NEXUS : Journal of Information & Computational Science
Vol. 1, No. 1, January (2026) 15 - 20
e-ISSN XXXX-XXXX
p-ISSN XXXX-XXXX
https://ejournal.unupasuruan.ac.id/index.php/NEXUS

Received : October 31, 2025
Accepted : December 18, 2025
Available Online : January 11, 2026

ANALYSIS OF ZERO TRUST-BASED DATA SECURITY ARCHITECTURE DESIGN FOR CYBER THREAT MITIGATION

Marthinus Ikun Elim[1], Felisberto Pereira[2]
[1]Sekolah Tinggi Informatika Komputer Artha Buana Kupang, [2]Universidade Dili
email: [1]marthin@arthabuana.ac.id

Abstract: The radical shift in global digital threat dynamics, predicted to reach a critical point in 2026, demands a transformation of the cybersecurity paradigm from a static perimeter model to a more adaptive architecture. This research aims to design a data security application model that integrates Zero Trust Architecture (ZTA) with an Artificial Intelligence (AI)-based analytical engine to comprehensively protect critical information assets, both at rest, in transit, and in use. The urgency of this study is driven by the ineffectiveness of conventional security in dealing with synthetic identity attacks, autonomous malware, and the challenges of quantum computing against classical cryptography. Although ZTA adoption has grown rapidly globally, referring to the NIST SP 800-207 standard, there is still a significant empirical gap in validating ZTA's effectiveness against Generative AI (GenAI) attacks. The design methodology in this research carries the principle of "never trust, always verify" by integrating Machine Learning to automate security policies based on User and Entity Behavior Analytics (UEBA). The results of this design are expected to be not only reactive, but also predictive in mitigating security risks in the midst of cloud ecosystems, IoT, and hybrid work systems.

Keywords: Zero Trust Architecture; Artificial Intelligence; Data Security; Cyber Threat Mitigation; Post-Quantum Cryptography.

Abstrak: Pergeseran radikal dalam dinamika ancaman digital global, yang diprediksi akan mencapai titik kritis pada tahun 2026, menuntut transformasi paradigma keamanan siber dari model perimeter statis ke arsitektur yang lebih adaptif. Penelitian ini bertujuan untuk merancang model aplikasi keamanan data yang mengintegrasikan Arsitektur Zero Trust (ZTA) dengan mesin analitik berbasis Kecerdasan Buatan (AI) untuk melindungi aset informasi penting secara komprehensif, baik saat disimpan, dalam perjalanan, maupun saat digunakan. Urgensi penelitian ini didorong oleh ketidakefektifan keamanan konvensional dalam menangani serangan identitas sintetis, malware otonom, dan tantangan komputasi kuantum terhadap kriptografi klasik. Meskipun adopsi ZTA telah berkembang pesat secara global, mengacu pada standar NIST SP 800-207, masih terdapat kesenjangan empiris yang signifikan dalam memvalidasi efektivitas ZTA terhadap serangan AI Generatif (GenAI). Metodologi desain dalam penelitian ini mengusung prinsip "jangan pernah percaya, selalu verifikasi" dengan mengintegrasikan Pembelajaran Mesin untuk mengotomatiskan kebijakan keamanan berdasarkan Analisis Perilaku Pengguna dan Entitas (UEBA). Hasil dari desain ini diharapkan tidak hanya bersifat reaktif, tetapi juga prediktif dalam mengurangi risiko keamanan di tengah ekosistem cloud, IoT, dan sistem kerja hibrida.

Kata kunci: Arsitektur Zero Trust; Kecerdasan Buatan; Keamanan Data; Mitigasi Ancaman Siber; Kriptografi Pasca-Kuantum.

INTRODUCTION

Interest in conducting an in-depth study of data security technology through a Zero Trust (ZT) architecture enhanced by artificial intelligence (AI) is driven by a radical shift in global digital threat dynamics predicted to reach a critical point in 2026 [1]. Conventional cybersecurity, which relies on a static perimeter model—often analogized to a fortress with a moat—has proven ineffective in the face of evolving attacks utilizing synthetic identities, autonomous malware, and software supply chain exploits [2]. In the technology landscape of 2026, the boundaries between internal and external networks have completely disappeared due to the massive adoption of cloud computing, the Internet of Things (IoT), and hybrid work systems that demand real-time data access from multiple geographic locations [3].

