trust Architecture (NIST Special Publication No. 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207:contentReference[oaicite:1]{index=1}

[11] ISO 27001: International Organization for Standardization. (2013). https://www.iso.org/standard/54534.html

[12] NIST Cybersecurity Framework (2018): Framework for improving critical infrastructure cybersecurity, https://doi.org/10.6028/NIST.CSWP.04162018

[13] CIS Controls: Center for Internet Security. (2021). CIS Controls v7.1. https://www.cisecurity.org/controls/

[14] GDPR: European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data. https://doi.org/10.1007/s10551-018-4054-0

[15] NIST SP 800-207 (Zero Trust Architecture): National Institute of Standards and Technology. (2020). https://doi.org/10.6028/NIST.SP.800-207

[16] ZTMM (*Zero Trust Maturity Model*): *Cybersecurity and Infrastructure Security Agency*. (2020). https://www.cisa.gov/zero-trust