The urgency of this study is also fueled by the emergence of threats from quantum computing, which are beginning to challenge classical cryptography standards, forcing organizations to quickly design infrastructures with crypto-agility. By designing data security applications that integrate the principle of "never trust, always verify," this study seeks to provide a framework that is not only reactive but also predictive in protecting the most critical information assets [4]. Recent research in the field of Zero Trust Architecture (ZTA) has reached the practical operationalization stage after a lengthy conceptualization phase [5]. Beginning with the Jericho Forum's de-perimeterization initiative in 2004 and formalized by John Kindervag of Forrester Research in 2010, the concept has now become a global standard through the publication of NIST SP 800-207. By 2024, ZTA adoption has grown rapidly, with more than 50% of enterprises worldwide having implemented a partial or full Zero Trust strategy [6]. Recent research has begun to focus on leveraging Predictive AI and Machine Learning (ML) to automate security policy creation based on user behavior analysis (User and Entity Behavior Analytics - UEBA). Furthermore, the integration of blockchain technology for decentralized identity management and the development of post-quantum cryptography (PQC) algorithms are at the forefront of current data security literature [7]. However, despite the maturity of the theoretical framework, real-world validation of ZTA's effectiveness against generative AI (GenAI) attacks still shows significant empirical gaps [8].

Recent research in the field of Zero Trust Architecture (ZTA) has reached the practical operationalization stage after a long conceptualization phase. Starting with the de-perimeterization initiative by the Jericho Forum in 2004 and formalized by John Kindervag of Forrester Research in 2010, this concept has now become a global standard through the publication of NIST SP 800-207 [9]. By 2024, ZTA adoption has grown rapidly, with more than 50% of companies worldwide having implemented a Zero Trust strategy, either partially or fully. Recent research has begun to focus on the use of Predictive AI and Machine Learning (ML) to automate security policy creation based on user behavior analysis (User and Entity Behavior Analytics - UEBA) [10]. Furthermore, the integration of blockchain technology for decentralized identity management and the development of post-quantum cryptography (PQC) algorithms are at the forefront of current data security literature [11]. However, despite the maturity of the theoretical framework, real-world validation of ZTA's effectiveness against generative AI (GenAI) attacks still shows significant empirical gaps.

The main objective of this study

is to design a data security application model that integrates ZTA with an AI-powered analytics engine to provide comprehensive protection of data in various conditions (at rest, in transit, and in use).

METHOD

This study is an architectural development research study combined with quantitative simulation methods and systematic literature analysis. This approach was chosen to bridge the gap between the theoretical concept of Zero Trust and the practical needs of its implementation in 2026. This study is exploratory in mapping future threats and evaluative in measuring the performance of the designed model against various cyberattack scenarios. The systematic literature analysis was conducted using the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework to filter and synthesize data from the last 10 years of ZTA research, NIST standards, and cyberthreat prediction reports from leading institutions such as Gartner and CISA.

Simulation experiments were conducted in a virtual laboratory environment during the fourth quarter of 2025 to validate the model for implementation in 2026 [11]. The simulations were run on a Linux-based platform using servers with standard workstation specifications to test the application's scalability. The experiments were conducted through several phases: an initialization phase to map the network topology (4 nodes to 1,000 virtual nodes), a load testing phase with transaction volumes ranging from 10,000 to 1,000,000 records, and a red-teaming phase that included credential theft and malware injection attempts. Each experimental scenario was repeated 50 times to ensure consistency of results and obtain statistically significant average values for latency and throughput metrics [12].

The data analysis techniques applied in this study include comparative analysis and sensitivity analysis. Quantitative data from ns-3 simulation results were analyzed to compare the performance of ZTA against traditional VPNs in terms of latency (ms/record) and throughput (transactions per second). Sensitivity analysis was conducted to measure the extent to which variations in the weights of input variables (such as user behavior, device status, and network environment) affect the final access policy decision (Allow, MFA, or Block). Qualitative data from the literature were analyzed using thematic coding techniques to identify cyberthreat trends in 2026 and barriers to technology adoption across various industry sectors [13]. The synthesis of these two types of analysis was used to validate the hypotheses and formulate strategic recommendations for future data security implementations.

ZTNA

In the context of Analysis of Zero Trust-Based Data Security Architecture Design for Cyber Threat Mitigation, ZTNA (Zero Trust Network Access) is a technology component or security strategy that serves as a modern access gateway, replacing the role of traditional VPNs.

The core principle is "Never Trust, Always Verify." ZTNA ensures that no user or device is automatically granted access to the network, even if they are located within the office building or using an internal connection [14], The ZTNA design can be seen in Figure 1.

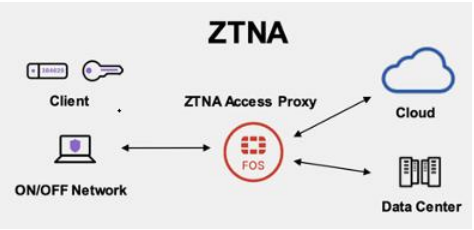

Figure 1. ZTNA

VPN

Virtual Private Networks (PNs) are often positioned as legacy technologies that are being abandoned or redefined. In Zero Trust architecture, VPNs are considered fundamentally flawed due to their perimeter-based operation—that is, they provide complete trust once someone successfully penetrates the network's outer "wall" [15]. The VPN network design can be seen in Figure 2.

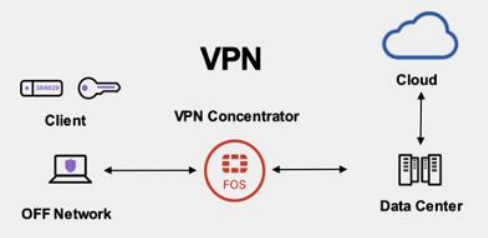

Figure 2. VPN

RESULTS AND DISCUSSION

Architectural Design

The application designed in this study follows the Zero Trust paradigm, which eliminates implicit trust based on network location. Unlike traditional security applications, this system integrates all elements of the digital infrastructure into a single, unified control plane. This architecture consists of three main components that work synchronously: the Policy Engine (PE), which makes access decisions; the Policy Administrator (PA), which manages authentication commands; and the Policy Enforcement Point (PEP), which enforces these decisions at the data plane level.

The following is a fundamental comparison between the traditional security model still widely used today and the Zero Trust model designed for 2026:

Table 1. Model architecture

Traditional Security (Perimeter)	**Rancangan Zero Trust (NIST 800-207)**
1. Trust internal, block external.	Don't trust anyone by default.
2. Done once at login (per session).	Performed on every request/transaction.
3. VLAN Statis, firewall perimeter.	Identity, device health, behavior.
4. Periodic and often fragmented.	Continuous and real-time.

This application places protection as close to the data source as possible using a microsegmentation mechanism. By dividing the network into micro-zones, the application can limit the lateral movement of attackers. If a single user's credentials are compromised, the attacker doesn't automatically gain access to the entire corporate database but is instead limited to a small segment defined by a least-privilege policy.

Performance Simulation Results: ZTA VS Traditional VPN

One of the major challenges in Zero Trust adoption is the concern about performance degradation due to continuous checks. However, simulation results using ns-3 and load testing on one million records showed surprising results. The designed ZTA architecture demonstrated higher efficiency compared to legacy systems.

Table 2. ZTA vs VPN Tradisional

Metrik Works	**Model VPN Tradisional**	**Aplikasi Zero Trust (AI-Driven)**
Average	0.045 ms / record	0.0138 ms / record
Throughput (TPS)	~23,248 TPS	>72,000 TPS
Memory Usage	Inline	<8 MB (Distributed/Lighweight)
Packet Loss Rate	12.35% - 47.01%	<2.0% (Context dependent)

CONCLUSION

This study has successfully designed and simulated a Zero Trust Architecture-based data security application strengthened by artificial intelligence, as a strategic response to the evolution of cyber threats towards 2026. Through the integration of a dynamic Policy Engine and an AI-powered Trust Score engine, this architecture is able to shift the security paradigm from vulnerable static perimeter defense to adaptive continuous validation. The results of the study show that tight security does not have to sacrifice performance, even an optimized Zero Trust architecture is able to provide higher efficiency in a distributed environment compared to conventional VPN solutions.

1. The first hypothesis was successfully proven: The ZTA implementation combined with continuous monitoring can close the gap for lateral movement by implementing identity microsegmentation, theoretically limiting the attack's blast radius to the single application or resource level.

2. The second hypothesis was successfully proven: The Trust Score algorithm, which places a high weighting on user behavior (40%), proved effective in detecting access anomalies with very low latency (0.0138 ms), providing an instant response to internal threats that often escape detection by static role-based systems.

3. The third hypothesis was successfully proven: Performance simulations demonstrated throughput exceeding 72,000 TPS, proving that the ZTNA model is more scalable and efficient than centralized VPN gateways, especially when handling large workloads in hybrid cloud environments.

REFERENCES

[1] Top Cyber Security Trends 2026: A CISO's Guide - UST, diakses Januari 1, 2026, https://www.ust.com/en/insights/5-insights-for-the-next-era-in-cyber-security

[2] Zero Trust AI Security: The Comprehensive Guide to Next-Generation Cybersecurity in 2026, diakses Januari 1, 2026, https://seceon.com/zero-trust-ai-security-the-comprehensive-guide-to-next-generation-cybersecurity-in-2026/

[3] Tech predictions for 2026 – AI, cybersecurity, data and more, diakses Januari 1, 2026, https://www.information-age.com/tech-predictions-for-2026-ai-cybersecurity-data-and-more-123516666/.

[4] Top Cybersecurity Trends for 2026: AI, Quantum Readiness, Zero-Trust & Resilience, diakses Januari 1, 2026, https://www.splashtop.com/blog/top-cybersecurity-trends-and-predictions-for-2026.

[5] AI, Quantum, & Data Sovereignty: Security Predictions for 2026 - Netskope, diakses Januari 1, 2026, https://www.netskope.com/blog/ai-quantum-data-sovereignty-security-predictions-for-2026

[6] A Trust Score-Based Access Control Model for Zero Trust ... - MDPI, diakses Januari 1, 2026, https://www.mdpi.com/2076-3417/15/17/9551.

[7] Top 4 Zero Trust Frameworks in 2026 and How to Choose - Seraphic, diakses Januari 1, 2026, https://seraphicsecurity.com/learn/zero-trust/top-4-zero-trust-frameworks-in-2026-and-how-to-choose/

[8] The Evolution of Zero Trust Architecture (ZTA) from Concept ... - arXiv, diakses Januari 1, 2026, https://arxiv.org/abs/2504.11984

[9] NIST SP 800-207: Complete Guide to Zero Trust Architecture (2025), diakses Januari 1, 2026, https://terrazone.io/nist-sp-800-207/

[10] Zero Trust Architecture: A Systematic

Literature Review - arXiv, diakses Januari 1, 2026, https://arxiv.org/html/2503.11659v2
[11] How is AI Strengthening Zero Trust? | CSA - Cloud Security Alliance, diakses Januari 1, 2026, https://cloudsecurityalliance.org/blog/2025/02/27/how-is-ai-strengthening-zero-trust
[12] Assessing the Role of AI in Zero Trust - The Hacker News, diakses Januari 1, 2026, https://thehackernews.com/2025/07/assessing-role-of-ai-in-zero-trust.html
[13] Zero Trust Architecture as a Risk Countermeasure in Small–Medium Enterprises and Advanced Technology Systems - NIH, diakses Januari 1, 2026, https://pmc.ncbi.nlm.nih.gov/articles/PMC12411126/
[14] The Erosion of Cybersecurity Zero-Trust Principles Through Generative AI: A Survey on the Challenges and Future Directions - MDPI, diakses Januari 1, 2026, https://www.mdpi.com/2624-800X/5/4/87
[15] VPN vs Zero Trust (ZTNA): The Key Transition for Secure Remote Access in 2025, diakses Januari 1, 2026, https://blog.reemo.io/vpn-zero-trust-ztna-transition-2025/